A Bibliography of Publications on Hashing Algorithms

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254
FAX: +1 801 581 4148

E-mail: beebe@math.utah.edu, beebe@acm.org,
beebe@computer.org (Internet)
WWW URL: https://www.math.utah.edu/~beebe/

02 November 2023
Version 2.350

Title word cross-reference

#2 [Cer85].

1 [PPS21]. 10 [GLM+10]. 11 [SY11]. 2 [EAA+16, GG92, HD72]. $2n$ [QG89, QG90]. 3 [CBA94, Fly92, GG92, GK94, LMJC07, LDY+16, SYW+20, WSSO12]. 5/8 [Sch11]. **$62m** [Nic17]. 64 [LK16]. * [LNS93]. + [Omi88, Omi89a]. ^{MT} [HRB13]. $_2$ [AK98, QJ97]. A [Lyo83]. $A*$ [MD97]. A^2 [Bie95]. α [ABC+16]. b [LK11]. B^+ [TB91]. c [SWQ+14]. d [FPS17, PRM16]. f [LG78]. $\mathrm{GL}_2(\mathbf{F}_{p^n})$ [TNS20]. H^2 [DRS12]. H_2A [CBB05]. K [Yuv75, APV07, CL85, CC91, CLC92, DKRT15, Die96, EFMRK+20, FPS17, Gui78, HC14, LLG+17, PT10a, PT16, PNPC20, RRS07, SS90b]. L [OOB12]. L_p [CJ19, HFF+17]. $\mathrm{SL}_2(\mathbf{F}_{2^n})$ [SGGB00]. N [BRM+09, BS91b, BS91a, CM01, Gir87, Ven86, WS93, War14, Coh97, Coh98, LHC05, QG89, QG90]. $O(1)$ [FKS84]. $O(\log\log n)$ [MN90]. $O(\log W)$ [LS07b]. $O(N)$ [HG77, MN90]. P^2 [VD21]. p^n [Ack74]. π [FFGL10]. q [OWZ14]. SL_2 [MT16]. Z/p [Mue04].

-approximate [SWQ+14]. **-ary** [CC91, CLC92, Gui78, RRS07]. **-Bit** [QG89, QG90, LK16, LK11]. **-Body** [WS93, War14]. **-codes** [Bie95]. **-dimension** [LHC05]. **-dimensional** [Yuv75]. **-Functions** [OOB12]. **-gram** [Coh98, Ven86]. **-Grams** [Coh97, BRM+09]. **-Hash** [BS91b, BS91a]. **-Independence** [PT16, PT10a]. **-mer** [HC14, PNPC20]. **-min-wise** [FPS17]. **-Nearest** [CL85]. **-partitions** [DKRT15]. **-Pipeline** [PRM16]. **-probe** [SS90b]. **-Round** [GLM+10, SY11].

-SHARP [VD21]. **-tree** [Omi89a, Lyo83]. **-trees** [CM01]. **-verarbeitung** [Nie75]. **-wise** [Die96].

0 [BCJ15, ITP14, NSS+06, WYY05d]. **'07** [ACM07]. **'08** [ACM08b].

1 [AMSM+09, AAE+14, BCJ15, Con17, DR06, JRPK07, KKRJ07, KRJ09b, KJS17, Nat95, SKP15, WYY05a, WYY05b, WYY05c]. **'10** [Ano10]. **100** [BLC12]. **100-Gb** [BLC12]. **100-Gb/s** [BLC12]. **10118-3** [ISO04]. **10th** [Ano93a, DSZ07a, DSZ07b, DJRZ06, IEE94a, Fre90]. **11th** [PV85, Shm00]. **128** [LP16, MNS12, WFLY04]. **128-bit** [MIO89]. **12th** [BJZ94, Bri92, Bri93, DJNR09, LC06]. **13th** [DJNR09, Sti93, Sti94c, Vid90]. **14th** [AAC+01, Bir07]. **15th** [BIP92, BJZ94, Cop95a, Cop95b, IEE74]. **160** [BDP97, PBD97]. **16th** [HM08, MSDS90]. **17th** [FS09, IEE76, IEE05, MS05, Pat90, Ano10]. **18** [Sar80]. **180** [Nat95]. **180-1** [Ano95b, Nat95]. **180-4** [Dan13]. **18th** [Deb03, Yua92]. **1969** [AFI69]. **1974** [Ros74]. **1975** [ACM75c, ACM75b, ACM75a, Ker75]. **1976** [ACM76]. **1977** [ACM77b, Gil77, TWW77]. **1978** [Win78, Yao78]. **1979** [ACM79, Ng79]. **1980** [dBvL80]. **1981** [Bai81, Mo92b]. **1982** [LFP82, VLD82, IEE82, NS82, Sch82a]. **1983** [Ano83, ST83b]. **1984** [ACM84b, ACM84a, DSS84]. **1985** [PV85]. **1985/11th** [PV85]. **1986** [ACM86b, CGO86, Fis87, Oxb86]. **1987** [DT87]. **1988** [ACM88b, BD88, WGM88]. **1989** [IJW89, ACM89c, MK89, PK89, RK89]. **1990** [ACM90, Jáj90, USE90, Vid90, WPY90]. **1990's** [Rie89]. **1991** [ACM91d, ACM91e, IEE91a, lWSS91]. **1992** [BIP92, Sto92]. **1993** [BJ93, IEE93]. **1993/sponsored** [HB93]. **1994** [SW94b]. **1996** [ACM96]. **1997** [ACM97a, ACM97b, ANS97]. **1998** [ACM98, GSW98, Kar98]. **1999** [AOV+99]. **19th** [ACM91b, Kui92, RRR99, Wie99, vL94, ABB93]. **1st** [CCC89, Coh94].

2 [BH86, GT63, KMV10, LS15, ST86, SK05]. **2000** [Shm00, ZC12]. **2001** [ACM01, AAC+01]. **2002** [ACM02]. **2003** [ACM03a, ACM03b, Deb03]. **2004** [ACM04]. **2005** [ACM05, ANS05]. **2006** [ABM06]. **2007** [ACM07]. **2008** [ACM08b, LL08]. **2009** [Mat09]. **2010** [Ano10]. **2011** [Van10, LCK11]. **20th** [AH03, Bel00, EF12, WGM88, BJZ94]. **21-January** [USE91]. **21./22** [Lut88]. **21st** [ACM91b, IEE80b, JY14]. **22nd** [AiNOW11, Yun02]. **23rd** [IEE82]. **24th** [??69, ABB93, Fra04]. **24th-27th** [ABB93]. **25/1989** [AW89]. **256** [AKY13, CMP07, MAK+12, PPS21, Sch11]. **25th** [Sho05, Vau06]. **26th** [IEE85a]. **27th** [ABB93]. **28-July** [Rei88]. **29-March** [IEE88a]. **29/Sept** [BD88]. **29th** [IEE88c]. **2HOT** [War14]. **2k** [USE00b]. **2nd** [ACM83a, ACM94a, ABM06, HL91, ICD86, Sch82a, KI94, Yu92].

3 [ABM+12, jCPB+12, NIS15, Sed93, Ruc15]. **30-May** [ACM84b]. **30th** [IEE89]. **31-November** [ST83b]. **320** [MJ08]. **320-bit** [MJ08]. **32nd** [CIM+05, IEE91b]. **33rd** [ACM01, IEE92b]. **34th** [ACJT07]. **35th** [ADG+08, Gol94]. **360** [Dit76]. **36th** [AMSM+09]. **37th** [AGK+10]. **39th** [ACM07]. **3rd** [Jáj90, LS89, Rei88, TWW77, Wol93a, Wol93b, ACM91c].

40th [ACM08b, IEE99]. **42-step** [AKY13]. **45** [Pro94]. **47th** [IEE06]. **48th** [IEE07]. **4th** [IJW89, BW92, Far93, HKNW07, JBJ94, Lom93, PSN95, USE00a].

5 [PW94]. **5-Independent** [TZ12]. **512** [GLM+10]. **51st** [IEE10]. **52nd** [IEE11b]. **54th** [IEE13]. **5G** [Cho21]. **5th** [BRW93, Boy95a, Boy95b].

68110a [Sar80].

'76 [Jen76]. **'79** [Ng79]. **7th** [ARA94, Bar83, CHK06, USE00b, Win78].

80f [Sar80]. **'83** [Ano83, CRS83a]. **'84** [ACM84a]. **'85** [IEE85b]. **'86** [AA86]. **'87** [CP87, CP88]. **'88** [ACM88a]. **'89** [ACM89a, BV89, BF89, Bra90, QV89, QV90, CP91c].

9-13 [ACJT07]. **'90** [AFK90, A+90, Dam90a, Dam91, IEE90, MV91c, SP90]. **'91** [ACM91a, Dav91, Fei91, HL91, IEE91a, IRM93, ACM91c]. **'92** [Bri92, Bri93, BW92, FNY92, IEE92a, KLT92, Rue93, SZ93, Yua92]. **'93** [Ano93c, BRW93, BJ93, Hel94, IEE93, Lom93, Sti93, Sti94c, vL94]. **93k** [Pro94]. **'94** [ACM94b, De 95, JBJ94, PSN95, SW94b, SW94a]. **'95** [Cop95b, GQ95, IEE95, Lev95, QG95]. **959** [ÁCZ16]. **'96** [Lak96]. **'99** [Wie99]. **9th** [DJRZ06, ST83a, IEE88d].

A. [Pro94]. **Aarhus** [Dam90a, Dam91, NS82]. **ability** [DLM07]. **abolishing** [DSS10]. **Abstract** [DP08, EjKMP80, Lum73, MW95, SW87, THS97]. **Abstraction** [CL83, DL06, Hil88, LPSW03]. **abstraction-safe** [LPSW03]. **Academic** [Cer85]. **ACCEL** [HKL04]. **ACCEL-RATE** [HKL04]. **accelerate** [GK12b]. **Accelerated** [Kri89, MW09, MWC12]. **Accelerating** [HAK+16, TT82, BLY20]. **Acceleration** [FAFK21, JMH02]. **Accelerator** [FM91, TLLL09]. **Access** [Ast80, BDPSNG97, BM76, CF89a, Cla77, Dum56, FNPS79, Fal85b, F+03, FP89b, FKS84, GG74, HB89a, HB92, KR86b, KR86a, KM88b, LK84, Lit84, LL86, LMR02, MY79, Mul72, Ols69, Pet57, SD85, SDKR87, SHRD09, Tra63, VB00, XHZ+19, YL04, And88, Bay73b, BCGS16, CS93a, FPSS05, HB89b, KFG15, Lar88b, Lin63, MBK00, Mil95, ML95, RT89, TKT+89, ZO13]. **access-pattern-driven** [ZO13]. **Accessed** [Ols69]. **Accesses** [Pan05]. **Accessing** [Cha88, Ore83, FK89]. **accommodation** [HO72]. **Accountable** [XHZ+19]. **Accumulated** [Nyb96]. **accumulating** [ZHW01]. **Accumulators** [CHKO08, PTT16, CHKO12]. **Accuracy** [YWH09, HKL07]. **Accurate** [LCL+20, PCV94, SL16, YGS+19, NTW09, TYSK10]. **Achieve** [LLL+16]. **achieved** [Con17]. **Achieving** [Lar88b, Lyo85]. **ACM** [ACM94d, ??69, ACM75c, ACM75b, ACM75a, ACM76, ACM77b, LFP82, ACM82, ACM83b, ACM84b, ACM85b, ACM85a, ACM86b, ACM86a, ACM87, ACM88a, ACM88b, ACM89b, ACM89a, ACM89c, SDA90, ACM90, ACM91c, ACM91d, ACM91a, SDA91, ACM91e, ACM96, ACM97a, ACM97b, ACM98, ACM01, ACM02, ACM03a, ACM04, ACM05, ACM07, ACM08a, ACM08b, ACM11, ACM12, Ano92, BIP92, BJ93, CLM89, FMA02, GMJ90, Van10, HF13, IEE02, Jen76, Kar98, LL08, Mat09, Nav85, Rie89, ACM77a, Shm00, SW94b, Sto92, YR87, ACM81, ACM91b, BV89, Lie81]. **ACM-SIAM** [ACM94d, SDA90, SDA91, ACM97a, ACM05, ACM08a, Kar98]. **ACM-SIGMOD** [Nav85, Lie81, ACM81]. **across** [HWZP18, SF88]. **Action** [BFR87]. **activation** [SZO+20]. **Active** [GHJ+93, EVF06]. **Actor** [TCP+17]. **Ad** [DPH08, JLH08, Cha12]. **Ad-Hoc** [JLH08]. **Ada** [BCS89, ST86, Tro06, Wol84]. **AdaBoost** [LLZ10]. **Adaptable** [NHS84]. **adaptation** [DOP+14]. **Adapted** [RJK79]. **Adaptive**

[Ahn86, Ahn87, BK90, CBB05, CS02, Gri98, HT88, IGA05, KR91, KL08, LBJ02, OL91, OL92, ST93, TC04, ZG90a, Zel91, GZ99, HAK+16, LYJ+13, LMLC14, TB91]. **Adaptive-Hash** [OL91, OL92]. **add** [FJ13]. **add-rotate-xor** [FJ13]. **Addendum** [CV85]. **addition** [FJ13]. **Additional** [LY72]. **Additive** [MBBS12]. **Address** [HP63, Jai89, Jai92a, Jai92b, Jaixx, LYD71, Lum73, PK87, SR63, Tam85, TK85, Wil96, LY72, MLP07, MPL09, RW07]. **Addressable** [Hin20, RSK17, Koh80, BB07]. **Addressed** [SVCC01]. **Addressing** [Bay74, Bra84a, Bra86, Buc63, Fab74, Fel87, Gon77, Gon80, JC88a, Joh61, Kno71, Kno88, KR79, KRJ+80, Lit80, Litxxa, LH03b, LH03a, Mot84, MC86, Pet57, RJK79, SS62, SD76, Som99, Tra63, CKW93, Lin63, NK16, TT81, Wan05, van73]. **Adelaide** [Bar83]. **Adjusting** [Pag85, Wog89]. **Administration** [Fis87]. **Adressing** [Bra85]. **Advanced** [Ano93d, CE95, HDCM11, Hsi83]. **Advances** [Buc82, AFK90, Bel00, Bra90, Bri92, Bri93, CRS83a, CP87, CP88, Cop95a, Cop95b, Dam90a, Dam91, Dav91, De 95, Fei91, Fra04, GQ95, Hel94, IRM93, JBJ94, LC06, MV91c, PSN95, QV89, QV90, QG95, Rue93, SP90, SZ93, Sho05, Sti93, Sti94c, Vau06, Wie99, Yun02]. **Advantage** [WSSO12]. **Adversaries** [LN93]. **Advisor** [Cer85]. **Aegean** [Rei88, Rei88]. **Aeronautical** [KCF84]. **Aeronautics** [Fis87]. **Aerospace** [Fis87, IEE94b]. **AES** [ABO+17, BOY11, BÖS11, GK08, Rog19a, Sas11, JNPP14]. **AES-like** [JNPP14]. **affects** [HL05]. **Again** [DRS12]. **Against** [DL17, ASBdS16, JL14, JG95, MSP12, Sho00b]. **Age** [Cro98]. **Agent** [BŠH12, DF01]. **Aggregation** [BJL16, PT10b]. **Agreement** [GB10, YLSZ19]. **agrometeorological** [WM93]. **Ahead** [Moh90, Moh93]. **AID** [Dos78b]. **Airport** [ICD88, ICD90]. **Akron** [Fis87]. **al.** [SPLHCB14]. **Alaska** [IEE01]. **Albuquerque** [ACM75c, ACM75a, IEE91a]. **Algebra** [Bra84b, KTMO83b, KTMo83c, EBD91, FP89a]. **Algebraic** [ACM94b, EjKMP80, Jen76, Lak96, Lev95, Mar71, Ng79, WX01, vdHvH12, BF08, GS89, LS06, Pon87, Coh94, AAGG16]. **Algebras** [CT96]. **Algol** [FR69]. **Algol-Based** [FR69]. **Algorithm** [ANS97, ANS05, AKS78, ABH+73, AEMR09, BH90, BI87, Bou12, Boy98, CS85a, jCPB+12, CdM89, CW09, CT12, Coh98, CHM92a, CHM92b, CM93, Dev93, DCM18, FL73, FFPV84, FCHD88, FCHD89, FCH92, Fro81, Get01, Han90, HCKW90, HR96, HW08, HG77, HC13, Jen97, JRPK07, KMM+06, KKRJ07, Leb87, LLDZ18, LLL11, LLW10, MXL+12, Man12, MHB90, MV01, MH00, NP91, OG94a, OOB17, OL91, Omi91, OL92, Pap94, PCY95, Pes96, Pit87, PVM97, Reg82, SS01, Sol93, Spe92, Sta99, TRN86, TTY93, Toy93, TSP+11, WG00, WWZ09, WZJS10, WS93, WVT90, Wil97, Wil71, WDYT91, WYT93, WL12, ZG90a, ZJM94b, ZPS90, ZPS93a, AS89, AT18, AGJA06, ATAKS07, CLS95, CLW98, DHKP97, FH79, FHC89, FKI+21, Gai82, GBY90, HLL18b, HL94, ISO97, ISHY88, JWM+18, Kim99, LEHN02, MMC01, MKSiA98, OT89]. **algorithm** [PCV94, PL21, Pri95, SB95, SM94, Sil02b, Ste18, WM93, War14, Wie86, YCJ12, ZJM94a, ZJM94c, ZPS93b, ÁCZ16, Sta94, TKI99]. **Algorithmen** [Meh77, Meh86, Wir75, Wir83, Zel91]. **Algorithmics** [Mat93]. **Algorithms** [ACM94d, ACM91c, ACM97a, ACM05, ACM08a, ANS97, AHU83, AOAAK20, AI06, Ano95a, iA91, iA94, AT90, AT93, AT91, BS97, Bur76b, CFP19, CV86, CRR18, CT96, DG85a, DG85b, Dev86, DS97, FM96, FW09, FM85, GRBCC19, Ger86a, Ger86b, Gon84, GBY91, GI77, Gra88, Gra89, GC95, GK81, GK82, Gui76a, Gui76b, GG80, GSB94, Har88, HS78, HL91, KR81, LLLC17, LS89, Lom93,

LTS90, LH03b, Mac95, MF92, MLD94, MLxx, Mat09, MS88a, MO92a, OG94b, OL89, PS93, Pip94, PV19, Pre97a, PB85, QG89, QG90, Reg85, Riv74b, RNR13, Sam76, SD89c, SD89a, Sed83b, Sed88, Sed90, Sed92, Sed93, SD76, SG88, SK98, Shm00, TR02, TY91, Vit81b, VC85, Wal88, WFHC92, Wie87b, Wir86, XCCK09, Yen91, ZG90b, AI08, BMS+17, BMQ98, Cra85, DG96]. **algorithms** [DJRZ06, DJNR09, DC94, EVF06, FJ13, GK05, Gui76c, HK95, HKNW07, JDW+19, JMH02, Kan90, Kar98, KP92, Kha95, MPL09, Mol90a, Mol90b, MMSY94, NM02b, PBGV89, QM98, Rei88, RLM87, RG89, Riv74a, SD89d, Sch91a, Sed83a, SG72, Vit82a, Vit01, SDA90, SDA91, A+90, AiNOW11, CT10, DSZ07a, DSZ07b, EF12, FS09, FBY92, HM08]. **Algorithmus** [BI87]. **Alignment** [BFMP11, BRM+09, LPT12, EASR22]. **Alignments** [BDD+10]. **All-in-one** [SV18]. **All-or-Nothing** [SRY99]. **Alley** [Boy98, Get01, Jen97, Pes96, Wil97]. **Allocating** [CC91, TC93]. **Allocation** [CC87, CLC92, Du86, MJBD11, Nak21, YCRY93, vdP72, vdP73, DW05, DW07, LCRY93, OOK+10, van73]. **Allocation-Based** [Nak21]. **Allocations** [ABKU99, PG95]. **Allowable** [Blo70]. **Almost** [BKST18, BM99, CKB83b, DW03, YSEL09, CKB83a, Duc08, IIL17]. **Almost-Minimum** [BM99]. **Almost-Universal** [BKST18]. **Alpha** [WM19]. **Alternative** [EMM07, HBL+10, IH95, SD89b, LS15]. **Alternatives** [GD87]. **am** [CE95, LC95]. **American** [CHK06]. **Among** [CC91, GP08, KW94]. **amortize** [KM07]. **amortized** [ANS09]. **Amplification** [BBR88]. **Amsterdam** [AW89, CP87, CP88]. **Analogue** [Cai84, DSGKS20]. **Analyses** [CS87]. **Analysis** [AP93, Ano95c, AD11, AM07, BYSP98, BRS02, BRSS10, BM89, BM90a, BF08, CF92, CL85, CC87, Cha88, CLNY06, CN08, CV83a, CV84, Che84a, Che84b, CV85, CK94, CS93b, CDW+19, DR11, FC87a, FPV98, FMM09, FMM11, GRBCC19, GK12a, GL73, GBY90, GK81, GK82, GLG+02, GS76, Gui76a, Gui76b, GS78, Gui78, Gur73, HMNB07, Hac93, Has72, Kut10, Lar80a, Lar80c, Lar82b, Lar83, Lar84, Lar85c, LCK11, Lev00, Lew82, LWWQ08, LPP91, LPP92, LM93c, Lum73, MK11, MCW78, MMMT09, MY80, Men82, MP12, Mol90a, Mol90b, NM02a, NCFK11, NAK+15, Omi91, Pit87, PVM94, PV19, Pre93, PB85, RM88, Ram88b, Ram89a, Reg85, Reg88, Riv74b, SS62, Sch79b, SYW+20, SB93, SA97, Vek85, VP96, VP98, Vit80b, Vit80c, Vit83, VC87, WB90, Yao80]. **Analysis** [de 69, Ati20, BGKZ12, BZZ12, CK89, DS09a, DM03, DK12, GLC08, GM77, Gui76c, KZ19, LŁA15, LM88, MJ08, MS13, MSV87, PS08, Pro94, QM98, RAD15, SS90a, SLC+07, Sed83a, SGK09, WL07, ZBB+06]. **Analyti** [Pro94]. **Analytical** [Bat81, DOP+14, WTN07]. **Analytics** [LMD+12, WZY+18]. **analyze** [FJ13]. **Analyzer** [CRdPHF12]. **Analyzing** [Kue82b, PVM97]. **anchor** [FKI+21, SZO+20]. **Anchorage** [IEE01]. **AnchorHash** [MVB+21]. **Anderen** [DS84a]. **Anfänger** [Sch76]. **Angeles** [ACM82, BD88, ICD86, ICD87, ICD88, ICD90]. **Ann** [ACM81, Bai81, Bor81, Lie81]. **annotated** [Pon87]. **Announcement** [DLH09, KS12, Nat92]. **Announcing** [SBK+17]. **Annual** [ACM75c, ACM75a, ACM76, ACM77b, ACM84b, ACM84a, ACM85a, ACM86b, ACM88b, ACM89c, SDA90, ACM90, ACM91c, ACM91d, SDA91, ACM91e, ACM97a, ACM01, ACM02, ACM05, ACM07, ACM08a, ACM08b, AH03, Ano93d, Ano10, BV89, BIP92, Bri92, Bri93, Cop95a, Cop95b, EF12, Fra04, Gol94, IEE74, IEE76, IEE80b, IEE82, IEE88c, IEE89, CTC90, IEE91b, IEE92b, IEE99, IEE06,

IEE07, IEE10, IEE11b, IEE13, Kna89, Mat09, ACM77a, Shm00, Sho05, Sti93, Sti94c, USE00a, YR87, Yun02, ACM94d, ACM91a, ACM96, ACM97b, ACM98, Bel00, DT87, FS09, HM08, IEE85a, IEE92a, IEE95, IEE01, Kar98, Rie89, Wie99]. **anonymity** [GTL21]. **anonymization** [RW07]. **Anonymous** [CZLC12a, ZJ09]. **Anti** [NT01]. **Anti-persistence** [NT01]. **Antonio** [ACM91b]. **Anwendungen** [Lut88]. **Any** [LP15, HR07, Lev89]. **Anzahl** [Dos78a]. **Application** [BKMP09, Cer81, CKB83b, Cha88, CP87, CP88, Dam90a, Dam91, Dav91, FFGOG07, GK76, HP63, Hel94, IRM93, Jou04, KTMo83a, KCB81, LC06, Lit77b, LLW10, Ngu06, Pip79, QV89, QV90, QG95, Rog95, Rog99, Rue93, Sas11, Sch01b, SZ93, SvEB84, Web72, WC94, Yao91, vW94, AT90, CKB83a, CO82a, De 95, GQ95, Kan90, QJ97, SRRL98, Zob70a, Zob70b]. **Applications** [AT93, BKST18, BG07, Bur81, CZLC12a, CZLC12b, CK15, CJ19, DR06, Deb03, DK02, DK15, DadH92, DR09, Fel50, FM85, HK12b, IEE80a, IEE95, KMM+06, Kna89, Lev89, LDY+16, LK93, MK11, PPS21, Pon87, RP91, Rey14, RNT90, Ter87, TZ12, TS76, TS84, Val15, Vau06, Wee12, WC79, WVT90, YZ00, AG10, ARA94, BZL+15, BDK16, DFMR15, HKNW07, KKP92, KZ19, LLC89, LK11, LG78, MJ08, MV91a, NY89b, NY89a, NN90, NW07, PW08, PSN95, RRS07, Shi17, SS16, Sie89, ZYWM20, Ano92]. **Applied** [CS93b, GNP05]. **Applying** [Cer87, Cer88, CHY93, CLYY95, CHY97]. **Approach** [BH93, CCH09, CK12, DL79, DC94, JV16, LT09, LQH18, MY80, RH95, Sch79a, SR89, SK98, Tsa96, ZO93, BJ07, BCCL10, DAC+13, GS89, JHL+15, NW07, PGV93e, PGV94, QZD+18, QD02, TKI99]. **APPROX** [DJRZ06, DJNR09]. **Approximate** [AEP18, AI06, CCH09, CLP17, DP08, DHL+94, DHL+02, Hac93, HC14, MW09, RSK17, AI08, DC94, HFZ+15, LZ06, LCH+14, LWWK20, MBKS07, Rön07, SWQ+14]. **Approximately** [DT14, Ind01]. **Approximating** [ASW87, Pob86]. **Approximation** [DJRZ06, AGJA06, DJRZ06, DJNR09]. **Approximative** [MYS12]. **APRICOD** [ZO13]. **April** [ACM75b, ACM81, ACM84b, Ano83, Ano94, CP87, CP88, Col93, Dav91, ICD91, ICD93, IEE01, Joy03, Lie81, QV89, QV90, SM12, USE90, WGM88]. **AquaHash** [Rog19a]. **arbitrary** [GHK+12]. **Arbor** [ACM81, Bai81, Bor81, Lie81]. **Arbres** [Kar82]. **Architecting** [LLL+16]. **Architectural** [GSL17]. **Architecture** [BCH87, HCJC06, Hsi83, Jou85, KP81, KCR11, KTMo83a, MK11, WG94, XBH06, ZHB06, ABO+17, BOY11, HLH13, LMP+08, MBK00, RG89]. **Architecture-conscious** [ZHB06]. **Architectures** [ACM91c, BRW93, DR92, Kie85, LC20, MKAA17, MKASJ18, RNT90, Bis12, BMQ98, GK05, HDCM11, adHMR93, LLA15, NW07, PJM88, PJBM90, Rei88]. **archival** [QD02]. **Area** [DD15, ABO+17, BOY11, Lar84]. **Area-Efficient** [DD15]. **areas** [JY14]. **ARES** [IH83]. **Argon2** [BDK16]. **Argon2i** [AB17]. **Arguments** [Yao83, ABM+12]. **ARIES** [Moh90, Moh93]. **ARIES/LHS** [Moh90, Moh93]. **ARIRANG** [HKKK10]. **Arising** [FS82]. **ARITH** [IEE05, MS05]. **ARITH-17** [IEE05, MS05]. **Arithmetic** [Die96, Ers58a, GSC01, HSK88, IEE05, MS05, ISO97]. **Arizona** [Gol92]. **Arlington** [ACM94d]. **Arrangement** [Riv76, Riv78]. **Arrangements** [Yao85a, Yao95, Wee88]. **Array** [Cob94, He87, YLB90, SV15b]. **Arrays** [BGS96, CP91a, Gra94a, LPWW06, RS77, Ros77, CP91b, CLS18, RS75, Tay89]. **Art** [Knu73, Knu75, Pre97b, Ruc15, PGV93c]. **Artificial** [Kak93, ARA94, LLC89, BCR04]. **ary** [CC91, CLC92, Gui76c, Gui78, RRS07]. **ASCII** [HF91]. **ASI** [Ano95c].

ASIACRYPT [IRM93, LC06, PSN95]. **ASIC** [MKAA17]. **ask** [Gre95]. **Aspects** [AH03, SS89a]. **Assembly** [ASW07]. **Assessment** [THY+18, DMP09]. **Assignment** [LL92, Wil71]. **Assignments** [Yao91]. **Assisted** [Wil96]. **Associated** [Sar10, FDL86, SB95]. **Association** [CL05, CT12, DT87, PCY95, TGGF10, HC02, HC07]. **Associative** [Bur76a, Bur77, DW83a, DD15, Dos78b, FM91, FR69, HNS84, KHW91a, KR79, Ouk83, Riv74b, WB87, dW83b, HDCM11, KHW91b, Koe72, YIAS89]. **Assoziativer** [GN80, Koe72]. **Assumptions** [Chr84, Dam93, Dam94, Sim98]. **Astronomical** [Gui89]. **Asymmetric** [CLP17, BR94, CFN18]. **Asymptotic** [CLS18, IK92, Ati20, Pro94, WL07]. **Asynchronous** [KFG15, PAKR93]. **Atlanta** [ACM83a, ACM83b, USE00a]. **Atlantic** [Fre90, GMJ90, IEE84]. **ATM** [SMS91]. **Atom** [LC12]. **Atomic** [LMR02]. **Attack** [CJP12, CMP07, JLH08, KK06, Pey15, PGV90a, Sho00b, WW09, WFW+12, ZF06, Ano09b, BSU12, CJP15, JG95, PGV93a, PGV93b, SXL16]. **Attacking** [CP95b]. **Attacks** [AB17, ABD+16, BDG+20, BPBBLP12, Bih08, BKMP09, CY06, DK07, DDS14, DL17, HKKK10, HRS16, JL14, KNR10, KLP98, KVK12, LK94, KKMS10, LLJ15, MRST10, MNS12, Saa12, SY11, Sas11, WYY05d, ZWW+12, BSU12, ITP14, KL95, KHK10, LS07a, MSP12, WYY05a, WS13]. **Attribute** [CS83b, CS87, GK94, GK95, HYH93, KG95, RSSD90, RL74, ZZM17, ASW87, HR93]. **Attribute-Based** [ZZM17]. **attributes** [HM03]. **Auction** [SKM01]. **Audio** [MV01, YTJ06]. **Audit** [SK99, Ano93a]. **Auditing** [LRY+15, DMB19, GB17]. **Aufteilungs** [vM39]. **Aufteilungs-** [vM39]. **Aug** [BD88]. **Augmented** [ZLC+18]. **August** [ACM79, LFP82, ABB93, AW89, A+90, Bel00, Bri92, Bri93, BW92, CRS83a, CGO86, Cop95a, Cop95b, DSS84, DSZ07a, DSZ07b, DJRZ06, DJNR09, Fra04, Gil77, GSW98, HB93, IEE95, Jen76, JY14, MK89, MSDS90, PV85, PK89, RK89, Ros74, Rov90, Sho05, Sti93, Sti94c, WPY90, Wie99, lWSS91, Yua92, Yun02]. **AUSCRYPT** [SP90, SZ93]. **Austin** [ACM87, ACM88a, ARA94, Nav85, USE00b]. **Australia** [Bar83, SP90, SZ93, DG96, MSDS90, PSN95]. **Australian** [Bar83]. **Austria** [Kui92, ICD93]. **Auswahl** [Pet83, Dos78a]. **Authenticate** [Yas07]. **Authenticated** [KV09, PTT16, Sar10, YLSZ19, BSNP96b, GL06]. **Authentication** [Abi12, Alb21, AS96, BCK96a, BCK96b, BKST18, BAN89, CJP12, DCM18, EPR99, FIP02a, GI12, GBL94, HMNB07, HCPLSB12, JRPK07, JK11, KKRJ07, MRW89, NR12, PGV93f, QJ97, RWSN07, Rog95, Rog99, Sho96, TW07, Tsu92a, VD21, WC81, WDP+12, WS03, YY07, ACP10, CBB05, CJP15, GTL21, HL12, Kra94, Kra95, KCL03, Ku04, KCC05, LLH02, LKY04, LW04, MS09, OCDG11, SPLHCB14, Sta99, Sti91, Sti94b, SV06, Tsa08, Tsu92b, YRY04]. **Authenticity** [Sch01b, ADF12]. **Auto** [EFMRK+20, Lit77a]. **Auto-structuration** [Lit77a]. **Auto-tuned** [EFMRK+20]. **Automata** [ACM82, IEE74, LP04, LK93, MMC01, AGK+10, ADG+08, AMSM+09, ACJT07, dBvL80, CIM+05, Kui92, NS82, Pat90]. **Automated** [DGM89, ZZ83, Cer85]. **Automatic** [GT80, Zam80, SB07]. **Automation** [IEE11a]. **Automaton** [DGV93, LLL11, MZI98, TLLL07, TLLL09]. **automaton-matching** [TLLL09]. **Automorphism** [PWY+13]. **autonomous** [SZO+20]. **AutoPlacer** [PRRR15]. **Auxiliary** [DL12, FXWW17]. **Availability** [Eng94, ADF12, DFMR15]. **Average** [Bra84a, Bra85, Bra86, Gon77, Kut10, Reg81,

TW91, MT16, THS97]. **average-case** [Mic02]. **avoid** [Pat94]. **Aware** [CJKK19, HNKO20, JLL+20, MZL+19, PG17, BB07, HFZ+15, HFF+17, NDMR08]. **awareness** [Li10]. **Awesome** [Knu19]. **AWOC** [Rei88].

B [BD84, FK89, Omi88, Omi89a]. **B-Trees** [BD84, FK89]. **Back** [DSSW90a, DSSW90b]. **Backoff** [SHRD09]. **Backtracking** [WKBA07, YD85]. **Backward** [CPP08, LLL11]. **Backyard** [ANS10]. **Balance** [IK92]. **Balanced** [AG10, ABKU99, DW05, DW07, Lep98, LB07, Oto86, Oto88b, PB80, WZ12, FP82, TLLL18]. **Balancing** [HC13, KJC11, Nak21, Omi91, RRS12, RK91, Top92, TP95, ZJM94a, ZJM94b, ZJM94c, DSD95, SX08, WL07, WTN09, XCCK09]. **Balatonfured** [Rue93]. **Balloon** [AB17, BCGS16]. **Balls** [CRSW11, CRSW13]. **Bally** [IEE84]. **Baltimore** [ACM90, FNY92, IEE02]. **Band** [Meh86, Sol93]. **Band-Join** [Sol93]. **Bands** [KCF84]. **bandwidth** [AS09]. **BANG** [THS97]. **Banked** [vdBGLGL+16]. **Banska** [Rov90]. **Barbara** [Bel00, Bri92, Bri93, CRS83a, Cop95a, Cop95b, Fra04, Sho05, Sti93, Sti94c, Wie99, Yun02]. **Barcelona** [DJRZ06, CTC90, LSC91]. **Barreto** [FT12]. **barrier** [MPST16]. **Base** [BCH87, CRdPHF12, Chr84, EE86, FM85, Gho77, Gho86, ISK+93, McC79, YBQZ17, Zam80, Mar75, Mar77, WLLG08]. **Based** [AK98, Abi12, Alb21, AP08, Aum09, AS16, Bal96, BG92, Ben98, BDM+12, BHH+15, BRS02, BCS09, BRSS10, BI12, Buc82, Bur83b, Bur83c, But17, CCF04, CFP19, CS83b, Cha84b, CS87, CW91, CdM89, CdM90, CW09, CTZD11, CZLC12a, CZLC12b, CZLC14, CT12, CDW+19, CadHS00, DGV93, Dae95, DK09, DG85b, DL17, DF01, DR11, DB12, EK93, Fab74, FL04, FR69, FRB11, FH69, FFGOG07, GGY+19, GRBCC19, GO07, GI12, GSC01, Gri98, GK08, GH07, HMNB07, Hal12, HDCM09, HHL10, HNKO20, HW08, HWZP18, HCPLSB12, HLC10, Hül13, HRS16, HBG+17, HM19, JXY07, JTOT09, JK11, KSSS86, KM09, KV09, KL87, KKRJ07, KJC11, KMV10, KTMO83b, KW12, KP96, KP97, KR79, KRJ+80, KK85, Kum89a, KKT91, LM93a, LYY+18, LYX+19, LW88, LMC07, LMJC07, LLDZ18, LLZ10, LLL09, LHC05]. **Based** [LLLC17, LRY+15, LXL+19, LG78, LTS90, LCM+20, MLD94, MKF+16, MCF17, MP12, Mil85, MKAA17, NIS15, NCFK11, Nak21, NNA12, NXB13, OL89, OSR10, PFM+09, PTT16, PCY95, PHG12, PRZ99, PSZ18, Pre97a, RGNMPM12, RTK12, Rey14, RWSN07, RNR13, RL74, RK91, SD85, SDKR87, Sch01b, Sch79b, Sch81, SBS16, SYW+20, SC90b, SC90a, SC90c, SK98, Sho96, SKC07, SSS05, SVCC01, Sun15, TWZW11, TGGF10, TZ12, TY91, TP15, TK07, US09, WWZ09, WSSO12, XBH06, XHZ+19, YNW+09, YSW+11, WL12, YY07, YTJ06, YD86a, ZJ09, ZWH17, ZZM17, ZQSH12, ZLC+12, vMG12, Adi88, AY14, ASM17, ACP10, AAGG16, BSNP96b, BLC12, BLY20, BCR04, BC06, BDS09, Bur83a, Cha12, CML+13, CCHK08, CJP12, CJP15, CLW98, CJ86, DG85a, DS09a, DHW08, EASR22, GB17, GL06, GLC08, GZ99, HLL18b]. **based** [HLL18a, HAK+16, HCJC06, HC11, HLMW93, HXMW94, HW88, HL03, JFDF09, JL14, JBWK11, JG95, KI94, KRJ09a, KST99, Kor08, Kra94, KCL03, Ku04, KCC05, KSC11, KSC12, LM93b, LDM92, LWG11, LND08, LLT21, LACJ18, LLJ15, LSZ+21, LMPW15, MSZ+20, MS09, Mei95, MZI98, MS13, MHT+13, Mul92, MFES04, MJ14, NADY20, NS16a, OT89, PCK95, Par18, PPB16, PL21, PW06, PBGV89, PGV91, PGV93e, PGV94, QZD+18, RP95, SPLHCB14, SN19, SV94b, SV95, SE21, SGK09, SX08, SRRL98, Sim98, SA17, SZO+20, TKH20, TWL+18, Tsa08,

TD93, UIY10, UHT95, VD05, VD21, Wil14, WY02, XLZC14, YCJ12, YSL05, YL97, YZ16, YD86b, ZYWM20, ZDI+15, FH96, TLLL18]. **basée** [LG78]. **Bases** [ABB93, VLD82, AW89, AAC+01, BD88, BDS88, BJZ94, CGO86, CKN18, DSS84, Gon83, Hil78b, Hil78a, Ker75, LT80, LSC91, MSDS90, PV85, ST83a, ST83b, Yua92, Yao78, LT80]. **Basics** [Dre17a]. **Basis** [BT12a, MW95, CHL07]. **Batch** [Lyo79]. **Batched** [Piw85, SG76b]. **Bay** [Ano10]. **Bayesian** [CSSP15, OGAB14, PKSB18, RH95, SP12]. **BC** [ACM05, LL08]. **BDDs** [MJT+02]. **Be** [Yao81, CP91c, GMW90, Sch91a, Sim98]. **Beach** [PDI91, RNT90]. **Bearbeitung** [Koe72]. **Beaverton** [ODB89]. **Beginner** [She17]. **Behavior** [Lev00, Sav90, TTY93]. **Beijing** [Ano93c, Yan10]. **Beitrag** [BI87]. **Belgium** [BW92, QV89, QV90, Vid90, PGV93c]. **Bell** [Lam70]. **belt** [BDPV06]. **belt-and-mill** [BDPV06]. **Bemerkung** [Eck74a]. **Benchmarked** [MKAA17]. **Benefits** [Bur79]. **Bergen** [Ytr06]. **Berkeley** [ACM86b, DJNR09, IEE06, IEE13]. **Berlin** [AH03, Yao78]. **beschränktes** [Wen92]. **Besetzungswahrscheinlichkeiten** [vM39]. **BESM** [Ers58b]. **better** [Mit17]. **Between** [Bra84a, Bra86, KCF84, PNPC20, Bra85, CCL91, GHW07, LC13, Omi89a, Sar11]. **Bewertung** [Hil82]. **beyond** [BLC12, LJW+17]. **BF-Based** [WL12]. **Bi** [MZL+19]. **Bi-Index** [MZL+19]. **bias** [NN90]. **Biased** [JCK+18, TSY98]. **bibliography** [Pon87, Sab94]. **Bicliques** [LLW10]. **Bid** [SKM01]. **Bidirectional** [Cle84]. **Big** [ADOAH19, LRY+15, PSSC17, WZY+18, YGS+19, LL13, SA17]. **BigDecimal** [Sun02]. **Bijective** [Oka88, SS15]. **Billion** [LLL+16, STS+13, ZBB+06]. **Billion-Requests-Per-Second** [LLL+16]. **billion-vertex** [ZBB+06]. **BiloKey** [MZL+19]. **Bin** [WLWZ19]. **Binaries** [ASWD18]. **Binary** [CLP17, DGGL16, DHT+19, Du86, Fro82, GRZ93, HSPZ08, LQH18, TYZO15, de 69, FP82, LMSF89, LMPW15]. **Binary-Relational** [Fro82]. **Binning** [PKSB18]. **Bins** [CRSW11, CRSW13, DW05, DW07]. **biological** [BW89]. **Biometric** [FFGOG07, MS12, SP21, YY07, SK20]. **biometrics** [AGBR19]. **Biomolecular** [ZLY+13]. **biomolecule** [FDL86]. **Biomolecules** [BRM+09]. **Bipartite** [Kut06]. **birth** [Ste18]. **birthday** [MPST16, MSP12, SXL16]. **Bit** [Blu95, Kil01, QG89, QG90, SP91, ASM17, BK07a, ISO97, LK16, LK11, MJ08, MIO89, TKI99, MKL21]. **bit-level** [TKI99]. **bit-parallelism** [ASM17]. **Bitcoin** [Nic17]. **Bitmap** [EVF06, FVS12]. **Bits** [Kil01, Nae95]. **Bitstate** [IJK13]. **BitVault** [ZLL+07]. **Bitvectors** [BMRV02]. **Black** [JLH08, Rja12, SV94b, SV95]. **Black-Box** [BRS02, Rja12]. **Black-Hole** [JLH08]. **BLAKE** [AMPH14, VNP10]. **Blind** [FL04]. **Block** [BRS02, Chu90, CV08, KP96, KLP98, LM93a, LK94, Men12, Pre97a, QG89, QG90, SDMS12, SDMS15, YLZ20, Zhe90, GLC08, HLMW93, HXMW94, ISO97, KL95, Lai92, LM93b, Men17, PW06, PGV93e, PGV94, RP95, Roe95, YL97]. **Block-Cipher-Based** [BRS02, GLC08]. **Blockchain** [Dre17a, HM19, KAS+22, LSZ+21, YLZ20, ZXL19]. **Blockchain-Based** [HM19, LSZ+21]. **Blockcipher** [AP08, BCS09, BRSS10, HKY12, LLJ15, PBGV89]. **Blockcipher-Based** [AP08, BCS09, LLJ15]. **Blockciphers** [RS08, PGV91]. **blocking** [PBBO12]. **Bloom** [DKT06, HKL07, HKLS12, HXLX13, LYW+18, MK11, PSS09, Ram89b, RKK14, RK15]. **BLS** [BP18]. **BNCOD** [Oxb86]. **Boas** [Wil00]. **Boca** [HB93]. **Body** [WS93, JWM+18, Lia95, War14]. **Bonaventure** [ICD86]. **bond** [ZBB+06].

Bonsai [DCW91]. **Bookshelf** [Cro98]. **Boolean** [AN96, ÁCZ16]. **booting** [LC95]. **Bordeaux** [AGK+10]. **Boston** [ACM84a]. **bottleneck** [MBK00]. **Boulder** [ACM77b]. **Bound** [Ari94, SG16, Sun91, Sun93, vT14]. **boundaries** [SS15]. **Boundary** [KSSS86]. **Bounded** [DS84a, LL86, Lom83, Lom88, MN90, GHK+12, RM88, TB91]. **bounded-depth** [GHK+12]. **Bounds** [BGS96, Cha94, CV08, DKM+94, GadHW96, Gon77, KM86, KM88a, KVK12, MNP08, OWZ14, Woe01, Woe05, Yao83, BvT13, DKM+88, DKM+91, GHK+12, Rad92]. **Box** [BRS02, Rja12, SV94b, BZZ12, SV95]. **braids** [LMP+08]. **Branch** [LBJ02]. **Branches** [DGGL16]. **Branching** [FS82]. **breaking** [DK94, MPST16]. **Brent** [FL73]. **Bridging** [ACM04]. **Brief** [DLH09, KS12]. **Brighton** [Dav91]. **bringing** [NMQ22]. **Brisbane** [DG96, MSDS90]. **British** [ACM08b, Oxb86]. **Broad** [PACT09]. **Broad-Phase** [PACT09]. **Broadband** [SMS91]. **Broadcast** [YSW+11, GBL94, SNW06]. **Broadcasting** [KCF84, OCDG11]. **Broken** [CP91c]. **Broker** [TGL+97]. **browser** [NM02b]. **Brussels** [Vid90]. **Brute** [CJP12, LS07a, CJP15]. **Brute-force** [CJP12, CJP15]. **BST** [AZ10]. **BTB** [LBJ02]. **Bubble** [Wri83]. **Bucket** [CS82, Dev86, Joh97, Kab87, KNT89, KO90, Lyo85, QCH+81, Rog95, Rog99, Tam81, TYZO15, Tra63, YD86b]. **Bucketing** [Pal92]. **Buckets** [Hac93, JV16, VP96, VP98, KHK12]. **Buffer** [LBJ02]. **Building** [AÖD19, BC06, HKL07, Mit17, PV95, RMB11, WHS+07, PvO95]. **Built** [Win84, DTM+18]. **built-in** [DTM+18]. **Burden** [Oak98]. **burst** [AZ10]. **Bushy** [CHY93]. **Business** [Bra88, Luh58]. **Bystrica** [Rov90]. **bytecodes** [SUH86]. **Byzantine** [HGR07].

C [Pla98, USE90, ÁCZ16, Blu95, Eug90, GBY91, Pro89, Sed90, Sed92, Sou92, Tay89]. **C/C** [Pla98]. **CA** [ACM03a, ACM08a, ACM11, DJNR09, IEE13, Joy03, Cop95a]. **Cache** [Ask05, CGLC20, PWYZ10, PWYZ14, Pro18, PSS09, SBS16, SKC07, YNW+09, YT16, ZH18, AZ10, BFCJ+12, CCHK08, HSMB91, KSC11, KSC12, MZK12, QM98, WLC20]. **Cache-** [PSS09]. **Cache-Conscious** [Ask05]. **Cache-Oblivious** [PWYZ14, PWYZ10]. **Cache-Optimized** [ZH18]. **cache-partitioned** [MZK12]. **Cache-tries** [Pro18]. **Caches** [SBS16, SVCC01]. **Caching** [DB12, KM92, Rey14, WBWV16, XBH06, BCR10, Cha12, HL05, KLL+97, KSB+99, She06, WZ12, WY00, WY02, ZO13]. **CAD** [KI94, Bar97]. **CAD-based** [KI94]. **Cake** [CHSC18]. **California** [ACM82, ACM86b, ACM07, Ano10, Bel00, Bri92, Bri93, CRS83a, Cop95b, Fra04, ICD86, ICD87, ICD88, ICD90, IEE11b, Kar98, Shm00, Sho05, Sti93, Sti94c, Sto92, USE90, Wie99, Yun02, Col93, IEE88a, IEE06]. **California/Special** [ACM82]. **Call** [HLC10]. **Cambridge** [ACM86a, BV89, Gol96, JBJ94, Kil05, And94]. **CAMELOT** [SPB88]. **Camera** [BH93]. **CAMsure** [RSK17]. **Can** [CP91c, Dam93, Pal92, Sim98, Dam94, GMW90, Sch91a]. **Canada** [ACM02, ACM05, ACM08b, AFK90, DSZ07a, DSZ07b, JY14, LL08, Lev95, Yua92]. **Canadian** [CCC89]. **candidates** [ABM+12]. **Canonical** [DNV81]. **canonicalizing** [FGFK10]. **Canterbury** [Oxb86]. **Capabilities** [RS12, Tra63]. **Capability** [Fab74, Wan84]. **Capability-Based** [Fab74]. **Capacity** [KK85, Tan83, HO72]. **Cape** [IEE05, MS05]. **cardinalities** [GGR04]. **Cardinality** [BHIMM12, GLLL17, HM03, NTW09]. **Cards** [Ku04]. **Carlo** [BF83, Rey14]. **Carolina** [ACM91c]. **Carry** [GK08, FJ13, LK16]. **Carry-Less**

[GK08, LK16]. **carry-truncated** [FJ13]. **Carter** [Sar80]. **Cartesian** [Du86]. **Cascade** [KZ84, RTK12]. **Cascaded** [Jou04]. **Cascading** [Wan14]. **Case** [ANS09, ANS10, AR17, DMV04, DS09c, Ell85b, F+03, FKS84, HBL+10, Kut10, Lar82a, YLB90, BGG94, FPSS05, Lar81, Mic02, MT16, SKD15]. **case/average** [Mic02]. **cash** [Bac01]. **Casino** [IEE84]. **Cassandra** [EH17]. **Catalonia** [LSC91]. **Catalunya** [CTC90]. **Categorization** [MBBS12]. **Categorized** [LLG+17]. **Cathedral** [IEE88a]. **Cauchy** [TI12]. **Causal** [SDZ21]. **Caution** [Mul91]. **Cayley** [GM18, Zém94]. **CBC** [BBKN01, BBKN12]. **CCA** [CZLC14]. **CCA-Secure** [CZLC14]. **Cell** [Mil99, Pag01, SZO+20, Sun93]. **Cells** [JCK+18, WH83]. **Cellular** [DGV93, MZI98]. **Center** [ACM91b, CGLC20, Fis87, IEE90, Rie89]. **Centers** [SWTX18]. **Centric** [LT12, SPSP16, WBWV16, XHZ+19, AK09]. **century** [ACM91b]. **Certain** [Chr84, van94]. **Certificate** [MFES04]. **Certificates** [LK07]. **Chain** [EAA+16, JLH08, LAKW07, LHC05, SKM01, YZ00, YSEL09, Bay73b, Par18]. **Chained** [Bay73a, HNS84]. **Chaining** [BBP88, Cha94, CPP08, DDMM05, GSC01, Joh61, Kue82b, MJBD11, Rag93, VC85, CBB05, Kno84, KdlT89, KFG15, Lar84, PW06, TT81, TT86, TLLL18, Kue82a, Kue82b]. **Chains** [BT12a, FL04, Jan08, Ngu06, YKLH10, ZQSH12, HL94, JFDF09, SN19]. **challenge** [GJM02]. **challenges** [BVF12, GJM02]. **Challenging** [MSP12]. **Chameleon** [BR14, GZX14, PWY+13, LWG11, CTZD11, Moh11, Zha07]. **Champion** [KI94]. **Change** [DHK+15]. **changeable** [HYLT99]. **Changes** [Dan13]. **Changing** [Lit78, Litxxb]. **Channel** [GO07, RWSN07, MS09]. **channels** [SNW06, Wu05]. **chaos** [McN03]. **Chaotic** [PPS21, Sch01a, YY07, GTL21]. **CHAP** [HDCM09]. **Character** [Dav73, YkWY83, Sab94]. **Characteristics** [Bay74, DR06, SDT75, DLH+79, RP95]. **Characterization** [BR14, CPP08, Lyo83, van94]. **Characterizing** [LH03a, RTK12, VZ12]. **checker** [Wie86]. **Checking** [CKN18, Hea72, IJK13, AD08, Wil96]. **Checkpoint** [LACJ18]. **Checkpoint-Restart** [LACJ18]. **Checkpointing** [FRB11]. **checks** [SB07]. **checksums** [GKKT10]. **Chemical** [WKO78, ZBB+06]. **Chennai** [RRR99]. **Chicago** [ACM88b, ABM06, BL88, IEE82, Lom93, IEE80a]. **Chile** [BJZ94, CHK06]. **China** [Ano83, HL91, IEE11a, LC06, Yan10]. **Chinese** [CS85b, YkWY83]. **Chinesizing** [Zou85]. **Chip** [MJBD11, Mot84, YNW+09]. **Chisel** [HCJC06]. **Cho** [SPLHCB14]. **Choices** [FP10, DKRT16, KM08]. **Choosing** [KLSY07]. **chopMD** [CN08]. **Chord** [KLSY07]. **Chosen** [CS02, Sho00b]. **Churn** [LMSM09, LMSM12, WTN07]. **Churn-Resilient** [LMSM09, LMSM12]. **Cichelli** [BF83, Cic80a, GS89, JO80]. **CICS** [Bra88]. **CIKM** [FNY92]. **Cincinnati** [BD08]. **CIoT** [ZZLZ18]. **Cipher** [And91, BRS02, Dae95, cLmL07, NCFK11, QG89, QG90, WSSO12, GLC08, HL03, ISO97, RS14, YL97]. **Cipher-Based** [NCFK11]. **Ciphers** [BBKN01, BBKN12, Fil02, KP96, LM93a, Pre97a, Roe94, SDMS12, SDMS15, Zhe90, DS09a, HLMW93, HXMW94, Lai92, LM93b, PGV93e, PGV94, RP95, Roe95]. **Ciphertext** [CS02, Sho00b]. **Circuit** [NRW90, Ste82]. **Circuitry** [Cai84]. **Circuits** [DLT98, MD05, GHK+12, Mil98]. **circulant** [AN20]. **Cirencester** [Boy95b, Boy95a, Far93]. **City** [VLD82, Fre90, GMJ90, IEE84, IEE99, JBWK11]. **Class** [CMW83, DadH90, DS09c, MCW78, AAGG16, DM11, Eug90, SN19]. **Classes** [ÁCZ16, CW77a, CW77b, CW79, KW12,

Mul91, Sie04, WC79, van94, Bie95, DS09b, Sar80, Sie89]. **Classification** [GCMG15, HSPZ08, McK89a, PT11b, SY08, And93, CKKK09, IG94, LS07b, McK89b, XLZC14]. **classifications** [LZ06]. **Classifier** [GK95, KG95]. **Clause** [CJ86, Llo81]. **Claw** [BHT98, BHT97]. **Claw-Free** [BHT98, BHT97]. **Client** [DR92, GTL21, TC04]. **Client-Server** [DR92]. **client-side** [TC04]. **Climbing** [CL95]. **Clocked** [LN93]. **clone** [Kos14, LG13]. **closed** [SS89a, SS90a]. **Closest** [Val15, DHKP97, TYSK10]. **closest-pair** [DHKP97]. **Closing** [PNPC20]. **Closure** [CdM89, CdM90, GC90]. **cloth** [TWL+18, TWL+18]. **Cloud** [HNKO20, HWZP18, LRY+15, Mir17, Nak21, DMB19, GB17, HLL18b, SZO+20]. **cloud-RANs** [SZO+20]. **Cluster** [SKC07, KSC11, KSC12, TC04, ZHX+21]. **Clustered** [Rot89]. **Clustering** [AII89, Bel70, Bel72, Bel83, BBS90, CdM89, CdM90, Gui75, Gui78, KBG18, Mac95, MNY81, PKSB18, SPSP16, AÖD19, Gui76c, NH74, SX08]. **Clustering/hashing** [AII89]. **Clusters** [TY03]. **Clutter** [MBBS12]. **CLV** [CF89a]. **CM** [PW94]. **CM-5** [PW94]. **CMAC** [CG92]. **CNF** [BHIMM12]. **CNN** [SYW+20]. **Co** [ZWCL10, HLH13]. **Co-hashing** [ZWCL10]. **co-processing** [HLH13]. **Coalesced** [CV83b, CV84, Che84a, Che84b, CV85, CV86, Jan08, MS88b, Pal92, Pit87, Vit81a, Vit82b, Vit83, VC87, CV83a, PY88, Vit80a]. **Coalescing** [Vit80b, Vit80c, Kno84, SSU+13]. **coalescing-lowering** [SSU+13]. **Coast** [SZ93]. **COBOL** [Bra88, Zou85]. **Cod** [IEE05, MS05]. **Codasyl** [Gra86]. **Code** [BK70, Bel70, Bel72, Bel83, BMB68, CLD82, Chu90, DC81, DL80, Eck74a, FIP02a, Gon81, KKRJ07, Lam70, LBJ02, Mau83, Mit73, SV15a, Sun15, CD84a, CLS95, Cli95, Mau68, Mer72, MF82]. **Coded** [Bay73c]. **codering** [Lit77a]. **Codes** [BKST18, BGS96, Bie97, CLP17, Fal85a, Har97, Irbxx, JP07, KP96, KP97, KGJØ18, LQH18, SVCC01, TW07, BJKS93, BJKS94, Bou95, Fal86, Fal88, FM89, GHK+12, Gob75, IG94, Kri89, Mil98, Sti91, Sti94b, vT14, Far93, Bie95]. **codification** [FDL86]. **Coding** [Blo70, Boo74, Bur77, Bur78, Bur79, CJ86, DA12, Dav73, Dos78a, FH69, Gon77, HP63, HJ75, HG77, Kam74, Lit77b, Mar64, Mar71, Pip79, SD85, SDKR87, Sta73, Web72, Boy95a, Boy95b, Bur76a, Coh94, DVS+14, Far93, LG78, Riv74a, Sab94, SDR83b, Sch79b, MKL21, Ytr06, HJ75]. **Coefficient** [KKN12]. **coherency** [FWG18]. **Coherent** [GLHL11]. **Coin** [CLP13]. **Coins** [HR04, Ros12]. **Collaboration** [JXY07]. **Collaborative** [ADOAH19, WY00]. **Collecting** [FW76, FW77]. **Collection** [AG93, LXL+19, TR02, UIY10]. **Collections** [BBD+82, BBD+86, LRY78, LRY80, DTM+18, SV15b]. **College** [Jáj90]. **collide** [GNP05]. **Collision** [Ask05, BG93, BR97, BM97, BK12, BKMP09, CHKO08, CJC+09, Dam87, HM96, HHL10, HCJC06, IKO05, IT93, IH95, KKT91, MS09, MNS12, Men12, Mit12, MOI90, MOI91, MC86, NSS+06, Pey15, PACT09, PBGV89, PGV90b, PGV91, Rus92, Rus93, Rus95, Sam81, SY11, SHRD09, SHF+17, Vau92, Vau93, WYY05a, WYY05d, XNS+13, YB95, ZBB+06, vW94, AKY13, BGG93, BF08, CHKO12, Con17, Gib91, ITP14, KdlT89, Men17, MT16, PGV93g, Sar11, SKP15, SBK+17, TWL+18, Van92, WS13]. **Collision-Free** [BM97, HM96, Rus92, Rus93, Rus95, SHRD09, BG93, HCJC06, PBGV89, Vau92, Vau93, ZBB+06, BGG93, Van92]. **Collision-Mitigation** [SHF+17]. **Collision-Resistant** [BR97, BK12, CHKO08, IKO05, CHKO12]. **Collisionful** [BPSN97, Gon95, Li95, BSNP96b, BSNP96c].

Collisions [Ano95a, BI87, BT94a, BT94b, CY06, DBGV93, GIS05, GL73, HR04, IP08, IP11, LCL+20, Pat95, VNP10, WFLY04, WYY05b, WYY05c, DV07, Gon95, Li95, Pat94, RVPV02, Sim98]. **Colloquium** [AGK+10, dBvL80, Kui92, NS82, Pat90, ADG+08, AMSM+09, ACJT07, CIM+05]. **Colony** [ACM83a, ACM83b]. **Colorado** [ACM77b, ACM79, ACM85a]. **Colored** [Ros12]. **coloring** [HK83]. **Columbia** [ACM08b]. **column** [DLM07]. **ComBack** [WKBA07]. **Combination** [Qui83, TYZO15, US09]. **Combinational** [MJT+02]. **Combinatorial** [BK07b, DD11, DT75, KP94, Sti94a, van94, DJRZ06, DJNR09, HKLS12, MN99, Sed83a]. **Combinatorics** [Wil85b]. **Combined** [KHK15, ZC77]. **Combiner** [HS08]. **Combiners** [BDG+20, FL08, FLP08, FLP14, Mit12]. **Combining** [AGBR19, GSC01, TW07, NM02b]. **Come** [PM89]. **Command** [CBA94, Gai82]. **Comment** [Ban77, FL73, Lam70, Pro94]. **Comments** [AA79b, AA79a, BMB68, CTZD11, Piw85, TY91, Gib90]. **Commitment** [HM96, HR07]. **Commitments** [ACP09, LP15, Wee07]. **Committee** [IEE84]. **Common** [DM90, GPGO16, ESRI14]. **Commonwealth** [Rie89]. **Communication** [Alb21, KM88b, Ano93c, HO72, KK96]. **Communications** [IJW89, GZX14, Sch01a, ACM94a, IEE92a, IEE01]. **communities** [ACM04]. **Community** [RMB11]. **Commutative** [CLS12]. **Compact** [Cle84, CD84b, DCW91, DHT+19, KRJ09b, Kul84, LYX+19, Oto88b, QP16, vdVL12, JCC00]. **compactage** [LG78]. **Compacte** [Kar82]. **Compaction** [HC87, Rag93, WKBA07, SD95]. **compactly** [VNC07]. **comparaison** [LG78]. **Comparative** [Cra85, DTS75, GLG+02, Hil78b, Hil78a]. **Comparator** [Bur84, Bur82]. **compare** [BVF12]. **compare-by-hash** [BVF12]. **Comparing** [MRL+19]. **Comparison** [CHS+18, EK93, GG80, Jai89, Jai92a, Jai92b, Jaixx, LG78, LH03b, QCH+81, RLH91, SDK91, Tro95, KK96, RLH90, TT86]. **comparisons** [FDL86, Rön07]. **COMPCON** [IEE88a]. **compensated** [ZRL+08]. **Competition** [Bur08, Bou12, jCPB+12, TSP+11]. **compilation** [HF13, SF88]. **compile** [MP90]. **compile-time** [MP90]. **Compiler** [ACM79, Dit76, Wil96, Sag85b]. **Compilerbau** [Wal74]. **Compiling** [DM81]. **Complete** [SDW14, Die90, GvR08, Rad92]. **completely** [Con17]. **Completion** [ZWH17]. **Complex** [KM92, Mar64, MW95, Sch90b, SD90b, SD90a, War86, WS76, TD93]. **Complexities** [GK76]. **Complexity** [Adi88, Dam93, GHK91a, GHK91b, CTC90, KVK12, LLW10, Mai83, Mai92, MNT90, Mor83a, NRW90, SS88a, VV86, YSEL09, Ati20, BSU12, CKM14, MNT93, Mil99, Pag01, SS90b, Sun93]. **Component** [BFMP11, Cha88, MW09, SY08, SA97, US09, SGK09]. **component-based** [SGK09]. **Components** [de 69]. **Composed** [HGH+12, YkWY83]. **Composite** [Oto85a, RL89]. **composites** [GPGO16]. **Composition** [Sho00a]. **Compositions** [SS16]. **Compound** [MH00]. **comprehensive** [NM02b]. **Compress** [BBD09a, LT09]. **Compressed** [GO15, GLB21, JL14, Zuk21, BLC12, Ind13, Mil95]. **Compressing** [WMB94, WMB99, MP16]. **Compression** [BC08, CW91, HKY12, LJF19, Lis07, LG78, RT87a, GLM+10, SMS91, SM08, SM12, AGJA06, BD82, CKW93, FS08, GSS01, Li10, Sab94]. **compression-oriented** [CKW93]. **COMPSAC** [IEE80a, IEE95, Kna89]. **Comput** [Sar80]. **Computability** [ACM82]. **Computation** [ACM94b, AiNOW11, Chi91,

Chi94, DJRZ06, IEE11a, Jáj90, Jen76, Lak96, Lev95, Ng79, RK91, Tam85, ZO93, ZLC+12, vdHvH12, Fis87, MYS12, Ano93d]. **Computational** [CCC89, Cer83, LYW+18, MNT90, Sab94, Wil00, de 69, Dam94, GvR08, IKOS08, MNT93, Sch82b]. **computations** [FHL+19, GK12b]. **Compute** [Bra84a, Bra85, Bra86, Tro92]. **Computed** [TT81, TT86]. **Computer** [IJW89, ACM91b, AFI63, AFI69, AH03, iA91, iA94, Bar83, BCH87, Bor81, DS97, Ell82, Gol94, GT63, HS78, IEE76, IEE80b, IEE80a, IEE82, IEE84, IEE85a, IEE88c, IEE88a, IEE88b, IEE89, IEE91b, IEE92b, IEE95, IEE99, IEE05, IEE06, IEE07, IEE10, IEE11b, IEE13, Jai89, Jai92a, Jai92b, Jaixx, Jou85, KCF84, KO90, Kna89, Knu73, Knu74, Knu75, Kon10, Leb87, LC86b, LC95, LL83, Mar75, Mar77, MS05, RRR99, RJK79, Rie89, Rov90, Ruc15, SK99, Wal88, Wil85b, Win78, ZZ83, ACM94c, Ano93c, Don91, Er86, FP89a, GK05, GBL94, HCF95, IEE92a, IEE01, MLP07, Mo92b, OT89, RG89, TWW77, vL94, ACM94a, Ano93a, PGV93c]. **Computer-Recognized** [RJK79]. **Computers** [FHMU85, MK93, PSR90, Rad83, SB93, RFB97, Deb03]. **Computing** [ACM75c, ACM75a, ACM76, ACM77b, ACM84b, ACM85a, ACM86b, ACM88b, ACM89c, ACM90, ACM91e, ACM96, ACM97b, ACM98, ACM01, ACM02, ACM03a, ACM04, ACM07, ACM08b, ACM11, ACM12, Bai81, DT87, IEE94c, KKRJ07, KLT92, LCK11, Ram87, Rei88, Tro95, AFK90, GHK+12, GB17, GC90, LVD+11, MN99, Pri95, Bai81, GT80, Rie89, ACM77a, WGM88]. **Concatenated** [CD84a, DC81, HS08]. **concatenation** [BJKS93, BJKS94]. **Concept** [Kie85, Lum73, Ter87, Ano09b]. **Concepts** [KTMO83b, vL94]. **Conceptual** [FZ87]. **Concise** [PT12b]. **Concomitant** [MWC12]. **Concrete** [GKP89, GKP94]. **Concurrency** [Ell85a, Ell87, Ell88, FK89, GG74, HSM95, Kum89b, Kum89a, LSV89, Moh90, Moh93, OA89, SDK91, GT16, MTB00]. **Concurrent** [AR16, CLP13, Cha88, CHS+18, CHSC18, Ell83, HYH89, HYH93, HY86, HTY90, Kum90, MSD16, MSD19, MSSWP90, Omi88, Omi89a, PBBO12, SDW14, SG88, WCW+22, CCL91, MMC01, MRL+19, Pro18, TMW10]. **Condensation** [CT96]. **Condensers** [ATS19]. **Conditionally** [ACP09]. **Conditions** [IKO05, IH95, Rus92, Rus93, Rus95, BDPV14]. **Conference** [ACM81, ACM85a, ACM91b, PDI91, ACM94c, ACM04, AFI69, ABB93, AFK90, VLD82, Ano89, AW89, AAC+01, AOV+99, AA86, Bai81, BD88, Bar83, BDS88, BV89, BIP92, Bel00, BJZ94, BRW93, BL88, Bor81, Boy95a, Bri92, Bri93, BJ93, CCC89, CGO86, CLM89, Cop95b, DSS84, Far93, FNY92, FMA02, Fra04, Fre90, GMJ90, Gol92, GSW98, HB93, IEE80a, IEE85b, ICD86, ICD87, IEE88a, IEE88d, ICD88, IEE88b, CTC90, ICD90, ICD91, ICD93, IEE94c, IEE95, IEE02, IEE11a, IRM93, JBJ94, Jou85, JY14, Joy03, Ker75, Kna89, KLT92, LC06, Las87, LCK11, Lie81, LS89, LT80, LSC91, Lom93, MK89, MSDS90, Mo92b, Nav85, Oxb86, PV85, PK89, QG95, RRR99, Rie89, RK89, RNT90, Sch82a, ST83a, ST83b, SP90, Sho05, SW94b, SC77, Sti93, Sti94c, Sto92, SM08, SM12, USE91]. **Conference** [USE00a, USE00b, Vau06, Vid90, WPY90, lWSS91, Yan10, Yao78, Yua92, Yun02, ACM94a, ARA94, Ano83, Ano93a, Ano93c, Boy95b, CE95, Cop95a, DG96, DT87, Deb03, HF13, IEE92a, IEE94a, IEE94b, IEE01, Kil05, PSN95, SW94a, TWW77, USE90, Wie99, ??69, ACM75c, ACM76, ACM77b, LFP82, ACM91d, AFI63, YR87]. **Confidence** [DGD02]. **Configurable** [vdBGLGL+16]. **configurations** [CL09a]. **Confinement** [NS16b]. **Confirmation** [MOI90, MOI91]. **Congress** [Gil77, Ros74]. **Conjecture** [KPS92]. **Conjunctive** [Stu85]. **Connected** [OL89, TY91, OT89].

Connection [And88, BM90b, Mic02, KK96, RH92]. **Connections** [LK07]. **Conscious** [Ask05, ZHB06]. **consed** [BJM14]. **consequences** [Woe06a]. **Consideration** [CJP12, CJP15]. **Considerations** [SM02, Wri83, PW06]. **consing** [AG93]. **Consistency** [LWZ+18, SDZ21]. **Consistent** [KLL+97, MVB+21, Nak21, Sun15, ZWY21, KSB+99, LDK12, WL07]. **consonant** [Wan05]. **Constant** [ANS10, BM99, F+03, LP15, Mul85, PP08, PPR09, Sie04, DW05, DW07, FPSS05, GMW90, IKOS08, MV91a, OP03, PPR07, Pro18]. **Constant-Round** [LP15]. **Constant-Time** [Sie04, Pro18]. **constrained** [RAL07]. **Constraints** [BHIMM12, NNA12, Ati20]. **Construct** [CDMP05, Han17, SGY11]. **Constructing** [CS85a, Cha86b, CFYT94, FFPV84, FCH92, HM12, Lis07, RS08, SS80, YD85, SL88, ZHX+21]. **Construction** [ACM79, AN96, BCK96b, BBKN01, EFMRK+20, Eld84, IT93, KR01, Kut10, PV92, SP91, ŠSaS01, Sar10, Sch01a, BGKZ12, BDPV08, CML+13, CL09b, Woe06a]. **Constructions** [AHV98, BBKN12, BRS02, Bla00, DA12, Jou04, SG16, WX01, GPV08, LS06, MvT08, NN90, VZ12, WC07]. **constructive** [CLS18]. **Container** [Hej89]. **Containers** [Ben98, LACJ18]. **containment** [KZ19]. **Content** [GH07, Hin20, Koh80, MHT+13, RSK17, WDP+12, YTJ06, MJ14, TLLL09, XCCK09, ZO13, BB07]. **Content-Addressable** [Hin20, RSK17, Koh80, BB07]. **Content-Based** [YTJ06, MHT+13, MJ14]. **Contention** [CadHS00, DG93, DG94]. **Continuous** [Coh98, PAPV08, GGR04, NW07]. **continuous-discrete** [NW07]. **Control** [BDPSNG97, CBA94, CL83, HLC10, JXY07, Kum89a, Moh90, Moh93, SDK91, XHZ+19, Ano93a, Ano93c, FK89, GJR79, HO72, Kum89b, MTB00, YL04]. **Controlled** [LRLW89, LRLH91, Mul81, WY02, CBA94]. **Controlling** [LK07]. **convened** [Ano83]. **Convention** [ACM91b, Rie89]. **convergence** [LLT21]. **Conversion** [Omi88, Omi89a, Sab94]. **Converting** [MV91a]. **convolution** [OS14]. **Convolutional** [DHT+19, NMQ22, WWG+18]. **Cool** [EMM07]. **cooperation** [JFDF09]. **Cooperative** [XBH06]. **Copenhagen** [BIP92, FS09]. **Copies** [RSSD89b, RSSD90, RSSD92, CWC10]. **coprocessor** [TLLL07]. **Copy** [LH20, MHT+13, YCJ12]. **Coq** [BJM14]. **Core** [Kil01, SvEB84, AKN12, BATÖ13, CZL12, KKL+09, Nae95]. **cores** [BMS+17]. **Corfu** [Rei88]. **Corporation** [Fis87]. **Corps** [RMB11]. **Correct** [SS88b, CE95, CE95]. **Correcting** [BGS96, Har97, FM89, GHK+12, Mil98, MF82]. **Correction** [Bur84, KR79, RJK79, Ven84, Zam80]. **correctness** [AR21, MMC01]. **Correlation** [TGGF10]. **Correlations** [Val15]. **Correspondence** [PH73]. **Corresponding** [AOAAK20]. **Corrigendum** [AA79b]. **Corruption** [DD11, DJSN09]. **Corruption-Localizing** [DJSN09]. **cosmological** [War14]. **Cost** [BM97, BBS90, CJP12, FCHD88, FCHD89, GI12, HMNB07, Kut10, LYW+18, Lyo83, PF88, CZ14, CJP15, VBW94]. **cost/performance** [VBW94]. **Costs** [HR96]. **could** [PES+12]. **Counter** [GRBCC19, LMP+08, MKASJ18, NS16b, Bac02]. **Counter-Terrorism** [GRBCC19]. **Countermeasure** [LAKW07, MMMT09]. **Counters** [WLWZ19]. **Counting** [Fla83b, FM85, McK89a, WVT90, DLM07, EVF06, McK89b, RKK14]. **coupled** [HLH13]. **course** [PGV93c]. **Couvrants** [Kar82]. **Coverage** [IJK13]. **covering** [CLS18, Rad92]. **CoveringLSH** [Pag18]. **CPHASH** [MZK12]. **CPHR** [WBWV16]. **CPU** [HLH13, QXL+20]. **CPU-FPGA**

[QXL+20]. **CPUs** [KKL+09]. **CR** [LACJ18]. **Cracking** [GAS+16]. **CRAY** [DS97]. **creating** [Sag85b]. **creation** [FVS12]. **Credential** [YLSZ19]. **credit** [JFDF09]. **credit-based** [JFDF09]. **Crete** [ACM01]. **Criss** [GRZ93]. **Criss-Cross** [GRZ93]. **Criteria** [Adi88, AII89]. **Criterion** [Sun15]. **critical** [NM10]. **Cross** [CJN20, GRZ93, LWZ+18, MLHK17, WB90, ZWY21, QZD+18]. **Cross-Media** [LWZ+18]. **Cross-Modal** [MLHK17, CJN20, ZWY21]. **cross-platform** [QZD+18]. **Cryptanalysis** [Aum09, BS91a, Bih08, BCJ15, BHT98, BP09, DGV93, Dae95, GO07, GIMS11, HPC02, JNPP14, Knu92, LP16, LKY04, MR07, Mon19, NXB13, GLM+10, SPLHCB14, SV94b, Wag00, WSSO12, WYW14, AP11, BS91b, BS91c, BHT97, CV05, RP95, SV95]. **Cryptanalytic** [CJMS19]. **CRYPTO** [Bel00, Bra90, Bri92, Bri93, CRS83a, Cop95b, Fei91, Fra04, MV91c, Sho05, Sti93, Sti94c, Wie99, Yun02, Hil05, CP91c]. **Crypto'91** [DBGV93]. **Cryptoanalysis** [HSIR02]. **Cryptographer** [Joy03]. **Cryptographic** [ARH+18, BDPSNG97, BCR04, BDP11, BDP97, Bur06, jCPB+12, CLG09, CP87, CP88, DA12, DC98b, Dam90a, Dam91, DDF+07, Dav91, DY90, DY91, GO07, Hel94, MKAA17, PTT16, Pre93, PGV93d, Pre94b, PBD97, Pre99, Pre94c, QV89, QV90, QG95, RRS06, Rja12, RS08, Rue93, SS01, Sch91b, Sch93a, SZ93, SGY11, Sti06, TSP+11, Vau06, AY14, ABO+17, BNN+10, BD92, BOY11, CP13, De 95, ESRI14, GPV08, GS94, GQ95, IN89, KR19, KTDB20, Mic02, NY89b, NY89a, RAL07, Sch93b, Sch93c, YZ16]. **Cryptographically** [PGV92, Aam03]. **Cryptography** [ANS97, ANS05, ÁCZ16, AG18, BD08, DK02, DK15, IKOS08, She17, Wol93b, Ytr06, BGG94, BBD09b, Far93, GNP05, JY14, KL15, Kil05, PGV93c, Wol93a, Boy95a, Boy95b, DG96]. **Cryptology** [Bri92, Bri93, CRS83a, CP87, Dam90a, Dav91, Fei91, Fra04, Hel94, IRM93, LC06, MV91c, QV89, Rue93, SP90, SZ93, Sti93, Sti94c, Vau06, Bel00, Bra90, CP88, Cop95a, Cop95b, Dam91, De 95, GQ95, Joy03, PSN95, QV90, QG95, Sho05, Wie99, Yun02]. **Cryptosystem** [Jun87, KKT91]. **Cryptosystems** [Oka88, Wee11]. **CS2** [NM02b]. **CT** [Joy03]. **CT-RSA** [Joy03]. **Cube** [OL89, TY91, OT89]. **cube-connected** [OT89]. **CubeHash** [AD11, BP09, BKMP09, KKMS10]. **Cuckoo** [ANS09, ANS10, ADW12, ADW14, BHKN13, BHKN19, DM03, DS09c, DMR11, FPS13, FMM09, FMM11, KMW08, KMW10, Kut10, Mit09, NSW08, PR01, PR04, Pag06, PRM16, PS12, SHF+17, TK07, DS09b, KM07, Kut06, DK12]. **Cumulative** [LPWW06]. **CUPID** [KS89a]. **Curve** [ANS05, MSTA17, OOB12, TK17]. **Curves** [BGH12, FT12, She17, WX01, BGH+13, BP18, CDS20, FSV09, FFS+13, Far14, GZ99, LS06]. **Cyber** [LSZ+21]. **Cyber-physical** [LSZ+21]. **Cycle** [MJBD11]. **Cyclic** [DH84]. **Cycling** [Saa12]. **cyphers** [Far93]. **Czechoslovakia** [Rov90].

D [CBA94, EAA+16, Fly92, GG92, GK94, LMJC07, LDY+16, PPS21, SYW+20, WSSO12]. **D-Based** [WSSO12]. **d'Acces** [Lit77b, Kar82, Lit77a]. **d'Adressage** [Lit79a]. **Dallas** [ACM98, IEE95, USE91]. **Damgård** [DGV93, Pat95, CDMP05, Gib90, Mir01]. **Dana** [Ano10]. **Darmstadt** [TWW77]. **Darstellung** [Koe72]. **Dartmouth** [Ano93d]. **Dash** [LHWL20]. **Data** [ACM81, ACM82, ABB93, AHU83, ABM06, ADOAH19, AHS92, VLD82, Ano85a, Ano89, AW89, AAC+01, ANT85, ADF12, BC08, BD88, BDS88, BJL16, BCH87, BJZ94, BFR87, BL88, Boy98, BJM14, BJ93, CLS12,

CGLC20, CJC+09, Chr84, CGO86, CLM89, DA12, DSS84, DT87, DSZ07a, DSZ07b, DP08, Dre17b, EjKMP80, Eld84, Ell83, Ell85b, Ell82, Fel88, FM85, Flo77, FB87, FBY92, FMA02, GMJ90, Gho77, Gho86, GCMG15, Gol92, Gon83, Gon84, GBY91, Gre21, Gri74, Har71b, Har73, HWZP18, Hel91, Hil78b, Hil78a, HZ86, Hil88, HS84, IEE85b, ICD86, ICD87, ICD88, ICD90, ICD91, ICD93, IH83, IABV15, JL14, Ker75, KP81, KS12, Kru84, KHH89, LC20, Lie81, LT85, LRY78, LRY80, Lit89, Lit84, LL87, LS89, LRY+15, LT80, LSC91, Lom93, LG78, LMR02, MLHK17, Mar75]. **Data** [Mar77, McC79, MSDS90, MEK+14, Nav85, NR12, PSSC17, PRRR15, PV85, PW94, RNR13, Rou09, RK91, Sar10, Sch01a, SDW14, ST83a, ST83b, SW86, SW94b, Ste82, Sto92, SM08, SM12, SW87, SWTX18, TKH20, Tan83, TC93, TY03, TA81, TA86, TGGF10, TS85, TGL+97, Top92, Toy86, TS76, TS84, VL87, Wal88, WPKK94, WZY+18, WCW+22, WS76, WH83, Win90a, Wir86, WDYT91, WYT93, Wu85, YDT83, YSW+11, YGS+19, YLB90, Yua92, Zam80, ZLLD18, ZO93, AK09, BR75, BZZ12, BVF12, BCGS16, BGG12, BPT10, BMLLC+19, CXLK19, CLW98, CRS83b, Col93, CH09, DMB19, FP89a, FVS12, GB17, Ged14, GP08, HC11, HF91, HSMB91, HF13, IGA05, IL90, JDW+19, Kak83, Kan91, Kan93, KRJ09a, Koe72, LNS96, MSK96, MV08, NT01, NM02b, OS88, PL21, SLC+07]. **data** [SB07, She06, Shi17, SE89, SW94a, SA17, TKT+89, VL97, Vit01, WM93, WTZ+13, Wil78, Wil85a, Yao78, YLC+09, Yu92, YG10, ZKR08, ZLL+07, ACM75b, GJM02, ICD87, IEE94a, MO92a, Vit01]. **Data-base** [Mar75, Mar77]. **data-centric** [AK09]. **data-driven** [TKT+89]. **data-independent** [BCGS16]. **data-intensive** [Shi17]. **Data-Parallel** [LC20]. **Data-stream** [Tan83]. **Data-structures** [Har73]. **Data/Knowledge** [BCH87]. **databanks** [FDL86]. **Database** [ACM82, ACM83a, ACM83b, ACM85b, ACM86a, ACM88a, ACM89b, ACM89a, AA86, Bab79, BG92, DCW91, DKO+84b, DKO+84c, DKO84a, DGG+86, DGS+90b, DGS+90a, DNV81, DT91b, GD87, GHJ+93, Van10, Han90, HCKW90, He87, Hsi83, HF13, IH83, KGJG12, Kie85, Kim80, KL87, KTMo83a, KO90, Kue84b, Kum89a, LC86a, LL08, Llo81, Ouk83, SD89b, Sch90b, SD90b, SD90a, Sha86, She91, SDK91, Sto88, Tan83, Toy86, Ull82, WVT90, Wie83, Wie87a, Yam85, YNKM89, ZJM94b, AS89, AKN12, DKO+84d, EH17, EBD91, FNY92, GC90, HF91, ISH+91, JBJ94, MBK00, PS08, SSW94, SK88, SE89, SP89, TL93, Vak85, WC94, ZJM94a, ZJM94c, ODB89, BF89, KKP92]. **Databases** [AS82, AOV+99, Bal96, Bal05, BDPSNG97, BG80, Bat81, BG82, BS94a, CCH09, Chu90, Chu91, DDF+07, DT91a, DT91b, FM91, FHCD92a, GY91, Gra92, Gra93c, GC95, GSW98, Heu87, HCY97, Kaw15, KR91, LOY00, LDM92, LÖON01, Oxb86, RZ90, RNT90, Sch82a, SPW90, SW91, TRN86, Toy93, ZHW21, AÖD19, AP92, BW89, FHCD92b, HC07, ISO97, KR88, MSZ+20, MIGA18, SB95, SB97, SI09, ZLC+18]. **Dataflow** [DGG+86, Ger86a, Ger86b, Gra94c]. **Datalog** [GST90]. **Datasets** [OGAB14, WZY+18, BZL+15, HAKM15, LRU14, Mil95]. **datastructure** [Büt86]. **Dateiorganisation** [Nie75, Wie89]. **Dateistrukturen** [Fri86]. **Datenbanken** [Lut88, Nee79, Stu82, Wie89]. **Datenbankmaschine** [Pet83]. **Datenbanksystemen** [Kue83, Kue84a]. **Datenorganisationen** [Oll89]. **Datenstrukturen** [DF77, LS85, Meh86, Nol82b, Oll89, Wir75, Wir83, OK80, Koe72]. **Datenverarbeitung** [Lut88]. **Dawning** [Cro98]. **Dayton** [IEE94b]. **DB2** [BFG+95].

DBJ [ZJM94a, ZJM94b, ZJM94c]. **DBMS** [Gra86, KR86b, KR86a, KP81]. **DC** [ACM84b, BJ93, Fis87]. **DCC** [SM08, SM12]. **DCT** [TLZL16, TCY+20]. **DDH** [Dev93]. **de-amortize** [KM07]. **De-amortized** [ANS09]. **De-duplication** [BC08]. **Dealing** [Bre91, Vit01]. **death** [For09]. **Deauville** [BF89]. **December** [PDI91, And94, AiNOW11, Boy95a, Boy95b, Far93, HL91, IEE88b, LC06, RRR99, SZ93, Yan10]. **Decentralized** [HNKO20, LB07]. **Decision** [Eng94, CKKW00, QP16]. **decision-trees** [QP16]. **Declustering** [FM89]. **Decomposition** [NS16a, Spe92]. **Decompositions** [GO15]. **Decoupled** [RKLC+11]. **Decoy** [MIGA18]. **decryption** [GBL94]. **Dedicated** [HKY12, ISO97, ISO04, NM02a, Pre94a]. **deduction** [PL21]. **Deductive** [Llo81, TRN86, SSW94]. **Deduplication** [PL21, ZHZ+19, BVF12]. **Deep** [CLYY92, CLYY95, CDW+19, DHT+19, LLT21, SHZ+20, ZZLZ18, WWG+18, XZPG21]. **defective** [Hui90]. **Deferred** [Gri77, Vek85]. **Defined** [YD84]. **definition** [FNY92]. **Definitions** [DCW91]. **Deflate** [NMQ22]. **Deflate-inflate** [NMQ22]. **del** [ACM82]. **Delay** [NDMR08]. **Deletion** [AHS92, CV86, GG80, IG77, KV91, MV88, TW91, VV86, Vit81b, Vit82a, MSV87]. **Deletions** [CF92, Knu77, PV19, KHK12]. **denial** [Bac02]. **Denmark** [BIP92, Dam90a, Dam91, FS09, NS82]. **density** [KD92]. **Denver** [ACM79, ACM85a]. **Dependencies** [CS83a]. **Dependency** [SGK09]. **Dependent** [DTS75, Sch01a, SDT75, NMS+08]. **depth** [GHK+12]. **Derandomization** [AN96]. **Derived** [HB89a, HB92, HB89b]. **Descent** [DM81]. **Description** [FC87a]. **Descriptor** [FLF11]. **Descriptors** [BRM+09, MBBS12, RLT83, SD85, Wu84]. **Design** [Adi88, AS82, AR16, Bat80, BMQ98, Bur84, CKB83b, CS83a, CS85c, CS85b, CS86, CCJ91, Che84a, Che84b, CCHK08, DGV93, Dae95, Dam90b, Dam93, DLT98, DY90, DY91, DHK+15, DNV81, DS09a, Dev93, DM90, Die07, DT91b, EE86, GDA10, GSI+82, GT93, Gro86, Jag91, JP07, KTMO83b, Kru84, LT09, LCLX19, LŁA15, OVY94b, PS93, PGV90b, Pre93, Pre94a, QM98, QXL+20, Rad83, RLM87, SD89b, Ull70, VC87, Wie83, Wie87a, XNS+13, YNKM89, AR21, Bur82, CE95, CKB81, CKB83a, CCL91, CZ14, Dam94, DMB19, Lai92, MSZ+20, MAK+12, Mol90a, Mol90b, OVY94a, PGV93g]. **Designing** [GM91, Lin96, Mor83a, Zhe90, DC94, MPL09]. **Designs** [Bat82, BR14, Bur75b, CC88a]. **Desirable** [LCL+20]. **Destaging** [NKT88]. **Detect** [WLWZ19]. **Detecting** [GAS+16, OTKH11, CWC10, MF82]. **Detection** [ADOAH19, CH12, CJC+09, Kue84b, LQZH14, LLDZ18, LH20, LCL+20, MKAA17, MKASJ18, PACT09, TWZW11, TP15, Zam80, ZC77, FNP09, FES09, GDGK20, Kos14, LG13, MHT+13, NADY20, PL21, YCJ12, ZLY+13]. **determination** [Kri89]. **Determine** [ZF06]. **Determining** [Bee83, Mar71]. **Deterministic** [HMP01, MNS07, TLLL07, BK07a, FFS+13, HXLX13, Mil98, Ruž08]. **Deutsche** [BN85]. **Develop** [TC93]. **Development** [BV89, BIP92, CN07, Hil88, McI82, SSS05, Vid90, Web72, YR87]. **Developments** [Ano95a, KR19, Lar85a]. **Devices** [KHK15, Sam81, YY07, Cho21]. **DFG** [MO92a]. **DHA** [AKY13]. **DHA-256** [AKY13]. **DHT** [HNKO20, RCF11, SX08, UPV11]. **DHT-Based** [HNKO20]. **DHTs** [CQW08]. **Diagonal** [PVM94]. **diagonalization** [Lia95]. **Diamond** [YGS+19]. **diced** [Nic17]. **Dichotomy** [HW08]. **Dicing** [Kon10]. **dictionaries** [DMPP06, DW05, DW07, GJM02, HMP01, MSK96, MN90, Mil98, RRS07, Ruž08, Wen92]. **dictionariis** [DMPP06]. **Dictionary** [CS82, DA93,

Dod82, Dos78b, McK89a, Rad83, Die90, DHW08, McK89b, Rön07, Sun91, Sun93]. **Diego** [ACM03a, ACM07, Ano10, Sto92]. **Differences** [Gri98]. **Different** [LH03b, BW89, Jan05, KS88a]. **Differentiability** [DRS12]. **Differential** [AS82, BS91b, BS91a, BS91c, CH94, Dae95, KKMS10, MMMT09, AGJA06, ITP14, RP95]. **difficulty** [SKD15, SL88]. **Diffusion** [SDMS12, SDMS15]. **Digest** [IEE88a]. **Digital** [ANS05, BDS09, Cai84, Cip93, Fox91, GK12a, GT63, LM95, Mek83, Oka88, Oto85a, PW93, PGV93f, Reg81, Rou09, Rul93, Ano09a, Ano13]. **Digram** [Wil79]. **DIMACS** [GJM02]. **Dimension** [CT96, LHC05]. **Dimensional** [AEP18, HYH89, KSSS86, Leb87, LOY00, MNY81, Ngu06, ML15, RAD15, SWQ+14, TYSK10, XMLC11, Yuv75]. **Dimensioning** [BP97]. **Dimensions** [AI06, GIM99, YWH09, AI08]. **Direct** [DS84b, Kno84, RB91, VC85, Bay73b, KdlT89, Mad80, TT81]. **direct-access** [Bay73b]. **Direct-chaining** [Kno84]. **Directories** [YY01]. **Directory** [Gri74, KS88b, KS88c, Oto84, Oto88a, PADHY93, AP93, Pro94, THS97]. **Dirty** [MZD+18]. **Disc** [CC87, CLC92, CF89b]. **Discovery** [LKI10, PKW09, ZO13]. **discredits** [Ano09b]. **Discrete** [ACM94d, SDA90, SDA91, ACM97a, ACM05, ACM08a, Gib91, Kar98, Li15, MLHK17, Mat09, SSL+18, Shm00, vW94, NW07]. **Discretionary** [BDPSNG97]. **Discretized** [RNR13]. **Discriminant** [SY08]. **discrimination** [CP95a]. **Discriminative** [OSR10, HXLX13]. **Discs** [CF89a, CF89b]. **discussed** [Gre95]. **Discussion** [BBR88]. **DISH** [SKC07]. **disjoint** [AAB+92]. **Disk** [BGF88, Cha88, Du86, Gra94a, ML95, TC93, WB03, Kor08, Wil14]. **disk-based** [Kor08, Wil14]. **Disk-tape** [ML95]. **Disks** [CC91, Vit85, CCL91]. **Disorder** [LL86, Lom88, RM88, TB91]. **Displace** [BBD09a, Pag99]. **Displacement** [Pet13, FWG18]. **Displacements** [Jan08, Jan05, Vio05]. **display** [Sab94]. **displaying** [Koe72]. **Dissemination** [RHM09, RCF11]. **Distance** [Bra84a, Bra85, Bra86, LH20, NNA12, Zha19a, LP04, MYS12, ZDI+15]. **Distances** [Bal96]. **Distinguisher** [Sch11]. **Distinguishers** [LJF19, SY11, AP11]. **Distinguishing** [HSR+01]. **Distortion** [CKPT19]. **distribute** [Die90]. **Distributed** [PDI91, APV07, Ano10, BMS+17, CCF04, DPH08, Dev93, EFMRK+20, Ell83, Ell85b, GGY+19, GYW+19, GSB94, adH93, HC13, HLC10, IK92, JXY07, KLadH93, KLM96, LK07, LMSM09, LC96, LB07, LACJ18, LMR02, ML86, MS02, MPP14, MT11, Mey93, MK12, NTW09, PRRR15, PAPV08, PF85, RHM09, RMB11, SPW90, SW91, SDK91, SM02, SPB88, Spe92, SWTX18, TT10, TP95, TCP+17, VBW94, Wil03, YLZ20, BVF12, BPT10, CCY91, DL06, DAC+13, HKW05, ISO97, KKP+17, KLL+97, Kha95, Kou93, LMSM12, LVD+11, LNS93, LNS96, MLP07, MPL09, MA15, SP89, WZ12, WTN07, WTN09, XLZC14, ZGG05, ZLL+07, ZO13]. **Distributing** [CDH19, KW94]. **Distribution** [AT93, BBS90, CM01, DTS75, EAA+16, JCK+18, LMC07, PK87, RR92, Sch01b, SDT75, WZY+18, AT90, GBL94, Vio05, XCCK09]. **Distribution-Dependent** [DTS75, SDT75]. **Distribution-Independent** [DTS75]. **Distributions** [KS86, KS87a, KS87b, KS89b, RTK12]. **Distributive** [NP91]. **Disturbance** [WLWZ19]. **Dither** [AP08]. **DITTO** [SB07]. **Diverses** [LG78]. **Divisible** [FL04]. **Division** [Eck74a, GL73, Gra88, Gra89]. **DLIN** [CK12]. **DM** [KL95]. **Do** [Bur06, HSR+01, HR04]. **Document** [ANT85, DGM89, LR96a, Wil79, KRML09]. **Documentation** [DM90]. **Documents** [WWZ09, WMB94, WMB99, ZWCL10,

WLLG08]. **Domain** [BR06, Cor00, Cor02, DOP05, KK12, KK18, LT12, LLG12, PG95, RS12, SGY11, SPSP16, ZNPM16]. **Donald** [Ruc15]. **Donnees** [Kar82, LG78]. **Don't** [BFCJ+12, YT16, BCR10]. **Dortmund** [Lut88]. **Double** [Boo72, Bur05, CdM90, GS76, GS78, KLP98, LK94, LM93c, MB03, Men12, OOB17, Pal92, Tho13, Yao85a, KL95, LM88, LLJ15, Men17, Mol90a, Mol90b]. **Double-Linked** [Pal92]. **Down** [LRY+15, PT11b, ZLC+12]. **DPA** [LRY+15]. **Draft** [MCF17]. **DRAM** [CJKK19, KHK15, WLWZ19]. **DRAMCache** [PG17]. **drive** [BC06]. **Driven** [Gra93b, Ven86, TKT+89, ZO13]. **DSS** [Ano09a, Ano13]. **Dual** [CDW+19, MNS12, Wee12, BR75, MJ08]. **Dual-Stream** [MNS12]. **Dublin** [ABB93]. **Dumping** [Fro81]. **d'une** [LG78]. **Duplicate** [LKI10, LQZH14, MD97, TW91]. **Duplicates** [Bre91]. **duplication** [BC08, PL21]. **durch** [Hil82]. **DWT** [THY+18]. **Dynamic** [AL86, AHS92, BGDW95, CS91, CR89, CBA94, DGGL16, Dev93, DKM+88, DadH90, DKM+91, DKM+94, ED88, FNPS79, FHL+19, FS82, GT93, adH90, Kaw85, Kie85, KNT89, Kou93, KS86, KS87a, KS87b, KSC11, KSC12, Lar78, Lar88a, Lar88b, LC88, LRY+15, LHWL21, MSW19, MS12, MS02, Mul84a, Mul84b, Mul85, NKT88, OG94a, Ore83, Oto85b, Ouk83, OS83a, OS83b, PLKS07, PG95, RZ90, RT89, RL82, RSSD89a, Reg81, Rob86, Ros21, Sch79b, Sch81, SSS05, TT10, Vek85, Wan14, YD84, YLSZ19, YBQZ17, YD86a, YD86b, ZRT91, ZJM94a, ZJM94b, ZJM94c, ZO93, CS93a, DTM+18, DMPP06, DHW08, FRS94, FF90, Fro81, HKLS12, HR93, KD92, Lev89, Lin96, Mil98, YG10, SKC07]. **Dynamically** [Lit78, Litxxb]. **dynamicis** [DMPP06]. **Dynamiques** [Kar82]. **Dynamischen** [DS84a]. **Dynamischer** [Hil82].

E-HASH [HGH+12]. **early** [CV83a, CKKW00, PY88]. **early-insertion** [CV83a, PY88]. **Easier** [Bor81, Eug90]. **Easily** [CMW83]. **Eat** [CHSC18]. **ECDSA** [ANS05]. **ECHO** [BOY11, Sch11]. **ECHO-256** [Sch11]. **ECIES** [KAS+22]. **EDBT** [JBJ94]. **Edge** [XHZ+19, NMQ22, QZD+18]. **Edge-Based** [XHZ+19]. **Edinburgh** [AOV+99]. **Edit** [NNA12, TK88]. **editing** [Koe72]. **Edition** [BFG+95]. **Editor** [BMB68, Fox91]. **Editors** [RW97]. **Education** [LC86b]. **Effect** [KNT89, Mac95, Mai92]. **Effective** [FCHD88, FCHD89, HW08, PCY95, WDYT91, MA15]. **effects** [QM98]. **Efficiency** [DB12, Leb87, PVCQ08, Ull72, AR21, KST99, PT10b, WLC20]. **Efficient** [AD08, ASWD18, ASBdS16, ASW07, Ast80, AEMR09, ADW12, ADW14, BR14, BCS09, BÖS11, BPZ07, CFP19, CKB85, CLS12, DDF+07, DD15, DGM89, FES09, F+03, FRS94, GGY+19, GM79, Gon83, GRZ93, Gri77, HT01, HM12, HDCM09, HHL10, HLC10, IN89, JDW+19, JD12, KU88, KR81, KLadH93, KLM96, KKRJ07, KJC11, KS12, KS86, KS87a, KS87b, KS89b, Kue84b, HGH+12, LW88, LCLX19, LWG11, LXL+19, LH20, MZD+18, MSW19, MP16, MJBD11, MEK+14, MH00, MO92a, MKASJ18, MJT+02, Mul85, NN90, OOK+10, Pag99, PAKR93, PAPV08, Pan05, PL21, Qui83, RT81, RFB97, Rém92, Ros06, Ros07, Sac86, SDMS15, Sch91b, Sch93a, SL16, SGY11, SS88b, SvEB84, SPSP16, SKM01, TY03, TYZO15, TYSK10, TW07, TS85, TGL+97, Tsa08, VL87, Vit85, WYY05d, WWZ09, Woe06b, XZPG21, XHZ+19, YSW+11]. **Efficient** [YBQZ18, YGC+12, ZWY21, BLP+14, BZL+15, BT93, CML+13, CZ14, CLW98, DS09a, FNP09, FPSS05, Gai82, HKL04, HCJC06, adHMR93, IIL17, KU86, Lin96, LCH+14, LŁA15, MSZ+20, MSK96, NADY20, NTW09, OCDG11, PCK95, PBBO12, PSS09, RCF11, SSW94, Sch93b,

Sch93c, SX08, Shi17, SV15a, UHT95, VL97, Wie86, WTN09, XLZC14, ZWT+14, ZHX+21, SV18]. **Efficiently** [AP08, Kim99]. **Effiziente** [Meh77, Meh86]. **eigenvalue** [JWM+18]. **Eight** [Van10]. **Eighteenth** [ACM86b, ACM91d, ACM91a]. **Eighth** [ACM76, ACM89b, ACM89a, ACM97a, VLD82, ACM96, Gol92]. **Einfuehrung** [Nol82b]. **Einschrittcompilers** [Dit76]. **Elastic** [Hac93]. **Elections** [EH12]. **Electronic** [Cip93]. **electronics** [IEE94b]. **elements** [IG94]. **elephant** [WLC20]. **Eleventh** [ACM87, IEE92a]. **ELFs** [Zha19b]. **Eliminate** [BT94a, BT94b]. **Eliminating** [Bel70, Bel72, Bel83, NH74]. **elision** [NM10]. **Elliptic** [BGH12, Gri98, MSTA17, OOB12, She17, BGH+13, FSV09, FFS+13, TK17, ANS05]. **Embedded** [SVCC01, vMG12, Hui90, TLLL07, TLLL09, UIY10]. **Embedding** [CLP17]. **Embeddings** [AEP18]. **EMD** [BR06]. **Emde** [Wil00]. **Emergence** [Fox91]. **Empirical** [DMP09]. **Employing** [Per73]. **Emulated** [EK93]. **Emulations** [Kel93, Kel96]. **en-route** [YG10]. **Enabled** [Alb21, BZZ12]. **Enabling** [GYW+19, HDCM09, LCLX19, SMZ18, TT10, SLC+07]. **Encapsulation** [HM12]. **Enciphering** [MKASJ18]. **Encipherment** [BM76]. **Encoding** [Ano95c, KP94, Wil79, CVR14, RRS07]. **Encodings** [BHIMM12]. **Encrypted** [GYW+19, HWZP18, Kaw15]. **Encryption** [AG18, CS02, DC98a, Kal93, NTY12, PPS21, PRZ99, Sar10, ZZM17, ZHZ+19, And94, BR94, Bir07, Gol96, GBL94, Sab94, ZCZQ19]. **Energy** [AS16, KYS05, HGH+12, YSW+11, CZ14]. **Energy-Efficient** [HGH+12]. **Energy-Harvesting** [AS16]. **Engine** [YNKM89, BC06, NM02b, PES+12, SSW94]. **Engineer** [Jac92]. **Engineering** [Gol92, Got83, ICD86, ICD87, ICD88, ICD90, ICD91, ICD93, Lew82, Wal88, ARA94, Ano93c, IEE94a, Yu92, Ano89]. **England** [ACM94b, Pat90]. **English** [CS82, Dit76, Wan05]. **Enhance** [Lit84, CZ14]. **Enhanced** [KAS+22, RS12, ZHW21, LG96]. **Enhancement** [HMNB07, SK20]. **Enhancements** [Gra93a]. **enhancing** [AGBR19]. **EnRUPT** [IP11]. **ensemble** [ZNPM16]. **Ensure** [Sch01a]. **Enterprise** [Rei03, FES09]. **Enterprises** [KCR11]. **entire** [FDL86, Nic17]. **entity** [ZLC+18]. **Entropy** [Ari94, ATS19, HHR+10, KM88b, NRW90, CKKK09, MV08]. **Entry** [YLB90]. **Environment** [DGM89, MLD94, MLxx, MS88a, RS92, RL74, SD89c, SD89a, SSS05, ZG90b, Kha95, QZD+18, SD89d, TMB02]. **Environments** [ZG90a, GDA10, RCF11]. **EOS** [BP94]. **EPGAs** [YTHC97]. **Equality** [TD93, WC81, AD08, GRF11, ZCZQ19]. **equalization** [PCK95, UHT95]. **Equations** [Aum09]. **Equijoin** [SW91]. **Equiprobable** [PB80]. **Equivalence** [Mar71, de 69]. **eraser**^{TM} [AAGG16]. **Erasure** [KGJØ18]. **Ergife** [IEE88d]. **Erlang** [TCP+17]. **Erratum** [FW77]. **Error** [BGS96, Har97, Kue84b, Mil98, MKASJ18, RJK79, WLWZ19, FM89, GHK+12, Rön07]. **Error-Correcting** [BGS96, GHK+12]. **Error-Correction** [RJK79]. **Errors** [Blo70, Zam80, MF82]. **ErsatzPasswords** [GAS+16]. **ESA** [EF12, FS09, HM08]. **ESAT** [PGV93c]. **essays** [BC39]. **Establishment** [DL12]. **estimate** [Rön07]. **estimated** [Nic17]. **Estimating** [Leb87, MBKS07]. **Estimation** [GLLL17, IJK13, TGGF10, TZ12, HKL04, LNS11, LDK12, NTW09]. **estimators** [HYKS08]. **eTCR** [HKKK13, RWSN07]. **Ethernet** [KCR11]. **Etude** [Mek83, LG78]. **Euclidean** [SWQ+14]. **Euler** [Cha84b]. **EUROCRYPT** [CP87, CP88, Dam90a, Dam91, Dav91, De 95, GQ95, Hel94, QV89, QV90, QG95, Rue93, Vau06]. **Europe** [BRW93]. **European** [EF12, FS09, HM08].

EUROSAM [Ng79]. **Evaluating** [HAKM15, MPP14, RS92]. **Evaluation** [Adi88, BGDW95, CRSW11, CRSW13, Chr84, Fla81, Fla83a, Gra93b, Gra93c, Gri77, HNS84, KTN92, LCLX19, LLL09, MXL+12, ML86, MLxx, MS88a, NMX19, Pag99, SD89c, SD89a, SC90b, SC90a, SC90c, Stu85, TNKT92, Web72, Woo89, YNKM89, CHS+18, GDA10, HCW+21, RLM87, SD89d, TMB02]. **Eve** [AAE+14]. **Even** [Bosxx, Tho00]. **Event** [McK89a, McK89b, ZLY+13]. **Every** [Kil01]. **Everything** [KTN92, MLD94, TNKT92]. **evolution** [PGV93c]. **Evolutionary** [DLT98]. **Exact** [Cor00, Ram88a, Vio05, Lia95]. **Examining** [Wil00]. **Example** [FHMU85]. **Exceed** [Pal92]. **Except** [OWZ14]. **Exchange** [KV09, BSNP96b, GL06, LW04]. **Exclusive** [DLN+18]. **executable** [NADY20]. **Execution** [CLYY92, CHY93, CHY97, Cra85, GHJ+93, GM98, Hea72, HCY94, HCY97, KL87, PAKR93, SS88b, Wu85, GMP95]. **exhaustive** [KJS17]. **Exhibit** [Gui75, Gui78, Gui76c]. **existence** [WC07, Woe06a]. **Existing** [LYD71, LY72]. **Expandable** [Kno71]. **Expander** [CLG09]. **Expanders** [BK07b, Tho13]. **expanding** [FNY92]. **Expansible** [CL95]. **Expansion** [ÁVZ11, Gri77, Mai92]. **Expansions** [Lar80b, Lar80c, Lar82b, Lar82c, Lar82d, Larxx, RSSD89a]. **expansive** [LS96]. **Expectation** [GM91]. **Expected** [Gon81, Lar81, Lar82a]. **Experimental** [ANS09, HCW+21, JHL+15]. **Experiments** [KL96, Wil79]. **expert** [ARA94]. **Explicit** [ADW12, ADW14, Bla00, CL83, LS06, MvT08, WX01, GJR79]. **exploit** [AZ10]. **exploitation** [MAK+12]. **Exploiting** [Bre91, CKKW00, GHW07, HL12, MSS96, MV08, NMQ22, HAK+16]. **Exploration** [CH94, PSSC17]. **Explore** [SP21]. **Exploring** [LVD+11]. **Exponent** [Ano95a]. **Exponential** [DS84a, HJ96, Lom83, LLT21, LH04, SHA97]. **Exponentiation** [Kak83]. **Exposure** [CTZD11]. **Expression** [BBP88, CKW09, Gri77, GGR04]. **Expressions** [Hol87, Mar71]. **Extendable** [NIS15]. **Extendable-Output** [NIS15]. **Extended** [DP08, HBG+17, Ter87, YNKM89, YD84, YTHC97]. **Extenders** [RS12]. **Extendible** [BK84, Bry84, Chu91, Chu92, DT91a, DT91b, Ell83, Ell88, FNPS79, Fla81, Fla83a, Hac93, HSM95, HYH89, HY86, KR86b, KR86a, Kum89a, LÖON01, Men82, MH00, Oto84, Oto86, Oto88a, RLH91, RS77, Tam81, Tam82, Yao80, Hua85, Kum89b, MKSiA98, RLH90, RS75, Wee88]. **Extending** [CMP07, JBJ94, SS01, WKBA07]. **Extensible** [BG92, Gra94c, Hel89, Kum90, Rém92, KR88, SS06, BP94]. **Extension** [BR06, CDW+19, Lit77a, LLG12, PSZ18, SGY11, WH83, Bak09, SFA+19]. **Extensions** [CSSP15, Heu87]. **External** [AS89, AGMT11, GL82, GL88, Gra94a, GT63, JP08, LR85, LRY78, LRY80, Vit01, Woe06b, RT89, RB91]. **External-Memory** [AGMT11]. **Extractable** [ACP09, CZLC12b, CZLC14, Wee11]. **Extracting** [HZ86]. **Extraction** [FC87b, KKN12, LLDZ18, LDY+16, ZLY+12]. **Extremely** [Sie04].

FA [CKW09]. **Face** [KGJG12]. **Fachgesprach** [Lut88]. **Facility** [VL87, FF90, VL97]. **Factor** [CFP19]. **Factoring** [CTZD11]. **Factorization** [FS82, ZWY21]. **Failure** [Ano95a]. **Fairfax** [ACM94a, WGM88]. **Fake** [Ano96, LAKW07]. **Fall** [AFI69]. **Fallen** [HCPLSB12]. **Falls** [AFK90]. **False** [Pag18, CVR14]. **Families** [ADW12, ADW14, BW98, Bla00, CRSW11, CRSW13, FK84, HHL10, SG16, WX01, AG10, BJ07,

BvT13, BJKS93, BJKS94, CRS83b, CL09a, CL09b, CLS18, CDH19, FH15, GW94, LS06, LC13, MvT08, WC07, Woe06a, vT14]. **Family** [BDM+12, BKST18, FLS+10, GK08, Ind01, IT93, MWCH92, MWHC96, SK05, ACP10, AMP12, BDPV12, FPS17, KRT07, Sar13, SRRL98]. **Fast** [AKS78, AP92, AB12, BH91, BRM+09, BS97, BS94b, BS94a, BGV96, BT12b, CH12, CS85a, CCW+17, CWC10, CD84b, CRR18, CS82, CKN18, DC98a, Dit91, EFMRK+20, EPR99, FNPS79, FFGL09, FKI+21, GM91, GM94, GM98, GC95, GK94, GK95, GO15, Gui89, HK95, HKLS12, HW08, HXLX13, KG95, Kel96, KP97, KLP98, KR79, KR01, KRML09, LQZH14, LM95, LK14, LR99, LZ06, Lit91, LL87, LCL+20, Mad80, MSD19, NR12, Nyb96, OS14, PPS21, Pea90, Pea91, PQ98, PQ99, PKSB18, PV95, Rey14, Rog95, Rog99, Rog19a, Rog19b, SG76a, Sav90, Sav91, SMZ18, ST86, She78, SY08, Sho96, Tho13, Tho17, Ven84, WH83, Yan05, YBQZ17, YBQZ18, YKLH10, AB96, BS94c, CXLK19, CCA+12, DC94, FFGL10, HF91, KKL+09, KHH89, MSD16, MPL09, Mer90a, MZI98, MPST16, PvO95, Sag85b, SP12]. **fast** [Sie89, SV15b, TKH20, Tho00, TLLL09, WWG+18, YTHC97, YZ16, ZO13, ZHC+13, And94, Bir07, Gol96]. **Faster** [ASM17, CRSW11, CRSW13, FCH92, LK16, McC79, Bosxx, HKL04, LS15, Sna87]. **Fault** [AAB+92, DSSW90a, DSSW90b, MKAA17, HGR07]. **Fault-tolerant** [DSSW90b, HGR07]. **Faulty** [JCK+18]. **FCD** [ISO97]. **FCSRs** [BDM+12]. **Fe** [Gol94]. **Feal** [BS91b, BS91a]. **feasibility** [CKM14]. **Feature** [LMC07, NS16a, Som99, TWZW11, Fly92, MHT+13]. **Feature-Based** [TWZW11]. **Features** [DHT+19, LLDZ18, MS12, MBBS12, PKW09, ŠSaS01, THY+18, Tsa96, Tsa94, ZLY+13]. **Feb** [Bar83]. **February** [AH03, Ano10, Gol96, Gol92, IEE84, ICD86, ICD87, IEE88a, ICD88, ICD90, IEE94a, KI94, Kil05, Rie89, USE00b, Wol93a, Wol93b, Yu92]. **Federal** [Dan13]. **fehlerbehandlung** [Kue84a]. **fehlererkennung** [Kue83]. **Feistel** [SY11]. **Fencing** [TYZO15]. **few** [CDH19]. **FFT** [BGG93, BG93, DBGV93, Sch91b, Sch93a, Sch93b, Sch93c, SV94a, Van92, Vau92, Vau93]. **FFT-Hash** [DBGV93, Sch93b, Sch93c, Sch93a, Van92]. **FFT-Hash-II** [Vau93, Vau92]. **FFT-Hashing** [SV94a, Sch91b]. **FGS** [KM09]. **Fichier** [Lit77a]. **Fields** [AU79, HJ96, WX01, LS06]. **Fifteenth** [AW89]. **Fifth** [ACM86a, ACM03a, Bai81, Mo92b, Oxb86, ACM94d, AOV+99, GJM02, CTC90, Mo92b]. **Fifty** [Kon10]. **File** [BGF88, Bat80, Bat82, BCH87, Buc63, Bur75b, CS83b, CF89a, CE70, DS84b, DGM89, DT91a, DT91b, FC87a, FZ87, GGY+19, GIS05, GG74, Gro86, HP63, Har88, KK85, KS88b, KS88c, Lar82c, Lar82d, LK84, Lar85c, LI80, Lit80, Litxxa, Lom88, Lum73, MF92, McI63, Mil85, MK93, NHS84, Ols69, Omi88, Ore83, PSR90, RL89, RSSD89b, RSSD90, RSSD92, Reg85, RL74, Sal88, SS62, Sch79b, Sch81, SWTX18, Tha88, Wie83, Wie87a, Wri83, WB03, YD86a, vdP72, vdP73, BY89, BR75, Bra88, CC88a, DAC+13, FES09, Inc81, Kou93, Omi89a, RM88, SG72, VBW94, YD86b, van73]. **Files** [AS82, ANT85, BM76, BH85, Bra84a, Bra86, CC87, CS87, CC91, CLC92, CL95, Cla77, CS93b, Du86, FNPS79, Fel87, Gri74, HB89a, HB92, Lar81, Lar82a, Lar85a, LR96a, LCML94, Lit79b, LYD71, MY79, Mil85, Oto85a, Piw85, RSSD89a, Reg82, Rot89, SG76b, TK88, ZRT91, Bra85, CS93a, CCL91, Con17, HB89b, LNS93, LY72, NADY20, ORX90, Omi89a, RB91, TC83]. **Filing** [FC87a, DH84]. **filling** [GZ99]. **Filter** [CCH09, Kaw15, MK11, LZ06, RKK14, RK15]. **Filtered** [Ahn93]. **filtering** [KRML09, MK12, RCF11, YG10]. **Filters** [CHY93, CHY97, Kie85, LYW+18, Ram89b,

DKT06, HKL07, HKLS12, HXLX13, ISO97, PSS09]. **Final** [MO92a]. **Financial** [ANS05]. **Find** [Hol13, Lan06, Pat94]. **Finding** [CBK83, Cer85, CBK85, Cer87, Cer88, Coh98, CH09, CM93, DR06, FCHD88, FCHD89, HK86, HG77, HR04, KH84, SH92, SH94, Sim98, Val15, WYY05b, WYY05c, Yuv75, FHC89, MI84]. **fine** [KLSV12, XZPG21]. **fine-grained** [KLSV12]. **fine-texture** [XZPG21]. **Fingerprint** [JTOT09, LMC07, LMJC07, ZHW21, SK20]. **Fingerprinting** [Rou09]. **Finite** [Gri98, HJ96, Ram88a, WX01, FH15, KHK12, LS06, LK93]. **FIPS** [Dan13, Ano93b, Ano95b, NIS93, Nat95]. **Firewalls** [Kal01]. **First** [ACM89c, SDA90, PDI91, BBD09b, FNY92, adHMR93, PM89, Con17, DLM07, Fis87, SBK+17]. **first-order** [DLM07]. **Fisher** [SY08]. **FishStore** [CXLK19]. **Fit** [Cip93]. **Fitted** [ZWT+14]. **Fixed** [GB10, RS08]. **Fixed-Key** [RS08]. **Fixed-Parameter** [GB10]. **FL** [ACM91a, HB93]. **flash** [BFCJ+12]. **FlashTrie** [BLC12]. **FLATS** [GSI+82]. **Flexible** [QXL+20, SR89, SPB88, ZWY21, ZLC+20, ZHW19, BCCL10]. **Flexible-resizing** [ZHW19]. **Flight** [Fis87]. **floor** [Sch82b]. **Florence** [IEE92a, ST83a, ST83b]. **Florida** [ACM91d, IEE88b, RNT90, PDI91, Kna89]. **Flow** [NS16b, SL16, FWG18, HKL04, LDK12, LMP+08, YGS+19]. **flow-level** [LDK12]. **flows** [EVF06]. **fly** [BK88]. **FM** [KCF84]. **FOCS** [IEE06, IEE07]. **FODO** [LS89, Lom93]. **fonction** [LG78]. **Fontainebleu** [PDI91]. **Footprints** [KSSS86, HW88]. **forbidden** [CL09a]. **force** [CJP12, CJP15, LS07a]. **Forensic** [BFMP11, DR11, PS08]. **Forensics** [DA12, JL14, Rou09, SK99, ZHW21]. **Forest** [LCM+20, KP92]. **Forest-Based** [LCM+20]. **Forgery** [CY06]. **fork** [ALS10, CMP07]. **FORK-256** [CMP07]. **fork-join** [ALS10]. **Form** [Aum09, HZ86]. **Formalization** [MMC01]. **Formats** [GIS05]. **Formatted** [LYD71, LY72]. **Formula** [GK76, Ram97]. **Forrealization** [FM96]. **Forth** [Gre95]. **FORTRAN** [FDL86, JC88b]. **Forward** [CPP08]. **Forwarding** [YBQZ17, YBQZ18, BB07, HDCM11, TKH20]. **FOSS** [ASWD18]. **FOSSIL** [ASWD18]. **foundation** [SXLL08]. **Foundations** [Ano85a, BCFW09, Gol94, IEE76, IEE80b, IEE82, IEE85a, IEE85b, IEE88c, IEE89, IEE91b, IEE92b, IEE99, IEE06, IEE07, IEE10, IEE11b, IEE13, LT85, Rov90, Win78, HKNW07, LS89, Lom93, RRR99]. **Four** [Gra88, Gra89, SD89c, SD89a, HM03, SD89d]. **Fourier** [Ind13, BH93]. **Fourteenth** [BD88]. **Fourth** [ACM85b, ACM02, IEE80a, ICD88, KLT92, Las87, Yao78, GSW98]. **FowlerNollVo** [VFN91]. **FoXtrot** [MK12]. **FP** [PHG12]. **FPGA** [AOAAK20, DLT98, KMM+06, MXL+12, MAK+12, QXL+20, TP15, TK07, WZJS10]. **FPGA-Based** [TK07]. **FPGAs** [DD15, MMMT09, SK05]. **Fractal** [Ano95c, YSEL09]. **fractals** [HCF95]. **Fragmentation** [Sac86]. **frameproof** [vT14]. **Framework** [BJL16, BKMP09, DGV93, FFGL09, GST90, KBG18, XHZ+19, EH17, FFGL10, GL06, PCK95, UHT95]. **Framingham** [Ker75]. **France** [AGK+10, BF89, Jou85, LS89, Ng79, QG95, GQ95, vdHvH12]. **Francisco** [ACM75b, ACM08a, DT87, IEE88a, Joy03, Kar98, Shm00, USE90]. **Frankfurt** [CE95]. **Fredman** [KM86]. **Fredman-Komlos** [KM86]. **Free** [AR16, BM97, BB07, BHT98, CLNY06, CTZD11, Dam87, HM96, HZ86, KKT91, LFD17, MOI90, MOI91, Ram89b, Rus92, Rus93, Rus95, SHRD09, ZLLD18, AR21, BGKZ12, BGG93, BG93, BHT97, Gib91, Gob75, HCJC06, MJ14, NK16, PBGV89, Pro18, SS15, Van92, Vau92, Vau93, ZBB+06, ZL12, SS06]. **Free-Form** [HZ86]. **Free-text** [Ram89b, Gob75].

Freestart [SKP15]. **French** [Coh94]. **French-Israeli** [Coh94]. **Frequency** [Lyo78a, TS85, CJP12, CJP15]. **Frequent** [OTKH11, CH09, BMLLC+19]. **Frequently** [She78]. **fridge** [WLC20]. **Friendly** [ZH18, BP18]. **frontends** [Sag85b]. **Frontiers** [Jáj90, Fis87]. **FSE** [Bir07]. **FSpH** [ZWT+14]. **Fugue** [AP11]. **Fujiyoshida** [IRM93]. **Full** [AC74, Bur75a, CMP07, Cor00, Day70, DOP05, KK12, KK18, LP16, LT12, LLL+16, MZD+18, Mue04, GLM+10, San76, WYY05b, WYY05c, YSW+11, ZKR08, NH74, RCF11, SKP15, QXL+20]. **Full-Stack** [LLL+16]. **Full-Text** [YSW+11, RCF11]. **Function** [Abi12, ÁVZ11, Aum09, AMPH14, BPSN97, BF83, BDM+12, BS94b, BS94a, BKST18, BRS02, Bla95, BKL+11, BDP97, CP91c, Cer81, CKB83b, CN08, Cob94, CBA94, CMP07, CO82b, CDMP05, DBGV93, DGV93, Dae95, DC98b, DLT98, Dat88, DL80, FLS+10, GIS05, Gei95, Gei96, GSC01, GIMS11, HPC02, Har97, Hol13, HLC10, JP07, Kal01, KAS+22, KRJ09b, KCB81, Kra82, Kul84, KKT91, LJF19, LWWQ08, LP15, Lis07, LI80, LG78, MR07, MRST10, MNS12, MIO89, NS16a, Oto84, PV92, PPS21, PHL01, PHG12, PBD97, GLM+10, RB01, Sch11, Sch90a, Sch91b, SGY11, Sta06a, TC93, TTY93, WW09, WSSO12, Win83, Win84, Wol84, WFW+12, YD84, Yan05, WL12, ZWW+12, AKY13, ACP10, AB96, AMP15, ABO+17, AP11, BGKZ12, BNN+10, BDPV06, BDPV12, BOY11, BS94c, BW89, CKB83a, CK89, Con17]. **function** [DK94, DF89, DMB19, FP82, GTL21, GM18, Gib91, HR07, Han17, HL03, ITP14, KTDB20, LW04, Lia95, LWG11, MJ08, Mer90a, MZI98, Mit17, Mon19, NSW09, Pat94, Pat95, PL21, PVCQ08, QJ97, RS14, SB14, SS92, Sch82b, SRRL98, SHA97, SXL16, Tsa08, VNP10, VFN91, WS13, WYW14, YL97, YZ16, ZHX+21]. **function-based** [PL21]. **Functional** [LFP82, GMP95, SV18, ZKR08, Jou85]. **Functions** [AHV98, AFK83, AFK84, AN96, ASWD18, ÁCZ16, AA79b, AA79a, And91, ABD+16, Ano95a, AEMR09, AR17, AM07, AP08, BSNP96a, BDPSNG97, BCK96a, BCK96b, BR14, BBD+82, BBD+86, BGS96, Bih08, BCS09, BRSS10, BCFW09, BK12, Bol79, BPZ07, BHT98, BH86, Bur78, BDMD19, Can97, CW77a, CW77b, CW79, CMW83, CBK83, Cer85, CKB85, CBK85, Cer87, Cer88, CS83a, CS83b, CS85c, CS85b, CS85a, CS86, Cha86b, CS87, CLNY06, CLG09, CK15, Chi91, Chi94, Cic80a, Cic80b, CE70, Coh97, CH94, CHM92a, CHM92b, CM93, DGV93, Dam87, Dam90b, DDF+07, DK07, DY90, DY91, DTS75, DadH90, DGMP92, Die07, DGKK12, EK93, EPR99, Fil02, FL08, FLP08, FLP14, FFGL09, FCHD88, FCHD89, FCDH90, FCDH91, FCH92, FHCD92a, FK84, GO07, Get01, Gir87, GHK91a]. **Functions** [GHK91b, GLG+02, GK08, HHR+10, Hal12, HM12, HJ96, HKY12, HS08, HK12b, HR04, Ind01, IT93, JO80, Jae81, Jen97, Jou04, JD12, KH84, KK06, Kil01, Kno75, KP96, KLP98, KVK12, LM93a, LK94, LT09, LM95, Lis07, LH03a, LLG12, Mai92, MWCH92, MCW78, Mar64, Meh82, MP12, Mer90b, Mir01, MRW89, Mit02, MOI90, MOI91, Moh11, Mul91, NIS15, NM02a, NCFK11, NP99, NR12, NAK+15, OOB12, Otk91, Pag99, PWY+13, PB80, PQ98, PQ99, PW93, PGV90a, PGV90b, PGV92, Pre93, PGV93d, PGV93f, Pre94a, PV95, Pre97a, Pre97b, Pre99, Pre94c, QG89, QG90, RP91, RR08, RWSN07, Rja12, Roe94, RS08, Rul93, SP91, Sag84, Sag85a, SDMS12, SDMS15, San76, SS01, SS88a, Sch91a, SRY99, Sho00a, Sho00b, Sie04, SvEB84, SDT75]. **Functions** [Spr77, Sti06, TNS20, Tv83, Tro92, Tro95, Ull70, Ull72, WFLY04, Wee12, WC79, WC81, WKO78, YD85, Zem91, Zha07, Zhe90,

ZMI91, vW94, van94, vdBGLGL+16, AY14, AAB+92, ADM+99, AG10, And93, AMP12, AAGG16, Ati20, BSNP96b, BSNP96c, BD92, BCR04, BDPV07, BDP11, BJKS93, BJKS94, BDK16, BSU12, BCGS16, Bra09, BHT97, BM01, CMR98, CDS20, CFN18, CKB81, CCHK08, DS09a, DW03, ESRI14, FPS17, FFGL10, FHC89, FHCD92b, GKKT10, Ged14, GW94, GPGO16, Gon95, GLC08, GK12b, HK86, HC11, HLMW93, HXMW94, HKKK13, HSK88, HYLT99, HL12, Hug85, ISO97, ISO04, JCC00, JG95, KST99, KL95, KRT07, KHK10, Kra95, Kri89, LS07a, LM93b, LLH02, LKY04, Li95, Li10, LC13, MS09, Mei95, Mic02, MV08, MS13, MSP12, MT16, Mul92, Nae95, NY89b]. **functions** [NY89a, OS14, OS10, PW08, PW06, Pob86, PGV93a, PGV91, PGV93b, PGV93e, PGV93g, Pre94b, PGV94, PvO95, RB91, RFB97, RZ97, RP95, Roe95, Sar80, SS90b, ST85, SH92, SH94, SL88, SS16, Sie89, Sim98, SV06, TZ94a, Tsu92a, Tsu92b, VD05, XCCK09, YL04, YRY04, Zém94, ZW05, ZBB+06, ZDI+15, RRS06]. **functions-based** [HC11]. **Fundamental** [LYD71, LY72]. **Fundamentals** [HS78, HS84]. **Further** [Lit85, Sar15, Ano09b, DM03]. **Fusion** [Wil00]. **Future** [SP21]. **Fuzzy** [HWZP18, LMC07, LMJC07, LII92, HC14].

G2 [BP18]. **Gallery** [BFR87]. **Galois** [HJ96]. **game** [Zob70a, Zob70b]. **Gamma** [DGS+90b, DGS+90a, GD87, DGG+86]. **Gap** [ATS19, PNPC20]. **Garbage** [AG93, FW76, FW77, UIY10]. **gates** [GHK+12]. **Gb/s** [BLC12]. **GBDD** [YTHC97]. **GCM** [Saa12]. **geeks** [McN03]. **Gen2** [LYDA19]. **Gene** [TGGF10]. **General** [Chi91, Chi94, DR06, ISO97, LW88, LQH18, LHC05, Lum73, MSD19, MSD16, Sch91a, Sim98]. **general-purpose** [Sch91a]. **Generalised** [CC87, KKW99, LPWW06]. **Generalized** [HB94, KVK12, LI80, SK88, Sev74, KHK10]. **generalizing** [AMP12]. **Generate** [HSR+01]. **Generated** [LMC07]. **Generating** [Bla95, CT96, CHM92a, CHM92b, Get01, Jae81, Sag84, Con17, FP82, GRF11, MFK+06]. **Generation** [GRZ93, LL92, MS12, She91, SSS05, Wan14, BK07a, BDK16, BK88, CCA+12, CT10, KKP92, Mo92b]. **Generator** [Ano86, BK12, Cai84, Gui89, Sag85a, Sch90a, ZF06, Aam03, CLS95, HC11, SS92, TSY98, VZ12]. **Generators** [MWCH92, NAK+15, SP91, BK07a, CP13]. **Generic** [BDG+20, DL17, DOP05, MP12, Sar10]. **Genetic** [FFGOG07, HSIR02, CV05]. **Genomic** [CCH09]. **genus** [CDS20]. **genus-2** [CDS20]. **Geo** [SDZ21, TYZO15, ZWH17]. **Geo-Fencing** [TYZO15]. **Geo-Replicated** [SDZ21]. **Geo-Tagged** [ZWH17]. **Geographic** [RRS12]. **geohash** [MKL21, BŠH12]. **Geometric** [Bar97, BG92, Bie97, BM90b, CO82a, GPA97, HB89c, HB94, KGJG12, LW88, LMC07, LMJC07, LH20, MV02, PW94, RH92, RH95, RW97, SA97, Tsa94, Tsa96, WPKK94, War86, WR97, BJKS93, BJKS94, GG92, JBWK11, LG96, MN99, MMG10, WC94]. **geometries** [FH15]. **Geometry** [CCC89, MPP14, Wil00]. **Georgia** [USE00a, ACM83a, ACM83b]. **Geospatial** [MPP14]. **German** [Zel91, BJMM94a, BI87, Eck74a, HJ75, Koe72, Sta73, Wen92, vM39]. **Germany** [AH03, BRW93, HM08, adHMR93, Yao78, CE95]. **Gestion** [Lit77b]. **Get** [Eug90]. **GHASH** [Saa12]. **GI** [Lut88, TWW77]. **GI-Fachgesprach** [Lut88]. **Gigabytes** [WMB94, WMB99]. **Girths** [Zem91]. **Give** [AT93, AT90]. **Global** [CLP13, Cli95, DL79, LPSW03, MD97]. **Globally** [HSW88]. **GLUON** [BDM+12]. **gMig** [MZD+18]. **GNU** [Wil14]. **Go**

[Bur06]. **Goddard** [Fis87]. **Goes** [Cip93]. **Gold** [SZ93]. **gone** [Nic17]. **Gong** [BPSN97]. **Good** [Bur92, Hol13, JP07, Lom88, Mit02, ADM+97, Kou93]. **Goodyear** [Fis87]. **GORDION** [EE86]. **gossiping** [GHW07]. **GOST** [LJF19, WYW14]. **GPERF** [Sch90a, SS92]. **GPU** [ASA+09, FRB11, HLH13, LC20, LŁA15, MZD+18, TWL+18]. **GPU-based** [TWL+18]. **GPUs** [CZL12, vdBGLGL+16]. **GRAB** [Les88]. **GRACE** [KTMO83b, KTMo83c, KNT89, KTN92]. **Graduate** [Ano93d]. **Grained** [PAKR93, KLSV12]. **Gram** [Ven86, Coh98]. **Grams** [BRM+09, Coh97]. **granular** [CLS12]. **Graph** [Ari94, BMQ98, EFMRK+20, Gre21, Hal12, HM93, JBWK11, KM88b, MD97, MBBS12, NRW90, TI12, YkWY83, BPT10, CML+13, CLL+14, FHL+19, FKI+21, Kor08, Mol90a, Mol90b, SZO+20, WLLG08, vL94]. **Graph-Based** [Hal12, JBWK11]. **Graph-Entropy** [Ari94]. **graph-structured** [BPT10, WLLG08]. **Graph-theoretic** [vL94]. **Graphic** [LLLC17]. **Graphics** [Leb87, RKLC+11]. **Graphischen** [Lut88]. **Graphs** [CLG09, HMWC94, KPS92, Knu98, Zem91, AD08, AAB+92, AS07, DW03, FGFK10, HK83, Kut06, LL13, SN19, Zém94]. **Gray** [CLD82, Fal85a, DL80, Fal86, Fal88]. **Greece** [ACM01, AMSM+09, Rei88]. **Greedy** [WTZ+13, AGJA06]. **Greenbelt** [Fis87]. **Grenoble** [vdHvH12]. **GREYC** [AGBR19]. **GREYC-Hashing** [AGBR19]. **Grid** [Gri98, KS88b, KS88c, Leb87, NHS84, Reg85]. **Grindahl** [KRT07, Pey15]. **grosser** [Dos78a]. **Grøstl** [ABO+17, ITP14, MRST10, WFW+12]. **Grøstl-0** [ITP14]. **Group** [ACM82, Alb21, DT87, DD11, KKW99, LND08, Mue04, TZ94a, YLZ20, SE21, YLC+09]. **Group-based** [LND08]. **Group-by** [KKW99, YLC+09]. **Group-theoretic** [TZ94a]. **grouped** [DLN+18]. **grouping** [BLY20]. **Groups** [HM12, LLW10, PWY+13, Reg82, CFYT94]. **growing** [KW94, MSZ+20]. **Growth** [Oto88a, Rey14]. **Guangdong** [IEE11a]. **guaranteed** [RT89]. **Guaranteeing** [LK84]. **Guarantees** [HC13]. **Guess** [ZF06]. **Guess-and-Determine** [ZF06]. **guest** [DLM07, Fox91, RW97]. **Guide** [AS82, SD76, She17]. **guided** [SSU+13].

h [Gra94b, SYW+20]. **H-CNN** [SYW+20]. **Hachage** [Lit79a, Mek83]. **hackers** [Nic17]. **HAIFA** [DL17]. **Halifax** [DSZ07a, DSZ07b]. **Hamiltonicity** [CKN18]. **Hamming** [Bal96, Bal05]. **HANA** [SFA+19]. **Handbook** [Gon84, GBY91]. **handle** [Eug90]. **Handling** [BI87, DNSS92, Lar85b, QCH+81, Sam81, Sch79a, Wil59, WB03, ZO93, TWL+18]. **Handwriting** [MS12]. **Handwritten** [FLF11]. **Hans** [Ste18]. **Haphazard** [CS87]. **happened** [Her07]. **Hard** [Hol13, Kil01, BDK16, BCGS16, GPV08, LSZ+21, Nae95]. **Hardness** [BHKN13, BHKN19]. **Hardness-Preserving** [BHKN19]. **Hardware** [ABM06, ARH+18, Bab79, BPBBLP12, Bur81, Bur84, CHSC18, DW83a, FAFK21, FW09, GD87, GLG+02, HDCM09, IG77, MXL+12, RP91, TK85, dW83b, ABO+17, BOY11, Bis12, Bur82, CE95, DS09a, FNP09, ISH+91, JMH02, KM07, KM10, MZI98, RFB97, RAL07]. **Hardware-Based** [HDCM09]. **hardware-constrained** [RAL07]. **harmonious** [HK83]. **HaRP** [PT11b]. **Harrison** [Boo73]. **Harvesting** [AS16]. **HAS-V** [PHL01]. **Hash** [ANS97, Abi12, Ack74, Adi88, AHV98, AFK83, AFK84, APV07, AOAAK20, AN96, ÁVZ11, AK74, ABD+16, Ano93b, Ano95a, Ano95b, Ano95d, Ano02, Ano08, Ano12, AG93, AR16, Ari68, Ask05, AEMR09, AR17, AM07, AP08,

Aum09, AHMNP12, AHMNP13, AMPH14, ADW12, ADW14, AS16, Bac01, BSNP96a, BPSN97, BDG+20, BDPSNG97, BM87, BVF12, Bat75, BFMP11, BLY20, BRM+09, Bay73c, Bay73a, Bee99, BBD09a, BK70, Bel70, Bel72, BF83, Bel83, BD84, BCK96a, BCK96b, BBKN01, BR06, BBKN12, BR14, BPBBLP12, Ben98, BDM+12, BHH+15, BMB68, BS94b, BS94a, BKST18, BS91b, BS91a, Bih08, BRS02, BCS09, BRSS10, BW98, Bla00, BM89, BM90a, Blo70, Bob75, BKL+11, BI87, BCFW09, BK12, Boo74, BDP97, BPZ07, BT12a, Bou12, Bra84a, Bra85, Bra86, BJM14, BHT98]. **Hash** [BW89, Bre91, BDS09, Bur77, Bur78, Bur79, Bur06, Bur08, BDMD19, But17, CCF04, CP91c, Can97, CLP13, CRdPHF12, CW77a, CW77b, CW79, CMW83, CDS20, CRSW11, CRSW13, Cer81, CKB83b, CBK83, Cer85, CKB85, CBK85, Cer87, Cer88, CS91, CBB05, CLNY06, CN08, CCH09, Cha12, jCPB+12, CLG09, CK12, CdM89, CdM90, CCY91, CLYY92, CHY93, CLYY95, CHY97, CZLC12a, CLS12, CZLC12b, CZLC14, CHSC18, CN07, Chi91, Chi94, CJP12, Cic80a, Cic80b, Cip93, Cle84, CD84b, Cob94, CBA94, Coh98, CRR18, CS82, CY06, CMP07, CS93b, Cor00, Cor02, CDMP05, CS02, CHM92a, CHM92b, CM93, DSGKS20, DBGV93, DGV93, Dae95, DK09, Dam87, Dam90b, DDF+07, Dan13, Dav73, DG93, DG94, DK07, DY90, DY91, DG85a, DG85b, DHK+15, Dev99, DAC+13, DadH90, DGMP92, Die07, DS09c]. **Hash** [DCM18, DL17, DOP05, DRS12, DF01, DC81, Dos78a, DMB19, DB12, DJS80, DHJS83, DGKK12, Eck74a, Eck74b, EAA+16, EK93, EMM07, EH12, EPR99, FIP93, FIP02b, FAFK21, FL04, FLS+10, FLF11, FRB11, FFPV84, Fil02, FL08, FLP08, FLP14, FFGL09, FB87, F+03, FCHD88, FCHD89, FCDH90, FCDH91, FCH92, FHCD92a, FK84, GRBCC19, GK05, GO07, GK12a, GIS05, Gei95, Gei96, GHR99, Ger86a, Ger86b, Get01, Gir87, GI12, GSC01, GHK91a, GHK91b, Gon77, Gon81, GLS91, Gra93a, Gra93b, Gra94a, GLS94, GBC98, Gra99, GIMS11, Gre21, GLG+02, GK94, GK95, GLB21, GK08, HMNB07, HHR+10, HP78, Hal12, HPC02, HM12, HDCM09, Har97, HHL10, HCJC06, HW08, HC11, Hel91, HJ96, HCPLSB12, HJ75, HG77, Hil82, HS08, HK12b, Hol13, HKKK10, Hop68b, HD72, HCY94]. **Hash** [HCY97, HR04, HC13, HLC10, Hül13, HRS16, HBG+17, ISO04, IK92, IG77, IG94, IP08, Ind01, Irbxx, IABV15, IT93, IL90, JO80, Jen97, JRPK07, JLH08, JL14, JXY07, Jou04, JD12, JK11, JP07, KG95, KMM+06, KK12, KK18, Kal01, Kam74, KHK12, KHK15, KH84, KM09, KR91, KK06, KKW99, KAS+22, Kil01, KKRJ07, KRJ09b, KJC11, KKC12, KMV10, KTMo83a, KTMO83b, KNT89, KO90, KTN92, KW12, Kno71, KdlT89, KP96, KLP98, KR79, KRJ+80, KK85, KVK12, KCB81, Kra82, Kue82b, Kue84b, Kul84, KKT91, LFD17, LK07, LM93a, LM93b, LK94, LYY+18, LYX+19, Lam70, Lan06, LT12, Lar81, Lar82a, Lar85a, Lar88a, LAKW07, LMJC07, LKI10, LMSM09, LT09, LM95, Lev00, LJF19, LLL09, LÖON01, LHC05, LWWQ08, LYDA19, Lip02, Lis07, Lit89, Lit77a, Lit77b, LC96]. **Hash** [LRY+15, LCL+20, LR96b, LL85, LB07, LACJ18, LTS90, LHWL21, LH03a, LLG12, LMR02, Lyo85, MXL+12, MD05, MSD19, Mai92, MSTA17, MWCH92, MS12, MS02, MPP14, MT11, MCW78, Mar64, Mar71, MLD94, ML75, Mau83, McC79, MKF+16, MCF17, McK89a, Meh82, Mei95, MR07, MRST10, MNS12, MVB+21, MP12, Mer72, Mer90b, Mil85, Mir01, MRW89, Mit12, MW95, Mit02, MIO89, MOI90, MOI91, Moh11, Mot84, MKAA17, MKASJ18, Mue04, MJT+02, Mul91, Mul92, MC86, Nat92, NIS93, Nat95, NIS15, NM02a, NCFK11, NKT88, NNA12, NS16a, NP99, NSW09, Ngu06, NTY12, NR12, NXB13,

NY85, NAK+15, OL91, Omi88, OL89, Omi91, OL92, Ore83, Oto86, Pag99, Pag85, PAPV08, PWY+13, PCL93a, PV92, PPS21, PFM+09, PTT16, PCY95, PHL01, PLKS07, PV07, PHG12]. **Hash** [PBDD95, PG95, PRK98, PRZ99, PW93, Pip94, Pla98, PGV90a, PGV90b, PGV92, Pre93, PGV93d, PGV93e, PGV93f, Pre94a, PGV94, PV95, PBD97, Pre97a, Pre97b, Pre99, Pre94c, Pro89, QG89, QG90, Ram88a, RRS06, RR08, GLM+10, RRS12, RJK79, Rey14, RWSN07, RS12, RG89, RB01, RHM09, Riv76, Riv78, Rja12, RNR13, Roe94, RS08, RMB11, Ros06, Ros07, Ros21, Rot89, RK91, Rul93, SP91, Sag85a, SDMS12, SDMS15, SD78, Sam81, SS01, Sch11, SS80, SS88a, Sch90a, Sch91a, Sch91b, Sch93a, SV94b, Sch79b, SBS16, SG16, SGY11, SW91, SX08, SRY99, SK98, Sho00a, Sho00b, Sie04, SM02, SK05, SvEB84, Sol93, Som99, SPSP16, Spe92, Sta94, Sta06a, Sti06, SKM01, Szy82, Szy85, TT10, TR02, TY91, TNS20, Top92, TP95, Toy93, Tso15]. **Hash** [TNKT92, Tsu92a, TSP+11, Van92, VD21, Vau92, Vau93, VB00, WX01, WFLY04, WLLG08, WW09, WZJS10, WSSO12, WBWV16, Web72, Wee11, WC79, WC81, WKBA07, Win83, Win84, WKO78, Woe06b, WDYT91, WYT93, Wol84, Wu05, WFW+12, XNS+13, XBH06, YNW+09, Yam85, YD84, YD85, Yan05, YSW+11, YT16, Yao95, YSL05, WL12, YLB90, Yen91, YZ00, YCRY93, YY07, YY01, YLZ20, YSEL09, YKLH10, ZG90a, ZG90b, Zel91, Zem91, Zém94, Zha07, ZLY+12, ZZM17, ZJM94a, ZJM94b, ZJM94c, ZQSH12, Zhe90, ZMI91, ZO93, ZLC+12, ZWW+12, Zuk21, ZHZ+19, vW94, van94, vdBGLGL+16, vdVL12, AY14, AAB+92, ATAKS07, AKY13, ACP10, ADM+99, AG10, And93, AB96, AMP12, AMP15, AAGG16, AN20, AR21, AZ10, ABO+17, Ati20, AP11, BGKZ12, BSNP96b, BSNP96c, Bak09, BATÖ13, BLC12, BLP+14, BNN+10, BJ07, BD92, BvT13, BCR04]. **hash** [BFCJ+12, BDPV06, BOY11, BJKS93, BJKS94, Bie95, BS94c, BSU12, BCGS16, Bra09, BHT97, BM01, BGG12, Bur76a, CMR98, CVR14, CFN18, CKB81, CKB83a, CK89, CD84a, CAGM07, CHS+18, CCHK08, CJP15, CM01, CLW98, CL09a, CL09b, CLS18, CDH19, Con17, DK94, DF89, DS09a, DW03, DS09b, EASR22, ESRI14, FXWW17, FPS17, FJ13, FFGL10, FPSS05, FHC89, FHCD92b, Fro81, FH15, GTL21, GB17, GKKT10, GM18, Gib91, GS94, Gob75, GPGO16, Gon95, GLC08, GM79, GK12b, HK86, Han17, HLL18b, HLL18a, HAK+16, HLH13, HC14, HLMW93, HXMW94, HKKK13, HSK88, HKW05, HYLT99, HL12, HL03, HCW+21, HXLX13, ISO97, ITP14, JFDF09, JHL+15, JCC00, JG95, KKP+17, Kha95, KST99, KL95, KRT07, KTDB20, KHK10, Kra95, Kri89, KCL03, Ku04, KCC05, LS07a, LLH02, LKY04, LW04, LL13]. **hash** [LMSM12, LPSW03, Li95, LVD+11, LWG11, LS06, LC13, LCRY93, LG78, LEHN02, LLJ15, MSZ+20, Mad80, MTB00, MMC01, MSD16, MvT08, MS09, MJ08, Mau68, McK89b, MRL+19, Mer90a, MZK12, Mic02, MZI98, MV08, Mit17, Mon19, MA15, MPST16, MF82, MS13, MSP12, MMSY94, MT16, MFES04, Nae95, NADY20, NY89b, NY89a, NK16, NTW09, ORX90, OS14, Omi89a, OT89, OS10, PCL93b, PCK95, Par18, Pat94, Pat95, PCV94, PPB16, PL21, PVCQ08, PW06, PGV93a, PGV91, PGV93b, PGV93g, Pre94b, PvO95, Pro18, PSS09, QP16, QJ97, Ram87, RP95, Riv74a, RS14, Roe95, Rön07, SB95, SB97, SPLHCB14, SB14, Sar13, SN19, Sar80, SS90b, SS92, SV95, ST85, SH94, SE21, SS06, SRRL98, Sie89, Sim98, SHA97, SP89, SV15a, SV15b, SV18, SD95, SXL16]. **hash** [SV06, TKH20, TC04, TZ94a, TMW10, Tsa08, Tsu92b, TMB02, UHT95, VD05, VNP10, VFN91, Wag00, WM93, WS13, WYW14, Wie86, Wil03, Wil14, Woe06a, Wog89, WY02, WTN07, WTN09, XCCK09,

XLZC14, YTHC97, YL04, YL97, YRY04, YZ16, Yu18, ZCZQ19, ZGG05, ZBB+06, ZLY+13, ZHX+21, ZYWM20, ZHW01, vT14, HGH+12, BJMM94b, BJMM94a, DBGV93, FIP02a, HJ75, KKL+09, Sta73, TLLL18, WC07, WWZ09, ZW05, Sch93b, Sch93c]. **hash-** [PSS09]. **Hash-and-Sign** [CK12, GHR99, PV07]. **hash-array** [SV15b]. **Hash-base** [WLLG08]. **Hash-Based** [AS16, BHH+15, But17, CdM89, CdM90, DK09, DG85b, DL17, DF01, FRB11, GRBCC19, GI12, HCPLSB12, Hül13, HRS16, HBG+17, JK11, KM09, KJC11, KMV10, KK85, LLL09, LTS90, MLD94, MKF+16, MCF17, MKAA17, NXB13, OL89, PFM+09, PCY95, PRZ99, RNR13, RK91, SBS16, TY91, YSW+11, YY07, Adi88, BDS09, CJP12, DG85a, HCJC06, SX08, YSL05, BLC12, BLY20, CJP15, CLW98, EASR22, HAK+16, KCL03, Ku04, KCC05, MSZ+20, Mul92, OT89, PCK95, PPB16, SPLHCB14, SE21, UHT95, TLLL18]. **Hash-Bucket** [CS82]. **Hash-CBC** [BBKN01, BBKN12]. **Hash-chaining** [CBB05]. **Hash-code-techniken** [Mer72]. **Hash-Coded** [Bay73c]. **Hash-codering** [Lit77a]. **Hash-Coding** [Bur77, Dos78a, HJ75, Lit77b, Mar64, Sch79b, Bur76a, LG78, Riv74a, HJ75]. **Hash-consed** [BJM14]. **Hash-consing** [AG93]. **Hash-Counter-Hash** [MKASJ18]. **Hash-Function** [BF83, BRS02, ACP10]. **Hash-Functions** [Gir87, QG89, QG90, ISO97, ISO04]. **Hash-Join** [Gra99, NNA12, GK05, RG89]. **Hash-Join-Algorithmen** [Zel91]. **Hash-Joins** [LR96b]. **Hash-Jpoin** [Omi91]. **Hash-Key** [MW95]. **Hash-Lookup** [CN07]. **Hash-Only** [EH12]. **Hash-Partitioned** [Ger86a, NKT88, SW91, Ger86b]. **Hash-Routing** [WBWV16, SPSP16]. **Hash-Search** [WWZ09]. **Hash-semijoin** [CCY91]. **Hash-Sequential** [Lit89, IL90]. **Hash-Speicherung** [BJMM94b, BJMM94a]. **Hash-Structured** [CS93b]. **Hash-Tabellen** [BI87]. **Hash-Tables** [LMSM09, LMSM12]. **Hash-tree** [BLY20]. **hash-tries** [SV18]. **hash-values** [GS94]. **Hash-verfahren** [Hil82]. **Hash/Table** [DAC+13]. **HAShCache** [PG17]. **Hashcash** [Bac02]. **Hashcodingverfahren** [Sta73]. **Hashed** [GJR79, GG74, HYKS08, KS12, LI80, MF92, Mul72, SVCC01, VL87, VL97, WS93, WM19, And88, GMW90, HSMB91, Ken73, War14]. **Hashedcubes** [PSSC17]. **Hashes** [BC08, Saa12, Sch01b, Sch01a, Wan14, GvR08, GP08, GNP05]. **hashfunctions** [PBGV89]. **HashGraph** [Gre21]. **Hashiguchi** [LP04]. **Hashimoto** [ŠSaS01]. **Hashing** [ACP09, AK98, Ahn86, Ahn87, Ahn93, AKS78, AAE+14, Alb21, Ald87, Ald88, AHS92, AB17, AP93, AA79b, AA79a, AI06, ASBdS16, ATT98, ANS09, ANS10, Ari94, ABH+73, AT93, ASW07, Ast80, AS96, AC74, Atk75, ADW12, ADW14, BYSP98, Bal96, Bal05, BH90, BP97, Bar97, BG93, BGH12, BH91, BK84, BR97, BM97, BHIMM12, BJMM94b, BBD+82, BBD+86, BHKN13, BHKN19, Bie97, Bin96, Bla95, BG07, Bol79, BÖS11, BGV96, BM90b, BI12, BK07b, BT90, BT94a, Bra84b, BT94b, BK90, BT12b, BH86, Bry84, BP18, Bur92, Bur76b, Bur81, Bur84, BC90, CP91a, CHKO08, CH12, CLM85, Cel86, CLM86, CF92, CSSP15, CLD82, CS83a, CS83b, Cha84b, Cha84c, CS85c, CS85b, CS85a, Cha85, CS86, CL86, Cha86a, Cha86b, CC87, CS87, CC88b, CCJ91, CW91]. **Hashing** [CC91, CLC92, CL95, CL05, CLC06, CV83b, CV84, Che84a, Che84b, CV86, CW09, CTZD11, CJN20, CZ17, CKPT19, Chi93, CT12, CJC+09, CJKK19, CK94, Chu91, Chu92, CV08, CKW09, CE70, Coh97, CO82b, CHK85, CH94, CG79, DA12, CDW+19, CadHS00, DW83a, DC98a, DKRT15, Dam93, DLT98, DPH08, Dat88, DD11, vdSDW74b, DS84a, DGD02, DTS75, DL79, Dev93,

DMV04, DJSN09, DadH90, DadH92, DKM+94, Die96, DH01, DS09c, DMR11, DY08, Dit91, Dod82, DHL+94, DHL+02, DLH09, DSSW90a, DR11, Dre17b, Dre17c, DL80, DT91a, DT91b, DT75, Dun89a, Dun89b, EFMRK+20, Ell83, Ell85a, Ell87, Ell88, ED88, FNPS79, Fal85a, FM96, Far14, Fel87, FNSS92, FGFK10, Fla81, FS82, Fla83a, FPV98, Flo87, FPS13, FT12, FFGOG07, FMM09, FMM11, Für88, GSS01, GL73].
Hashing
[GM91, GM94, GadHW96, GM98, GIM99, Gon80, GL82, GL88, GRZ93, GK76, GI77, GT80, Gra86, GPY94b, Gre95, Gri77, Gri79, GT93, GPA97, Gui75, GS76, Gui76a, Gui76b, GS78, Gui78, GG80, GH07, GZX14, Gur73, HB89a, HB92, Hac93, HSPZ08, HT01, HR14, HM96, HK12a, Ham02, Har71a, HCF95, Hea82, Hea72, HB89c, HB94, adH90, adH93, Hel89, HST08, HNS84, HSM95, HKY12, HYH89, HYH93, Hol87, HC87, HT88, HY86, HTY90, HSW88, IJK13, IKO05, IH95, Jac92, Jae81, Jag91, Jai89, Jai92a, Jai92b, Jaixx, Jan08, JV16, JP08, JTOT09, Joh97, JCK+18, Kab87, KBG18, KU88, KKN12, KV09, KGJG12, Kaw85, Kaw15, Kel93, KR86b, KR86a, KV91, KMW08, KMW10, KZ84, Kno75, KP97, Knu19, KM86, Kon10, KM88a, KP94, Kri84, KS86, KS87a, KS87b, KS88b].
Hashing [KS89b, KR01, Kum89a, Kum90, Kut10, LW88, Lar78, Lar80a, Lar80b, Lar80c, Lar82b, Lar82c, Lar82d, Lar83, LR85, Lar85b, Lar85c, Lar88b, Larxx, Leb87, LMC07, LK14, Lep98, LC20, LC88, cLmL07, Li15, LCLX19, LCML94, Lia95, LLZ10, LLL11, LLLC17, LRY78, LRY80, LN93, Lit91, LI80, Lit78, Lit79b, Lit80, Lit81, Lit85, LZL88, LSV89, LRLW89, LRLH91, Litxxa, Litxxb, LC12, LZ16, LWZ+18, LH20, Lom83, LPP91, LPP92, LM93c, LH03b, LSZ+21, Lyo78a, Lyo83, MLHK17, Mac95, MD97, MSW19, MWHC96, Man12, MK11, MNT90, MB03, MBBS12, MV88, MV90, MV91b, MW09, MHB90, MSSWP90, Men82, Men12, Mey93, MV01, MV02, Mit73, Mit09, MH00, Moh90, Moh93, MNP08, MWC12, Mul84a, Mul81, Mul84b, Mul85, MS88b, Nak21, NSW08, NRW90, NI83, Nyb96, OWZ14, OTKH11].
Hashing [OG94a, OG94b, OOB12, OOB17, OVY94b, Otk91, Oto84, Oto85a, Oto88b, Oto88a, OT91, OSR10, Ouk83, OS83a, OA89, OS83b, PR01, Pag06, PP08, PWYZ14, Pag18, Pal92, Pan05, PB80, Pap94, PV07, PT12a, PH73, Pea90, Pea91, Per73, Pes96, Pet13, PNPC20, PS93, PQ98, PQ99, PKW09, Pip79, Pit87, PM89, PVM94, PVM97, PV19, PT11b, PRM16, PKSB18, PS12, PACT09, PF85, PADHY93, PW94, Qui83, RT87a, Ram88b, RL89, RP91, RR92, Ram92, RL82, RLT83, RSD84, RSD85, RSSD89a, RSSD89b, RSSD90, RSSD92, Ram97, RGNMPM12, RLH91, Reg81, Reg82, Reg88, RRS12, RH92, RH95, RW97, Rob86, Rog95, Rog99, Rog19a, Rog19b, RS75, RS77, Ros77, Rou09, RT87b, Rus92, Rus93, Rus95, SDR83a, SNBC98, SnC05]. **Hashing** [Sag84, SY11, Sas11, SG76a, Sav90, Sav91, Sch79a, SD90b, SD90a, Sch91b, Sch93a, Sch81, SMZ18, SY91, SR89, SPW90, SYW+20, SB93, SSL+18, SHZ+20, SY08, Sho96, SR01, SSS05, SDT75, Spr77, SHRD09, SGGB00, Sti94a, Stu85, Sun15, SHF+17, SA97, Tam81, Tam82, TK88, TC93, TL95, TWZW11, TYZO15, THY+18, TCY+20, TI12, TW07, TK85, TZ12, TTY93, TZ94b, Tv83, Tor84, TK07, Tro92, Tro95, Tsa96, US09, Ull70, Ull72, VV84, VV86, Vek85, VP96, VP98, Vit80b, Vit80c, Vit81b, Vit81a, Vit82b, Vit83, VC87, WG00, WPKK94, War86, WFHC92, Wee07, Wee12, WPS+12, WSZ+16, WFT12, WP10, WDP+12, WS03, Wil96, Wil00, Wil79, Wil71, Win90b, Win90a, Woe01, WR97, WZ93, Wu84, YDT83, YWH09, Yao80, Yao85a, Yao85b, Yao91, Yas07, YB95, YTJ06, YBQZ18, YGC+12].
Hashing [YD86a, ZWY21, ZZLZ21, ZPS90, ZPS93a, ZHW21, ZLC+20, ZH18, ZHW19, dW83b, vdSdW74a, vMG12, AT18, ASM17,

ASA+09, ADM+97, AI08, AII89, AT90, BGG93, BL89, BGH+13, BBPV11, BD82, BGG94, BDPV14, BDK16, BMQ98, BCGS16, Boo72, Bosxx, BT89, BCCL10, Bur05, Bur82, BMLLC+19, CP91b, CP95a, CHKO12, CS93a, CW93, CJMS19, CP95b, CV83a, CCL91, CHL07, CLL+14, CWC10, CKKK09, CZL12, CR89, CP13, CO82a, CHM97, Cze98, Dam94, DM03, DOP+14, DKM+88, DKM+91, DHW08, DS09b, D+92, DLH13, DSSW90b, DK12, DLN+18, Duc08, DM11, EH17, EBD91, Fal86, FWG18, FSV09, FFS+13, FNSS88, FKI+21, GLHL11, GG92, GDGK20, Gib90, GW94, GM77, GLJ11, GS89, GRF11, GPY94a, GZ99, Gui76c, Gup89, HB89b, HDCM11, HKL07, HR93, HM93, HMWC94, HL05, HC02]. **hashing** [Hua85, HFZ+15, HFF+17, Hui90, IMRV97, Ind13, IIL17, Jan05, JWM+18, JBWK11, Kan90, KYS05, KLL+97, KSB+99, KU86, KL96, KR88, KK96, Kim99, KM07, KM08, KM10, KR19, Kos14, KD92, Kou93, Kra94, KR06, Kum89b, Kut06, KSC11, KSC12, LG96, Lar84, LNS11, LH06, LK16, Lev89, LK11, LOZ12, Lin96, LS96, LNS93, LYJ+13, LMLC14, LLT21, LLA15, LWXS18, LHWL20, LM88, LH04, LMPW15, LJW+17, ML15, MIGA18, MI84, ML94, MNT93, MLP07, MPL09, MV91a, MC89, MMG10, MP16, Men17, Mil95, Mil98, MYS12, MKSiA98, Mol90a, Mol90b, MSV87, NMQ22, Nil94, NMX19, OP03, OVY94a, OS88, Pag01, PR04, PWYZ10, PJM88, PJBM90, PCM15, PT11a, PT13, PY88, Pon87, Pro94, QM98, QZD+18, Ram89a, RT89, RB91, RFB97, RZ97, RLH90, RAD15, SK20]. **hashing** [Sab94, Sar11, SP12, SS89a, SS90a, Sch93b, Sch93c, ST93, SH92, SL88, SS16, Sil02b, Sna87, Sta99, Ste18, Sti91, Sti94b, SZO+20, Sun91, STS+13, TLZL16, TB91, Tho00, Tho17, TK17, TKI99, Tsa94, TLLL07, TD93, Vak85, Vio05, Vit80a, Vit82a, Wan05, WL07, Wee88, Woe05, WC94, WY00, WWG+18, XZPG21, XMLC11, YCJ12, Zha19a, ZWCL10, ZL12, ZWT+14, ZHX+21, ZPS93b, ZZLZ18, ZHC+13, Zob70a, Zob70b, ZHB06, AGBR19, BJMM94a, JMH02, KS88c, SV94a, SKC07, SA17, CV85]. **Hashing-Based** [Alb21, LMC07]. **HashMap** [Oak98]. **Hashnet** [Fah80]. **Hashtabellen** [Kue82a, Kue82b]. **Hashtable** [Oak98, Bee83]. **Hashtag** [RTK12, KGJØ18]. **Hashverfahrens** [Dos78a]. **HashXor** [Cho21]. **Haskell** [MRL+19]. **HAVAL** [WFLY04, ZPS90, ZPS93a, ZPS93b]. **HAVAL-128** [WFLY04]. **Hawaii** [Deb03, SC77]. **HCC** [Har97]. **HDDs** [HGH+12]. **Head** [ACM91c]. **Heap** [FW76, FW77]. **Heaps** [CCA+12]. **Heavy** [TP15, Ind13]. **Hebrew** [Sch82a]. **Hecke** [CT96]. **Hedge** [Sho00b]. **Height** [Dev99, Reg81, THS97]. **Heights** [Jen76]. **Heinz** [adHMR93]. **Held** [Jáj90, Fis87]. **Help** [PVM97]. **Helper** [ALS10]. **Herding** [KK06, BSU12]. **Here** [Bur06]. **Hershey** [ACM76]. **Hersonissos** [ACM01]. **hesitate** [Gre95]. **Hessian** [Far14]. **Heterogeneity** [PG17, WB03]. **Heterogeneity-Aware** [PG17]. **Heterogeneous** [HNKO20, PG17, WSZ+16, GDA10, Kha95, SX08, SV18]. **Heuristics** [Omi89b]. **Hidden** [Leb87]. **Hide** [Can97]. **Hiding** [MMMT09, MV01, Wee07, HR07]. **Hierarchical** [FWG18, PACT09, TK88, VL87, GP08, VL97]. **Hierarchy** [Wil71, YL04]. **High** [ACM04, AS09, AEP18, AI06, ASBdS16, CT96, DGG+86, DadH92, DS97, Flo87, GIM99, HSM95, IEE94c, KMM+06, KMV10, LCK11, LPT12, McK89a, McK89b, OT91, PSR90, RSSD90, RW07, Rön07, She91, TK88, Tho13, TP15, MKL21, WZJS10, XLZC14, YNKM89, YWH09, ZHW19, AI08, BCCL10, EVF06, HKL07, Inc81, MV91a, MAK+12, MA15, RFB97, SLC+07, Shi17, Sie89, SWQ+14, SXLL08, TYSK10, TLLL07, XMLC11].

High-bandwidth [AS09]. **High-Dimensional** [AEP18, TYSK10]. **High-error** [Rön07]. **High-Performance** [DS97, Flo87, IEE94c, She91, MKL21, ZHW19, Shi17]. **High-Speed** [KMM+06, KMV10, McK89a, YNKM89, McK89b, RW07, EVF06, SLC+07, SXLL08, TLLL07, XMLC11]. **High-Throughput** [LPT12, XLZC14, MAK+12]. **HighEnd** [LVD+11]. **Higher** [HKKK13, DH84]. **higher-order** [DH84]. **Highly** [BCS09, KHW91a, Mat93, PAKR93, KHW91b, ZLL+07]. **Highly-Associative** [KHW91a, KHW91b]. **Highly-Efficient** [BCS09]. **Hill** [IEE88a]. **Hilton** [ACM91c, PDI91, ICD88, ICD90, IEE90, IEE01]. **Histogram** [Gra93b, MNY81, PCK95, UHT95]. **Histogram-Driven** [Gra93b]. **History** [BG07, MNS07, NSW08, Reg82, NT01]. **History-Independent** [BG07, MNS07, NSW08]. **Hitter** [TP15]. **hitters** [Ind13]. **HMAC** [FIP02a, BCK96b, CY06, DRS12, MAK+12, RR08, Sta99]. **Hmap** [YTHC97]. **Hoc** [DPH08, JLH08, Cha12]. **Hole** [JLH08]. **Holistic** [LCM+20]. **Holographic** [BGF88]. **Homepage** [GCMG15]. **Homomorphic** [CFN18, KKN12, CZL12, MT16]. **Honolulu** [Deb03]. **Hood** [CLM85, Cel86, CLM86, DMV04, PV19]. **Hop** [RHM09, MA15]. **Hopscotch** [HST08]. **hostile** [LC95]. **hot** [KLL+97]. **Hotel** [ACM75b, ACM82, ACM83a, ACM83b, ACM85a, ACM87, ICD86, ICD87, IEE88a, IEE88d, IEE01, Kna89, Nav85]. **Hotspot** [JLL+20]. **Hotspot-Aware** [JLL+20]. **Hough** [HB89c, HB94]. **House** [IEE80a]. **Houston** [IEE76, IEE94a]. **Houthalen** [QV89, QV90]. **Hover** [EH12]. **HTM** [CCW+17]. **HTML** [UCFL08]. **HTTP** [DB12]. **Human** [Bor81, TCW+13]. **humanities** [Bai81]. **Hungary** [Rue93]. **Hwang** [KCL03]. **Hyatt** [Kna89]. **Hybrid** [BM89, BM90a, CBB05, Gra93a, Gra93b, Gra94a, JLL+20, KNT89, HGH+12, LLL11, Sch79a, TYZO15, PCV94, TT81]. **Hybrid-Hash** [BM89, BM90a]. **Hypercube** [OL91, OL92]. **hyperelliptic** [FFS+13]. **hypergraph** [KKP+17]. **Hypergraphs** [FP10, HMWC94, Rad92]. **hyperspace** [DOP+14]. **hypersphere** [LWWK20].

I-cloth [TWL+18]. **I/O** [MMC01, Vit85]. **IB** [CZLC14]. **IBE** [Zha07]. **IBM** [Dit76, Dit76, MS02]. **IBM/360** [Dit76, Dit76]. **ICALP** [AGK+10, ADG+08, AMSM+09, ACJT07, CIM+05]. **ICCI** [AFK90, KLT92]. **ICDT** [AA86]. **Iceland** [ADG+08]. **ICICTA** [IEE11a]. **Icon** [GG86b, GT93]. **iconic** [WC94]. **ID** [ZJ09]. **ID-Based** [ZJ09]. **Idea** [Gra94b, HL03, WPS+12]. **Ideal** [Lis07]. **identical** [Lia95]. **Identification** [MV01, ST86, CJP12, CJP15, GS94, IG94, LWG11, WWG+18]. **Identifier** [BŠH12, Sev74]. **Identifiers** [DB12, Wil59]. **Identifying** [ASWD18]. **Identity** [CZLC12a, CZLC12b, CZLC14, KM92, LYX+19, Cho21, ZYWM20]. **Identity-Based** [CZLC12a, CZLC12b, CZLC14, LYX+19, ZYWM20]. **IEC** [ISO04]. **IEEE** [ACM04, Col93, IEE80a, IEE88a, IEE92a, IEE01, IEE05, IEE06, IEE07, IEE10, IEE11b, IEE13, MS05, Yan10, IEE84]. **IEEE/ACM** [ACM04]. **IFIP** [Gil77, Ros74]. **Igniting** [ACM03b]. **II** [BS91c, Sch93a, Sch93b, Sch93c, Van92, Vau92, Vau93]. **III** [Nol82b, OK80, Sed83a]. **Illinois** [ACM88b, ABM06, BL88, Lom93]. **im** [DS84a, Wal74]. **IMA** [Boy95b]. **Image** [Alb21, Ano95c, BFMP11, BS94a, BI12, DCM18, DHT+19, DR11, GPA97, GH07, HW08, LKI10, LQZH14, Li15, LÖON01, LC12, LYJ+13, LH20, MV02, OSR10, RGNMPM12, SB97, TWZW11, THY+18, US09, WP10, WDP+12, ZWH17, ZZLZ21, HC11, LMLC14, Mit12, SB95, TCW+13,

TLZL16, XZPG21]. **image-keyword** [LMLC14]. **Images** [FLF11, MNY81, PKW09, RT81, ŠSaS01, WMB94, WMB99, GG92, LMLC14]. **Imaging** [FHMU85]. **Imai** [PGV93a, PGV90a, PGV93b]. **imbalance** [WZ12]. **immutable** [SV15b]. **Impact** [GD87]. **imperative** [NMS+08]. **Imperfect** [Ven84]. **Implement** [CL83]. **Implementation** [BCS89, BS94b, BGDW95, Dat88, DF89, DKO+84b, DKO+84c, DKO84a, DKO+84d, Dee82, Dev93, Dit76, DT75, EE86, EjKMP80, FW09, GG86b, GT93, Gro86, Har71a, Hek89, ISK+93, JD12, Kah92, KMM+06, KU88, KM92, KR86b, KR86a, KKRJ07, KRJ09b, KTN92, LK84, Lit79b, LPP92, NM02a, PRM16, SDR83a, She91, SK05, Ste82, TGL+97, TNKT92, VL87, BDP+12, BS94c, BW92, DS09a, DHW08, DM11, EBD91, GN80, GJM02, Inc81, IIL17, KU86, KKL+09, McD77, MZI98, MFES04, Tai79, MKL21, Dit76]. **Implementations** [GLG+02, Vit82b, WPKK94, WZJS10, DMP09, RAL07]. **Implemented** [CMW83, MRL+19]. **Implementierungstechniken** [Nee79]. **Implementing** [Bab79, Blu95, BJM14, GHJ+93, Gra86, Jun87, KHW91a, KHW91b, Lin96, Llo81, LB07, VL97]. **Implications** [Chr84, CHS+18, RAD15]. **Implicit** [OS88, Kor08]. **Impossibility** [BCS09, HM12]. **Improve** [LBJ02, BM01]. **Improved** [Ari94, BvT13, BMB68, Bih08, Bre91, CN08, DDS14, DL17, FB87, HSM95, HW88, JNPP14, KM86, Kut10, LW04, LJF19, KKMS10, LH04, Mau83, Mic02, Mul72, NSS+06, Nak21, PS12, Rad92, RP95, SS80, SD95, TK17, UIY10, WM19, GM77, Mau68, War14, ZW05]. **Improvement** [CH94, Fel87, LCM+20, RGNMPM12]. **Improvements** [CTZD11, Lev00, Nam86]. **Improving** [ATAKS07, ÁVZ11, BDS88, CHY93, CHY97, CAGM07, Cla77, DB12, GCMG15, JHL+15, KZ19, MS12, RT87b, Sch82a, TCP+17, YWH09, ZGG05]. **Impure** [Dee82]. **In-Bucket** [TYZO15]. **In-Memory** [CCW+17, JLL+20, MZL+19, QXL+20, ZHW01, WLC20]. **In-Network** [WBWV16]. **Inaccessible** [HHR+10]. **Inadequacy** [GY91]. **Includes** [FW76, FW77]. **Including** [DGV93, KL95]. **Incoming** [LK07]. **Incompatibilities** [KCF84]. **Incorporating** [CBA94]. **Increased** [PRM16, MSP12]. **Increment** [Ban77, Luc72, RKK14]. **Incremental** [BGG94, CT12, FRB11, GSC01, ISHY88, PW06, TWL+18, UIY10]. **Incrementality** [BM97]. **incrementalization** [SB07]. **Indeed** [Yas07]. **Indentify** [KCF84]. **Independence** [KW12, PPR09, PT16, Tho13, DT14, PPR07, PT10a]. **Independent** [BG07, CCJ91, DGD02, DTS75, Die96, Ind01, MNS07, NSW08, TZ12, BCGS16, FPS17, Han17, NT01]. **Independently** [AU79]. **Index** [BM89, BM90a, Buc82, Bur83b, Bur83c, DS84a, GPY94b, LC86a, Lom83, MZL+19, OL89, Oto85b, Qui83, TY91, Wil79, ZHW19, Bur83a, Fro81, GPY94a, HM03, KZ19, LCH+14, McD77, SWQ+14]. **Index-Based** [OL89, TY91]. **indexable** [RRS07]. **Indexed** [Chu91, Chu92, KHT89, Mul72, GB17, SN19, Tay89, WM93, TKI99]. **indexed-hash** [WM93]. **Indexed-Sequential** [Mul72]. **Indexes** [Les88, Omi89b, Pip94, WCW+22, FVS12, HCW+21]. **Indexing** [CJ86, Dum56, KGJG12, Li15, Llo81, Per73, SE89, Tor84, Wil79, WMB94, WMB99, YWH09, CXLK19, CWC10, Fly92, LG96, MSZ+20, MIGA18, MMG10]. **India** [RRR99]. **Indiana** [Van10]. **Indianapolis** [Van10]. **Indicator** [YD84]. **indicators** [Er86]. **Indices** [LR99, Val87]. **Indifferentiability** [CN08, LLG12, MPST16, BGKZ12, BDPV08, GLC08]. **Indifferentiable**

[BGH12, CLNY06, FFS+13, FT12, BGH+13]. **Indirect** [Bal96, DGGL16, Joh61]. **Indirectly** [Ols69]. **Individual** [Jan05, Jan08, Vio05]. **Induced** [de 69]. **industrial** [PGV93c, ARA94]. **Industry** [ANS05]. **Infeasibility** [FS08]. **inference** [NMQ22]. **Infinite** [GHK91a, GHK91b, LII92, Bra09]. **infinity** [Hil05]. **inflate** [NMQ22]. **Influence** [RTK12]. **INFOCOM** [IEE01, IEE92a]. **Inform** [Pro94]. **informal** [CK89]. **Informatics** [CHK06]. **Informatik** [Nol82a, Nol82b, OK80]. **Information** [PDI91, BV89, BIP92, Can97, Cha84a, Dan13, DSSW90a, Ell82, FC87b, FH69, FCDH90, FCDH91, GPY94b, ISO97, ISO04, KLT92, KM86, KM88a, LC06, LXL+19, MV01, MNS07, PGV93f, SKC07, SPSP16, SC77, Sta06b, Sun15, Vid90, WBWV16, XHZ+19, Yan10, YR87, YBQZ17, AFK90, DSSW90b, GPY94a, KSC11, KSC12, SG72, SXLL08, FNY92, FBY92, Gil77, Ros74]. **Information-Based** [SKC07, KSC11, KSC12]. **Information-Centric** [SPSP16, WBWV16]. **Information-Theoretic** [Sun15, SXLL08]. **Informix** [Ger95]. **Infrastructure** [MJ14, Nak21]. **Infrastructure-free** [MJ14]. **ingestion** [CXLK19]. **Ingres** [Sne92]. **inheritance** [DMP09]. **Inhibiting** [GAS+16]. **Initial** [vdP72]. **Initiative** [MO92a]. **Injection** [NCFK11]. **Inner** [PWY+13]. **Innesbrook** [IEE88b]. **Innovation** [ACM03b]. **Innovative** [OG94b]. **Input** [AB12, Sab94]. **Insecurity** [DOP05]. **insensitive** [CyWM91]. **inserting** [Gup89]. **Insertion** [FPS13, PS12, CV83a, Jan05, Kou93, PY88]. **inside-out** [AP11]. **Insight** [CQW08, IEE02]. **Installation** [LAKW07]. **instance** [FS08]. **instantaneously** [DV07]. **Instantiated** [RR08]. **Institute** [Ano93d]. **Instruction** [BÖS11, SS83]. **instrumentation** [Ano83]. **Integer** [Ano86, Die96, MV90, MV91b, Woe01, Woe05]. **integers** [BCS89, Han17]. **Integral** [LJF19, Rog19b]. **Integrated** [DGKK12, PG17, NM02b]. **integrating** [ATAKS07]. **Integrative** [LLDZ18]. **Integrity** [CLS12, Sch01b, Sch01a, Wil96]. **Intel** [JHL+15]. **Intellectual** [DGKK12, IEE88a]. **Intelligence** [Kak93, Luh58, ARA94, LLC89]. **Intelligent** [IEE11a, LJW+17]. **intensify** [HL12]. **intensive** [Shi17]. **inter** [Kos14]. **inter-system** [Kos14]. **Interacting** [LLW10]. **Interaction** [ZLY+12, Bor81]. **Interactive** [CBK83, Cer85, CBK85, Dam93, Dam94, Dos78b, GK94, GK95, HR14, KG95, MS09, OVY94a, OVY94b, Rad83, Wee07, RWSN07, RW73, TCW+13, TWL+18, MS09]. **Interconnection** [Fah80]. **Interest** [ACM82, DT87, OSR10]. **interesting** [VNC07]. **Interface** [Vit85, WGM88, Bor81]. **Interfaces** [DCW91]. **interleaved** [RH90]. **Internal** [GL82, GL88, ITP14, LC88, Wil59]. **International** [ACM81, IJW89, PDI91, ACM94b, ACM11, ACM12, AGK+10, ABB93, ABM06, AFK90, ARA94, VLD82, Ano89, Ano93c, AW89, AAC+01, A+90, AiNOW11, AOV+99, AA86, Bai81, BD88, BDS88, BV89, BIP92, Bel00, BBD09b, BJZ94, BRW93, BL88, BF89, Bri92, Bri93, BW92, BD08, BJ93, CGO86, CLM89, Cop95b, DG96, DSS84, DSZ07a, DSZ07b, DJRZ06, DJNR09, FNY92, FMA02, Fra04, Fre90, GMJ90, Gol92, GSW98, HB93, HL91, IEE80a, IEE84, IEE85b, ICD87, IEE88a, IEE88d, ICD88, IEE88b, ICD90, ICD91, ICD93, IEE94a, IEE95, IRM93, JBJ94, JY14, Ker75, Kna89, KLT92, Kui92, LC06, Lak96, Las87, LCK11, Lev95, Lie81, LS89, LT80, LSC91, Lom93, MK89, MSDS90, Mo92b, Nav85, Ng79, Pat90, PSN95, PV85, PK89, QG95, RK89, RNT90, ST83a, ST83b, SP90, Sho05, SW94b]. **International** [SW94a, SC77, Sti93, Sti94c,

Sto92, Vau06, Vid90, WPY90, lWSS91, Yan10, Yao78, Ytr06, YR87, Yu92, Yua92, Yun02, vL94, vdHvH12, ADG+08, AMSM+09, ACJT07, Bir07, CIM+05, Cop95a, Deb03, Gol96, HKNW07, HF13, Wie99, ICD86, IEE11a, Sch82a]. **Internet** [ATAKS07, Ano95d, HLC10, MCF17, McN03, She06, SXLL08, ZNPM16]. **Internet-Draft** [MCF17]. **Internet-scale** [ZNPM16]. **Interpolation** [Buc82, Bur83a, Bur83b, Bur83c, Wu84, FWG18]. **Interpolation-Based** [Buc82, Bur83b, Bur83c, Bur83a]. **interpretation** [Fly92, GvR08]. **Interpreter** [CBA94, Gai82]. **interprocessor** [KK96]. **Interrogating** [HLC10]. **Interrogating-Call** [HLC10]. **Intersection** [PSZ18]. **Interval** [GY91, Lip02, BL89]. **Intractable** [IT93, IH95]. **Intrinsics** [Rog19a]. **Introduction** [AG18, Cob94, DK02, DK15, Fel50, Fox91, Har85, Hua82, KL15, RW97, TS76, TS84]. **Invariance** [SvEB84]. **Invariant** [HSPZ08, LH20, NS16a, Fly92, SB07]. **Inverse** [CPP08, HCF95]. **Inversion** [DK07]. **inversions** [Pat95]. **Inverted** [Les88, HC02, McD77]. **IoT** [Alb21, Cho21, HLL18b, KAS+22, NADY20]. **IoT-Enabled** [Alb21]. **IoVs** [VD21]. **IP** [BLC12, BM01, HDCM09, IGA05, JL14, MPL09, RW07, SXLL08]. **IPSec** [KMM+06]. **IPv4** [PT12b]. **IPv6** [PT12b]. **Ireland** [ABB93]. **iris** [MMG10]. **Irreversible** [ANS97]. **ISA** [HL91]. **ISAAC** [AiNOW11]. **ISCA** [Deb03]. **Island** [Rei88, IEE07]. **ISO/IEC** [ISO04]. **isogenies** [CDS20]. **Isolated** [MMMT09]. **Israel** [Sch82a, BDS88]. **Israeli** [Coh94]. **ISSAC** [ACM94b, Lak96, Lev95, vdHvH12]. **Issued** [LG78]. **Issues** [MP90, LMSF89, LG78, Yu92]. **Italian** [FFPV84]. **Italy** [AAC+01, AA86, ST83a, ST83b, Ano94, De 95, IEE88d, IEE92a]. **Item** [WYD+18]. **items** [Bay73b, CH09]. **Itemsets** [BMLLC+19]. **Iterated** [Jou04, KVK12, HLMW93, HXMW94, KHK10]. **iterations** [OS10]. **Iterative** [MV02, PNPC20, SXL16]. **IV** [Far93, Sil02a]. **IWDM** [BF89].

J [Sar80]. **January** [ACM91d, ACM91a, ACM97a, ACM05, ACM08a, Kar98, Mat09, SP90, Shm00, USE91]. **Japan** [IJW89, A+90, AiNOW11, CGO86, Got83, IEE85b, IRM93, Mo92b, IEE85b, ICD91, LT85]. **Java** [Sun02, CHL07, LBJ02, NM10, OOK+10, SB07, SSS05, Tym96]. **JEqualityGen** [GRF11]. **JERIM** [MJ08]. **JERIM-320** [MJ08]. **Jersey** [Fre90, IEE84]. **Jersey/sponsored** [IEE84]. **Jerusalem** [BDS88, Sch82a]. **Johnson** [SG16]. **Johnson-type** [SG16]. **Join** [Adi88, AT91, BM89, BM90a, CS83a, CHY97, DG85a, DG85b, FP89b, Gra93a, Gra93b, Gra94a, Gra94b, Gra99, HR96, KR91, KKW99, KL87, KNT89, KHT89, KO90, KTN92, LR99, LDM92, LTS90, MLD94, MLxx, MS88a, NKT88, NNA12, NP91, OL91, OL89, Omi89b, OL92, PAPV08, PG95, Pip94, RK91, SD89c, SD89a, SD90b, SD90a, Sha86, SM87, Sol93, Spe92, TR02, TY91, Top92, TP95, Toy93, TNKT92, Val87, WYT93, YNW+09, Yam85, ZG90a, ZG90b, Zel91, ZJM94a, ZJM94b, ZJM94c, ZO93, ALS10, BMS+17, CAGM07, CyWM91, GK05, ISO97, Kha95, KKL+09, LNS11, LEHN02, MMSY94, Mul92, OT89, PCK95, PCV94, RLM87, RG89, SD89d, SM94, SA17, SP89, TL93, UHT95, WL07, NNA12]. **Joining** [NP91]. **Joins** [CLYY92, CLYY95, DG93, DG94, DNSS92, GBC98, Gra86, HCY94, HCY97, LR99, LR96b, NNA12, PCL93a, SC90b, SC90a, SC90c, WDYT91, YCRY93, AKN12, BATÖ13, BLP+14, HLH13, JHL+15, LCRY93, ML95, PCL93b]. **Joint** [IJW89, AFI63, AFI69, MO92a, IEE92a, IEE01, ZC12]. **Jose** [ACM11].

JPEG [ZC12]. **JPEG-2000** [ZC12]. **Jpoin** [Omi91]. **Juan** [IEE91b]. **Judy** [Sil02a]. **July** [IJW89, ACM91c, ACM94b, ACM01, AGK+10, ADG+08, AMSM+09, Ano95c, ACJT07, dBvL80, CIM+05, Coh94, DG96, CTC90, Kui92, Lak96, Lev95, NS82, Oxb86, Pat90, Rei88, vdHvH12]. **June** [ACM84a, ACM03a, ACM07, ACM11, ABM06, BDS88, BV89, BIP92, BRW93, BL88, BF89, FMA02, Fre90, Van10, HF13, IEE05, LL08, LS89, MS05, Ng79, Rei88, Sch82a, Sto92, Vau06, vL94]. **Just** [Yas07]. **JVM** [SV15b].

k-ary [Gui76c]. **Karlsruhe** [HM08]. **Karp** [GBY90]. **Karp-Rabin** [GBY90]. **Katapayadi** [Ram97]. **Katholieke** [BBD09b]. **KD** [KHT89]. **KD-Tree** [KHT89]. **KDL** [PSR90]. **KDL-RAM** [PSR90]. **Keccak** [BDPV09, BDPV12, DDS14, LŁA15, MS13, BDP+12]. **KEM** [CZLC14]. **Kent** [Oxb86]. **Kerkyra** [Rei88]. **Kernel** [CSSP15, Lev00, ZLY+12]. **Key** [ANS97, ANS05, iA91, BD82, Bol79, Boo74, CS83b, CC87, CS87, CC91, CLC92, CTZD11, CY06, CG79, CS02, Dam87, DL12, Dos78a, EAA+16, GG86a, Gri79, GG80, GYW+19, HB89b, HB89a, HM12, IG77, JLL+20, Joh97, KM09, KV09, KR86b, KR86a, LYX+19, LAKW07, LLL+16, LCML94, Lin63, LCM+20, LYD71, Lum73, MZL+19, Men12, MW95, NTY12, PRRR15, QXL+20, RSSD89b, RSSD92, Rob86, RS08, SY11, SR63, SSS05, SDZ21, Sta99, YLSZ19, Yao95, Yub82, ZQSH12, And88, BSNP96b, CCL91, GL06, GBL94, LW04, LND08, LY72, ML94, Men17, NM02b, Oka88, SD85, Sar11, SN19, Shi17, WLC20, ZCZQ19]. **Key-Exposure** [CTZD11]. **key-node** [SN19]. **Key-Recovery** [CY06]. **Key-Sequential** [HB89a, HB89b]. **Key-to-Address** [LYD71, Lum73, SR63, LY72]. **Key-Value** [PRRR15, Shi17]. **Keyed** [Ano95a, BSNP96a, KKRJ07, Gon95, Li95, SV06, FIP02a]. **Keyed-Hash** [KKRJ07, FIP02a]. **Keying** [BCK96a]. **keypoints** [MMG10]. **Keys** [Gon80, Gur73, JC88a, Joh61, KR01, LMJC07, LL87, Oto85a, PB80, Riv76, Riv78, SD78, She78, Yao85a, CFN18, FP82, GMW90, Wan05]. **Keyword** [HWZP18, WWZ09, LMLC14, ZLC+18]. **Keywords** [Coh98]. **Khafre** [BS91c]. **Kinetic** [Rey14]. **Kingdom** [JBJ94, ACM94b]. **KLIPA** [GT63]. **Knapsack** [CP91c, JG95, Pat94]. **Knowledge** [BDS88, BCH87, CLP13, CRdPHF12, Dam93, ISK+93, OVY94b, Dam94, FNY92, OVY94a]. **Known** [SY11]. **Known-Key** [SY11]. **Knoxville** [IEE94c]. **Knuth** [DM90, Ruc15]. **Kobe** [ICD91]. **Kollisionsstrategien** [BI87]. **Kolmogorov** [CG92, Sch01b]. **Komlos** [KM86]. **KPS** [SN19]. **KV** [LCLX19, QXL+20]. **KY** [Rie89]. **Kyoto** [CGO86, Got83, IEE85b, LT85].

L [Sar80]. **Label** [LQH18, ZWY21]. **labeling** [TCW+13, YSL05]. **labels** [LLT21]. **Lam** [Wag00]. **LaMansion** [Nav85]. **lamp** [McN03]. **Landau** [SV06]. **Landmark** [NNA12]. **Landmark-Join** [NNA12]. **Landsat** [MNY81]. **langage** [LG78]. **Language** [Cer81, CKB83b, Dit76, FR69, GHJ+93, GT63, GG86b, Har85, ISK+93, KCB81, LG78, Wil59, BW92, CP95a, CKB83a, Lev89, YIAS89, YMI89]. **Languages** [ACM91d, dBvL80, BRW93, CL83, Cra85, IEE84, Jou85, Kui92, NS82, Pat90, ACM91a, AGK+10, ADG+08, AMSM+09, ACJT07, CIM+05, DTM+18, DLH+79, DL06, GMP95, GJR79, Inc81]. **LAPI** [MS02]. **Laplacian** [ZWCL10]. **Large** [ABB93, VLD82, AW89, AAC+01, AOV+99, BD88, BH85, BCH87, BJZ94, BI12, CKB85, CML+13, CGO86, Chu90, Coh98, DSS84, DS09c, Dos78a, DT91a, DT91b, FM91, Fel87,

FHCD92a, FHMU85, GGY+19, GLLL17, Gra92, Gra93c, Gri74, GSW98, HB89a, HB92, Hil78b, Hil78a, Ker75, KCR11, KRRH84, KK85, Kos14, LM95, Li15, LT80, LSC91, LYD71, MSDS90, MEK+14, MWC12, OGAB14, PAKR93, PV85, ST83a, ST83b, Sha86, SHF+17, SXLL08, Tan83, Win90a, XNS+13, YWH09, Yua92, YGC+12, Zam80, Zem91, ZZLZ21, ZHW21, BZL+15, BT89, CFYT94, FWG18, FES09, FHCD92b, GC95, HB89b, LK93, LY72, MSK96, Shi17, TBC+05, Yao78, YMI89, Zha19a]. **Large-Grained** [PAKR93]. **Large-Scale** [GGY+19, GLLL17, Li15, MEK+14, SHF+17, YGC+12, ZZLZ21, CML+13, Kos14, SXLL08, FES09, Shi17, Zha19a]. **Last** [PM89, KR19]. **Last-Come-First-Served** [PM89]. **Latency** [QXL+20, Sam81, SL16, WY00, KLSV12, LDK12, ZGG05]. **Latency-sensitive** [WY00]. **later** [Roe95]. **Latin** [CHK06, DMPP06, CHK06]. **Lattices** [KV09, LYY+18, LYX+19, GPV08]. **lava** [McN03]. **laws** [AK09]. **Layer** [YSEL09]. **Layered** [Man12, ZC12]. **Layers** [SDMS12, SDMS15]. **Lazy** [AHS92, BJMM94b, BJMM94a, CF92, Hug85, KV91, MV88, VV86, MSV87]. **LCCR** [Cer85]. **LCFS** [PVM97]. **Leakage** [NTY12, ZZM17]. **Leakage-Resilience** [NTY12]. **Leakage-Resilient** [ZZM17]. **lean** [SV15b]. **Learn** [McC79]. **Learned** [WCW+22]. **Learning** [GK94, GK95, KG95, KKC12, KRJ+80, LQH18, LLZ10, Val15, Wan84, BC06, SZO+20]. **Least** [OG94b]. **Lecture** [Dev86]. **LEDA** [MN99]. **Lee** [KCL03]. **Leftover** [DSGKS20]. **Leistungsanalyse** [Kue82a, Kue82b]. **Leitmotiv** [Kah92]. **Lemma** [DSGKS20]. **Lemmas** [GK76]. **Lemmatized** [DS84b]. **Length** [Dit91, Gon81, KLP98, LK94, Lit91, MF92, Men12, Mit73, PHL01, Pea90, Pea91, Sav90, Sav91, ZPS90, ZPS93a, GS94, KL95, LLJ15, Men17, ZPS93b]. **Lengths** [Bra84a, Bra85, Bra86]. **Less** [DH01, GK08, KHK12, LK16]. **Lett** [Pro94]. **Letter** [BMB68, CS85c, CS85b, Cha85, CL86, Cha86a, CW91, CO82b, JC88a, TL95, Tro95, Wan05]. **Letter-Oriented** [CS85c, Cha86a, JC88a, TL95, CL86, CW91, Wan05]. **Leuven** [BBD09b, BW92, PGV93c]. **Level** [CJC+09, ZHW19, BGG12, DAC+13, HL94, Inc81, LDK12, MTB00, SDR83b, TKI99]. **level-set** [BGG12]. **Levelled** [LRY+15]. **leverage** [IEE88a]. **leverage/COMPCON** [IEE88a]. **Lexical** [CRdPHF12, ISHY88]. **lexically** [FF90]. **lexicographic** [BMLLC+19]. **Lexicon** [CKB81, CKB83b, CKB83a]. **Lexicons** [CKB85]. **LFSR** [DS09a, Kra94]. **LFSR-based** [Kra94]. **LH** [LNS93]. **LH*** [LNS96]. **LHlf** [ZL12]. **LHS** [Moh90, Moh93]. **Li** [KCL03]. **libdbh** [Wil14]. **libhashckpt** [FRB11]. **Library** [ÁCZ16, Bee99, Sou92]. **Life** [BCR04]. **light** [ARH+18]. **Lightweight** [AHMNP12, AHMNP13, BDM+12, BKL+11, HKY12, Cho21, GTL21]. **like** [JNPP14, RS14]. **Limited** [GL82, GL88, SS90a, Wen92]. **limitedness** [LP04]. **Limits** [KST99, MMSY94, BVF12]. **Line** [AS82, Bry84, FFGOG07, HO72, IABV15, Leb87, SS83, Tsa96, BBKN12, HHL10, KRRH84, RW73, Tsa94]. **Line-Oriented** [Bry84]. **Line-Rate** [IABV15]. **line/Off** [HHL10]. **Linear** [Ald88, ADM+99, ATT98, Ano95a, AD11, BYSP98, Ban77, BK70, BGS96, BW98, CFP19, Cle84, CL09a, CM93, Dae95, Ell85a, Ell87, FPV98, HB89a, HB92, HH85, HYH93, HTY90, HSW88, Jak85, JV16, Kno88, Knu19, Knu98, Kor08, KD92, Lar80b, Lar80c, Lar82b, Lar82c, Lar82d, Lar85b, Lar85c, Lar88b, Larxx, KKMS10, Lit79b, Lit80, Litxxa, Luc72, Lyo78a, MSSWP90, MY80, Moh90, Moh93, Mul81, Omi88, OGAB14, OT91, OS83a, OA89, OS83b, PPR07, PPR09, PT16, Pet13, PK87, PVM97, RSD84, RSD85, RSSD89a,

RS92, RLH91, Reg82, Rob86, RT87b, SDR83a, SPW90, TW91, TZ12, Toy93, VP96, VP98, WVT90, YD86a, Ald87, ADM+97, BJ07, Bou95, HB89b, HCF95, Jan05, LNS93, MTB00, MMC01, ML94, Omi89a, OP03, OS88, PT10a, RLH90, Sar13, SS16]. **linear** [TMB02, Vio05, ZL12]. **Linear-density** [KD92]. **Linear-Time** [WVT90, Kor08]. **Linearizability** [SDW14]. **Linearization** [BKMP09]. **Linearizing** [Oto88a]. **Lingo** [McC79]. **Linguistics** [Cer83]. **link** [BR75]. **Linked** [Fel87, Pal92, ZLLD18, ZKR08]. **Linking** [Bob75]. **Linkless** [CJC+09]. **links** [EVF06]. **Linux** [USE00a, Lev00, LACJ18]. **Lisbon** [CIM+05]. **Lisp** [LFP82, Hek89, Nam86, FH96, GSI+82]. **Lisp-Based** [FH96]. **List** [McI82, Ter87]. **Lists** [BH86, HK87, LLC89, Lyo79, MY79, Kno84, ST85, SS06]. **literate** [Sab94]. **little** [DMPP06, PES+12]. **Live** [MZD+18]. **Ljubljana** [EF12]. **LLE** [TLZL16]. **Load** [HC13, IK92, KJC11, LRLW89, LRLH91, Omi91, RRS12, RK91, Top92, TP95, WL07, KL08, SX08, TLLL18, WZ12, WTN09, XCCK09]. **load-balanced** [TLLL18]. **Load-balancing** [WL07, XCCK09]. **Loading** [vdP72]. **Local** [MD97, MNY81, MJT+02, PKW09, RT81, SY08, BGG12, EASR22]. **Locality** [BT12b, CSSP15, CKPT19, Chi91, Chi93, Chi94, EFMRK+20, HNKO20, IMRV97, KBG18, Kaw15, MZL+19, MNP08, OWZ14, OTKH11, Pag18, ZHW21, AT18, GDGK20, HAK+16, HFZ+15, HFF+17, LNS11, LWXS18, LJW+17, QZD+18, SP12, STS+13, ZHX+21, SA17]. **Locality-Aware** [HNKO20, MZL+19]. **Locality-Preserving** [Chi91, Chi93, Chi94, IMRV97]. **Locality-Sensitive** [BT12b, OWZ14, Pag18, ZHW21, EFMRK+20, HFZ+15, HFF+17, QZD+18, STS+13, ZHX+21, SA17]. **Localizing** [DD11, DJSN09]. **Locally** [KS88a, Oto88b]. **Locating** [WL12]. **Location** [CCF04, TY03, ZWH17]. **Location-Based** [ZWH17]. **Lock** [AR16, NM10, ZLLD18, AR21, NK16, Pro18, ZL12, SS06]. **Lock-Free** [AR16, ZLLD18, AR21, NK16, Pro18, ZL12, SS06]. **locks** [ALS10]. **Lofthus** [Hel94]. **log** [FHC89]. **logarithm** [Gib91]. **Logarithms** [vW94]. **Logging** [Moh90, Moh93]. **Logic** [AR16, BM87, BAN89, Cra85, IEE84, Las87, dKC94, BW92, DLM07, YIAS89]. **Logical** [CPP08]. **Logs** [SK99]. **LOKI** [BS91c, Knu92]. **London** [Ano93a]. **Long** [Mit12]. **Longest** [DKT06, Gon81, PT12b]. **Look** [CP91b, Sna87, AY14, CP91a]. **look-up** [AY14]. **Lookup** [CN07, HDCM09, Jai89, Jai92a, Jai92b, Jaixx, Pri71, She78, SWTX18, Tro06, YBQZ18, BLC12, HXLX13, Mad80, MSK96, MLP07, MPL09, MA15, PT12b, WTZ+13, WTN07, ZGG05]. **Lookups** [Pan05, BM01, IGA05]. **Loss** [ATS19, FC87b]. **Lossy** [PW08, Wee12]. **Louisiana** [ACM91e, ACM97a]. **Louisville** [Rie89]. **Low** [GI12, HMNB07, HGR07, Les88, LYW+18, PSSC17, QXL+20, TBC+05, ABO+17, BOY11, CZ14, HM03, MA15]. **low-area** [ABO+17, BOY11]. **Low-Cost** [GI12, HMNB07]. **Low-overhead** [HGR07]. **Lower** [DKM+94, GadHW96, Gon77, MNP08, OWZ14, Yao83, DKM+88, DKM+91, Sun91, Sun93]. **lowering** [SSU+13]. **LR** [HC87]. **LSH** [AT18, AÖD19, CKM14, CK15, LCH+14, LJW+17, ZNPM16]. **LSH-Preserving** [CK15]. **Lucifer** [BS91c]. **Luhn** [Ste18]. **Luxembourg** [Bir07]. **LXCloud** [LACJ18]. **LXCloud-CR** [LACJ18]. **Lymphocytic** [ŠSaS01]. **Lyra2** [ASBdS16].

M [Sar80]. **MA** [ACM84a, Ker75, Kil05, CP91b, ACM86a, CP91a]. **MAC** [HLL18a, PV95, PvO95, Pre97a, SRRL98, SRY99, Eug90]. **Machine** [And88, CCJ91, DGG+86, DGS+90b, DGS+90a, GD87, GSI+82, Hsi83, KLadH93,

KLM96, KTMo83a, KTMO83b, KTMo83c, Tan83, EBD91, Vak85, BM90b, KK96, RH92]. **Machine-Independent** [CCJ91]. **Machinery** [DT87]. **Machines** [BF89, adH93, Mey93, SD89b, Sch90b, SD90b, SD90a, TR02, CHS+18]. **MACs** [DL17, GO07, PV95, PvO95, Pre97b, Saa12]. **Made** [Cic80b, PV07]. **Madison** [FMA02]. **Magic** [Hin20, Zha19b]. **Magnetic** [Wri83]. **MAHT** [CRdPHF12]. **Main** [AP93, CE95, CRdPHF12, DKO+84b, DKO+84c, DKO84a, KR91, KL87, KK85, Kum89a, LC86a, SPW90, Sha86, TP95, ZHZ+19, AKN12, AP92, BATÖ13, DKO+84d, JHL+15, Pro94]. **Main-Memory** [KR91, BATÖ13]. **Maintaining** [Woe06b]. **Maintenance** [Buc82, Bur83b, Bur83c, Oto85b, Bur83a]. **Making** [BR97, Cob94, Hel91, LT09, CCA+12]. **Malicious** [AAE+14]. **malleable** [BCFW09]. **Malo** [GQ95, QG95]. **Malware** [ASWD18, LLDZ18, NADY20]. **Management** [ACM75b, ACM81, ACM82, ABM06, BL88, BJ93, BC90, CGLC20, CLM89, DT87, EE86, Flo77, FMA02, GGY+19, GMJ90, Gho77, Gho86, ISK+93, JLL+20, KM09, LC86a, Lie81, McC79, MKF+16, Nav85, SW94b, SC77, Sto92, ZZ83, ZQSH12, DAC+13, FNY92, FRS94, HF13, SW94a, WM93]. **Manager** [Pro89]. **Managing** [WMB94, WMB99, WYT93]. **MANETs** [Alb21, JFDF09]. **Manipulation** [GK76, Ng79, Pon87]. **Manual** [RWSN07, Sil02a, WG94]. **Manuscript** [FLF11]. **Many** [BGF88, CZL12, JWM+18, Lia95, SV18]. **many-body** [JWM+18, Lia95]. **many-core** [CZL12]. **Map** [GRZ93, LFD17, PPS21, Som99, AR21]. **Maple** [PVM97]. **mapped** [SV15b]. **mapper** [YTHC97]. **Mapping** [Oto84, WH83, YD85]. **Mappings** [OS83a, OS83b]. **MapReduce** [LMD+12]. **maps** [HC14, JBWK11, SV18]. **March** [ACM82, ACM83a, ACM83b, ACM85b, ACM86a, ACM88a, ACM89b, ACM89a, ACM91b, AH03, Ano10, Bir07, CHK06, Deb03, IEE88a, IEE11a, JBJ94, RNT90, SM08, TWW77, Ytr06]. **marching** [ZRL+08]. **Marina** [ACM82]. **markerless** [JBWK11]. **Markets** [Mir17]. **Markov** [HL94]. **Marseille** [Ng79]. **marshalling** [LPSW03]. **Maryland** [ACM90, FNY92, Jáj90]. **Marz** [Lut88]. **Mass** [Col93]. **Massachusetts** [BV89, IEE05, MS05]. **Massive** [SMZ18, HAKM15, LRU14, Vit01, XCCK09]. **Massively** [AKN12, Jáj90, MK93, RH92, YLB90, Yen91, CZL12, Fis87]. **Massively-Parallel** [MK93]. **Master** [LYX+19]. **Match** [AU79, Bur75b, Bur76b, Bur76c, Bur78, Bur79, CLD82, Chu90, Jag91, Mor83a, RLT83, RSD85, RSSD90, RSSD92, YD86a, AT18, CC88a, Fal88, Hua85, RSSD89a, RSSD89b, Riv74a, SDR83b, YD86b]. **Matches** [Dav73, PRK98]. **Matching** [iA94, BH85, CFP19, CCH09, CG79, Gri79, Han90, HCKW90, HW08, KSSS86, KR81, KPS92, LLLC17, RH92, RH95, TK07, ASM17, CLS95, CWC10, DKT06, DC94, GBY90, HC14, HW88, ISHY88, KP92, KS89a, Kim99, MHT+13, PT12b, Sch91a, TKT+89, TLLL07, TLLL09, XMLC11]. **Matchings** [CKN18]. **Materialized** [BM89, BM90a]. **materials** [SE89]. **math** [McN03]. **Mathematica** [Jac92]. **Mathematical** [BC39, LG78, LII92, NAK+15, Sed83a, Hil05, GT80, Rov90, Win78]. **Mathematics** [FH96, GKP89, GKP94, GK81, GK82, Knu74]. **mathématique** [LG78]. **Matrices** [ASW07]. **Matrix** [AN96, Atk75, BH90, vdSDW74b, ZWY21, vdSdW74a, BT90, CFYT94, JCC00]. **Matsumoto** [PGV93a, PGV90a, PGV93b]. **Max-Poly** [DSS17]. **maxima** [MI84].

Maximizing [KHK15]. **Maximum** [AHS92, GB10, KV91, MV88, Pet13, CKKK09]. **Maximums** [MNY81]. **maxmin** [AII89]. **May** [ACM75c, ACM75a, ACM76, ACM77b, ACM81, ACM84b, ACM86b, ACM88b, ACM89c, ACM90, ACM91e, ACM94c, ACM96, ACM97b, ACM98, ACM02, ACM08b, ACM12, AFK90, ARA94, Bai81, Bor81, BJ93, Dam90a, Dam91, DT87, De 95, FIP93, GMJ90, GQ95, Hel94, IEE85b, IEE94b, IEE94c, KLT92, Lie81, LT85, Nav85, PGV93c, QG95, Rue93, SW94b, SW94a, Vau06]. **McGill** [CCC89]. **MD** [Fis87, IEE02, PvO95]. **MD-x** [PvO95]. **MD4** [Ano95a, WFLY04]. **MD5** [Ano09b, For09, WFLY04, WZJS10]. **MD6** [BKMP09]. **MDC** [LS15]. **MDC-2** [LS15]. **MDS** [TW07]. **MDx** [PV95, SRRL98]. **MDx-family** [SRRL98]. **MDx-MAC** [PV95]. **Me** [Lan06]. **Mean** [Bra84a, Bra85, Bra86]. **Means** [Bab79]. **measure** [Bac02]. **Measurement** [NS16b, SL16, YGS+19, LMP+08, RW07, ACM94c]. **measurements** [KLSV12]. **Measures** [MY79]. **Mechanism** [DGD02, Kum89a, Cha12, HKL04, JFDF09, SF88]. **Mechanisms** [DF01, Sev74]. **Media** [LWZ+18, CBB05, ZO13]. **media-streaming** [CBB05]. **Median** [HSPZ08, She78]. **Medical** [FHMU85, GPA97]. **Meet** [Sas11]. **Meet-in-the-Middle** [Sas11]. **Meeting** [ACM84a]. **Mega** [TKT+89]. **Mega-access** [TKT+89]. **Mehods** [Du86]. **Mehrfachattribut** [Stu82]. **Mehrfachattribut-zugriffsverfahren** [Stu82]. **Mehrschluesselzugriff** [Fri86]. **Membership** [BM99, DP08, HKLS12, Pag01]. **MemGuard** [CZ14]. **memo** [Hug85]. **memo-functions** [Hug85]. **Mémoires** [Lit77b, Lit79a]. **Memories** [DD15, KHW91a, MNS07, Sha86, vdBGLGL+16, CCHK08, CCA+12, Hui90, KHW91b, Koh80, Lin63, RH90]. **Memory** [AP93, ASBdS16, AGMT11, BLP+14, BC90, CRdPHF12, CCW+17, CadHS00, DG93, DG94, DKO+84b, DKO+84c, DKO84a, DHK+15, DadH92, Dum56, EK93, adH93, HNS84, JP08, JLL+20, JCK+18, KHK15, KU88, KLadH93, KLM96, KR91, KL87, KK85, Kum89a, LC86a, LTS90, LHWL21, LSZ+21, MZL+19, MLxx, Mey93, Omi91, PSSC17, Pan05, PG95, PS12, PGV90b, QXL+20, RSK17, Ros21, RL74, SPW90, SS88b, TR02, TP95, Vit81a, Wil71, Woe06b, Wri83, YBQZ18, ZH18, ZHZ+19, AS09, AKN12, AP92, BATÖ13, BDK16, Bor84, CJMS19, CZ14, DKO+84d, Don91, GLJ11, HDCM11, HKL04, HCW+21, JHL+15, KU86, KFG15, LHWL20, MSZ+20, MBK00, MSS96, PGV93g, Pro94, Shi17, SG72, SV15a, TKT+89, Vit01, WLC20, XLZC14, YIAS89, ZHW01]. **Memory-Contention** [DG93, DG94]. **Memory-Efficient** [YBQZ18, BLP+14, Shi17, XLZC14]. **Memory-hard** [LSZ+21, BDK16]. **mer** [HC14, PNPC20]. **Merge** [Gra94b, Gra99, AKN12]. **Merge-Join** [Gra99]. **merging** [SSU+13]. **Merkle** [Bak09, CDMP05, GB17, LRY+15, Mir01, MFES04]. **Merkle-Damgård** [Mir01]. **Mesh** [CRR18]. **Mesh-to-Mesh** [CRR18]. **Message** [ÁVZ11, BCK96a, BCK96b, EPR99, FIP02a, HK12a, KKRJ07, MRW89, NCFK11, RWSN07, Rog95, Rog99, Sho96, TC83, Tsu92a, Tsu92b, WS03, Yas07, GK12b, Kra95, MS09, Sta99, SV06]. **Metabase** [KP81]. **Metadata** [GGY+19, SWTX18, DAC+13]. **MetaFlow** [SWTX18]. **Metagenomic** [PKSB18, KZ19]. **Method** [AA79b, AA79a, Ari68, Bat75, Bel70, Bel72, Bel83, CS91, CC87, CLC92, CPP08, CLS12, Cic80a, Dos78a, DT75, FNPS79, HD72, JO80, Jae81, Joh61, KR86b, KR86a, KNT89, KO90, KR79, KRJ+80, Lam70, LK84, LPT12, LL86, LL87, Mal77, MNY81, McI63,

Moh90, Moh93, Mul72, NKT88, NI83, PG95, Per73, Ram92, RJK79, RT87b, SD85, Sag84, SG76a, SS62, SR63, SSS05, Spr77, SHRD09, Ven84, WKBA07, Wu85, YD85, Zou85, BGG12, EASR22, HW88, Kan91, Kan93, LP04, MI84, MF82, MFK+06, NH74, Vit80a, WLLG08, Woe06a, Zob70a, Zob70b]. **Methode** [Kar82]. **Méthodes** [Lit77b]. **Methodologie** [Lit77a]. **methodologies** [CE95]. **Methodology** [Hea82, GJM02]. **Methods** [AS16, Bay74, Bla00, Bra84b, CSSP15, CF89a, Eck74b, Fal85b, FC87a, Gri98, HB89a, HB92, Kab87, Lit84, Lum73, MWHC96, ML75, MV02, Pip94, QCH+81, SDKR87, SM87, TK88, CE95, CLS18, GRF11, HB89b, Lev89, Mul92, RAD15]. **Metric** [Bal05, TWZW11]. **Mexico** [ACM75c, ACM75a, VLD82, IEE91a, Gol94]. **MGR** [BDMD19]. **MHT** [GB17]. **Miami** [PDI91, RNT90]. **Michigan** [ACM81, Bai81, Bor81, Lie81, Lie81]. **Miconex** [Ano83]. **Micro** [LHC05, ZZ83]. **Micro-Computer** [ZZ83]. **Micro-payment** [LHC05]. **Microarray** [TGGF10]. **Microblog** [CDW+19]. **Microcomputer** [Mil85]. **Micropayment** [Ngu06]. **Microprocessor** [CBA94, TKT+89]. **Microprocessor-controlled** [CBA94]. **Microprocessors** [DGD02, FAFK21]. **Microsoft** [GBC98]. **Mid** [ACM85a]. **Mid-80** [ACM85a]. **Middle** [Sas11]. **middleware** [ZO13]. **Migration** [MZD+18, HSMB91]. **Milan** [Ano94]. **mill** [BDPV06]. **MIMD** [RG89]. **Min** [DSS17, Ind01, LKI10, CWC10, FPS17, GP08]. **Min-Hash** [LKI10]. **min-hashes** [GP08]. **min-hashing** [CWC10]. **Min-Wise** [Ind01]. **Min/Max** [DSS17]. **Min/Max-Poly** [DSS17]. **MinHash** [HWZP18, KZ19]. **MinHash-Based** [HWZP18]. **Minimal** [BPZ07, BH86, CKB83a, CKB83b, CS83a, Cha84b, Cha84c, CS85c, CS85b, Cha85, CS86, CL86, Cha86b, CC88b, CT12, Cic80a, Cic80b, CO82b, CHM92a, CHM92b, CM93, DH01, Die07, FCDH90, FCDH91, FCH92, FHCD92a, GHK91a, GHK91b, HT01, Irbxx, JO80, Jae81, JD12, KH84, MWCH92, Pag99, PV92, Pes96, Sag84, Sag85a, ST85, TW91, Tro92, Tro95, Win90b, Win90a, BBPV11, FHC89, FHCD92b, HK86, SH92, SH94, TKI99]. **Minimean** [Yao95]. **Minimization** [YY01]. **minimized** [CVR14]. **minimizing** [CCY91]. **Minimum** [BM99]. **Mining** [CL05, CLC06, CT12, HC02, JL14, LRU14, PCY95, PKW09, SK98, YGC+12, HC07, BMLLC+19, Nic17]. **Minneapolis** [SW94b, SW94a]. **Minnesota** [SW94b]. **Minor** [Gri77]. **Minus** [NXB13]. **Minutiae** [JTOT09]. **Minutiae-Based** [JTOT09]. **Minwise** [PT16, DT14, LK11, PT10a]. **Misson** [Ano10]. **Misspelt** [KR79]. **Mitigating** [HRS16]. **Mitigation** [SHF+17]. **Mix** [LT09]. **Mix-Compress-Mix** [LT09]. **Mixed** [LMLC14]. **Mixing** [Cai84, LMPW15]. **MJH** [LS15]. **ML** [Ano92]. **MMIX** [Ruc15]. **MN** [SW94a]. **Mobile** [DF01, KKRJ07, KRJ09b, YY07, Cho21, HKW05, QZD+18, ZC12]. **Modal** [MLHK17, WSZ+16, CJN20, ZWY21, ZLC+20]. **Mode** [PHG12, ZHZ+19, Wan05]. **Model** [BG80, Bat81, BG82, CLP13, GadHW96, IJK13, ISK+93, KSSS86, KCF84, LYX+19, LW88, LT12, NY85, PV19, Ram88a, RH92, RH95, Sev74, VC85, WYD+18, Web72, YLZ20, GvR08, GMP95, HW88, LMSF89, MTB00, Sun91, TMB02]. **Model-Based** [KSSS86, LW88, HW88]. **Modeling** [BY89, LLW10, ACM94c, PCV94]. **Modelisation** [Lit77b]. **Modelle** [Kue82a, Kue82b]. **modelling** [DOP+14]. **Models** [AT91, GHJ+93, HBL+10, Kue82b, SK88]. **Modern** [AG18, FAFK21, Ram97, Ros06, Ros07, She17, Bis12, BMQ98, DLH+79, GK05, KL15, KKL+09]. **Modes** [AR17, LLG12, SY11, Sas11, WPS+12, BDPV14]. **Modified**

[HPC02, KGJG12, Kaw85, KJS17]. **Modula** [Fel88, SW86, SW87, BH86, ST86, Sed93]. **Modula-2** [Fel88, SW86, SW87, BH86, ST86]. **Modula-3** [Sed93]. **Modular** [GSC01, LT09, ISO97, Mei95, Mon19]. **Module** [KRJ09b]. **Modulo** [CC87, CLC92, Gir87, Kak83]. **Modulo-** [Gir87]. **Modulus** [PV92]. **molecular** [IG94]. **Moment** [TZ12]. **Monitoring** [SS83, SLC+07]. **monotone** [BBPV11]. **Monte** [BF83, Rey14]. **Monterey** [Col93]. **Montgomery** [WS03]. **Montréal** [ACM02, CCC89, JY14, Lev95]. **Morphological** [CRdPHF12]. **Moscow** [Ers58b]. **Most** [AT93, AT90, ESRI14]. **Motion** [CBA94, Cli95]. **Motivating** [She06]. **move** [KM10]. **Moving** [Lep98, SR01]. **MPEG4** [KM09]. **MPHF** [Zou85]. **MR** [Pro94, Sar80]. **MRD** [SNBC98, SnC05]. **MS** [JC88b]. **MS-DOS** [JC88b]. **MTAC** [GT80]. **Muenster** [Dit76]. **Multi** [AP93, BATÖ13, BŠH12, BR06, CS83b, CC87, CS87, Cha88, CHY97, CLS12, CJC+09, Coh84, FL08, FLP08, FLP14, GPY94a, GPY94b, HYH89, HYH93, HRS16, KR86b, KR86a, KL87, LÖON01, LRY+15, LCM+20, MTB00, MNY81, Ngu06, PADHY93, RSSD90, SD85, SMZ18, VB00, WSZ+16, YNW+09, YLB90, ZJ09, ZHW21, ZLC+20, AKN12, Ano83, CLL+14, HR93, HL94, KKL+09, LJW+17, Pro94, Sar13, SV18, TL93, Tsa08, XZPG21, XMLC11]. **Multi-Agent** [BŠH12]. **Multi-Attribute** [CS83b, CS87, HYH93, RSSD90, HR93]. **Multi-core** [BATÖ13, AKN12, KKL+09]. **Multi-Dimensional** [HYH89, MNY81, Ngu06, XMLC11]. **Multi-Directory** [PADHY93, AP93, Pro94]. **Multi-Disc** [CC87]. **Multi-Disk** [Cha88]. **Multi-Entry** [YLB90]. **Multi-granular** [CLS12]. **multi-graph** [CLL+14]. **Multi-Index** [GPY94b, GPY94a]. **Multi-Join** [CHY97, TL93]. **Multi-Key** [KR86b, KR86a, SD85]. **Multi-Level** [CJC+09, MTB00, HL94]. **multi-linear** [Sar13]. **multi-maps** [SV18]. **Multi-Modal** [WSZ+16, ZLC+20]. **multi-national** [Ano83]. **Multi-Precision** [LÖON01]. **multi-probe** [LJW+17]. **Multi-Processor** [KL87, YNW+09]. **Multi-Property** [FLP14, FL08, FLP08]. **Multi-Property-Preserving** [BR06]. **Multi-Proxy** [ZJ09]. **Multi-Replica** [LRY+15]. **Multi-Sensor** [ZHW21]. **multi-server** [Tsa08]. **Multi-Stage** [LCM+20]. **Multi-target** [HRS16]. **Multi-Threaded** [VB00]. **Multi-Threading** [SMZ18]. **Multi-Version** [Coh84]. **multi-view** [XZPG21]. **Multiattribute** [CLD82, Fal85a, Fal86, Rot89]. **Multicast** [DPH08, TW07, ATAKS07, CBB05]. **Multicollision** [KHK10, KVK12]. **Multicollisions** [Hal12, Jou04]. **Multicomputer** [BGF88, OL91, OL92]. **Multicomputers** [OL89, TY91, HSMB91]. **Multicore** [WCW+22, CHS+18]. **multidatabase** [DSD95]. **Multidimensional** [Cob94, Hua85, HSW88, KS86, KS87a, KS87b, KS89b, LOY00, Oto84, Oto85a, Oto86, OS83a, OA89, OS83b, Stu85, Toy93, WFT12, IMRV97, LS07b]. **multidisk** [CC88a]. **multigrid** [GZ99]. **multihop** [ADF12]. **Multikey** [DL80, KR88, NHS84, SDKR87, VV84]. **multilabel** [CML+13, LMLC14]. **Multilevel** [BK90, DT91a, DT91b, Gri98, LZL88]. **Multimaps** [AGMT11]. **multimatch** [XLZC14]. **Multimedia** [CJN20, Fox91, HLC10, ISK+93, LQH18, LZ16, RZ90, SSL+18, ZLC+20, ZHC+13]. **multimodal** [MHT+13]. **Multipermutations** [SV94b, SV95]. **Multiple** [Abi12, AS96, BP97, Bol79, CS83b, CC87, CS87, CC91, CLC92, CLYY95, FB87, FP10, GK94, GK95, HDCM09,

HHL10, HWZP18, HCY94, KG95, KKC12, HGH+12, LCML94, LOY00, LLLC17, MK11, MB03, Mit02, RSSD89b, RSSD90, RSSD92, SM87, Tra63, WB87, BM01, CCL91, DH84, DMP09, HKLS12, XCCK09]. **Multiple-Attribute** [GK95, KG95]. **Multiple-Collision** [HHL10]. **Multiple-Key** [Bol79, RSSD89b, RSSD92]. **multiple-set** [HKLS12]. **multiple-valued** [DH84]. **Multiplication** [AN96, GK08, Woe01, Bis12, Woe05]. **multiplications** [LK16]. **Multiprocessor** [DG85a, DG85b, Ger86a, Ger86b, KTN92, MLxx, Omi91, RS92, SD89b, SD89c, SD89a, Sch90b, SD90b, SD90a, TNKT92, ZJM94b, SD89d, ZJM94a, ZJM94c]. **Multiprocessors** [Bor84, LTS90]. **multiqueue** [Has72]. **Multiset** [MSTA17, CP95a]. **multisets** [Büt86, NTW09, RRS07]. **multisignature** [Oka88]. **Multispectral** [DCM18]. **Multiterm** [Bur84, Bur82]. **multithreaded** [GK05]. **Multithreading** [Cro98, MIGA18]. **Multiuser** [ZG90a, ZG90b]. **Multivariate** [AM07, OS10]. **Multivariates** [DY08]. **Multiview** [LWZ+18, SSL+18]. **Munich** [BRW93]. **Münster** [Dit76]. **MuR** [LRY+15]. **MuR-DPA** [LRY+15]. **Mutual** [CJP12, GI12, CJP15, FF90, SPLHCB14].

N [Sar80, FHC89, ISO97]. **n-bit** [ISO97]. **Naehrig** [FT12]. **name** [WTZ+13]. **named** [WTZ+13]. **Names** [ABC+16, Dos78a]. **Nancy** [Jou85]. **Nanowire** [Rey14]. **NASA** [Fis87]. **Nashville** [ACM94c]. **National** [??69, Fis87, Oxb86, Ano83, IEE94b]. **Native** [SFA+19]. **NATO** [Ano95c]. **Natural** [Cer81, CKB83b, Har85, KCB81, LG78, YMI89, CKB83a]. **naturel** [LG78]. **NC** [IEE89]. **NDN** [TKH20]. **NDSS** [Ano10]. **Near** [AI06, AI08, BT89, DD15, LQZH14, GJM02, SB97, Yuv75]. **Near-Associative** [DD15]. **Near-Duplicate** [LQZH14]. **Near-Optimal** [AI06, AI08]. **Near-perfect** [BT89, SB97]. **Nearest** [AEP18, AI06, CL85, KBG18, MW09, PACT09, SY08, AI08, CW93, FH79, HFZ+15, JDW+19, LCH+14, LWWK20, SWQ+14, TYSK10, MKL21]. **nearest-neighbor** [FH79]. **Nearly** [HT01, FP82, MV91a]. **nearly-constant** [MV91a]. **Necessary** [IH95, Rus92, Rus93, Rus95]. **Need** [HR04]. **Negative** [DDF+07, SB95]. **Negatives** [Pag18]. **Neighbor** [AEP18, AI06, CL85, KBG18, MW09, PCM15, PACT09, SY08, AI08, CW93, FH79, GJM02, HFZ+15, JDW+19, LCH+14, LWWK20, SWQ+14, TYSK10, MKL21]. **Neighbor-sensitive** [PCM15]. **Neighborhood** [DHL+94, DHL+02, D+92, SG72, ZLY+13]. **neighbours** [Yuv75]. **Neither** [CP91a, CP91b]. **neophytes** [Gre95]. **Nested** [HBL+10, FK89, MMC01, TMB02]. **netflow** [LDK12]. **Netherlands** [dBvL80, CP87, CP88, vL94, AW89]. **Network** [Ano10, HCJC06, HLC10, JL14, KHK15, MK11, PLKS07, Ven86, WBWV16, YBQZ18, AS09, CVR14, Cho21, DFMR15, Die90, FVS12, KL08, RAL07, TLLL07]. **Networking** [ACM04, LCK11, LZ16, WBWV16, WTZ+13]. **Networks** [CGLC20, DK09, DPH08, Jai89, Jai92a, Jai92b, Jaixx, JLH08, Kak93, Kul84, LDY+16, MJBD11, PLKS07, SV94b, SPSP16, SMS91, TGGF10, XHZ+19, ZQSH12, AK09, ADF12, BCCL10, Cha12, GDGK20, GBL94, LG13, LND08, MLP07, NMQ22, PES+12, SV95, SX08, TBC+05, WHS+07, WWG+18, YG10, ZBB+06, BB07, CT10]. **neuer** [BI87]. **Neural** [Kak93, NMQ22, WWG+18]. **Nevada** [IEE10, AFI69]. **Next** [DCW91, She91, CCA+12, CT10, KKP92]. **Next-Generation** [She91, CCA+12, KKP92]. **Niagara** [AFK90]. **NiceHash** [Nic17]. **NIDS** [KJC11, TK07]. **NIDS/NIPS** [TK07].

Nineteenth [ACM08a, IEE95]. **Ninth** [ACM77b, NS82, ACM77a, ACM97b, Kar98, ICD93, ST83b]. **NIPS** [TK07]. **NIST** [Bou12, RRS06]. **Nixdorf** [adHMR93]. **NJ** [GMJ90]. **NL** [DSS17]. **NMAC** [CY06, RR08]. **NMAC/HMAC** [RR08]. **NMF** [TCY+20]. **NN** [EFMRK+20]. **No** [AKS78, CP91a, KR01, CP91b, GBL94, Pro94, Sar80]. **Node** [YLZ20, LG13, SN19, THS97, WL07]. **Nodes** [BGF88, RAL07]. **Non** [BCFW09, Boo74, FNSS88, KS86, KS87b, LT12, LS96, RWSN07, SD78, SA97, TSY98, ZH18, AY14, Ald87, Ati20, CCA+12, ESRI14, FP82, MSZ+20, MLP07, MP16, PBBO12, Sar15, SXL16, Lut88]. **non-asymptotic** [Ati20]. **Non-biased** [TSY98]. **non-blocking** [PBBO12]. **non-compressing** [MP16]. **non-cryptographic** [AY14, ESRI14]. **Non-expansive** [LS96]. **Non-interactive** [RWSN07]. **non-iterative** [SXL16]. **Non-malleable** [BCFW09]. **Non-oblivious** [FNSS88]. **Non-programmable** [LT12]. **non-random** [FP82]. **non-randomness** [Sar15]. **Non-rigid** [SA97]. **Non-standard** [Lut88]. **Non-Uniform** [KS86, KS87b, Ald87]. **non-uniformly** [MLP07]. **Non-Unique** [Boo74, SD78]. **Non-Volatile** [ZH18, CCA+12, MSZ+20]. **nonchalantly** [Gre95]. **Nonclustered** [Omi89b]. **noncontinuous** [ZO13]. **nondestructive** [AD08]. **Nonlinear** [MLHK17, LC13]. **Nonmalleable** [LP15]. **nonnumeric** [JMH02]. **Nonoblivious** [FNSS92]. **Nonstationary** [WB90]. **NonStop** [Eng94]. **Nonuniform** [Ald88, KS87a, KS89b, PK87]. **nonuniformly** [MPL09]. **Nonvolatile** [ZHZ+19]. **Noordwijkerhout** [dBvL80]. **NOrec** [DSS10]. **Norm** [Aum09, HFF+17]. **Normalization** [RGNMPM12]. **Norway** [Hel94, Ytr06, Ano95c]. **NoSQL** [EH17]. **Nostradamus** [KK06]. **Notary** [Cip93]. **Notation** [FGFK10]. **Note** [Bob75, CC91, Dit91, GIS05, Gei95, Gei96, Gur73, Lit91, Pea91, Sav91, SVCC01, Ull72, Yao80, Bay73b, FH79, Sar80]. **Notes** [Dev86]. **Nothing** [SD89c, SD89a, SRY99, SD89d]. **Nouvelle** [Lit79a]. **Novel** [DCM18, DR11, LYY+18, LYX+19, cLmL07, LCM+20, LSZ+21, NW07, PHG12, YSW+11, YLSZ19, ZZM17, ZYWM20, AR21, HLL18b, LMP+08, ZHX+21]. **November** [ACM87, ACM94a, ACM03b, ACM04, AFI69, FNY92, Gol94, adHMR93, IEE82, IEE88d, IEE89, IEE90, IEE91a, IEE93, IEE02, IRM93, LCK11, PSN95, ST83a, ST83b]. **NP** [FS08]. **Nroff** [Hol87]. **NTRUSign** [ZJ09]. **NTRUSign-Based** [ZJ09]. **Number** [Ano86, Bat75, Dos78a, Gui89, WL12, Aam03, ASW87, BK07a, CP13, HC11, Hua82, KW94, TSY98]. **numbering** [Cli95, DM11, VNC07]. **Numbers** [BJMM94b, BJMM94a, Coh98, HSR+01, OG94a, MFK+06, OS10]. **Numerals** [Hol87]. **NV** [CCA+12]. **NV-Heaps** [CCA+12]. **NY** [ACM12, GSW98, Mat09, IEE80b, IEE88c].

O [FHC89, MMC01, Vit85]. **OBDD** [Woe01, Woe05]. **OBDD-Size** [Woe01, Woe05]. **Object** [BDPSNG97, BP94, EE86, GK94, GK95, Hej89, ISK+93, KG95, KM92, LDM92, MBBS12, PKW09, PW94, SA97, TR02, WPKK94, YWH09, WL12, DMP09, DM11, Fly92, GMP95, GG92, LG96, BM90b]. **Object-Oriented** [BDPSNG97, ISK+93, LDM92, TR02, DMP09, DM11]. **Objects** [Bar97, BS94b, KM92, SR01, BS94c, CCA+12, GP08, TD93]. **Oblivious** [Cha94, GM98, HK12a, PWYZ14, SS88a, CHL07, FNSS88, PWYZ10, SS90b]. **Observations** [Bal96, Sti06]. **obstacles** [HM93]. **obtain** [Vit80a]. **Occupation** [vM39]. **Occurrences** [ZC77]. **Occurring**

[She78]. **OCR** [Wan84]. **Oct** [IEE80b, WS93, War14]. **Oct-Tree** [WS93, War14]. **October** [ACM85a, Ano93a, Ano93c, BD08, CE95, IEE74, IEE76, IEE80a, IEE85a, IEE88c, IEE89, IEE91b, IEE92b, IEE99, IEE06, IEE07, IEE10, IEE11b, IEE13, Jáj90, Lom93, Mo92b, ST83a, ST83b, USE00a]. **Octree** [CJC+09]. **ODBF** [ODB89]. **odyssey** [IEE01]. **off** [CJMS19, GW94, Sar11]. **Off-line** [HHL10]. **Office** [DGM89, FC87a]. **Offline** [GAS+16]. **Offs** [ASBdS16, Blo70]. **offset** [HLL18b]. **OFL** [GMP95]. **OH** [BD08, IEE94b]. **Ohio** [Fis87]. **OHLCAP** [HMNB07]. **Old** [FLF11]. **Omnibus** [GDGK20]. **On-Chip** [MJBD11]. **On-Line** [AS82, FFGOG07, SS83, BBKN12, HHL10, KRRH84, RW73]. **On-line/Off-line** [HHL10]. **Once** [MNS07]. **One** [BCFW09, DGV93, Dit76, GK08, HHR+10, HYLT99, JLH08, HGH+12, LK84, Lar88b, LAKW07, LOZ12, LMD+12, LHC05, LP15, Lyo85, Mer90b, Moh11, OGAB14, PWY+13, Par18, RHM09, Roe94, Rul93, SP91, Sch91a, Sho00a, Tsu92a, Wee07, Win83, Win84, Yas07, YZ00, ZPS90, Zhe90, ZMI91, ZPS93a, CMR98, Gib91, HR07, HL03, IEE92a, KST99, KM10, LW04, Mer90a, MZI98, NY89b, NY89a, Roe95, Sim98, SV18, STS+13, Tsa08, Tsu92b, YL04, ZW05, ZPS93b, HMNB07]. **One-access** [Lar88b]. **One-Hop** [RHM09]. **One-Pass** [LMD+12]. **One-Step** [Dit76]. **One-Time** [LAKW07, Moh11, PWY+13, Par18]. **One-Way** [BCFW09, DGV93, GK08, HHR+10, JLH08, LP15, Roe94, Rul93, Sch91a, Sho00a, Tsu92a, Wee07, Win83, Win84, YZ00, Zhe90, HYLT99, LHC05, ZPS90, ZMI91, ZPS93a, CMR98, HR07, HL03, KST99, LW04, Mer90a, MZI98, NY89b, NY89a, Sim98, Tsa08, Tsu92b, YL04, ZW05, ZPS93b, HMNB07]. **Online** [BBKN01, Dos78b, FXWW17, Ger95, Kue83, Kue84a, Mir17, SI09, TP15, PES+12]. **Online-fehlerbehandlung** [Kue84a]. **Online-fehlererkennung** [Kue83]. **Only** [EH12, MT11, NM10]. **Ontario** [KLT92]. **Open** [AMP15, Bra84a, Bra85, Bra86, Fel87, Gon77, Gon80, Kno71, Kno88, LH03b, LH03a, Mit09, MC86, SS80, NK16, NMX19, TT81, van73]. **Open-Addressing** [Gon77, Gon80]. **Operating** [ACM87]. **Operation** [CLS12, KL87, PHG12, AS89]. **Operationen** [Nee79]. **Operations** [ANS10, Bra84b, Ell83, Ers58a, FAFK21, Gir87, He87, HYH89, HYH93, HY86, HTY90, Kum90, Kut10, MSSWP90, SG76a, Wu85, JMH02, Pro18]. **Opportunistic** [LDK12]. **OPS5** [KS89a]. **Optical** [CF89a, Vit85, CF89b, FWG18]. **OPTIK** [GT16]. **Optimal** [AU79, AI06, Bat80, Bat82, BR94, BBP88, BW98, BMRV02, CC88a, Cha84a, CHM92a, CHM92b, DA93, FC87b, FP89b, HR93, HRB13, Jag91, KK12, KK18, KP92, Kri84, LL92, LCML94, Lip02, MLP07, Men12, Men17, Mor83a, OWZ14, PP08, RR92, Riv76, Riv78, Tro06, Yao85a, Yao85b, Yao95, YCRY93, YSEL09, AI08, GSS01, LCRY93]. **Optimality** [Bol79, CLC92, JP08]. **optimally** [Woe06a]. **Optimierungsfragen** [Wal74]. **Optimistic** [GT16, SDZ21]. **Optimistically** [GLB21, Zuk21]. **Optimization** [AOAAK20, ODB89, AR17, BG92, Kie85, Kim80, MXL+12, Mir17, MWC12, Tv83, XNS+13, YNW+09, Yub82, DJRZ06, DJNR09, Loh89, MP90]. **Optimized** [ARH+18, CVR14, EPR99, MZD+18, ZH18]. **Optimizer** [ML86]. **Optimizing** [DGGL16, DOP+14, LOY00, MBK00, PF88, SW91, SV15b, WL12, TCW+13, WLC20, WTN07]. **Optimum** [VC85, vdP72, vdP73, van73, Vit80a]. **OR-parallel** [Cra85]. **Oracle** [GHR99, LT12]. **Oracles** [Can97]. **Order**

[FCDH90, FCDH91, GG86a, HB92, HM12, HSW88, Oto88a, Ouk83, Rob86, Tam81, AKY13, BMLLC+19, DH84, DLM07, HKKK13, Pri95]. **Order-Preserving** [GG86a, Ouk83]. **Ordered** [AK74, CS83a, Cha84b, Cha84c, CS86, Cha86b, CC88b, MY79, MN90, SH92, SH94, SS06, JMH02]. **Ordering** [Lyo78a, GM79, Sab94]. **Ordinal** [ZZLZ21]. **Ordinal-Preserving** [ZZLZ21]. **Oregon** [IEE93, ACM85b, CLM89]. **Organisation** [Lit77a, Wie87a]. **Organization** [ACM75b, Ano85a, ANT85, Ast80, Buc63, DS84b, Gho77, Gho86, IEE85b, KK85, LK84, LT85, LI80, Lit89, LS89, Lom88, Lom93, Mar75, Mar77, Ols69, QCH+81, RL89, RL74, Tha88, TS85, Wie83, Wu85, BR75, Bat65, IL90, Kou93, RM88, VBW94]. **Organizations** [CF89a, Sch79b, Sch81, Toy86, YD86a]. **Organized** [FLF11]. **Organizing** [HH85, Som99, TY03]. **Orientability** [FP10]. **Orientation** [BH93]. **Oriented** [BDPSNG97, Bry84, CS85c, CS85b, Cha85, Cha86a, CO82b, DCW91, ISK+93, JC88a, Kie85, LDM92, PV92, TL95, TR02, Tro95, CL86, CW91, CW93, CKW93, DMP09, DM11, Wan05]. **Orlando** [ACM91d, ACM91a, Kna89]. **Orleans** [ACM91e, ACM97a, IEE74]. **Orthogonal** [BGS96, LCML94, CCL91, Wil78, Wil85a]. **Oscar** [GDA10]. **OT** [PSZ18]. **Othello** [YBQZ18]. **Other** [PV19, Saa12, Bee83, BDK16]. **OTS** [Hül13]. **outbreak** [FNP09]. **outfit** [Nic17]. **outlier** [GDGK20]. **Output** [Mit12, NIS15, NR12, PHL01, ZPS90, ZPS93a, Sab94, ZPS93b]. **outsourced** [YLC+09]. **Overflow** [Bra84a, Bra85, Bra86, Hop68b, Lar85b, Mul72, Mul81, NY85, Sam76, Sch79a, Tam82, Tor84, Bay73b, CS93a, KD92, Kou93, Ram87, YD86b]. **Overflow-Handling** [Lar85b]. **Overhead** [Les88, HGR07, IKOS08, MA15]. **overheads** [SSU+13]. **Overlapping** [MJT+02]. **Overlay** [PFM+09, GDA10, TBC+05]. **overlays** [GHW07]. **Overview** [PGV92, Ros12, WR97, BFG+95, BDP+12]. **ownership** [DSS10, LWG11]. **Oxford** [ACM94b].

P [Lev89]. **P-any** [Lev89]. **P2P** [HNKO20, NW07]. **PA** [ACM04, ACM89b, ACM89a, KI94]. **Pache** [CGLC20]. **Pacific** [ACM75b]. **Pacifica** [ICD87]. **Package** [SY91]. **Packed** [Lyo78b, DW05, DW07]. **Packet** [CGLC20, KMV10, MJBD11, PT11b, CKKK09, HDCM11, LS07b, XLZC14]. **Packetization** [SMS91]. **packing** [BT90]. **Padded** [HK87]. **Padding** [CLNY06]. **Paderborn** [adHMR93]. **Page** [GRZ93, MZD+18, YT16, BCR10, Wee88]. **Paged** [BC90, RL74]. **Pages** [DMR11]. **Paging** [Bry84, HBL+10]. **Pair** [GSC01, Val15, DHKP97, PW06, TYSK10]. **pairing** [BP18]. **pairing-friendly** [BP18]. **Pairwise** [DL12, ZLY+12]. **Palace** [ACM75b, IEE88d]. **Palm** [IEE11b]. **Palmer** [IEE80a]. **PANAMA** [DC98a, DV07, RVPV02, BDPV09, DC98b]. **Paper** [Cer85, Pro94, SV15a, ZL12]. **Papers** [ACM75c, ACM76, ACM77b, LFP82, LC86b, SC77, ACM79, ACM91d, Bai81, Bor81, GJM02, IEE88a, Ytr06, Bir07, FNY92, JY14]. **Paradeisos** [JWM+18]. **Paradigm** [BM97, CS02]. **paradox** [RK15]. **Parallel** [ACM91c, PDI91, And88, Ano93d, AEMR09, AR17, AT91, BFG+95, BH91, Bis12, BRW93, Bor84, Bur81, CdM89, CdM90, Chi91, Chi94, CT96, DNSS92, DA93, DS97, GST90, GM94, GM98, GI77, Gra94c, GZ99, GC90, HB93, HNS84, HC07, HCY94, HCY97, IG77, Jáj90, KU86, KU88, KR91, KJC11, KR19, KO90, KTN92, LC20, LLLC17, LPP91, LPP92, MD97, MLD94, MV90, MV91b, Mat93, MK89, Mil85, MK93, NM02a, PAKR93, Pap94, PK89, PRM16, PSR90, PW94,

Rag93, Ram89b, RS92, RH92, RC94, RK89, RNT90, RK91, SS01, SD89c, SD89a, SV94a, SPW90, SS88b, SB93, SK98, SA17, TR02, TK85, Top92, TP95, TNKT92, WPY90, WPKK94, WS93, WYT93, Woo89, Wu85, lWSS91, YLB90, Yen91, YB95, ZWH17, ZO93, dKC94, vW94, vdVL12, ALS10]. **parallel** [AKN12, ASA+09, Ati20, CZL12, CyWM91, Cra85, Don91, EASR22, FHL+19, Fis87, GLHL11, HK95, KP92, MV91a, MP90, Mol90a, Mol90b, OT89, PCK95, RLM87, SK88, SD89d, STS+13, TL93, UHT95, War14, adHMR93, KL95]. **parallel-DM** [KL95]. **parallelism** [ASM17, Ged14, MMSY94]. **parallelizable** [MP16]. **Parallelization** [DTM+18]. **Parallelizing** [GK12b, WDYT91]. **Parameter** [CC88b, GB10]. **parameterization** [SS15]. **Parameterized** [SS89b]. **Parameters** [HRB13, HYLT99]. **parazoa** [AMP12]. **PARBASE** [RNT90]. **PARBASE-90** [RNT90]. **Paris** [LS89, Coh94]. **Parities** [Val15]. **Park** [IEE84, IEE89, Jáj90]. **PARLE** [BRW93]. **Parser** [HC87]. **parsing** [Tai79]. **Part** [ANS97, Bor81, ISO97, ISO04, MBBS12, Sed83a, ADG+08, AMSM+09, KMV10, Wil03]. **Part-Graph** [MBBS12]. **Partial** [AU79, Bur75b, Bur76b, Bur76c, Bur78, Bur79, Can97, CLD82, Chu90, CY06, Cor02, Jag91, Lar80b, Lar80c, Lar82b, Lar82c, Lar82d, Larxx, LKI10, Mor83a, PF88, RLT83, RSD85, RSSD89a, RSSD89b, RSSD90, RSSD92, TGGF10, YLZ20, YD86a, CC88a, Fal88, Hua85, Pri95, Riv74a, SDR83b, SNW06, YD86b]. **Partial-Domain** [Cor02]. **Partial-Match** [AU79, Bur75b, Bur76b, Bur78, Bur79, Jag91, RLT83, RSSD90, RSSD92, RSSD89a, RSSD89b, Hua85, Riv74a]. **Partial-Relation** [PF88]. **Partially** [PCL93a, PCL93b]. **particles** [Lia95]. **Partition** [LKI10, LC96, WZ12]. **Partitioned** [Ger86a, LR96a, NKT88, SW91, Ger86b, HKL07, MZK12]. **partitioner** [KKP+17]. **Partitioning** [Bre91, Ged14, PFM+09, SBS16, WBWV16, ZRT91, vM39, CKKK09, CKKW00, EH17, HAK+16, Kim99, LL13, LWWK20, PCK95, SKD15, UHT95, AP11]. **partitions** [DKRT15]. **Partly** [OTKH11]. **PASCAL** [Dit76, Hil88, HS84, Dit76, GBY91, Hej89, Sch76, TA81, TA86]. **Paso** [ACM97b]. **Pass** [LMD+12, OGAB14, YDT83]. **Passbits** [MB03, Bur05]. **Passed** [Gra94b]. **passive** [RW07]. **Password** [ASBdS16, GAS+16, JK11, KV09, LSZ+21, WG00, BSNP96b, BDK16, CJMS19, GL06, KJS17, KCL03, Ku04, KCC05, NMX19, Par18]. **Password-Based** [KV09, BSNP96b, GL06]. **Pastry** [Her07]. **Patch** [BI12, BZL+15]. **PatchTable** [BZL+15]. **Path** [GO15, CVR14, CHL07, VNC07]. **Paths** [Kul84, AAB+92, VNC07]. **Patricia** [KS12]. **Pattern** [iA94, BT94a, BT94b, CG79, Fre90, Gri79, IEE88d, KR81, TK07, CLS95, ISHY88, Kim99, Sch91a, ZO13, YIAS89]. **Pattern-Matching** [KR81]. **Patterns** [BH85, CLC06, HSPZ08, OTKH11, SK98, BCGS16, BCCL10, KRML09]. **pauco** [DMPP06]. **Pay** [LHC05]. **Pay-Word** [LHC05]. **payment** [LHC05]. **PCA** [BLY20]. **PCPs** [FS08]. **PDE** [GZ99]. **PDEs** [Gri98]. **PDF** [Con17]. **Pebbled** [Dev99, CM01]. **Peer** [CCF04, JXY07, KLSY07, KS12, LMSM09, PFM+09, SM02, LMSM12, WHS+07]. **Peer-To-Peer** [PFM+09, CCF04, JXY07, KS12, LMSM09, SM02, LMSM12, WHS+07]. **Peers** [RMB11]. **Pennsylvania** [ACM76, LFP82, ACM96, HB93, IEE92b]. **Pentium** [BGV96, Bosxx]. **Peoples** [Ano83]. **peptides** [MIGA18]. **Per-Flow** [NS16b, SL16, YGS+19, HKL04, LMP+08]. **Perceptual** [DCM18, LC12, MV01, MV02, NS16a, RGNMPM12, SB14, THY+18, WDP+12]. **Perfect** [AN96, AA79b, AA79a, Ari94,

BHIMM12, BBD+82, BBD+86, BS94b, BS94a, BW98, Bla00, Bla95, BPZ07, BT90, BT94a, BT94b, BH86, Bur92, BC90, Cer81, CKB83b, CBK83, Cer85, CKB85, CBK85, Cer87, Cer88, CLD82, CS83a, Cha84b, Cha84c, CS85c, CS85b, Cha85, CS86, CL86, Cha86b, CC88b, CCJ91, CW91, CL05, CLC06, CT12, CJC+09, CRS83b, Cic80a, Cic80b, CO82b, CHK85, CKN18, CHM92a, CHM92b, CM93, CHM97, Dat88, DKM+94, DH01, Die07, DJS80, DHJS83, Duc08, DM11, FM96, FCHD88, FCHD89, FCDH90, FCDH91, FCH92, FHCD92a, FK84, FH15, Get01, GHK91a, GHK91b, HT01, JO80, Jae81, JD12, KH84, KM86, KM88a, KCB81, Kra82, KP94, LR85, LH06, LLLC17, Mai92, MWCH92, MWHC96, Meh82, NRW90, Nil94, OG94a, OG94b, Pag99, PV92, PG95]. **Perfect** [Pes96, RL89, RP91, Ram92, Rog19b, SB95, Sag84, Sag85a, Sch90a, SvEB84, Spr77, Tro92, Tro95, WX01, Win90b, Win90a, Wol84, YDT83, YD84, YD85, AAB+92, AG10, BJ07, BBPV11, BS94c, BT89, CKB81, CKB83a, CK89, CL09b, CLS18, Cze98, DF89, DKM+88, DKM+91, DHW08, FHC89, FHCD92b, GS89, HK86, Han17, HM93, JWM+18, Lia95, LC13, MvT08, Mil95, Mil98, Pag01, RB91, SB97, SS92, ST85, SH92, SH94, SL88, Sil02b, TKI99, XMLC11, WC07]. **Perfectly** [CMR98]. **Performance** [ACM04, AP93, ANS09, BM89, BM90a, Bre91, Bur83c, CL85, CC87, CS87, Chr84, CH94, DGG+86, DR92, DadH92, DS97, Don91, ESRI14, FC87a, Fla81, Fla83a, Flo87, GD87, Gra88, Gra89, Gra93a, Gra93b, Gri74, Hac93, HSMB91, HC13, IEE94c, IG77, KS89a, Kha95, KK96, KTN92, Kue82b, Kum90, Lar80c, Lar81, Lar82a, Lar82b, Lar85c, LCK11, LCLX19, LLL09, LMSF89, Lit84, Lit85, Lom88, LCM+20, LYD71, Lum73, Lyo83, MXL+12, Mac95, ML86, ML94, MY79, Mil85, Mul85, NM02a, NP99, Omi91, Pal92, PB80, Pro94, Ram89b, RZ97, RSSD90, RLH90, RLH91, Roe94, Roe95, RT87b, SD85, SD89c, SD89a, Sch79b, SC90b, SC90a, SC90c, She91, TNKT92, TMB02, Tym96, Vit83, Yen91, YB95, BMQ98, BW89, CAGM07, CF89b, HM03, Kou93, LŁA15]. **performance** [LY72, MRL+19, MA15, RFB97, SK20, SS89a, SD89d, Shi17, Sie89, MKL21, VBW94, Vit80a, WL07, WTN07, XCCK09, Yu18, ZHW19]. **Performances** [Mek83]. **Performed** [Wil71]. **Performing** [FP89b]. **Period** [AC74, Eck74b]. **Periodicity** [HG77]. **Permutation** [DLH09, HSR+01, NIS15, PHG12, Sch01a, CFYT94, DLH13, HK95, KST99, LOZ12, LMPW15]. **Permutation-Based** [NIS15, PHG12, KST99]. **Permutations** [ARH+18, JNPP14, MP12, Wee07, BK88]. **persistence** [NT01]. **Persistent** [HCW+21, KM92, LHWL21, Ros21, ZHW19, CCA+12, LHWL20]. **person** [WWG+18]. **Personal** [Rad83]. **Personalized** [WYD+18]. **Perspective** [ACM85a, CSSP15, Ros21, Wil00, Zuk21, LWXS18, Mit17]. **Pert** [Kul84]. **Pertaining** [Wri83]. **Perugia** [De 95]. **Peter** [Ste18]. **Petersburg** [Vau06]. **Peterson** [Kno88]. **PGV** [BRS02, BRSS10]. **Phase** [DHK+15, PACT09]. **PHash** [Shi17]. **PhD** [HF13]. **Phi** [JHL+15]. **Philadelphia** [ACM89b, ACM89a, ACM96]. **Phoenix** [ACM03b]. **Photomosaic** [US09]. **PHP** [GSL17]. **Phrase** [JD12]. **Phylogenetic** [BT12b]. **Physical** [BG80, Bat81, BG82, DT91b, DGKK12, LSZ+21]. **Picture** [BS94b, BS94c]. **pilfered** [Nic17]. **pipe** [MPST16]. **Pipeline** [PRM16]. **Pipelined** [CLYY92, He87, HCY94, MD05, MS88a, RS92, YCRY93, ISHY88, LCRY93, RLM87, XLZC14]. **pipelines** [AS09, RKLC+11]. **Pipelining** [CLYY95]. **Pittsburgh** [LFP82, ACM04, IEE92b]. **PKC'98** [HPC02, HKKK10]. **PKC98-Hash** [HKKK10]. **PKE** [HLL18a, Zha07]. **PKI** [YY01]. **Place** [Dos78a, IEE84]. **Placement**

[MEK+14, PRRR15, BPT10]. **Plagiarism** [CH12]. **Plains** [IEE88c]. **plane** [AII89]. **Platform** [ADOAH19, LMD+12, LLL+16, Sun02, TCP+17, FNP09, MN99, QZD+18, ZLL+07]. **Platforms** [AS16, NMX19]. **Play** [But17]. **playing** [Zob70a, Zob70b]. **PLILP** [BW92]. **PLOP** [KS88b, KS88c]. **PLOP-Hashing** [KS88c, KS88b]. **PLS** [TGGF10]. **PODS** [HF13, ACM88a, ACM89a]. **PODS'08** [LL08]. **PODS'10** [Van10]. **PODS'13** [HF13]. **Point** [BL89, TK17]. **Pointer** [LDM92, SC90b, SC90a, SC90c, SVCC01]. **Pointer-Based** [SC90b, SC90a, SC90c, LDM92]. **Points** [AT93, Bat80, Bat82, AII89, AT90]. **Poisson** [Pob86, PVM94]. **Poland** [ACJT07, Win78]. **policies** [Jan05]. **Policy** [GGY+19, DG96]. **Politecnica** [CTC90]. **Polling** [LXL+19]. **Polling-Based** [LXL+19]. **Poly** [DSS17]. **polylog** [DLM07]. **Polynomial** [DGMP92, FS82, Saa12, Sag85a, San76, WSSO12, Win90b, Bis12, GPGO16, Kak83]. **Polynomial-Advantage** [WSSO12]. **Polynomials** [DY08, OS10, Sar11]. **PolyR** [KR01]. **Pools** [Woo89]. **POPL** [ACM91a]. **Popular** [CLNY06, RR08]. **Portable** [Hek89, NADY20]. **Portland** [ACM85b, CLM89, IEE85a, IEE93]. **Portugal** [CIM+05]. **positives** [CVR14]. **Post** [BBD09b, MKAA17, SE21, BBD09b, BD08]. **Post-Quantum** [BBD09b, MKAA17, SE21, BD08, BBD09b]. **Postal** [Dos78a]. **poster** [ZL12]. **Postortsnamen** [Dos78a]. **Postprocessing** [RJK79]. **Pour** [Kar82]. **Power** [Dun89a, FP10, HD72, MK11, MMMT09, PT12a, PGV90b, ACP10, Ano93c, DKRT16, GP08, KM10, PT11a, PGV93g, Sch82b]. **powerful** [Tho17]. **PQCrypto** [BD08]. **Pracniques** [Dod82]. **Practical** [AS82, AB17, AG18, BR97, BHH+15, CHK85, DNSS92, DDS14, EMM07, FHCD92b, GIS05, GLLL17, HM96, IP11, LT09, Ram89b, ZZ83, Con17, JG95, LWXS18, Sil02b, SXLL08]. **Practicality** [TT82]. **Practice** [KGJØ18, Mir17, Ram88b, BBPV11, RZ97, Sta06b, Tso15, KKP92]. **Practitioner** [SD76]. **PRAM** [GM91, KLadH93, KLM96, Kel93, Kel96, Lep98]. **Pramanik** [Pro94]. **Pre** [Mit12]. **Pre-image** [Mit12]. **PRECI** [BD82, DNV81]. **precise** [Ati20, DK12]. **Precision** [LÖON01]. **Precomputation** [AS16]. **Predecessor** [KS12]. **Predicate** [Han90, HCKW90, VV84]. **Predicates** [RS92]. **Predictability** [LBJ02]. **Prediction** [TW07, DFMR15]. **Predictive** [DCW91, RT87a]. **Predictors** [DGD02, NI83, TT86]. **predistribution** [LND08, SN19]. **Preemptible** [PCL93a, PCL93b]. **Preferential** [VNC07]. **prefetch** [TKH20]. **prefetching** [CAGM07]. **Prefix** [CLNY06, BGKZ12, BLC12, DKT06, PT10b, PT12b, RRS07, RW07]. **prefix-compressed** [BLC12]. **Prefix-Free** [CLNY06]. **prefix-preserving** [RW07]. **Prefixes** [PT11b]. **Preimage** [ABD+16, HKKK10, Li10, Sas11, WW09, WS13, WFW+12, ZWW+12, MS13]. **preliminary** [CMR98]. **preparing** [ACM91b]. **Preprocessing** [KR01]. **Presence** [RK91, WDYT91]. **Presented** [ACM75c, ACM76, ACM77b, LFP82, DBGV93, ACM79, ACM91d]. **preservation** [DL06]. **Preserve** [Knu77, RS12, Vit81b, Vit82a]. **Preserving** [ADOAH19, BR06, BJL16, BHKN13, BHKN19, CK12, CK15, Chi91, Chi93, Chi94, DHL+94, DHL+02, FL08, FCDH90, FCDH91, GG86a, GZX14, HB92, HSW88, LQH18, Oto88a, Rob86, SHZ+20, Tam81, VD21, ZZLZ21, D+92, IMRV97, Ouk83, QZD+18, RW07, SG72, Zha19a]. **pretty** [Tho00]. **Prevention** [JLH08]. **PRF** [AB12]. **primary** [ML94]. **Prime** [Bat75, HM12, Mue04, OG94a, WS03, Lar84]. **Primes** [Die96, ACP10]. **Primitive**

[Kil01, Mue04]. **Primitives** [LYDA19, MP16, RAL07]. **Principal** [Cha88, MW09, SA97, US09]. **Principle** [Dam90b, FDL86, Gib90]. **Principles** [ACM82, ACM83a, ACM83b, ACM85b, ACM86a, ACM87, ACM88a, ACM89b, ACM89a, ACM91d, ACM91a, DK02, DK15, Van10, HF13, LL08, Pre94a, Ull82, Wal88, Zhe90, KKP92, Sta06b]. **Print** [Cip93]. **Priority** [AFK83, AFK84, RT87b, GJM02]. **Privacy** [ADOAH19, Ano95d, BJL16, BBR88, GZX14, KAS+22, VD21, ZXL19, Cho21, QZD+18]. **Privacy-Preserving** [ADOAH19, BJL16, GZX14, QZD+18]. **Private** [PSZ18]. **Probabilistic** [Bla00, BK07b, Fla83b, FM85, Pit87, Sch91a, Tsa96, WVT90, Yao83, CMR98, SD95]. **Probabilities** [Ald88, PRK98, vM39, Ald87]. **Probability** [Fel50, Gon80, LL83, NY85, Ram88a, ZZLZ21, MV91a, NN90, Nil94, Ram87, Sar11]. **Probe** [AA79b, AA79a, Gon81, OT91, Spr77, LJW+17, Mil99, Pag01, SS88a, SS90b, Sun93]. **Probes** [Lyo85, Ros06, Ros07]. **Probing** [Ald88, BBS90, Cle84, FPV98, JV16, Knu98, Lar85b, Lyo78a, MY80, PPR09, PT16, Pet13, PK87, PVM97, PV19, SL16, TZ12, VP96, VP98, Ald87, Jan05, LJW+17, PPR07, PT10a, Ram89a, Vio05]. **Problem** [DSS17, DM90, GB10, HP63, Hop68b, Mit73, NAK+15, Val15, BC06, DHKP97, HCF95, LP04, Loh89, Mon19, Sun91, Sun93]. **problem-based** [BC06]. **Problems** [DJRZ06, FHMU85, Yub82, ZO93, AMP15, CP95a, CO82a, JWM+18, WZ12]. **Proceedings** [ACM84a, ACM88a, ACM89a, ACM91a, ACM94b, ACM04, ACM12, Ano85a, ODB89, AW89, Bar83, BV89, BRW93, BL88, CRS83a, CGO86, DSS84, Gil77, Got83, ICD87, CTC90, IEE02, Jáj90, Jou85, KLT92, Lak96, LCK11, Lev95, LSC91, Ros74, WGM88, YR87, Yua92, vdHvH12, ACM81, ACM91b, ACM07, ACM08b, ADG+08, AMSM+09, Ano83, AA86, Deb03, Fis87, Van10, HL91, HF13, IEE01, Jen76, Mo92b, SM12, USE90, Win78, Wol93b, ACM94d, ??69, ACM75a, ACM79, ACM82, ACM83a, ACM83b, ACM84b, ACM85b, ACM85a, ACM86b, ACM86a, ACM87, ACM88b, ACM89b, IJW89, ACM89c, SDA90, ACM90, PDI91, SDA91, ACM91e, ACM96, ACM97a, ACM97b, ACM98, ACM01, ACM02, ACM03a, ACM05, ACM08a, ACM11, AFI63, ABB93, ABM06, AH03, Ano92, AAC+01, A+90, AiNOW11, AOV+99, BD88, BDS88, BIP92, BF89, Bor81, Bri92, Bri93, BD08, BJ93, CP87, CLM89]. **Proceedings** [Col93, CHK06, Dav91, DT87, DSZ07a, DSZ07b, EF12, Fei91, FMA02, Fra04, Fre90, GMJ90, Gol94, GSW98, HB93, Hel94, IEE80a, IEE85b, ICD88, ICD90, IEE90, IEE91b, IEE91a, ICD91, IEE92b, IEE92a, ICD93, IEE93, IEE94c, IEE95, IEE01, IEE05, IEE07, IEE10, IEE11b, IEE13, IRM93, Joy03, Kar98, Ker75, Kna89, Kui92, LC06, Las87, LL08, LT85, LS89, Lom93, Mat09, MK89, MV91c, MS05, Nav85, Oxb86, Pat90, PK89, QV89, RRR99, RK89, Rov90, Rue93, ACM77a, SZ93, Shm00, SW94b, SC77, Sti93, Sti94c, Sto92, USE91, USE00a, USE00b, Vau06, Vid90, WPY90, lWSS91, Yan10, Yun02, AGK+10, AFK90, ACJT07, Bel00, BJZ94, Boy95b, Bra90, BW92, CIM+05, CP88, Cop95b, Dam90a, Dam91, DJRZ06, DJNR09, FS09, Gol96, HM08, adHMR93, HKNW07, IEE11a, JBJ94, Kil05]. **proceedings** [Lut88, QV90, QG95, Rei88, SP90, Sho05, SM08, Wie99, vL94]. **Proceedings/Ninth** [ICD93]. **Proceedings/Seventh** [ICD91]. **Proceedings/Third** [ICD87]. **Process** [FS82, Pro94]. **Processes** [WB90]. **Processing** [APV07, BG92, CCW+17, Dan13, Eld84, GST90, Ger86a, Ger86b, Gil77, GSL17, Gra92, Gra94c, HB93, Har85, HCJC06, IABV15, KMV10, LLLC17, LC96,

MK89, MS88a, Omi89b, PAPV08, Pip94, PK89, RK89, Sac86, Sch90b, SD90b, SD90a, Sha86, Sol93, SPB88, Spe92, Tha88, Toy86, WPY90, lWSS91, YkWY83, BZZ12, Bra88, CP95a, CKKW00, Ged14, GC90, HLH13, Kan91, Kan93, LLC89, RAD15, Ros74, Sab94, SK88, SP89, WLLG08, YMI89, Yu92]. **Processor** [Adi88, KL87, SM87, YCRY93, ISH+91, LCRY93, TLLL07, YNW+09]. **Processors** [Pap94, Ros06, Ros07, Wil59, JHL+15, KL08, KW94, TLLL09, YIAS89]. **Producing** [DV07, RVPV02, Win83]. **Product** [Du86, YGC+12, OS14]. **Productive** [Bor81]. **Profile** [SSU+13]. **Profile-guided** [SSU+13]. **profiling** [VNC07]. **Program** [Hil88, Kru84, Mai83, Mai92, Meh82, SS80, BZZ12]. **Programmable** [HM12, HK12b, CFN18, LT12]. **Programmer** [Cro98]. **Programmiersprache** [Dit76]. **Programming** [LFP82, ACM91d, dBvL80, BM87, BGS96, Dit76, Dun89a, Ers58a, Ers58b, GG86b, Har71b, Har73, IEE84, Jou85, Knu73, Knu75, Kui92, LII92, Mau68, NS82, Pat90, Ruc15, SSS05, dKC94, ACM91a, AGK+10, ADG+08, ALS10, AMSM+09, ACJT07, BW92, CIM+05, DLH+79, Er86, Sab94, TMW10, YIAS89, BW92, Las87]. **Programs** [AR16, Hea72, PAKR93, SS88b, Ers58b, FDL86, MP90, NMS+08]. **Progress** [Wol93b, Wol93a]. **progressive** [XMLC11]. **Progressively** [DVS+14]. **Project** [DGS+90b, DGS+90a, Tro92, NM02b]. **Projecting** [AT93, AT90]. **Projection** [Bur78, SPW90, AS89]. **Projective** [ACP09, HK12a, KV09, Wee12, FH15]. **PROLOG** [CJ86, Bor84, Coh84]. **Proof** [Ano09b, CZLC12a, CZLC14, Cor02, LYY+18, LYX+19, LT12, SDW14, ZZM17, DLM07, HLL18a, ZCZQ19, ZYWM20]. **proofing** [CHL07]. **Proofs** [CZLC12b, CS02, KK12, KK18, NTY12, WG00, Wee11, Li10]. **Propagation** [DSSW90a, CML+13, DSSW90b]. **Properties** [Bal05, Bol79, CS83b, CLC92, Lit85, RS12, TS85, WS76, ZMI91, GW94]. **Property** [BR06, DGKK12, FLP14, Rja12, SRY99, Ter87, FL08, FLP08]. **proposal** [LLJ15]. **Proposed** [CP91c, HPC02]. **protected** [AGBR19]. **Protecting** [LMJC07]. **Protection** [DF01, DGKK12, SP21]. **Protein** [LLW10, ZLY+12]. **Protein-Protein** [ZLY+12]. **Protocol** [Ano95a, BT12a, Dam93, GI12, HMNB07, HCPLSB12, HLC10, JRPK07, JK11, OVY94b, TY03, VD21, YLSZ19, CJP15, Dam94, GB17, LW04, OVY94a, SPLHCB14, CJP12, JL14]. **Protocols** [LLL09, SDK91, KLL+97]. **Provable** [ANS09]. **Provably** [BCGS16, DY90, DY91, GTL21, HM96, JP07, LM95, Sho96, IN89, SXL16]. **Provably-Secure** [DY90, DY91, HM96]. **Provide** [Sch01b]. **Providence** [IEE07]. **Proving** [Kil01, WS76]. **proxies** [TC04]. **Proximity** [MPP14, SX08]. **Proxy** [ZJ09]. **Pruning** [CT12, MD97, HC02]. **Pseudo** [DW83a, FLF11, WFW+12, dW83b, MFK+06, PVCQ08, TSY98, WS13]. **Pseudo-Associative** [DW83a, dW83b]. **pseudo-collision** [WS13]. **pseudo-random** [MFK+06]. **pseudo-randomness** [PVCQ08]. **Pseudo-structural** [FLF11]. **Pseudochaining** [HP78]. **pseudoentropy** [VZ12]. **Pseudorandom** [BK12, NAK+15, OS10, SP91, Aam03, CP13, VZ12]. **PUB** [Nat95, FIP93, NIS93]. **Public** [ANS97, ANS05, BBR88, CLP13, Cip93, CS02, Dam87, HR04, LYX+19, LRY+15, NTY12, ZCZQ19, CFN18, LW17, Oka88]. **Public-Coin** [CLP13]. **Public-Key** [CS02, NTY12, Oka88]. **Publication** [Nat92]. **publish** [MJ14]. **publish/subscribe** [MJ14]. **Puerto** [IEE91b]. **purely** [SV18]. **Purpose** [Chi91, Chi94, Sch91a]. **Put** [WLC20].

putting [Col93]. **pyramid** [MHT+13].

QC [JY14]. **Quadratic** [Ack74, AC74, Bat75, Bel70, Bel72, Bel83, BI87, Bur75a, Day70, Eck74b, HD72, Lam70, Rad70, NH74, Pri95]. **quadratischen** [BI87]. **Quality** [THY+18, YWH09, GW94]. **quality-size** [GW94]. **Quantification** [GC95]. **Quantile** [KS87b, KS89b]. **Quantitative** [Hea82, LLT21]. **quantities** [Bee83]. **Quantization** [YWH09, YGC+12]. **Quantum** [BBD09b, BHT97, BHT98, MKAA17, SE21, BD08, BBD09b]. **Quark** [AHMNP12, AHMNP13]. **Quasi** [Cze98, LLW10, MD05]. **Quasi-Bicliques** [LLW10]. **Quasi-perfect** [Cze98]. **Quasi-Pipelined** [MD05]. **Quaternary** [KP96]. **Québec** [ACM02]. **Queensland** [SZ93]. **Queries** [APV07, Bur75b, CLD82, Cha84a, CHY97, DHL+94, DHL+02, GST90, GYW+19, KS12, LCML94, LOY00, LLG+17, LB07, ML86, MPP14, PAPV08, PF88, SD90b, SD90a, SW91, Sol93, Stu85, BZL+15, DH84, Fal88, HYKS08, HAKM15, HAK+16, HR93, HF91, Hua85, LL13, MBKS07, SWQ+14, TL93, Wil78, Wil85a]. **Query** [ODB89, BG92, FB87, Ger86a, Ger86b, Gra92, Gra93c, Gra94c, HLC10, HFZ+15, HFF+17, Kie85, Kim80, LC96, MS88a, Sac86, SD89b, Sch90b, Spe92, TS85, Toy86, CCY91, CKKW00, DSD95, GMP95, LYJ+13, LMLC14, Loh89, RAD15, SP89, WLLG08, YLC+09, Yu92]. **query-adaptive** [LYJ+13]. **Query-aware** [HFZ+15, HFF+17]. **Querying** [CN07, LÖON01, TT10, AK09, NDMR08]. **Questions** [Mit09]. **Queue** [KV91, MV88, KM07]. **queueing** [MSV87]. **Queues** [AFK83, AFK84, Woo89, GJM02]. **quick** [FDL86]. **QuikFind** [Cha91]. **Quotient** [BK70, Bel70, Bel72, Bel83, Bur75a, Lam70].

r [KKT91, LJF19, WYW14]. **R*** [ML86]. **r-th** [KKT91]. **Rabin** [FH79, GBY90]. **race** [Hil05]. **radio** [CJP12, CJP15]. **radio-frequency** [CJP12, CJP15]. **RadioGatún** [BDPV06, BDPV09, BF08]. **Radisson** [ACM85a]. **Radix** [FB87, Lin63, SKD15]. **Radon** [GH07, RGNMPM12]. **Ragged** [Ros77]. **RAM** [PSR90]. **RAMA** [MK93]. **Ramanujan** [SV06]. **RANDOM** [DJRZ06, DJNR09, AD85, Ano86, BH90, BM76, BBS90, Can97, Cha84a, Cla77, Dev99, Die96, Dum56, EAA+16, FP10, FMM09, FMM11, GHR99, Gui89, HSR+01, JTOT09, KLSY07, KM88b, LT12, MY79, Mil95, MEK+14, ORX90, Ols69, Ore83, Pet57, PV19, Sie04, Tra63, Yao91, de 69, BR75, BK07a, BK88, CM01, DW03, FP82, GW94, HC11, JCC00, KLL+97, Kut06, Lin63, MYS12, MFK+06, Ram89a, TSY98, WL07, ZGG05]. **Random-Access** [MY79, Pet57, Tra63]. **Random-Walk** [FMM09, FMM11]. **Randomization** [GSB94, DJRZ06, DJNR09]. **Randomize** [GK12a]. **Randomize-Hash-then-Sign** [GK12a]. **Randomized** [AEP18, KR81, LQZH14, Mat93, YWH09, DHKP97, MSS96]. **randomly** [RH90]. **Randomness** [AY14, Knu77, Vit81b, LW17, PVCQ08, Sar15, SS90a, Vit82a]. **Range** [ACM85a, LCML94, LB07, CCL91, Fal88, HR93, Wil85a]. **Rank** [TC93]. **Ranking** [LR96a]. **RANs** [SZO+20]. **RANSAC** [FWG18]. **Rapid** [CG79, Dum56, Gri79, LG96, PT11b, WKO78]. **Rapidly** [Dav73]. **Rate** [CJKK19, IABV15, KL95, HKL04]. **Raton** [HB93]. **raw** [CXLK19]. **Ray** [ACM82, SS89b, ZRL+08]. **RBIBDs** [Woe06a]. **RC4** [IP08, RS14, Sar15, YZ16]. **RC4-Hash** [IP08]. **RC4-like** [RS14]. **RC4A** [Sar15]. **Rdbm** [Pei82, Pet83]. **Rdbm-verwaltungsdaten** [Pei82]. **RDF** [AÖD19, HAKM15, LL13]. **RDMA** [CCW+17]. **re** [Par18, WWG+18]. **re-identification** [WWG+18].

re-registration [Par18]. **Reactive** [BT12a]. **Read** [MT11, NM10]. **Read-Only** [MT11, NM10]. **Reading** [LYDA19]. **Readings** [Sto88]. **Real** [ASA+09, Ano96, DadH90, Dre17c, FVS12, LHWL21, Lyo83, Man12, NS16b, PSSC17, Ros21, ZRL+08, AY14]. **Real-Time** [Lyo83, NS16b, PSSC17, ASA+09, FVS12, Man12, ZRL+08, AY14]. **Realizing** [Can97, PBDD95, Rul93]. **Reallocation** [Bay73c]. **Reasoning** [BJM14]. **Reassignment** [DDMM05]. **Rebound** [KNR10, MRST10]. **Rechenanlage** [Dit76]. **Reciprocal** [CS85a, Cha86a, Jae81]. **Recognition** [BM90b, CFP19, Fre90, GK94, GK95, IEE88d, KG95, KR79, KRJ+80, KRRH84, LW88, PW94, ŠSaS01, SR89, SA97, WPKK94, Fly92, GG92, LG96]. **Recognized** [RJK79]. **Recommendation** [BK07a, WYD+18, QZD+18]. **Reconfigurable** [PJBM90]. **Reconstruction** [BT12b, Tv83, Ven84]. **Record** [ACM75c, ACM76, ACM77b, LFP82, KS86, KS87a, KS87b, ACM91d]. **Records** [Bra84a, Bra85, Bra86, MF92, Ols69, Rém92, SD78, DSS10]. **Recovering** [JCK+18]. **Recovery** [AS82, CY06, Moh90, Moh93]. **recreations** [BC39]. **Recurrence** [MC89]. **recursion** [FF90]. **Recursive** [Coh97, DM81, Gra93b, RSD84, RSD85, RS92, SDMS12, SDMS15, ATAKS07, CL09b]. **Recyclable** [NS16b]. **Redesigning** [AZ10]. **REDOC** [BS91c]. **REDOC-II** [BS91c]. **Reduce** [CKW09]. **Reduced** [AD11, BM97, BCJ15, DDS14, HSR+01, HKKK10, KNR10, MRST10, MNS12, THY+18, WFW+12, ZWW+12, AKY13, CV05, ITP14, MS13, WS13]. **Reduced-Reference** [THY+18]. **Reduced-Round** [AD11, CV05, ITP14]. **Reducing** [Bre73, CJKK19, Dod82, DSD95, Kab87, Mal77, NI83]. **Reduction** [Bla95, Ken73, LT12, MT16, PL21]. **Reduction-Centric** [LT12]. **Reductions** [BHKN13, BHKN19]. **Reducts** [Wan14]. **Reduits** [Kar82]. **Redundancy** [Bur79, CJKK19, CQW08, FES09, MSS96]. **Redundant** [KR79, KRJ+80, RJK79, Som99]. **Reference** [THY+18]. **refined** [DVS+14]. **refinement** [CKW93, ZDI+15]. **Refresh** [CJKK19]. **Region** [FB87, OSR10, KHH89]. **Regions** [JCK+18]. **Registration** [GPA97, JBWK11, Par18]. **Regression** [OGAB14, TGGF10]. **Regular** [CKW09, CH94, IIL17, MSP12]. **regularization** [LLT21]. **Regularized** [TGGF10]. **Rehashable** [LBJ02]. **Rehashed** [Bin96, Kno88]. **Rehashing** [Kel93, Kel96, Mad80]. **reinforcement** [SZO+20]. **Related** [Eck74b, Mit09, BSU12, GJM02]. **Relation** [Knu74, PF88, de 69, GC90, MC89]. **Relational** [Bab79, Bra84b, FP89b, Fro82, Gra88, Gra89, He87, Heu87, IH83, KR86b, KR86a, KP81, Kim80, KTMO83b, KTMo83c, MS88a, PF88, Wu85, Yam85, YNKM89, AS89, EBD91, ISH+91, KR88, SP89]. **Relationalen** [Nee79, Pet83]. **Relations** [KHT89, NP91, SW91, PCK95, UHT95]. **relationship** [LMSF89]. **relationships** [LC13]. **Relative** [GB17]. **relatively** [HF91]. **relativistic** [TMW10]. **RelaxDHT** [LMSM12]. **Reliability** [MS12, CZ14]. **Reliable** [BH91, DGMP92, MKASJ18, RHM09, DHKP97, ZLL+07, ZC12]. **Reliably** [TCP+17]. **relieving** [KLL+97]. **Remaps** [CRR18]. **Remark** [MRW89, Eck74a]. **Remote** [LC95, YY07, HL12, LLH02]. **Removal** [Leb87]. **Rendering** [War86, ZRL+08]. **Rendezvous** [EH17]. **Reorganisation** [Bat80]. **Reorganization** [Bat82, Reg82, Szy82, Szy85, SI09]. **Reorganizing** [JCK+18]. **Repair** [Bar97, CJKK19, BRM10]. **Repairing**

[ZJ09]. **Repeated** [Lar80a]. **Repetitions** [YGC+12]. **Replacement** [Jak85, JCK+18]. **replay** [BRM10]. **Replica** [CCF04, LRY+15]. **Replicated** [SDZ21]. **Replication** [HNKO20, LMSM09, LMSM12, UIY10, WY02]. **replication-based** [UIY10]. **Report** [jCPB+12, MO92a, TSP+11]. **reporting** [YG10]. **Repository** [XNS+13]. **Represent** [Rém92]. **Representation** [ANS10, CD84b, DCW91, BL89, BT93, JCC00, MHT+13, TK17]. **Representations** [DHT+19, KKC12, SD89b, CRS83b, CFYT94]. **representing** [LK93]. **reprinted** [LT80]. **Reprogramming** [PLKS07]. **Republic** [Ano83, HL91]. **Reputable** [RMB11]. **Requests** [LLL+16]. **Required** [PT16, PT10a]. **Requirements** [BD92, NSW09]. **Rescue** [YY01]. **Research** [BV89, BIP92, IEE89, cLmL07, Rad70, SVCC01, Vid90, Wol93b, CE95, Wol93a, Yu92, YR87]. **Researcher** [GCMG15]. **Researchers** [Con17]. **Reserved** [ST86, Tro06, Wol84, Zou85, ST85]. **Residue** [Ari68, KKT91, Mue04, Rad70]. **Resilience** [NTY12]. **Resilient** [ASWD18, BGS96, LMSM09, WTN09, ZZM17, LMSM12]. **Resistance** [Mit12, BF08, MSP12]. **Resistant** [BR97, BK12, CHKO08, IKO05, PGV90b, CHKO12, KHK12, PGV91, PGV93g, MS09]. **resisting** [SXL16]. **Resizable** [Boy98]. **resizing** [ZHW19]. **Resolution** [Ask05, CadHS00, MC86, YB95, KdlT89]. **Resort** [PDI91, IEE88b]. **Resource** [DB12, HM19, TL93]. **response** [DSD95]. **Responsible** [IH83]. **Responsive** [DG93, DG94]. **Responsiveness** [BDS88, Sch82a]. **Restart** [LACJ18]. **Restklassenhash** [Eck74a]. **Results** [ANS09, Bur83c, DR06, DRS12, Jv86, RR08, CV05, LY72]. **RETCON** [BRM10]. **Retention** [CJKK19, ZLL+07]. **Retrieval** [AU79, ANT85, BV89, BIP92, BI12, Bre73, Bur76b, Bur76c, Bur77, Cha84a, CJN20, CJP12, CF89b, Chu90, DS84b, DP08, DHT+19, DSSW90a, DGM89, FH69, FCDH90, FCDH91, FBY92, GPY94b, Irbxx, Kab87, Kno71, LK84, Lar88b, LQH18, Mal77, MH00, Mor83a, NI83, OT91, RLT83, RSD85, RSSD89a, RSSD89b, RSSD90, RSSD92, Riv74b, RT87b, SHZ+20, TS85, Vid90, WH83, Wil79, WKO78, YDT83, YWH09, YR87, YTJ06, YD86a, ZWH17, ZWY21, ZZLZ21, ZLC+20, Bur76a, CCL91, CJP15, DSSW90b, Gob75, GPY94a, LYJ+13, ML94, RT89, Riv74a, SDR83b, WC94, XZPG21, YD86b, Zha19a, ZZLZ18]. **retrieve** [SG72]. **Retrieving** [AA79b, AA79a, Spr77]. **Return** [Wil96]. **Reusing** [ZHS94]. **Revelation** [VD21]. **Reversible** [DR11, SLC+07]. **Revised** [SZO+20, Ytr06, BK07a, Bir07, JY14]. **Revisited** [AHS92, BYSP98, CDMP05, FLP08, GLS91, GLS94, HR96, HK87, KK12, KK18, KVK12, AN20, BATÖ13, Ham02, KKL+09, LP04]. **Revisiting** [DHK+15, HLH13, Yu18]. **Revocation** [Wee11, MFES04]. **Reykjavik** [ADG+08]. **RFID** [CJP15, CJP12, FW09, GI12, GLLL17, HCPLSB12, JRPK07, LLL09, LLG+17, LXL+19, LCL+20, SPLHCB14]. **RFIDs** [LYDA19]. **Rhode** [IEE07]. **Rhodes** [AMSM+09]. **Rich** [GYW+19]. **Richelot** [CDS20]. **Rico** [IEE91b]. **riding** [BB07]. **riding-aware** [BB07]. **Right** [CLYY92, CLYY95]. **Right-Deep** [CLYY92, CLYY95]. **rigid** [SA97]. **Rigorous** [GLLL17]. **RIMS** [Got83]. **Rinda** [ISH+91]. **Ring** [DSGKS20, GGY+19, OL89, TY91]. **Ring-Based** [GGY+19]. **Rings** [HJ96]. **RIPEMD** [BDP97, LP16, MNS12, PBD97, WFLY04, WW09]. **RIPEMD-128** [LP16, MNS12]. **RIPEMD-160** [BDP97, PBD97]. **ripple** [LEHN02]. **risks** [DS09b]. **RITS** [GB17]. **RKA** [HLL18a]. **RNA** [BDD+10]. **Road** [BDPV09, HR04]. **Robin**

[CLM85, Cel86, CLM86, DMV04, PV19]. **Robust** [BFMP11, CJN20, FLP08, FLP14, KMW08, KMW10, KO90, Li15, LDY+16, MMG10, MV01, MV02, OCDG11, TLZL16, WDP+12, CWC10, EAA+16, YCJ12]. **Rockefeller** [IEE90]. **Roma** [AAC+01]. **Roman** [Hol87]. **Rome** [AA86, IEE88d, Wol93b, Wol93a]. **Root** [LAKW07, TLLL07]. **root-hashing** [TLLL07]. **Roots** [Mue04]. **rotate** [FJ13]. **Rotated** [US09]. **Rotation** [Bla95, PQ98, PQ99]. **Rotation-Symmetric** [PQ98, PQ99]. **Rotational** [KNR10]. **Rotationally** [HSPZ08]. **Round** [AD11, jCPB+12, DDS14, HSR+01, LP15, PT11b, GLM+10, SY11, TSP+11, WFW+12, ABM+12, CV05, ITP14]. **Round-Down** [PT11b]. **Round-Reduced** [DDS14, WFW+12]. **Rounds** [GK08, HSIR02, Sch11]. **Route** [ABC+16, DF01, BLC12, YG10]. **Router** [JL14, KLSV12]. **routers** [ATAKS07, PT12b, TKH20]. **Routine** [Hea82]. **Routing** [ABC+16, BT12a, WBWV16, Cha12, HLL18b, PT10b, SPSP16, TC04, TBC+05, WY02]. **routing-based** [WY02]. **rows** [CDH19, FH15]. **RSA** [Joy03, Ano95a, Jun87]. **Rule** [BG92, Han90, HCKW90]. **Rule-Based** [BG92]. **rulebase** [CKKK09]. **Rules** [CL05, CT12, PCY95, HC02, HC07]. **runtime** [OOK+10]. **Russia** [Vau06]. **Ryu** [KCC05].

s [PES+12, BLC12]. **S.** [Pro94]. **S81** [KTN92]. **SAC** [JY14, HSR+01]. **safe** [CCA+12, LPSW03, Lin96]. **SAGA** [HKNW07]. **Saint** [GQ95, QG95]. **Saint-Malo** [GQ95, QG95]. **saliency** [FXWW17]. **same** [Con17]. **SAMOSA** [PHG12]. **Sampler** [Mil87]. **Samplers** [CJ19]. **samples** [HYKS08]. **Sampling** [AD85, Jak85, WM19, BZZ12, CyWM91, ORX90, RKLC+11, ZGG05]. **San** [ACM75b, ACM91b, ACM03a, ACM07, ACM08a, ACM11, Ano10, DT87, IEE88a, IEE91b, Joy03, Kar98, Shm00, Sto92, USE90]. **Sandwich** [Yas07]. **Santa** [Bel00, Bri92, Bri93, CRS83a, Cop95a, Cop95b, Fra04, Gol94, Sho05, Sti93, Sti94c, Wie99, Yun02]. **Santiago** [BJZ94]. **SAP** [SFA+19]. **sat** [DK07, MS13]. **SAT-based** [MS13]. **Satzuebergreifende** [Nee79]. **says** [Nic17]. **SC'11** [LCK11]. **SC2002** [IEE02]. **SC2003** [ACM03b]. **Scalability** [DR92, Eng94, TCP+17, ATAKS07]. **Scalable** [CKKK09, DPH08, GLJ11, Gre21, IEE94c, LMD+12, MZL+19, MD97, MVB+21, MEK+14, PRRR15, PSZ18, PW94, SSL+18, SKC07, SWTX18, TMW10, WPKK94, WSZ+16, YLZ20, ZLC+20, CLL+14, KKP+17, KYS05, KSC11, KSC12, LNS96, LHWL20, LEHN02, NMQ22, NK16, PT12b, SB14, SE21, TLLL09, VBW94, KCR11, NTW09]. **Scale** [BI12, GGY+19, GLLL17, Li15, MEK+14, MWC12, NS16a, SHF+17, YGC+12, ZZLZ21, CML+13, FES09, Kos14, Shi17, SXLL08, Zha19a, ZNPM16]. **Scale-Invariant** [NS16a]. **Scaling** [AK09, LL13, LHWL21, Ros21, TCP+17, FHL+19, PES+12, YSL05]. **SCALLA** [LMD+12]. **scanner** [ISHY88]. **Scanning** [Bur81, LLL11]. **Scatter** [Ban77, BMB68, Bre73, Day70, FL73, FW76, FW77, Luc72, Lyo78b, Mal77, Mau83, Mor68, Mor83b, Mau68]. **Scenes** [War86]. **Schanuel** [KPS92]. **schedules** [GK12b]. **Scheduling** [Lyo79, TL93]. **Scheme** [AK98, Alb21, BP97, Bur84, CLD82, Cha84b, Cha84c, Cha85, CL86, Cha86a, Cha86b, CC88b, CCJ91, CW91, CGLC20, Dat88, DJS80, DHJS83, Fah80, Hül13, JLH08, KJC11, LW88, Lar88b, LHC05, LSZ+21, NXB13, Oto85a, Oto85b, PPS21, PVM94, PACT09, SGGB00, SHF+17, TC93, VV84, Vit81a, YSW+11, YY07, ZJ09,

ZQSH12, ZH18, Bur82, CBB05, CW93, CKW93, CP95b, Cho21, DF89, EAA+16, GTL21, HL12, HL03, HFF+17, KCL03, Ku04, KCC05, LLH02, LKY04, LWG11, MSZ+20, MMG10, Oka88, SDR83b, Tsa08, WZ12, YRY04, YG10, ZW05, ZC12, FF90]. **Schemes** [BDS09, CL05, CLC06, Cor02, Dam87, DSS17, ED88, HM96, HDCM09, HHL10, Jai89, Jai92a, Jai92b, Jaixx, Kal01, KM09, LM95, LRY78, LRY80, MY80, MKASJ18, Ngu06, Ouk83, PWY+13, PF88, RL82, RS77, SDR83a, TL95, CJMS19, CQW08, DH84, GS94, HDCM11, HSMB91, IN89, KK96, KM10, ML94, NMX19, OS88, RS75, SNW06, ZHS94]. **Schluesselwoertern** [Dos78a]. **Schnellen** [Kue84a]. **Schnorr** [DBGV93, NSW09]. **Sci** [Sar80]. **Science** [ACM91b, AH03, Bar83, Gol94, Got83, IEE76, IEE80b, IEE82, IEE85a, IEE88c, IEE89, IEE91b, IEE92b, IEE99, IEE06, IEE07, IEE10, IEE11b, IEE13, Knu74, Kon10, LC86b, LL83, RRR99, Rie89, Rov90, Wal88, WGM88, Wil85b, Win78, TWW77, vL94, AT18]. **science/3rd** [TWW77]. **Sciences** [SC77]. **scientific** [Fis87]. **Scope** [CL83, GJR79]. **scoped** [FF90]. **Scopus** [AT18]. **scoring** [NADY20]. **Scotland** [AOV+99]. **Scratchpad** [vdBGLGL+16]. **SDC** [KO90]. **SE** [Sun02, HLL18a]. **Sealed** [SKM01]. **Sealed-Bid** [SKM01]. **Search** [Ack74, iA91, Ban77, BM76, Boo74, Bra84a, Bra85, Bra86, Cer81, CKB83b, CKB85, Cha91, CLP17, CS82, Eck74b, GIM99, HWZP18, HH85, KCB81, Kra82, Kut10, LL85, Luc72, MD97, MW09, Mue04, NSS+06, Pal92, PACT09, Reg81, RSK17, SD78, San76, Sev74, SG88, SSL+18, Tam85, TYZO15, TKI99, Ven86, Vit83, WYY05d, WWZ09, WSZ+16, XNS+13, YSW+11, ZLC+12, vW94, AP92, BC06, CKB83a, CK89, CLL+14, FP82, GP08, HFZ+15, KJS17, Kor08, KW94, Lin96, LCH+14, LWWK20, MKSiA98, MT16, NM02b, NH74, PY88, Rön07, SP12, STS+13, TYSK10, MKL21, WYY05a, WZ93, ZWT+14, ZLC+18, ZHC+13, ZNPM16, WWZ09]. **Searches** [LL87, Lyo85, GJM02, KHH89]. **Searching** [Bay74, BS97, Bur75a, CL85, CS82, Dav73, Day70, Dos78b, Fla81, FS82, Fla83a, Flo87, Gon81, Gon83, Knu73, Knu75, Lam70, Mai83, McI63, Meh84, Ouk83, Piw85, RT81, Ram89b, RC94, SG76b, TT82, Wie87b, WB87, YTJ06, Yub82, CW93, CLW98, ISH+91, Mol90a, Mol90b, PH73]. **Seattle** [ACM89c, LCK11, KCR11]. **Seaweed** [NDMR08]. **Second** [ACM83b, ACM90, SDA91, AKY13, ABD+16, Ano93d, BD08, Kil05, LLL+16, Mit12, TZ12, ABM+12, IEE88b, TSP+11]. **Second-Preimage** [ABD+16]. **Secondary** [Bel70, Bel72, Bel83, Fel87, FP89b, Gui75, Joh61, NH74, YMI89]. **Secrecy** [BKST18]. **Secret** [HR04, LMJC07, LPWW06, SNW06, AGBR19, Par18, ZHS94]. **sections** [NM10]. **Secure** [AHV98, AOAAK20, Alb21, Ano93b, Ano95b, BT12a, CZLC14, CS02, Dan13, DK07, DY90, DY91, DR11, FIP93, FFGL09, GHR99, GZX14, HM96, HR04, JTOT09, JK11, KMM+06, KAS+22, KP97, LM95, LRY+15, MKAA17, NIS93, Nat95, NR12, PLKS07, PV07, PGV92, Rei03, RSK17, SK99, Sho96, Sta06a, VD21, Win84, XHZ+19, Yas07, YY07, Zhe90, ZHZ+19, Aam03, FFGL10, GTL21, GM18, GBL94, HLL18a, IN89, JFDF09, Sim98, SXL16, YRY04, ZC12, ANS97, Ano02, Ano08, Ano12, Bou12, FIP02b, Nat92, Sta94]. **Security** [AK98, Abi12, And94, ASBdS16, CLNY06, CN08, Cor00, Cor02, FW09, GK12a, HMNB07, HLMW93, HXMW94, ISO97, ISO04, KK12, KK18, Kil01, LC06, LT12, LLL09, MP12, Men12, NAK+15, PW06, RS12, SK20, SM02, WG00, WPS+12, Yan10, ZXL19, ACM94a, ACP10, ABM+12, AMP15, Ano93a, AGBR19, BGKZ12, Kak83, Lai92, LC95, Men17, MPST16, PGV93c, SF88, Sta06b, UPV11]. **Seed** [PNPC20].

Segmented [CLYY92, CLYY95]. **Segments** [Bor84]. **Sekundaerspeichers** [Pet83]. **select** [FNY92]. **selectable** [BSNP96c, Gon95, Li95]. **Selected** [SC77, Ytr06, Bir07, Bor81, JY14, JY14]. **Selecting** [MHB90, Sou92]. **Selection** [DC81, FFGOG07, Hea82, MS12, OGAB14, TYZO15, CD84a, HYKS08, Dos78a]. **Selective** [DHT+19, LYDA19]. **selectivity** [HYKS08, MBKS07]. **Selects** [Bou12]. **Self** [HH85, Pag85, PRRR15, SS83, Som99, TY03, Wil96, Wog89, ZF06, AÖD19, TKI99]. **Self-Adjusting** [Pag85, Wog89]. **Self-checking** [Wil96]. **self-clustering** [AÖD19]. **Self-Indexed** [TKI99]. **Self-Monitoring** [SS83]. **Self-Organizing** [HH85, Som99, TY03]. **Self-Shrinking** [ZF06]. **Self-Tuning** [PRRR15]. **Semantic** [CDW+19, Li15, LWZ+18, ZZLZ21, LL13, MTB00]. **Semantics** [IH83]. **Semi** [CBK83, CLL+14]. **Semi-Interactive** [CBK83]. **Semi-supervised** [CLL+14]. **semijoin** [CCY91]. **Semite** [LII92]. **Semite-Infinite** [LII92]. **sensing** [Ind13]. **Sensitive** [BT12b, CSSP15, CKPT19, KBG18, Kaw15, MNP08, OWZ14, OTKH11, Pag18, ZHW21, AT18, EFMRK+20, FWG18, GDGK20, HFZ+15, HFF+17, LNS11, LWXS18, LJW+17, PCM15, QZD+18, SP12, STS+13, WY00, ZHX+21, SA17]. **Sensor** [DK09, LDY+16, PLKS07, ZQSH12, ZHW21, AK09, ADF12, GDGK20, LG13, LND08, RAL07, YG10]. **Sensors** [DL12, DVS+14]. **Sentence** [CH12]. **Sentences** [Ven86]. **sentiment** [ZZLZ18]. **Separate** [Kue82b, Mul81, Kue82a]. **Separating** [FK84, SG16, BvT13, LS06, vT14]. **Separators** [Lar88b, Moh90, Moh93, CS93a]. **Sept** [BD88, Jou85]. **September** [VLD82, AAC+01, AOV+99, AA86, BJZ94, EF12, FS09, Fis87, HM08, HKNW07, Ker75, Kna89, LSC91, Vid90, Win78, Yao78]. **Sequence** [BC08, FP89b, Gon81, HG77, LPT12, LL85, MS88b, BJ07, CLW98, EASR22, Wog89]. **Sequences** [Som99, KS88a, QJ97]. **sequencing** [KRML09]. **Sequential** [AD85, BCCL10, CT96, GSB94, HB89a, KKC12, Lit89, Mul72, Ore83, Piw85, SK98, SG76b, BDPV14, HB89b, IL90]. **Series** [BJL16]. **Serious** [AG18]. **Served** [PM89]. **Server** [DR92, GSL17, GBC98, Gra99, LLL+16, VB00, Tsa08]. **Server-Side** [GSL17]. **Servers** [HWZP18, SKC07, KSC11, KSC12]. **Serves** [Ano95d]. **Service** [CCF04, SWTX18, Bac02, BPT10, QZD+18, TLLL18]. **Services** [ANS05, Ano85b, HLC10]. **Session** [HLC10]. **Set** [BÖS11, Kie85, PSZ18, SG76a, WC81, YD85, BGG12, GGR04, HYKS08, HDCM11, HKLS12, HM03, MI84, SA17]. **set-expression** [GGR04]. **Set-Oriented** [Kie85]. **set-valued** [HM03]. **Setl** [BFR87]. **Sets** [AA79b, AA79a, GHK91a, GHK91b, GT93, Lit89, PBDD95, Ram92, Spr77, Win90a, BT89, BT93, FP82, IL90]. **seven** [RAD15]. **seven-dimensional** [RAD15]. **Seventeenth** [LC86b, LSC91, Rie89]. **Seventh** [ACM75c, ACM75a, ACM88a, dBvL80, LL08, AAC+01, ICD91]. **several** [DLH+79, Kan90]. **SHA** [ANS97, Bou12, TSP+11, AAE+14, ABM+12, BCJ15, jCPB+12, Con17, DR06, GLG+02, JRPK07, KKRJ07, KRJ09b, KJS17, MAK+12, NIS15, NSS+06, PPS21, SK05, Sta94, SKP15, WYY05a, WYY05d, WYY05b, WYY05c]. **SHA-0** [BCJ15, NSS+06, WYY05d]. **SHA-1** [ANS97, AAE+14, BCJ15, Con17, DR06, JRPK07, KKRJ07, KRJ09b, KJS17, SKP15, WYY05a, WYY05b, WYY05c, GLG+02]. **SHA-2** [SK05]. **SHA-256** [MAK+12, PPS21]. **SHA-3** [Bou12, TSP+11, ABM+12, jCPB+12, NIS15]. **SHA-512** [GLG+02]. **SHA1** [Con17, SBK+17]. **Shading** [ZDI+15]. **Shading-based** [ZDI+15]. **Shanghai** [Ano83, LC06]. **Shape** [SR89, SYW+20]. **Share** [SS88b]. **Shared**

[Bor84, CadHS00, DadH92, EK93, adH93, KBG18, KU88, KTN92, LTS90, MLD94, MLxx, Mey93, Omi91, PG17, SD89c, SD89a, TR02, TNKT92, VB00, Vit81a, WB03, YNW+09, Don91, GLJ11, Kan91, Kan93, KU86, MSS96, Par18, SD89d]. **Shared-Disk** [WB03]. **Shared-Everything** [KTN92, MLD94, TNKT92]. **Shared-Memory** [MLxx, TR02, Vit81a, Bor84]. **Shared-Nothing** [SD89c, SD89a, SD89d]. **shares** [ZHS94]. **Sharing** [LPWW06, KL08, KD92, SNW06, YD86b, ZHS94]. **SHARP** [VD21]. **SHAvite** [GLM+10]. **SHAvite-3-512** [GLM+10]. **Shell** [Rei03]. **Shenzhen** [IEE11a]. **Sheraton** [ACM75b]. **Sheraton-Palace** [ACM75b]. **Shop** [Sil02a]. **Short** [AB12, CW09, CDW+19, DK09, Lyo79, NR12, MT16, SV15a]. **Short-Input** [AB12]. **Short-Output** [NR12]. **Short-Time** [CW09]. **Shorter** [Hül13, PPB16]. **Should** [Yao81]. **Shoup** [Mir01]. **Showcase** [USE00a]. **Shrinking** [ZF06]. **SHS** [Ano08, Ano12, NIS93, Nat92]. **SIAM** [ACM94d, SDA90, SDA91, ACM97a, ACM05, ACM08a, Kar98, Mat09, Shm00]. **Sichere** [BN85]. **Side** [GO07, GSL17, TC04]. **SIFT** [MMG10]. **SIGACT** [ACM82, ACM83a, ACM83b, ACM85b, ACM86a, ACM88a, ACM89b, ACM89a, Van10, LL08]. **SIGACT-SIGMOD** [ACM83a, ACM83b, ACM85b, ACM86a]. **SIGACT-SIGMOD-SIGART** [ACM88a, ACM89b, ACM89a]. **SIGAL** [A+90]. **SIGART** [ACM88a, ACM89b, ACM89a, Van10, LL08]. **SIGCSE** [LC86b]. **SIGIR** [BIP92, YR87, BV89]. **SIGMOD** [ACM82, ACM83a, ACM83b, ACM85b, ACM86a, ACM88a, ACM89b, ACM89a, BJ93, CLM89, FMA02, GMJ90, Van10, HF13, LL08, Nav85, SW94b, Sto92, ACM81, ACM84a, BL88, HF13, Lie81, SW94a]. **SIGMOD-SIGACT-SIGART** [Van10, LL08]. **SIGMOD/PODS** [HF13]. **SIGMOD/PODS'13** [HF13]. **Sign** [CK12, GHR99, PV07, GK12a]. **Signal** [Cai84]. **Signature** [ANS05, Ano09a, Ano13, BDS09, CS91, Cor02, Dam87, FC87a, FC87b, HHL10, Hül13, Kal01, LR96a, LM95, LL92, NXB13, PWY+13, RZ90, RR92, ZRT91, ZJ09, CR89, Con17, SE21, ZW05]. **Signatured** [SS83]. **Signatures** [AS16, BHH+15, But17, CK12, DK09, FL04, FFGOG07, GK12a, GHR99, Hül13, HRS16, HBG+17, MKF+16, MCF17, Moh11, MKAA17, PW93, PGV93f, RR92, Rul93, TT82, CFN18, NSW09, PPB16, ST93]. **Signed** [Sch01b, ZDI+15, SN19]. **Significance** [SP21]. **significant** [BCCL10]. **signing** [BGG94]. **SIGPLAN** [ACM79]. **Silbentrennung** [BN85]. **SIMD** [AT91, RG89]. **SIMD-MIMD** [RG89]. **Simhash** [LLDZ18]. **Simhash-Based** [LLDZ18]. **Similar** [RC94]. **similarities** [UCFL08]. **Similarity** [GIM99, HCF95, LNS11, LÖON01, NADY20, NNA12, SHZ+20, TWZW11, WSZ+16, YTJ06, CLL+14, GP08, HYKS08, SP12, SA17, STS+13, ZWT+14]. **Similarity-Preserving** [SHZ+20]. **Simple** [BPZ07, Cic80b, DH01, DS09c, GM94, GM98, IT93, KM08, Lom88, PSSC17, PT12a, Ram92, Sar10, Tho13, CLS95, DKRT16, DW03, DS09b, DLM07, MV08, PT11a, Pri95, SKD15, SF88]. **Simplicity** [Rag93]. **Simplifies** [OVY94b, OVY94a]. **Simplify** [Dam93, Dam94]. **simplifying** [VZ12]. **Simulating** [adH93, Mey93]. **Simulation** [EK93, Hil82, Hui90, KLadH93, KLM96, KHW91a, YkWY83, KHW91b, TWL+18, War14, DS84a]. **Simulation-Based** [EK93]. **Simulations** [CadHS00, DadH92, Lep98, Rey14, MSS96]. **Simultaneously** [LOY00]. **Sindhi** [SSS05]. **Sine** [PPS21]. **Singapore** [DSS84]. **Single** [AKS78, AA79b, AA79a, CS93a, CC88b, GIS05, Lar82c, Lar82d, Lar85c, LLL+16,

Men12, MJBD11, OT91, Spr77, YDT83, YSEL09, Men17, MA15, RT89]. **Single-Cycle** [MJBD11]. **Single-File** [Lar82c, Lar82d, Lar85c]. **single-hop** [MA15]. **Single-Layer** [YSEL09]. **Single-Pass** [YDT83]. **Single-Probe** [OT91]. **Singular** [NS16a]. **Sinkhole** [JL14]. **Sinnentsprechende** [BN85]. **Sintering** [Rey14]. **SipHash** [AB12]. **sites** [OOK+10]. **Sixteenth** [ACM84b, ACM05]. **Sixth** [BF89, ICD90, GJM02, LT80]. **Size** [Ack74, AHS92, Bat75, CKW09, Dev99, Dod82, FK84, HD72, Joh97, Kab87, KV91, KNT89, MV88, Meh82, Sam76, Wil79, Woe01, Bee83, CM01, DW05, DW07, GW94, Han17, LNS11, Sar11, Woe05]. **SK** [LCH+14]. **Skein** [AEMR09, FLS+10, KNR10]. **Skeleton** [LDY+16]. **Sketch** [BI12, TP15, YGS+19]. **sketches** [NTW09, SLC+07]. **Sketching** [Ind13]. **Skew** [Bre91, CyWM91, DNSS92, KO90, RK91, Top92, WDYT91, WYT93, ZO93]. **Skip** [AS07, Coh98, BCR10]. **SL2** [CP95b, TZ94b]. **Slack** [AEP18]. **SLCA** [WWZ09, ZLC+12]. **SLCA-Based** [WWZ09]. **Slicing** [Kon10, MEK+14]. **SLISCP** [ARH+18]. **SLISCP-light** [ARH+18]. **sloth** [LW17]. **Slovenia** [EF12]. **SM3** [MXL+12, WS13, ZWW+12]. **Small** [FHMU85, Ind01, Joh97, KR01, NN90, NY85, YLC+09, YBQZ17, MP16, Sag85b]. **Small-bias** [NN90]. **Smaller** [CRSW11, CRSW13]. **Smalltalk** [SUH86]. **Smart** [Ku04]. **Smartcards** [JK11]. **smoke** [ZRL+08]. **Smooth** [ACP09, HK12a, KV09, LYY+18]. **snapshots** [PBBO12]. **Snefru** [BS91c, Bih08]. **Snowbird** [SM08, SM12]. **SOAR** [SUH86]. **Social** [KKP+17, ZWH17, PES+12, ZZLZ18]. **Societies** [IEE92a, IEE01]. **Society** [IEE80a, IEE84, IEE88a]. **Soft** [DGKK12]. **Softswitches** [TLLL18]. **Software** [Ano85b, DT75, Eld84, FHMU85, GN80, GD87, Got83, IEE80a, IEE95, Kna89, Lew82, MZD+18, Mil87, MW95, NP99, RRR99, Sch01b, SBS16, Wal88, And94, Bir07, Gol96, Mer90a, SGK09, TKH20]. **Software-implementation** [GN80]. **Solution** [DM90, Hop68b, Mit73, WSZ+16, HCF95, HL94]. **Solvability** [BF83]. **solve** [CP95a, WZ12]. **solved** [Loh89]. **solver** [GZ99]. **Solvers** [DK07]. **solving** [SWQ+14]. **Some** [Bay73a, CV85, Gib90, Gri74, Lar85a, Mit09, MOI90, MOI91, Nam86, Sti06, Wri83, BSU12, GLC08, Inc81]. **Sonographic** [ŠSaS01]. **Sophisticated** [BPBBLP12]. **Sort** [GLS91, Gra94b, GLS94, KKL+09, KTMO83b, OOB17, TR02, AKN12, BATÖ13]. **Sort-Hash** [TR02]. **sort-merge** [AKN12]. **Sort-Merge-Join** [Gra94b]. **Sorted** [Yao81, YLB90]. **Sortieren** [Meh86]. **Sorting** [BS97, DS97, Gra94a, Gup89, Knu73, Knu75, MV90, MV91b, Meh84, ASW87, CKKW00, ISH+91, Kan90]. **Sound** [GvR08, KCF84, SDW14, BDPV14]. **Source** [KP94, CBB05, Cha12, HC11, NMX19]. **source-based** [Cha12]. **Sources** [CV08]. **South** [ACM91c]. **SPAA** [ACM91c]. **Space** [Bal05, Blo70, BPZ07, BM99, CH94, DH01, Fis87, F+03, FPSS05, HT01, JD12, MSW19, PP08, SvEB84, TW91, YY01, BD82, BCGS16, CF89b, DMPP06, GZ99, Kou93, MN90, OP03, PSS09, Sie89, SWQ+14, TYSK10, WHS+07, Yuv75]. **Space-Efficient** [BPZ07, JD12, PSS09]. **space-filling** [GZ99]. **space-hard** [BCGS16]. **Space/Time** [Blo70]. **Spaced** [PNPC20]. **spaces** [IMRV97, NN90]. **Spain** [DJRZ06, LSC91, CTC90]. **Spam** [ADOAH19, LZ06, UCFL08]. **Spamdoop** [ADOAH19]. **SPARC** [WG94]. **SPARQL** [HAKM15, HAK+16]. **Sparse** [AL86, ASW07, vdSDW74b, FKS84, Gre21, Gri98, Gri77, KKN12, RT81, TY79, ZHC+13, vdSdW74a, Bis12, BT90, BT93, CML+13, JCC00, CW91, Ind13]. **Spatial**

[LR96b, SS88a, SYW+20, WYD+18, DLN+18, LH06, SS90b, ZBB+06, ZLC+18]. **spatio** [CWC10, DMPP06, FXWW17]. **spatio-temporal** [CWC10, FXWW17]. **speaking** [LC95]. **Special** [ACM82, DT87, Dos78a, GIS05, MO92a]. **specialization** [SV15a]. **Specialized** [Bab79, ISH+91]. **Specific** [RTK12, ARH+18, JDW+19]. **Specifications** [Nat92]. **Specified** [AU79]. **Specifying** [GHJ+93]. **Spectral** [KKC12, Li15, WFT12, WB90, ZWT+14]. **Speech** [CW09, RJK79]. **Speed** [FP89a, KMM+06, KMV10, McK89a, PSR90, TK88, WZY+18, YNKM89, BCCL10, EVF06, McK89b, MSS96, RW07, SLC+07, SXLL08, TLLL07, XMLC11]. **Speeding** [FH96]. **Speicher** [GN80]. **Speicherstrukturen** [Kue84a]. **Speichertechniken** [LS85]. **Speicherung** [BJMM94b, BJMM94a]. **Speicherungsstrukturen** [Kue83]. **Speicherverfahren** [DS84a]. **Spelling** [CS82, McI82, Rad83, Zam80, MF82, Wie86]. **speziellen** [Dos78a]. **SPHINCS** [BHH+15]. **Spiral** [CK94, Mul85]. **Split** [LL85, MS88b, SS06, She78, Wog89]. **Split-ordered** [SS06]. **splits** [BY89]. **Splittable** [CP13]. **Splitting** [DR09, RT87b, Vek85]. **Spoken** [KRRH84]. **Sponge** [ARH+18, BDPV07, AMP12, BDPV08, BDP11, BDPV12]. **Sponge-specific** [ARH+18]. **spongent** [BKL+11]. **spongy** [RS14]. **sponsored** [Fis87, HB93, IEE84]. **spots** [KLL+97]. **Spotting** [FLF11]. **Sprache** [BN85]. **SPRC** [Wol93b]. **Spreading** [KO90]. **Spring** [AFI63, IEE88a]. **Springs** [IEE11b]. **Spritz** [RS14]. **SQL** [Bra88, Eng94, GBC98, Gra99]. **Square** [ACM83a, ACM83b, EPR99]. **Squares** [OG94b]. **squaring** [Mei95]. **SRAM** [KHK15]. **SRAM/DRAM** [KHK15]. **SRS** [SWQ+14]. **SSD** [HGH+12]. **SSPIN** [Cob94]. **St** [Vau06]. **Stability** [CW09]. **stable** [HF91]. **Stack** [Bor84, KHW91a, LLL+16, KHW91b]. **STACS** [AH03]. **Stage** [LCM+20, QZD+18]. **STAIRS** [RCF11]. **stamped** [GB17]. **Stamping** [Cip93, Lip02, SL16]. **Standard** [Ano93b, Ano95b, Ano08, Ano09a, Ano12, Ano13, Dan13, FIP93, LYX+19, NIS93, Nat95, NIS15, SK05, CV83a, GvR08, Nam86, Ano02, Dan13, FIP02b, Nat92, Pla98, Lut88]. **Standards** [Bur06, Fox91, Kal93]. **Stash** [ADW12, ADW14, KMW08, KMW10]. **State** [But17, CH94, HB93, MKF+16, Pre97b, Pre99, Wol93b, vdP73, ATAKS07, HL94, PGV93c, Wol93a]. **Stateful** [NTY12, Ged14]. **Stateless** [BHH+15, MKAA17, NTY12]. **Stateless/Stateful** [NTY12]. **Static** [AA79b, AA79a, LC88, Ram92, Spr77, DMP09]. **Statistical** [Fil02, HZ86, Sav90, TTY93, LZ06, MJ08]. **Statistically** [HR07, Wee07]. **Statistically-hiding** [HR07]. **Statistics** [Rob86, WGM88, DKRT15]. **Status** [TSP+11]. **Steady** [vdP73, HL94]. **steady-state** [HL94]. **Steering** [TLLL18]. **Step** [Dit76, ZWW+12, AKY13, WS13]. **Step-Reduced** [ZWW+12, WS13]. **Steps** [HKKK10]. **Stereo** [ZZ83]. **Stereo-Warehouse** [ZZ83]. **stimulating** [JFDF09]. **STL** [Ben98]. **STM** [DSS10]. **STOC** [ACM07, ACM08b]. **STOC'12** [ACM12]. **Stochastic** [HKNW07]. **stock** [She06]. **Stockholm** [PV85, Ros74]. **Storage** [ACM04, Bay74, BMB68, Bre73, Col93, Day70, FL73, Fel87, FB87, FP89b, Fro82, GL82, GL88, HCJC06, HNKO20, Hin20, Kno71, HGH+12, LCK11, Les88, LCLX19, LRY+15, MSK96, Mal77, Mau83, MEK+14, Mor68, Mor83b, Mul81, Mul85, Omi88, OT91, OS83a, OS83b, Pet57, Sam81, SHF+17, TY03, TS85, Tra63, WZY+18, WCW+22, WH83, Wil71, WKO78, WB87, YDT83, YLZ20, vdP72, vdP73, AY14, AK09, CRS83b, DMB19, HGR07, Mau68, MSS96,

PT10b, QD02, YSL05, YMI89, van73]. **storage-efficiency** [PT10b]. **Storage-efficient** [HCJC06, MSK96]. **Store** [DW83a, LLL+16, LCM+20, MZL+19, QXL+20, dW83b, SFA+19, Shi17, BP94]. **Stores** [Bry84, GYW+19, JLL+20, PRRR15, SDZ21, WLC20]. **Storing** [AL86, FKS84, MNS07, Ros77, TY79]. **Stouffer** [ACM87]. **Strategies** [iA91, iA94, BI87, Dae95, Die07, adH90, adH93, KL87, KHT89, MD97, Mey93, MNS07, Tro95, YB95]. **Strategy** [CdM90, LMSM09, LC96, NKT88, RS92, GC90, LMSM12]. **Stream** [DC98a, cLmL07, MNS12, NCFK11, TW07, TS85, DS09a, Ged14, MV08, OCDG11, RS14, Tan83]. **Streaming** [CN07, STS+13, YSW+11, YGS+19, CBB05, FVS12, ZC12]. **streamlining** [DSS10]. **Streams** [Coh98, SS83, YGC+12, BMLLC+19, CH09, GGR04, SLC+07, YLC+09]. **street** [Sim98]. **Strength** [HS08, FH15, Ken73]. **Stretching** [BVF12]. **String** [iA94, Ask05, BRM+09, BH85, Bur84, CFP19, CCH09, Cha91, Dav73, LK14, LLLC17, NNA12, TK88, Tay89, TT82, ASM17, AZ10, Bur82, DC94, GBY90, Kim99, MBKS07, RZ97, XMLC11]. **String-indexed** [Tay89]. **string-pattern** [Kim99]. **Strings** [BS97, Dit91, FM96, GLB21, Lit91, Pea90, Pea91, RC94, Sav90, Sav91, Zuk21, Eug90]. **Strong** [CHKO08, CHKO12, JRPK07, HLL18a, Ku04]. **strong-password** [Ku04]. **Strongly** [BG07, LK14, Tho00]. **Structural** [BRM+09, TWZW11, Wil96, ZMI91, FLF11, MK12, ZBB+06]. **structuration** [Lit77a]. **Structure** [AHS92, CK12, CJC+09, DGM89, DT91a, DT91b, FLF11, Flo77, FB87, GHK91a, GHK91b, Gre21, CTC90, KS12, NHS84, Omi88, SG88, WH83, Wri83, ZHW19, BR75, BGG12, IG94, KRJ09a, KHH89, LNS96, LCH+14, MMC01, MSK96, SB07, TMB02, YD86b]. **Structure-Preserving** [CK12]. **Structured** [CS93b, GDA10, Nak21, Piw85, SG76b, SM87, WWG+18, BPT10, GHW07, WHS+07, WLLG08]. **Structures** [AHU83, BDD+10, BFR87, Boy98, BJM14, CE70, Coh84, DSZ07a, DSZ07b, DP08, Ell85b, Ell82, Fel88, FZ87, FBY92, Fro82, Gon84, GBY91, Gri74, Har88, Har71b, HS84, Kru84, LC86a, LRY78, LRY80, Lit84, MO92a, RW73, Sal88, SDW14, SW86, Sne92, Ste82, SW87, TA81, TA86, TGL+97, TS76, TS84, VL87, WS76, WKO78, Wir86, YLB90, ZLLD18, BY89, CRS83b, FP89a, GJM02, Har73, HM03, Inc81, IGA05, Koe72, Lin96, MTB00, NT01, NM02b, OS88, She06, VL97, Vit01, Wil78, Wil85a, ZKR08]. **Structuring** [Bay73a]. **Studies** [Ano93d, GT80, GG80, Yub82]. **Study** [AR17, BF83, BK07b, Cha84c, Cha85, Cra85, DTS75, DJS80, DHJS83, Ell85b, Gri74, Hil78b, Hil78a, LC86a, LG78, LYD71, TL95, YLB90, HM03, LY72, Wee88, WTN07]. **style** [UCFL08]. **Sub** [WZY+18, Pri95]. **Sub-Datasets** [WZY+18]. **sub-quadratic** [Pri95]. **Subgraph** [ZLY+12, WLLG08]. **sublinear** [CFN18]. **Subquadratic** [Val15]. **subscribe** [MJ14]. **Subscripts** [Atk75, vdSDW74b, vdSdW74a]. **subset** [IN89, Mon19, Pri95]. **Subspace** [KRJ+80, Sch11]. **Substring** [Boo73, Har71a, MKSiA98]. **Subsystem** [HLC10]. **subtype** [Duc08]. **subtyping** [DL06]. **Succinct** [ANS10, DP08, RRS07, FS08, SH92, SH94]. **Suchen** [Meh86]. **Suffice** [ADW12, ADW14]. **Sufficiency** [NY85]. **Sufficient** [BDPV14, IKO05, IH95, Rus92, Rus93, Rus95]. **suffix** [BGKZ12, Kos14]. **suffix-free-prefix-free** [BGKZ12]. **Suitable** [PPS21, MZI98]. **sum** [IN89, Mon19]. **summaries** [KM08]. **Summary** [DLH+79]. **Sums** [HJ96, RRS07]. **Super** [Ano95d, HLL18a, KO90]. **Super-strong** [HLL18a]. **supercomputers** [GLJ11]. **Supercomputing**

[ACM04, IEE90, IEE91a, IEE93, Kha95]. **Superimposed** [CJ86, FH69, SD85, SDKR87, SDR83b]. **superior** [PT10b]. **Superjoin** [TRN86]. **superspecial** [CDS20]. **Supertree** [GB10]. **supervised** [CLL+14]. **Supplement** [SC77, Ruc15]. **Supplementary** [PLKS07]. **Support** [CN07, Eng94, GSL17, KJC11, SK99, YCRY93, CZ14, CKKW00, JMH02, KLSV12, LCRY93]. **Supporting** [CLS12]. **SURF** [YCJ12]. **Surface** [Leb87, LDY+16]. **surprising** [SKD15]. **Surrogate** [BCH87]. **Surrogates** [Dee82]. **Surveillance** [PPS21]. **Survey** [CZ17, CJ19, Kal93, Sev74, Mil99, RAL07, UPV11]. **SUSE** [PT10b]. **Sweden** [Ros74]. **Switching** [IEE74]. **Switzerland** [HKNW07, Lak96]. **Sydney** [SP90]. **Symbol** [CL83, Bat65, GJR79]. **Symbolic** [ACM94b, CLD82, DL80, FH96, Jen76, Lak96, Lev95, Ng79, vdHvH12, GvR08, Kan91, Kan93, Ng79]. **Symbols** [Wil59]. **Symmetric** [FW09, Fil02, HC13, NHS84, Oto85b, PQ98, PQ99, QG89, QG90, Roe94, SK20]. **Symmetry** [KTN92]. **Symposia** [Got83]. **Symposium** [ACM94d, ACM75c, ACM75a, ACM76, ACM77b, ACM79, LFP82, ACM82, ACM83a, ACM83b, ACM84b, ACM85b, ACM86b, ACM86a, ACM87, ACM88a, ACM88b, ACM89b, ACM89a, ACM89c, SDA90, ACM90, ACM91c, ACM91d, SDA91, ACM91e, ACM94b, ACM96, ACM97a, ACM97b, ACM98, ACM01, ACM02, ACM03a, ACM05, ACM07, ACM08a, ACM08b, ACM11, ACM12, AH03, Ano10, A+90, AiNOW11, BW92, Col93, CHK06, EF12, Gol94, Van10, adHMR93, HL91, HF13, IEE74, IEE76, IEE80b, IEE82, IEE84, IEE85a, IEE88c, IEE89, IEE91b, IEE92b, IEE99, IEE05, IEE06, IEE07, IEE10, IEE11b, IEE13, Jáj90, Jen76, Lak96, LL08, Lev95, LC86b, Mat09, MS05, Ng79, ACM77a, Shm00, WGM88, Win78, Wol93a, Wol93b, vdHvH12, ACM91a, FS09, Fis87, HM08, HKNW07, Kar98, IEE82]. **Symsac** [Jen76]. **Synchronization** [Oak98]. **synchronizing** [DTM+18, ML95]. **Syndicate** [HM19]. **Syndrome** [vMG12]. **Syndrome-Based** [vMG12]. **synergy** [GHW07]. **Synonym** [QCH+81]. **synopses** [YLC+09]. **Syntactic** [Ven86]. **synthesis** [Sab94]. **synthetic** [GLC08, PGV93e, PGV94]. **Syracuse** [IEE80b]. **System** [ASWD18, Ano10, BGF88, BG92, CBK83, Cer85, CBK85, CZLC12a, CZLC14, CBA94, CJ86, DNV81, EE86, FH69, GRZ93, Gra94c, He87, ISK+93, JXY07, KL87, Koe72, KRJ+80, HGH+12, LYX+19, Luh58, Mil85, MK93, MFK+06, PRZ99, PSR90, QXL+20, Sar80, SBS16, SPB88, SC77, TC93, YkWY83, ZZM17, ZZ83, AS09, CZ14, Gob75, HLL18a, KJS17, Kos14, MFES04, WM93, YMI89, ZCZQ19, ZYWM20]. **Systematic** [ŠSaS01]. **Systems** [ACM82, ACM83a, ACM83b, ACM85b, ACM86a, ACM87, ACM88a, ACM89b, ACM89a, PDI91, And91, ANT85, BŠH12, Bor81, Cer81, CS83b, CC87, Col93, DKO+84b, DKO+84c, DKO84a, Dum56, DGKK12, Ell82, Fox91, FK84, GGY+19, GI12, GLLL17, Gro86, Van10, Han90, HCKW90, Har88, HNKO20, HBL+10, HF13, Kim80, KS12, KCB81, Kue84b, Kum89a, LYY+18, LC86a, LL08, LLG+17, LXL+19, LCL+20, Llo81, LSZ+21, Man12, MEK+14, Mor83a, Ouk83, PFM+09, PG17, Sha86, She91, SHF+17, SWTX18, Toy86, Ull82, Web72, WB03, Yam85, YLB90, ZJM94b, ZH18, dKC94, ACM94c, AKN12, ARA94, DKO+84d, DAC+13, FP89a, FES09, GPGO16, KKP92, Lia95, Mo92b, RW07, SK88, SGK09, SP89, TL93, UIY10, WZ12, WTN07, ZGG05, ZJM94a, ZJM94c, SC77, Sto88]. **systolic** [EBD91, PJM88, PJBM90].

T3D [DS97]. **Tabellen** [BI87]. **Table** [AL86, Bat75, BRM+09, Bee99, Bur75a,

CCF04, CW91, CHSC18, CL83, Day70, DHK+15, DAC+13, FKS84, FW76, FW77, GK94, GK95, Hop68b, HD72, HLC10, IABV15, JL14, JXY07, JMH02, JD12, KG95, Kno71, LMJC07, Lev00, Lit80, Litxxa, LACJ18, Lyo85, Mai83, Mai92, MT11, ML75, Mue04, MJT+02, Pri71, Pro89, Rey14, Riv76, Riv78, Sam76, Sam81, San76, Sne92, Szy82, Szy85, TY79, Tro06, VB00, YD84, YT16, YLB90, YLZ20, vdVL12, AY14, AZ10, BCR10, Bay73b, BGG12, Fro81, GSS01, HXLX13, KdlT89, MZK12, MA15, NK16, NH74, PH73, Ram87, SB95, SB97, TKH20, Tsa08, WTN07, Yu18, ZGG05]. **Table-Based** [HLC10, TKH20]. **table/urn** [Ram87]. **Tabled** [AR16]. **Tables** [Ack74, APV07, AK74, Ask05, Ban77, BM87, Bay73c, Bay73a, BPBBLP12, Ben98, BI87, CRdPHF12, Cle84, CD84b, EMM07, FFPV84, F+03, Gre21, GT93, GLB21, HP78, Hop68b, HC87, HC13, IK92, Jv86, KHK15, Kue82b, Kue84b, LK07, Lar88a, LMSM09, LC88, Lit79b, LB07, LHWL21, Luc72, LMR02, Lyo78b, MSD19, MS02, MPP14, Mit02, MC86, NY85, Pag85, PAPV08, PV92, PTT16, PBDD95, Pla98, Qui83, Ram88a, RRS12, RHM09, RMB11, Ros21, SD78, Sch79a, SS80, SM02, TT10, Woe06b, Yao81, Yao95, Zuk21, Bat65, CHS+18, Fly92, FPSS05, FRS94, GM79, GJR79, HKW05, KHK12, LMSM12, LVD+11, Mad80, MSD16, MRL+19, PT10b, PT12b, QP16, SS06, Tai79, TKH20, TBC+05, TMW10, Tso15, Wil03, Wil14, Wog89, WTN09, XLZC14, YTHC97, ZHW01]. **tabu** [WZ93]. **Tabulation** [KW12, PT12a, TZ12, Tho13, DT14, DKRT16, PT11a, PT13, Tho17]. **Tabulation-Based** [KW12, TZ12]. **Tabulative** [GT80]. **Tag** [JRPK07, ZWH17, CJP15, HLL18a, SPLHCB14, CJP12]. **tag-based** [HLL18a]. **Tagged** [ZWH17]. **tagging** [TCW+13]. **Tags** [LCL+20]. **Taipei** [HL91]. **Tamed** [NXB13]. **Tampa** [IEE88b]. **Tamper** [CHL07]. **Tamper-proofing** [CHL07]. **Tampering** [TWZW11, PS08]. **Tangle** [ÁVZ11]. **Tape** [SvEB84, ML95]. **Target** [LBJ02, Mit12, HRS16, MIGA18]. **Tash** [LYDA19]. **task** [JDW+19]. **task-specific** [JDW+19]. **Taxonomy** [CZ17]. **TBE** [Zha07]. **TBE/IBE** [Zha07]. **TCC** [Kil05]. **Tcl** [USE00b]. **Tcl/2k** [USE00b]. **Tcl/Tk** [USE00b]. **TEA** [CV05, HSR+01, HSIR02]. **Teams** [GBC98, KKW99]. **Technical** [IEE84, LC86b, Ros21, Zuk21, Mit17, SE89]. **techniken** [Mer72]. **Technique** [AP93, Boo73, CL85, CS82, CT96, Dod82, HC87, KM92, Lit79a, Mau68, McK89a, RZ90, Ram97, SDW14, She78, TK88, Wan84, Yam85, CCY91, GM77, Kan90, KK96, MIGA18, McK89b, Pro94, Sac86, Sag85b, MKL21]. **Techniques** [AOAAK20, Bay73a, Bih08, Bre73, CP87, CP88, CZ17, Dam90a, Dam91, Dav91, DKO+84b, DKO+84c, DKO84a, DL79, Dun89a, Dun89b, Fel87, Gra92, Gra93c, Gui75, Gui78, Hel94, KMV10, Kue84b, LC20, LDM92, LYD71, Mal77, Mor68, Mor83b, MC86, Pri71, QV89, QV90, QG95, RLH91, Rue93, SD85, SDKR87, SZ93, She91, SPSP16, Sta73, Sti94a, Vau06, YTJ06, BF08, De 95, DKO+84d, DJRZ06, DJNR09, GQ95, ISO97, ISO04, LY72, PH73, RLH90, SXLL08, UPV11, YSL05]. **Technology** [IEE11a, RRR99, ISO97, ISO04, JBJ94]. **Teil** [Pei82]. **Teletraffic** [CS93b]. **Tempe** [Gol92, Yu92]. **Template** [LMC07, SP21, SK20]. **Templates** [JTOT09, AGBR19]. **Temporal** [GY91, SHZ+20, WYD+18, CWC10, FXWW17, MHT+13]. **temporaries** [Ken73]. **TENCON** [Ano93c]. **Tennessee** [IEE94c]. **Tenth** [DSS84, SC77, YR87]. **Terabytes** [IEE02]. **term** [KP92, LLT21]. **termination** [Er86]. **Terms** [Wil79, ZWCL10, vT14]. **ternary** [Bou95, KTDB20]. **Terrorism** [GRBCC19]. **Tertiary** [Gui75]. **Test** [Har71a, RT87a, Sav90, Duc08, ZCZQ19].

Testbed [SDK91]. **Testing** [Boo73, DD11, Fil02, Sam76, WM19, AY14, HKLS12, TD93]. **Tetris** [GSS01]. **Tetris-Hashing** [GSS01]. **Tex** [ACM91b]. **Texas** [ACM91b, ACM97b, ACM98, IEE76, USE00b, ACM88a, IEE95, Nav85]. **Text** [Bur81, Coh98, CDW+19, DS84b, Dit91, Fal85b, Gon83, HZ86, Lit91, Pea90, Pea91, Sav91, TT82, Ven84, YSW+11, Gob75, HC07, Ram89b, RCF11, Sab94, ZZLZ18, ZHW01]. **textes** [LG78]. **Texts** [LG78]. **Textual** [BH85, MLHK17]. **Texture** [HSPZ08, ŠSaS01, XZPG21]. **th** [KKT91]. **Their** [CZLC12b, CK15, CJ19, Deb03, Gra88, Gra89, Heu87, HK12b, NR12, RNT90, SDT75, WC81, AG10, adHMR93, NY89b, NY89a, PW08, Pob86, Sie89]. **Theorem** [Cha84b, CG92, HR14, Kno88, Sho00a]. **Theoretic** [Sun15, HM93, SXLL08, TZ94a, vL94]. **Theoretical** [AH03, CHK06, RRR99, TWW77]. **Theory** [ACM75c, ACM75a, ACM76, ACM77b, ACM82, ACM84b, ACM86b, ACM88b, ACM89c, ACM90, ACM91e, ACM96, ACM97b, ACM98, ACM01, ACM02, ACM03a, ACM07, ACM08b, ACM11, ACM12, AA86, BBPV11, CP87, CP88, CS93b, Dam90a, Dam91, Dav91, Fel50, HP63, Hel94, IEE74, CTC90, IRM93, KM86, KM88a, KGJØ18, LC06, LK11, LL83, Mir17, Pip79, QV89, QV90, QG95, Rue93, ACM77a, SZ93, Sti06, Vau06, Yan10, De 95, GQ95, Hua82, ISO97, Kil05, PSN95, Tso15, Kil05]. **There** [AKS78]. **thesaurus** [RW73]. **things** [SKD15]. **Think** [DCW91]. **Third** [ACM91e, jCPB+12, ICD87, IEE88a, BDS88, Gol96, Ano89]. **Third-Round** [jCPB+12]. **Thirteenth** [Kna89]. **thirtieth** [ACM98]. **Thirty** [ACM03a, IEE88a]. **Thirty-Fifth** [ACM03a]. **Thirty-Third** [IEE88a]. **Thiry** [ACM02]. **Thiry-Fourth** [ACM02]. **Thousand** [KRJ+80]. **Thousand-Word** [KRJ+80]. **thousands** [BMS+17, Nic17]. **thrash** [BFCJ+12]. **Threaded** [VB00]. **Threading** [SMZ18]. **Threads** [Lep98]. **Three** [Ano95a, MLxx, MP12, SP89, Tro95, FH15]. **Three-way** [SP89]. **Threshold** [Wee11]. **Throughput** [KHK15, LPT12, LLL+16, PRM16, TP15, WZJS10, MAK+12, XLZC14]. **Thyroiditis** [ŠSaS01]. **Tiger** [AB96, MR07]. **Tight** [Cha94, CV08, GHK+12, vT14]. **Tightly** [Mul81, DW05, DW07]. **Tillich** [Gei95, Gei96, GIMS11, PVCQ08, TNS20]. **Time** [ASBdS16, BJL16, Blo70, Bre73, BM99, CW09, CJKK19, Cip93, Cla77, CM93, DadH90, F+03, FPS13, FKS84, GK76, Gra94b, Jak85, Kab87, LAKW07, Lip02, Lyo83, Moh11, NI83, NS16b, PP08, PSSC17, PWY+13, PS12, Sag85a, SL16, Sie04, TW91, Val15, WVT90, Win90b, AY14, ASA+09, CJMS19, CCY91, DSD95, FPSS05, FVS12, GB17, GMW90, Han17, Kor08, Man12, MV91a, MN90, MP90, OP03, Par18, Pro18, Sie89, ZRL+08]. **Time-Memory** [ASBdS16, CJMS19]. **Time-Series** [BJL16]. **time-space** [Sie89]. **Time-Stamping** [Cip93, Lip02]. **Timer** [VL87, VL97]. **Times** [Mal77, SD78, PY88]. **Timestamps** [GY91]. **Timing** [VL87, VL97]. **Tiny** [GW94, OWZ14, SWQ+14]. **title** [Dit76]. **Tk** [USE00b]. **TMIS** [GTL21]. **TN** [ACM94c]. **To-many** [SV18]. **to-one** [SV18]. **Tokyo** [IJW89, A+90, Mo92b]. **Tolerant** [DSSW90a, AAB+92, DSSW90b, HGR07]. **Too** [CHSC18]. **Tool** [Lit79b, Lit80, Litxxa, MV01]. **Toolbox** [Jac92]. **Toolkit** [FZ87]. **Tools** [Mil87, JC88b]. **Top** [APV07, LRY+15, LLG+17, ZLC+12]. **Top-** [APV07, LLG+17]. **Top-Down** [LRY+15, ZLC+12]. **Topic** [RTK12, Gre95]. **Topic-Specific** [RTK12]. **Topics** [Joy03]. **Topology** [RHM09, Ati20]. **Toronto** [Gil77, KLT92]. **torrent** [Bak09]. **Towers**

[ICD88, ICD90]. **TPM** [WYD+18]. **Traceback** [JL14, SXLL08]. **Tracing** [SS89b]. **Track** [Joy03]. **Tracking** [GGR04, LLL11, UCFL08, FXWW17, ML15, OOK+10]. **Tractability** [GB10]. **Trade** [ASBdS16, Blo70, CJMS19, GW94, Sar11]. **trade-off** [CJMS19, GW94, Sar11]. **Trade-Offs** [ASBdS16, Blo70]. **tradeoff** [Sie89]. **Tradeoffs** [SD89b, SD90b, SD90a]. **Traditional** [EMM07]. **Traffic** [TLLL18, HKL04, MA15, TBC+05]. **tragen** [BJMM94b, BJMM94a]. **Transaction** [CCW+17, SPB88, MTB00, SSU+13, TMB02, Yu92]. **Transactional** [ZLLD18, BRM10, SSU+13]. **Transactions** [CHSC18, FK89, MMC01, SSU+13]. **Transfer** [HK12a]. **Transform** [BR06, GH07, HB89c, HB94, LC12, LYD71, NS16a, PVM94, RGNMPM12, LY72, Pob86, Ind13]. **Transform-Based** [RGNMPM12]. **Transformation** [Lum73, NXB13, SR63, ZLLD18, Lin63, PT10b]. **Transformations** [GG86a]. **Transforms** [Zha07]. **Transition** [SP21]. **Transitive** [CdM89, CdM90, GC90]. **Translated** [WSZ+16]. **Translation** [BCR10, TK85]. **Translators** [DGGL16]. **Trapdoor** [HHL10, Wee12, LWG11, PW08]. **Trapdoors** [GPV08]. **Traversal** [CLC06, Lip02, YSEL09]. **Tree** [And91, AR17, BT12b, FB87, GadHW96, KHT89, Lip02, LRY+15, LB07, Lyo83, Omi88, Oto86, Piw85, SD89b, SG76b, SM87, WS93, Wil00, Ati20, BLY20, BDPV14, BPT10, CLS95, DSD95, GB17, HLL18b, KW94, LŁA15, MFES04, Omi89a, THS97, War14]. **Tree-Structured** [Piw85, BPT10]. **Trees** [BM76, BD84, BBP88, CLYY92, CHY93, CLYY95, CN07, CD84b, DCW91, Dev99, LQZH14, Reg81, She78, VV84, Wil00, AD08, Bra09, CM01, FP82, FK89, KLL+97, Kos14, Lev89, QP16, RRS07, TB91, BD84]. **Trends** [Rie89]. **Triangle** [IEE89, JTOT09]. **triangular** [GPGO16]. **Trick** [DR09, NMQ22]. **Trie** [AR16, Bur76b, Bur77, CCH09, Fla81, FS82, Fla83a, KS12, Lit81, Lit85, LZL88, LSV89, LRLW89, LRLH91, Oto88b, Reg88, Tv83, AR21, AZ10, BLC12, Bur76a]. **Trie-** [KS12]. **Tried** [ATT98]. **Tries** [BT94a, BT94b, GO15, Tam81, PBBO12, Pro18, SV15a, SV15b, SV18]. **trigger** [ZLY+13]. **Trigram** [Wil79]. **triple** [LWG11]. **triple-trapdoor** [LWG11]. **triplet** [LLT21]. **Troika** [KTDB20]. **Trondheim** [Ano95c]. **truncated** [FJ13]. **Truncating** [Sol93]. **Truncation** [Wil79]. **Trusted** [KKRJ07, KRJ09b]. **Trustworthy** [EH12, LW17]. **trx** [LW17]. **Tsunami** [CZL12]. **Tulip** [XBH06]. **Tunable** [AÖD19]. **Tunable-LSH** [AÖD19]. **tuned** [EFMRK+20]. **Tuning** [KNT89, PRRR15, Tym96, Vit80a]. **tuple** [WHS+07]. **Turbo** [Hej89]. **TV** [YGC+12]. **Tweakable** [MKASJ18]. **Tweaking** [Zha07]. **tweets** [STS+13]. **Twelfth** [BV89, CGO86, Col93]. **Twentieth** [ACM88b, IEE01, Mat09]. **Twenty** [ACM89c, ACM90, ACM91e, AAC+01, AOV+99, Van10, GSW98, LL08, ACM96, ACM97b, IEE01]. **Twenty-Eight** [Van10]. **twenty-eighth** [ACM96]. **Twenty-fifth** [AOV+99]. **Twenty-fourth** [GSW98]. **twenty-ninth** [ACM97b]. **Twenty-Seventh** [LL08, AAC+01]. **twig** [KRML09]. **Twisted** [PT13, DT14]. **TWISTER** [FFGL10, FFGL09]. **Twitter** [RTK12]. **Two** [DDMM05, DAC+13, HK12a, HSIR02, Jv86, KSSS86, Leb87, LMPW15, Lyo85, ML15, Pan05, Pip94, PGV90a, TC93, CCL91, Con17, DKRT16, GP08, Li10, MS09, McN03, PGV93a, PGV93b, QZD+18, SDR83b, MKL21]. **two-bit** [MKL21]. **two-channel** [MS09]. **Two-Dimensional** [KSSS86, Leb87]. **Two-Disk** [TC93]. **Two-level** [DAC+13]. **Two-Message** [HK12a]. **Two-permutation-based** [LMPW15]. **two-stage** [QZD+18]. **Two-Way** [DDMM05]. **TWOBLOCK**

[Yan05]. **TX** [USE91, ACM87, ARA94, IEE94a]. **Type** [KPS92, KRJ09a, TNS20, SF88, SG16, SV18]. **Type-based** [KRJ09a]. **Type-Graphs** [KPS92]. **type-heterogeneous** [SV18]. **Types** [EjKMP80, Hej89, Rog19b, SW87, Wal88, LPSW03, NMS+08]. **TYPHOON** [HKW05]. **typing** [DMP09].

Überlegungen [Kue84a]. **Uebersicht** [Mer72]. **UK** [AOV+99, Boy95b, Dav91, Gol96]. **UL** [DSS17]. **Ultra** [QXL+20, WZJS10, YBQZ18]. **Ultra-Fast** [YBQZ18]. **Ultra-Low-Latency** [QXL+20]. **uncertain** [BZZ12]. **Undergraduate** [Tro92]. **Undergraduates** [Pag06]. **Understanding** [Dun89a, Dun89b]. **Unequal** [Gon80]. **Unequal-Probability** [Gon80]. **unicast** [ATAKS07]. **unicorn** [LW17]. **Unification** [Büt86, Cra85]. **Unified** [JV16, Mul84a, Mul84b, ABO+17, BOY11]. **Uniform** [ABH+73, AT93, Gui89, Kie85, KS86, KS87b, Lar83, Leb87, LQZH14, LPP91, LPP92, Mal77, OP03, PP08, PCK95, Ruž08, UHT95, Yao85b, Ald87, AT90, MC89, Rad92]. **Uniform-Grid** [Leb87]. **uniformly** [MLP07]. **Unifying** [BG80, BG82]. **Unique** [Boo74, DLH09, DLH13, SD78, ASW87]. **Uniqueness** [Kah92]. **Unit** [BC90, HO72]. **United** [ACM94b, JBJ94]. **Units** [LLLC17, WB87, SF88]. **Universal** [Abi12, AS96, BKST18, Bie97, Bra09, CW77a, CW77b, CW79, CJKK19, CS02, DadH90, DadH92, Die96, DS09c, EPR99, Für88, GC95, HHR+10, HJ96, JCK+18, Kil01, KR01, LK14, MNT90, MCW78, Meh82, Mul91, Nae95, NY89b, NY89a, NP99, NR12, Ram88b, Sar80, Sho96, Sho00a, Sie04, Sti91, Sti94a, Sti94b, Woe01, van94, ACP10, Bie95, DS09b, IIL17, KYS05, KL96, KR06, LK16, LC13, MNT93, Sar11, Sar13, Sie89, Tho00, Woe05, Woe06a]. **universality** [SS89a]. **universe** [Bra09, Wen92]. **Universes** [DS09c]. **Universitat** [CTC90, Dit76]. **Universiteit** [BBD09b]. **University** [ACM81, IJW89, CCC89, CRS83a, HB93, IEE74, Jáj90, Lie81, Oxb86, Pat90, Sch82a, Dit76]. **universum** [Wen92]. **UNIX** [SY91, WG00]. **Unknown** [LCL+20]. **Unlabeled** [GCMG15]. **unleash** [McN03]. **Unlimp** [Kah92]. **unsafe** [Con17]. **unsigned** [BCS89]. **Unstructured** [Gon83, PFM+09]. **Unsupervised** [CJN20, PKW09]. **Untersuchung** [Stu82]. **Unveiling** [WZY+18, BCCL10]. **UOWHFs** [BR97]. **updatable** [ZYWM20]. **Update** [Ano95a, GO07, GGR04]. **Updates** [LCLX19]. **Upon** [CS83b, Cha84b, CS87, CW91]. **Upper** [DKM+88, DKM+94, GadHW96, DKM+91]. **URAL** [GT63]. **URAL-2** [GT63]. **URLs** [AY14]. **urn** [Ram87]. **USA** [ACM03a, ACM07, BD88, Bel00, Bri92, Bri93, BD08, Cop95b, Deb03, DJNR09, FNY92, Fra04, Fre90, Van10, GSW98, Joy03, Ker75, Kil05, Lom93, Sho05, Sti93, Sti94c, Wie99, Yun02, ACM94d, ACM11, ACM12, FMA02, HF13, ICD86, ICD87, ICD88, IEE88b, ICD90, IEE01, IEE02, IEE05, IEE10, IEE11b, IEE13, MS05, USE91, USE00a, USE00b]. **Usability** [BDS88, Sch82a]. **Use** [ACM75b, AT18, Bal05, BK84, Bor81, Bra84a, Bra85, Bra86, BC90, Gur73, NR12, Rad70, WC81, Er86, adHMR93, RK15, Vak85, YIAS89]. **Used** [Stu85, GS94, Sch91a]. **USENIX** [USE91, USE00b, USE90]. **User** [RTK12, YY07, Bor81, DFMR15, HL12, LLH02, LKY04, YRY04]. **Using** [ANS97, ASW07, BDPSNG97, Bar97, BRM+09, BCK96b, Bor84, BÖS11, BM90b, BI12, BT94a, BT94b, BM01, BT12b, BMLLC+19, CP95a, CRdPHF12, CKB85, CdM89, CdM90, CLYY92, CCW+17, CJC+09, CJKK19, Cle84, CD84b, CE70, CRR18, CY06, DLT98, Dav73, DK07, Dod82, DL12, DSSW90a, DGKK12,

EFMRK+20, Fal85a, FLF11, FRB11, FJ13, GRBCC19, Ger86b, Gir87, Gre21, Gri77, GPA97, GAS+16, Har97, HG77, HNS84, HKY12, JRPK07, JTOT09, JD12, JK11, Kab87, KSSS86, KM07, LK07, LAKW07, LQZH14, LR99, LMD+12, Lum73, MS02, MPP14, MBBS12, MNY81, McK89a, MH00, Moh90, Moh93, MJT+02, Mul72, NKT88, NI83, OTKH11, OG94a, Omi89b, PAPV08, PPS21, PLKS07, PKW09, PF88, PW94, QG89, QG90, RL89, RLT83, RSD85, RSSD92, Rey14, Rob86, SD78, SS83]. **Using** [SRY99, Sho00b, SW86, SK05, Som99, SA97, SKM01, TK88, TC93, TA81, TA86, TGGF10, TK85, TS85, Tsa96, US09, VV84, WPKK94, Wan14, WLWZ19, WDP+12, Wil96, Wil79, WM19, YY07, YBQZ18, AÖD19, BSNP96b, BLC12, BK07a, BF08, BT90, BGG12, CDS20, CKB81, CHL07, CKKK09, CP13, CT96, DS09a, DMPP06, DKT06, DS09b, DSSW90b, EH17, Fal86, FM89, Fly92, GTL21, GKKT10, GG92, Ger86a, GDGK20, Gob75, GBL94, HDCM11, HKL07, HKLS12, HC14, Hil88, HC02, HW88, HXLX13, ISO97, JFDF09, JLH08, JL14, JCC00, JBWK11, JMH02, Ken73, Kim99, KJS17, Kos14, Ku04, LG96, LLH02, LKY04, LW04, LNS11, LDK12, LK16, MMC01, McK89b, MMG10, MP16, Mue04, Oka88, PCK95, RSSD89a, RSSD89b, RGNMPM12, Rön07, SK20, SB95, Sar11, STS+13, Tho17, UHT95]. **using** [XZPG21, YTHC97, YL04, YRY04, ZGG05, ZW05, ZLY+13, ZRL+08]. **USSR** [GLB21, Zuk21]. **Utah** [SM08, Nam86, SM12]. **utentibus** [DMPP06]. **Utilisation** [OT91]. **Utility** [HNKO20]. **Utility-** [HNKO20]. **Utilization** [PS12, Wil71, CF89b]. **Utilizing** [KAS+22, KK85]. **Utrecht** [vL94]. **UUID** [BŠH12].

V [PHL01]. **v1.4.0** [Sun02]. **VA** [ACM94d, ACM94a]. **Valdivia** [CHK06]. **Validation** [ML86]. **valuation** [JDW+19]. **Value** [DGD02, GIS05, Gra99, GYW+19, JLL+20, LLL+16, LCM+20, MZL+19, NS16a, PRRR15, PRK98, QXL+20, SDZ21, Cli95, MK12, Mil95, Shi17, WLC20]. **valued** [DH84, HM03]. **values** [ASW87, GS94, SB95]. **Vancouver** [ACM05, LL08, Yua92]. **Variable** [Dit91, Lit91, MF92, Mar64, OGAB14, PHL01, Pea90, Pea91, Sam76, Sav90, Sav91, ZPS90, ZPS93a, RKK14, ZPS93b]. **variable-increment** [RKK14]. **Variable-Length** [MF92, Pea90]. **Variables** [Die96]. **Variant** [AAE+14, McI63, PS12, PVCQ08]. **Variants** [CV83b, CV84, CV85, VNP10]. **Variationally** [KR06]. **varieties** [FH15]. **variety** [Zha19a]. **Various** [LG78, WPS+12]. **Varying** [Wil79]. **Vault** [LMC07, LMJC07]. **VAX** [JC88b]. **VAX/VMS** [JC88b]. **VBF** [ÁCZ16]. **Vector** [ÁCZ16, Kaw15, LH20, PG95, SB93, Kan91, Kan93]. **Vectorization** [Kan90]. **Vectors** [Blu95, MI84, WZ93]. **Vegas** [AFI69, IEE10]. **vehicle** [LWG11]. **Vehicular** [GZX14]. **Venti** [QD02]. **verarbeitung** [Nie75]. **verfahren** [Hil82]. **Verfahrens** [Pet83]. **Vergleich** [DS84a]. **Vergleichende** [Hil82]. **Verification** [CLS12, EH12, Lew82, MJT+02, YKLH10, CE95, KRJ09a, SD95, Tsa08, YLC+09, ZKR08]. **Verified** [BGH12, BGH+13]. **Versa** [Hol13]. **Versatile** [CBA94]. **Version** [Coh84, HPC02, JXY07, Kut10, Lar82c, Lar82d, Lar85c, WG94, CMR98, GM18]. **Versions** [HSR+01, CV05]. **Versus** [BD84, CF89b, DSS17, GLS91, SvEB84]. **vertex** [ZBB+06]. **Verwaltung** [Pet83]. **verwaltungsdaten** [Pei82]. **Very** [ABB93, VLD82, AW89, AAC+01, AOV+99, BD88, BCH87, BJZ94, CGO86, Chu90, DSS84, DT91a, DT91b, Gon83, GSW98, HB89a, HB92, Hil78b, Hil78a, Ker75, KR79, KS87a, KS87b, LT80, LSC91, MSDS90, PV85, ST83a, ST83b, Yao78, Yua92, DC94, HB89b, KS89b, VLD82, AW89, CGO86, DSS84,

LSC91, MSDS90, PV85, Yao78, Yua92]. **VHAM** [Lit77b]. **VHP** [LWWK20]. **Via** [CKN18, GH07, YTJ06, BHKN13, BHKN19, BDPV09, BJKS93, BJKS94, CFN18, DOP+14, Die96, EPR99, GIM99, HHR+10, Ind13, KM86, KM88a, KZ19, Lep98, LCLX19, LC12, LWWK20, PT11b, PKSB18, SD90b, SD90a, TYZO15, TLZL16, TMW10, Wee11, Woe01, Woe05, ZCZQ19, ZHX+21]. **Vice** [Hol13]. **Victoria** [ACM08b]. **Video** [GRBCC19, OTKH11, PPS21, SHZ+20, TCY+20, WP10, CWC10, DVS+14, OCDG11, QJ97, SB14, YCJ12]. **Vienna** [ICD93]. **View** [BM89, BM90a, GRZ93, XZPG21]. **viewed** [vT14]. **Viewpoint** [Mal77]. **Virginia** [WGM88]. **Virtual** [Lit78, Lit79b, Litxxb, Ste82, TK85, YLZ20, AS09, Lev89, LWWK20, Wie86]. **Virtual-Circuit** [Ste82]. **Virtualization** [MZD+18]. **Virtualized** [HBL+10]. **Virtuel** [Lit77b, Lit79a]. **Virus** [LLL11]. **Vision** [IEE88b, HCF95, KI94]. **Visual** [MLHK17, PSSC17, XNS+13, YWH09, DVS+14, ML15]. **Visual-Textual** [MLHK17]. **Visualization** [MW95]. **VLDB** [Yua92]. **VLSI** [Rei88, AS89, EBD91, Für88]. **VMPC** [Sar15]. **VMS** [JC88b]. **Vocabularies** [Wil79, LK93, ZHW01]. **Vocabulary** [KRRH84, LLZ10, YWH09, YMI89]. **Vocabulary-Based** [LLZ10]. **Voice** [SMS91]. **Volatile** [ZH18, CCA+12, MSZ+20]. **Volcano** [Gra94c]. **volumes** [Ruc15]. **volumetric** [ZDI+15]. **Vorschlaege** [Kue83]. **Vortex** [GK08]. **Vowel** [Wan05]. **Vowel-consonant** [Wan05]. **VPN** [KMM+06]. **vs** [BATÖ13, GLS94, KKL+09, Oak98]. **Vulnerability** [BPBBLP12].

W [Hül13]. **W-OTS** [Hül13]. **WA** [LCK11]. **WADS** [DSZ07a, DSZ07b]. **Wait** [LFD17]. **Wait-Free** [LFD17]. **Walk** [FMM09, FMM11, BCR10]. **wallet** [Nic17]. **Warehouse** [ZZ83]. **Warwick** [Pat90]. **Was** [HJ75]. **Washington** [ACM84b, ACM89c, BJ93, Fis87]. **Watermarking** [DR11, WDP+12]. **Wave** [LC12]. **Wavelet** [GH07]. **Way** [BCFW09, DGV93, DDMM05, GK08, HHR+10, JLH08, LP15, McC79, Mer90b, Roe94, Rul93, SP91, Sch91a, Sho00a, Tsu92a, Wee07, Win83, Win84, YZ00, Zhe90, CMR98, Gib91, HR07, HYLT99, HL03, KST99, LW04, LHC05, Mer90a, MZI98, NY89b, NY89a, Sim98, SP89, Tsa08, Tsu92b, YL04, ZW05, ZPS90, ZMI91, ZPS93a, ZPS93b, HMNB07]. **WCC** [Ytr06]. **WDDL** [MMMT09]. **Weak** [CFP19, HS08, Lis07, PV07]. **Weaknesses** [BPSN97, DS09c, KCL03, KCC05, SGGB00]. **web** [KSC11, KSC12, NMX19, AT18, KLL+97, KSB+99, NM02b, Sch01b, SKC07, TC04, UCFL08, WY00, WY02, XBH06]. **Web-Based** [Sch01b]. **webcam** [McN03]. **Wegman** [Sar80]. **Weight** [LR96a, LL92]. **Weight-Partitioned** [LR96a]. **Weighted** [Ban77, Luc72, THY+18, Yao91, YZ00, SN19]. **Weighting** [DSS17]. **West** [Yao78]. **WG** [vL94]. **WHAM** [LPT12]. **Wheels** [VL87, VL97]. **Where** [Bur06, SW91]. **Which** [FW76, FW77]. **WHIRLPOOL** [RB01, Sas11, Sta06a]. **Whirlwind** [BNN+10]. **White** [BZZ12, IEE88c]. **whole** [Pat95]. **whom** [LC95]. **Whose** [Gra94b]. **WI** [FMA02]. **Wide** [KLL+97, MPST16]. **Wien** [Kui92]. **Will** [DCW91]. **windowed** [GDGK20]. **Winner** [Bou12]. **Winter** [USE91]. **Wireless** [DK09, DPH08, LDY+16, PLKS07, SHRD09, YSW+11, ZQSH12, AK09, ADF12, Cha12, LG13, LND08, YG10]. **Wise** [Ind01, Die96, FPS17]. **within** [Bay73b]. **Without** [GHR99, PV19, SL16, ASW87, Ati20, BK84, BRM10, CP95a, Dam93, Dam94, Die96, Jak85, KS88b, KS88c, Ku04, LW04, Mul81, Pag18, Par18, Reg82, SUH86, Tsa08, ZW05]. **Witnesses** [AN96]. **Wollongong** [PSN95].

Word [BH86, FLF11, KRJ+80, LHC05, BT89, Han17, ST85]. **Words** [Chu90, DM90, Dos78a, KR79, KRRH84, MH00, ST86, Tro06, Wol84, Zou85]. **work** [Col93, MV08]. **Working** [Cer85, CE95]. **works** [Gre95, LWXS18]. **Workshop** [IJW89, ABM06, ODB89, Ano92, BBD09b, BF89, BD08, CP87, CP88, Dam90a, Dam91, Dav91, De 95, DSZ07a, DSZ07b, DJRZ06, DJNR09, GQ95, Hel94, QV89, QV90, RRS06, Rei88, Rue93, SZ93, Ytr06, vL94, And94, Bir07, Coh94, Gol96, KI94, Yu92, Ano94, Heu87]. **World** [Ano93a, Dre17c, IEE92a, LC95, KLL+97]. **worm** [FNP09, CF89b]. **Worst** [ANS09, ANS10, DMV04, F+03, FKS84, Lar81, Lar82a, FPSS05, Mic02, MT16]. **Worst-Case** [ANS09, ANS10, DMV04, Lar82a, Lar81, Mic02]. **worst-case/average-case** [Mic02]. **Wörterbücher** [Wen92]. **Write** [Moh90, Moh93, MNS07, ZH18, ZHZ+19]. **Write-Ahead** [Moh90, Moh93]. **Write-Friendly** [ZH18]. **Write-Once** [MNS07]. **Wrocław** [ACJT07]. **WSN** [DL12]. **WSNs** [YLSZ19]. **Wyner** [DVS+14].

x [PvO95]. **X9.30** [ANS97]. **X9.30-2** [ANS97]. **X9.62** [ANS05]. **Xeon** [JHL+15]. **XML** [CN07, KRML09, MK12, WLLG08, WWZ09]. **XMSS** [HRB13, HBG+17]. **xor** [FJ13, CCHK08, MLP07, VD05, vdBGLGL+16]. **XOR-based** [CCHK08, VD05]. **XPS** [Ger95]. **XRDB** [YNKM89]. **XSB** [SSW94]. **XTEA** [CV05].

year [Roe95]. **Years** [Kon10, IEE01, KR19]. **Yi** [Wag00]. **Yi-Lam** [Wag00]. **Ynot** [NMS+08]. **Yokohama** [AiNOW11]. **Yoo** [KCC05]. **Yoon** [KCC05]. **York** [ACM12, GSW98, HF13, IEE90, IEE99, Mat09, IEE90, IEE99, Jen76]. **Yorktown** [Jen76]. **YY** [Nat92].

Zahlen [BJMM94b, BJMM94a]. **Zakopane** [Win78]. **Zeiteffizienten** [Kue83]. **Zemor** [Gei95, Gei96, GIMS11, PVCQ08, TNS20]. **Zero** [CLP13, Dam93, OVY94b, Dam94, OVY94a]. **Zero-Knowledge** [CLP13, Dam93, OVY94b, Dam94, OVY94a]. **Zheng** [PGV93a, PGV90a, PGV93b]. **Zheng-Matsumoto-Imai** [PGV93a, PGV93b]. **Zipper** [LWWQ08]. **Ziv** [DVS+14]. **Zoning** [GRZ93]. **Zugriffsoperationen** [Pei82]. **zugriffsverfahren** [Stu82]. **zum** [Eck74a]. **zur** [Koe72, Kue83, Kue84a, Pet83]. **Zurich** [HKNW07, Lak96].

References

ACM:1969:PAN

[??69] ??, editor. *Proceedings 1969 ACM 24th National Conference*. ACM Press, New York, NY 10036, USA, ?? 1969. LCCN ??

Asano:1990:ISS

[A+90] Tetsuo Asano et al., editors. *Algorithms: International Symposium SIGAL '90, Tokyo, Japan, August 16–18, 1990: Proceedings*, volume 450 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. ISBN 0-387-52921-7. LCCN QA9.58 .I58 1990.

Anderson:1979:CPH

[AA79a] M. R. Anderson and M. G. Anderson. Comments on perfect hashing functions: a sin-

gle probe retrieving method for static sets. *Communications of the Association for Computing Machinery*, 22 (2):104, February 1979. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Corrects errors in [Spr77]. See also corrigendum: [AA79b].

Anderson:1979:CCP

[AA79b] M. R. Anderson and M. G. Anderson. Corrigendum: "Comments on Perfect Hashing Functions: A Single Probe Retrieving Method for Static Sets". *Communications of the Association for Computing Machinery*, 22 (10):553, October 1979. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Corrects [AA79a].

Ausiello:1986:IIC

[AA86] Giorgio Ausiello and Paolo Atzeni, editors. *ICDT '86: International Conference on Database Theory, Rome, Italy, September 8–10, 1986: proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1986. ISBN 3-540-17187-8. LCCN QA76.9.D3 I55824 1986.

Ajtai:1992:FTG

[AAB+92] M. Ajtai, N. Alon, J. Bruck, R. Cypher, C. Ho, M. Naor, and E. Szemerédi. Fault tolerant graphs, perfect hash functions and disjoint paths. In IEEE-FOCS'92 [IEE92b], pages 693–702. ISBN 0-8186-2900-2. LCCN QA 76 S979 1992.

Apers:2001:PTS

[AAC+01] Peter M. G. Apers, Paolo Atzeni, Stefano Ceri, Stefano Paraboschi, Kotagiri Ramamohanarao, and Richard T. Snodgrass, editors. *Proceedings of the Twenty-seventh International Conference on Very Large Data Bases: Roma, Italy, 11–14th September, 2001*. Morgan Kaufmann Publishers, San Francisco, CA, 2001. ISBN 1-55860-804-4. LCCN QA76.9.D3 I559 2001.

Albertini:2014:MHE

[AAE+14] Ange Albertini, Jean-Philippe Aumasson, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Malicious hashing: Eve's variant of SHA-1. In Joux and Youssef [JY14], pages 1–19. ISBN 3-319-13050-1 (print), 3-319-13051-X (e-book). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25. URL `http://eprint.iacr.org/2014/694`; `http://link.springer.com/chapter/10.1007/978-3-319-13051-4_1`; `https://maliciousshaa1.github.io/`.

Anshel:2016:CHF

[AAGG16] Iris Anshel, Derek Atkins, Dorian Goldfeld, and Paul E.

Gunnells. A class of hash functions based on the algebraic eraser^{TM}. *Groups. Complexity. Cryptology*, 8 (1):1–7, 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Aamodt:2003:CSP

[Aam03] Ken S. Aamodt. *A cryptographically secure pseudorandom number generator*. Ph.D. thesis, Purdue University, West Lafayette, IN, USA, December 2003. 147 pp. URL `http://catalog.lib.purdue.edu/Find/Record/1380784`; `http://search.proquest.com/docview/305316022?accountid=14677`.

Anderson:1996:TFN

[AB96] Ross Anderson and Eli Biham. Tiger: a fast new hash function. *Lecture Notes in CS*, 1039:89–97, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/link.asp?id=fx0261047446n136`; `http://www.springerlink.com/openurl.asp?genre=article&id=doi:10.1007/3-540-60865-6_46`; `http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=1039&spage=89`.

Aumasson:2012:SFS

[AB12] Jean-Philippe Aumasson and Daniel J. Bernstein. SipHash: a fast short-input PRF. *Lecture Notes in CS*, 7668: 489–508, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-34931-7_28`.

Alwen:2017:TPA

[AB17] Joël Alwen and Jeremiah Blocki. Towards practical attacks on Argon2i and balloon hashing. In IEEE, editor, *Proceedings 2nd IEEE European Symposium on Security and Privacy, 26–28 April 2017, Paris, France*, pages 142–157. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2017. ISBN 1-5090-5761-7. LCCN ???? URL `https://ieeexplore.ieee.org/document/7961977`. IEEE Computer Society Order Number E6100. See [BDK16, BCGS16].

Agrawal:1993:ICV

[ABB93] Rakesh Agrawal, Seán Baker, and David Bell, editors. *19th International Conference on Very Large Data Bases, August 24th-27th 1993, Dublin, Ireland Proceedings*, Proceedings of the International Conference on Very Large Data Bases. Morgan Kaufmann Publishers, San Francisco, CA, 1993. ISBN 1-55860-152-

X. ISSN 0730-9317. LCCN QA76.9.D3 I61 1993.

Ahmed:2016:RN

[ABC+16] Reaz Ahmed, Faizul Bari, Shihabur Rahman Chowdhury, Golam Rabbani, Raouf Boutaba, Bertrand Mathieu, Reaz Ahmed, Faizul Bari, Shihabur Rahman Chowdhury, Golam Rabbani, Raouf Boutaba, and Bertrand Mathieu. αroute: Routing on names. *IEEE/ACM Transactions on Networking*, 24 (5):3070–3083, October 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Andreeva:2016:NSP

[ABD+16] Elena Andreeva, Charles Bouillaguet, Orr Dunkelman, Pierre-Alain Fouque, Jonathan Hoch, John Kelsey, Adi Shamir, and Sébastien Zimmer. New second-preimage attacks on hash functions. *Journal of Cryptology*, 29(4):657–696, October 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s00145-015-9206-4`; `http://link.springer.com/article/10.1007/s00145-015-9206-4`.

Arnold:1973:UHA

[ABH+73] R. F. Arnold, W. E. Bass, M. H. Hartung, F. D. Snow, and R. D. Stephens III. Uniform hashing algorithm. *IBM Technical Disclosure Bulletin*, 16(7):2214–2216, December 1973. CODEN IBMTAA. ISSN 0018-8689.

Abidin:2012:SUH

[Abi12] Aysajan Abidin. On security of universal hash function based multiple authentication. *Lecture Notes in CS*, 7618:303–310, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-34129-8_27`.

Azar:1999:BA

[ABKU99] Yossi Azar, Andrei Z. Broder, Anna R. Karlin, and Eli Upfal. Balanced allocations. *SIAM Journal on Computing*, 29(1):180–200, February 1999. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/28849`.

Ailamaki:2006:PIW

[ABM06] Anastassia Ailamaki, Peter Boncz, and Stefan Manegold, editors. *Proceedings of the 2nd International Workshop on Data Management on New Hardware: 2006, Chicago, Illinois, June 25–25, 2006*. ACM Press, New York, NY 10036, USA, 2006. ISBN 1-59593-466-9. LCCN

QA76.9.D3 I58388 2006. URL http://portal.acm.org/toc.cfm?id=1140402.

Andreeva:2012:SAS

[ABM+12] Elena Andreeva, Andrey Bogdanov, Bart Mennink, Bart Preneel, and Christian Rechberger. On security arguments of the second round SHA-3 candidates. *International Journal of Information Security*, 11(2): 103–120, April 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0156-7.

At:2017:LAU

[ABO+17] Nuray At, Jean-Luc Beuchat, Eiji Okamoto, Ismail San, and Teppei Yamazaki. A low-area unified hardware architecture for the AES and the cryptographic hash function Grøstl. *Journal of Parallel and Distributed Computing*, 106(??): 106–120, August 2017. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731517300485.

Amdahl:1953:xxx

[ABRS53] Gene M. Amdahl, Elaine M. Boehme, Nathaniel Rochester, and Arthur L. Samuel. ??? The year is uncertain (???). Amdahl originated the idea of open addressing with linear probing, which was later independently rediscovered and published [Ers58b]. The term 'open addressing' was apparently first used in [Pet57] [see [Kno75, page 274].], 1953.

Atkinson:1974:FPQ

[AC74] L. V. Atkinson and A. J. Cornah. Full period quadratic hashing. *International Journal of Computer Mathematics*, 4(2):177–189, September 1974. CODEN IJCMAT. ISSN 0020-7160.

Arge:2007:ALP

[ACJT07] L. (Lars) Arge, Christian Cachin, Tomasz Jurdzinski, and Andrzej Tarlecki, editors. *Automata, languages and programming: 34th international colloquium, ICALP 2007, Wrocław, Poland, July 9-13, 2007: proceedings*, volume 4596 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-73419-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267 .I55 2007. URL http://site.ebrary.com/lib/stanford/Doc?id=10251846; http://www.myilibrary.com?id=135198; http://www.springerlink.com/content/978-3-540-73419-2; http://www.springerlink.com/openurl.

asp?genre=book\%26isbn=978-3-540-73419-2; http://www.springerlink.com/openurl.asp?genre=issue\%26issn=0302-9743\%26volume=4596.

Ackerman:1974:QSH

[Ack74] A. Frank Ackerman. Quadratic search for hash tables of size p^n. *Communications of the Association for Computing Machinery*, 17(3): 164, March 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

ACM:1975:PSA

[ACM75a] ACM, editor. *Proceedings of Seventh Annual ACM Symposium on Theory of Computing, Albuquerque, New Mexico, May 5–7, 1975*. ACM Press, New York, NY 10036, USA, 1975.

ACM:1975:DUO

[ACM75b] *Data: Its Use, Organization and Management: ACM Pacific 75, Sheraton-Palace Hotel, San Francisco, April 17–18, 1975*. ACM Press, New York, NY 10036, USA, 1975.

ACM:1975:CRS

[ACM75c] *Conference Record of Seventh Annual ACM Symposium on Theory of Computing: Papers Presented at the Symposium, Albuquerque, New Mexico, May 5–7, 1975*. ACM Press, New York, NY 10036, USA, 1975.

ACM:1976:CRE

[ACM76] *Conference Record of the Eighth Annual ACM Symposium on Theory of Computing: Papers Presented at the Symposium, Hershey, Pennsylvania, May 3–5, 1976*. ACM Press, New York, NY 10036, USA, 1976.

SIGACT:1977:PNA

[ACM77a] ACM SIGACT, editor. *Proceedings of the Ninth Annual ACM Symposium on Theory of Computing*. ACM Press, New York, NY 10036, USA, 1977. LCCN QA76.6 .A13 1977.

ACM:1977:CRN

[ACM77b] *Conference Record of the Ninth Annual ACM Symposium on Theory of Computing: Papers Presented at the Symposium, Boulder, Colorado, May 2–4, 1977*. ACM Press, New York, NY 10036, USA, 1977.

ACM:1979:PSS

[ACM79] *Proceedings of the SIGPLAN Symposium on Compiler Construction: papers presented at the symposium, Denver, Colorado, August 6–10, 1979*, SIGPLAN notices; v. 14, no. 8. ACM Press, New York, NY 10036, USA, 1979. LCCN QA 76.7 A1095 v.14 pt.2.

ACM:1981:ASI

[ACM81] ACM, editor. *ACM-SIGMOD 1981 International Conference on Management of Data: [proceedings] April 29–May 1, The University of Michigan, Ann Arbor, Michigan*. ACM Press, New York, NY 10036, USA, 1981. ISBN 0-89791-040-0. LCCN QA76.9.D3 I59 1981.

ACM:1982:SPD

[ACM82] *Proceedings of the ACM Symposium on Principles of Database Systems: 29–31 March 1982, Marina del Ray Hotel, Los Angeles, California/Special Interest Group for Automata and Computability Theory (SIGACT), Special Interest Group for the Management of Data (SIGMOD)*. ACM Press, New York, NY 10036, USA, 1982. ISBN 0-89791-070-2. LCCN QA76.9.D3 A33 1982. US$24.00.

ACM:1983:PAS

[ACM83a] ACM, editor. *Proceedings of the 2nd ACM SIGACT-SIGMOD Symposium on Principles of Database Systems: 21–23 March 1983, Colony Square Hotel, Atlanta, Georgia*. ACM Press, New York, NY 10036, USA, 1983.

ACM:1983:PSA

[ACM83b] *Proceedings of the Second ACM SIGACT-SIGMOD Symposium on Principles of Database Systems: 21–23 March 1983, Colony Square Hotel, Atlanta, Georgia*. ACM Press, New York, NY 10036, USA, 1983. ISBN 0-89791-097-4. LCCN QA76.9.D3 A15 1983. US$25.00.

ACM:1984:SPA

[ACM84a] *SIGMOD '84: Proceedings of Annual Meeting, Boston, MA, June 18–21, 1984*. ACM Press, New York, NY 10036, USA, 1984. ISBN 0-89791-128-8. LCCN QA76.9.D3 A15 1984.

ACM:1984:PSA

[ACM84b] *Proceedings of the Sixteenth Annual ACM Symposium on Theory of Computing: Washington, DC, April 30-May 2, 1984*. ACM Press, New York, NY 10036, USA, 1984.

ACM:1985:RCM

[ACM85a] *The Range of Computing: Mid-80's Perspective: 1985 ACM Annual Conference, October 14–16, 1985, Radisson Hotel Denver, Denver, Colorado: Proceedings*. ACM Press, New York, NY 10036, USA, 1985. ISBN 0-89791-170-9. LCCN QA 76 R36 1985.

ACM:1985:PFA

[ACM85b] *Proceedings of the Fourth ACM SIGACT-SIGMOD Symposium on Principles of Database Systems, March*

25–27, 1985, Portland, Oregon. ACM Press, New York, NY 10036, USA, 1985. ISBN 0-89791-153-9. LCCN QA 76.9 D3 A296 1985.

ACM:1986:PFA

[ACM86a] *Proceedings of the Fifth ACM SIGACT-SIGMOD Symposium on Principles of Database Systems, March 24–26, 1986, Cambridge, MA*. ACM Press, New York, NY 10036, USA, 1986. ISBN 0-89791-179-2. LCCN QA76.9.D3 A296 1986. US$24.00.

ACM:1986:PEA

[ACM86b] *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing: Berkeley, California, May 28–30, 1986*. ACM Press, New York, NY 10036, USA, 1986. ISBN 0-89791-193-8. LCCN QA76.6 .A14 198.

ACM:1987:PEA

[ACM87] *Proceedings of the Eleventh ACM Symposium on Operating Systems Principles: 8–11 November 1987, Stouffer Austin Hotel, Austin, TX*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. ISBN 0-89791-242-x. LCCN QA76.6 .O625 v.21:5.

ACM:1988:PPS

[ACM88a] ACM, editor. *PODS '88. Proceedings of the Seventh ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems: March 21–23, 1988, Austin, Texas*. ACM Press, New York, NY 10036, USA, 1988. ISBN 0-89791-263-2. LCCN QA76.9.D3 A15 1988.

ACM:1988:PTA

[ACM88b] *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing: Chicago, Illinois, May 2–4, 1988*. ACM Press, New York, NY 10036, USA, 1988. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988.

ACM:1989:PPE

[ACM89a] ACM, editor. *PODS '89. Proceedings of the Eighth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, March 29–31, 1989, Philadelphia, PA*. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-308-6. LCCN QA 76.9 D3 A26 1989.

ACM:1989:PEA

[ACM89b] *Proceedings of the Eighth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, March 29–31, 1989, Philadelphia, PA*. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-308-6. LCCN QA 76.9 D3 A26 1989.

ACM:1989:PTF

[ACM89c] *Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing: Seattle, Washington, May 15–17, 1989*. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989.

ACM:1990:PTS

[ACM90] *Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing: Baltimore, Maryland, May 14–16, 1990*. ACM Press, New York, NY 10036, USA, 1990. ISBN 0-89791-361-2. LCCN QA 76.6 A13 1990.

ACM:1991:PPE

[ACM91a] ACM, editor. *POPL '91. Proceedings of the eighteenth annual ACM symposium on Principles of programming languages, January 21–23, 1991, Orlando, FL*. ACM Press, New York, NY 10036, USA, 1991. ISBN ???? LCCN ????

ACM:1991:ACS

[ACM91b] *ACM Computer Science Conference (19th: 1991: San Antonio, Tex.) 1991 ACM Computer Science Conference: March 5–7, 1991, San Antonio Convention Center, San Antonio, Texas: proceedings: preparing for the 21st century*. ACM Press, New York, NY 10036, USA, 1991. ISBN 0-89791-382-5. LCCN QA76.5 .A137 1991.

ACM:1991:AAS

[ACM91c] *3rd Annual ACM Symposium on Parallel Algorithms and Architectures, July 21–24, 1991, Hilton Head, South Carolina: SPAA '91*. ACM Press, New York, NY 10036, USA, 1991. ISBN 0-89791-438-4. LCCN QA76.58 .A27 1991.

ACM:1991:CRE

[ACM91d] *Conference record of the Eighteenth Annual ACM Symposium on Principles of Programming Languages: papers presented at the symposium, Orlando, Florida, 21–23 January 1991*. ACM Press, New York, NY 10036, USA, 1991. ISBN 0-89791-419-8. LCCN QA76.7 .A15 1991.

ACM:1991:PTT

[ACM91e] *Proceedings of the Twenty Third Annual ACM Symposium on Theory of Computing: New Orleans, Louisiana, May 6–8, 1991*. ACM Press, New York, NY 10036, USA, 1991. ISBN 0-89791-397-3. LCCN QA 76.6 A13 1991.

ACM:1994:CCS

[ACM94a] ACM, editor. *Computer and communications security: 2nd conference — November 1994, Fairfax, VA*, ACM

CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 1994; 2nd. ACM Press, New York, NY 10036, USA, 1994. ISBN 0-89791-732-4. LCCN ????

ACM:1994:IPI

[ACM94b] ACM, editor. *ISSAC '94: Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation: July 20–22, 1994, Oxford, England, United Kingdom*. ACM Press, New York, NY 10036, USA, 1994. ISBN 0-89791-638-7. LCCN QA76.95.I59 1994.

ACM:1994:MMC

[ACM94c] ACM, editor. *Measurement and modeling of computer systems: Conference — May 1994, Nashville, TN*, volume 22 (1) of *PERFORMANCE EVALUATION REVIEW 1994*. ACM Press, New York, NY 10036, USA, 1994. CODEN PEREDN. ISBN 0-89791-659-X. ISSN 0163-5999 (print), 1557-9484 (electronic). LCCN ????

ACM-SIAM:1994:ASD

[ACM94d] *Proceedings of the fifth annual ACM-SIAM Symposium on Discrete Algorithms, Arlington, VA, USA*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1994. ISBN 0-89871-329-3. LCCN QA76.6 .A278 1994.

ACM:1996:PTE

[ACM96] ACM, editor. *Proceedings of the twenty-eighth annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, May 22–24, 1996*. ACM Press, New York, NY 10036, USA, 1996. ISBN 0-89791-785-5. LCCN QA 76.6 A13 1996. ACM order no. 508960. Also known as Federated Computing Research Conference (FCRS '96).

ACM:1997:PEA

[ACM97a] ACM, editor. *Proceedings of the Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, New Orleans, Louisiana, January 5–7, 1997*. ACM Press, New York, NY 10036, USA, 1997. CODEN PAAAF2. ISBN 0-89871-390-0. LCCN ????

ACM:1997:PTN

[ACM97b] ACM, editor. *Proceedings of the twenty-ninth annual ACM Symposium on the Theory of Computing: El Paso, Texas, May 4–6, 1997*. ACM Press, New York, NY 10036, USA, 1997. ISBN 0-89791-888-6. LCCN QA76.5 .A849 1997. ACM order no. 508970.

ACM:1998:PTA

[ACM98] ACM, editor. *Proceedings of the thirtieth annual ACM Symposium on Theory of Computing: Dallas, Texas,*

May 23–26, 1998. ACM Press, New York, NY 10036, USA, 1998. ISBN 0-89791-962-9. LCCN QA75.5 .A14 1998. ACM order number 508980.

ACM:2001:PAA

[ACM01] ACM, editor. *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing: Hersonissos, Crete, Greece, July 6–8, 2001*. ACM Press, New York, NY 10036, USA, 2001. ISBN 1-58113-349-9. LCCN QA76.6 .A13 2001. ACM order number 508010.

ACM:2002:PTF

[ACM02] ACM, editor. *Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing, Montréal, Québec, Canada, May 19–21, 2002*. ACM Press, New York, NY 10036, USA, 2002. ISBN 1-58113-495-9. LCCN QA75.5 .A22 2002. ACM order number 508020.

ACM:2003:PTF

[ACM03a] ACM, editor. *Proceedings of the Thirty-Fifth ACM Symposium on Theory of Computing, San Diego, CA, USA, June 9–11, 2003*. ACM Press, New York, NY 10036, USA, 2003. ISBN ???? LCCN QA75.5 .A22 2003. ACM order number 508030.

ACM:2003:SII

[ACM03b] ACM, editor. *SC2003: Igniting Innovation. Phoenix, AZ, November 15–21, 2003*. ACM Press and IEEE Computer Society Press, New York, NY 10036, USA and 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2003. ISBN 1-58113-695-1. LCCN ????

ACM:2004:SHP

[ACM04] ACM, editor. *SC 2004: High Performance Computing, Networking and Storage: Bridging communities: Proceedings of the IEEE/ACM Supercomputing 2004 Conference, Pittsburgh, PA, November 6–12, 2004*. ACM Press and IEEE Computer Society Press, New York, NY 10036, USA and 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2004. ISBN 0-7695-2153-3. LCCN ????

ACM:2005:PSA

[ACM05] ACM, editor. *Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms, Vancouver, BC, Canada, January 23–25, 2005*, Discrete Mathematics and Computer Science Ser. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2005. ISBN 0-89871-585-7. LCCN QA76.6 A184p 2005.

URL http://dl.acm.org/citation.cfm?id=1070432.

ACM:2007:SPA

[ACM07] ACM, editor. *STOC '07: proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11–13, 2007*. ACM Press, New York, NY 10036, USA, 2007. ISBN 1-59593-631-9. LCCN ????

ACM:2008:PNA

[ACM08a] ACM, editor. *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms: [San Francisco, CA, January 20–22, 2008]*. ACM Press, New York, NY 10036, USA, 2008. ISBN 0-89871-647-0. LCCN QA76.9.A43 A34 2008.

ACM:2008:SPA

[ACM08b] ACM, editor. *STOC '08: proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17–20, 2008*. ACM Press, New York, NY 10036, USA, 2008. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

ACM:2011:PAI

[ACM11] ACM, editor. *Proceedings of the 2011 ACM International Symposium on Theory of Computing: June 6–8, 2011, San Jose, CA, USA*. ACM Press, New York, NY 10036, USA, 2011. ISBN ???? LCCN ???? URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

ACM:2012:SPA

[ACM12] ACM, editor. *STOC'12: Proceedings of the 2012 ACM International Symposium on Theory of Computing: May 19–22, 2012, New York, NY, USA*. ACM Press, New York, NY 10036, USA, 2012. ISBN 1-4503-1245-4. LCCN ???? URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Abdalla:2009:SPH

[ACP09] Michel Abdalla, Céline Chevalier, and David Pointcheval. Smooth projective hashing for conditionally extractable commitments. *Lecture Notes in CS*, 5677: 671–689, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-03356-8_39.

Alomair:2010:PPS

[ACP10] Basel Alomair, Andrew Clark, and Radha Poovendran. The power of primes: security of authentication based on a universal hash-function family. *Journal of Mathematical Cryptology*, 4 (2):121–148, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Alvarez-Cubero:2016:AVL

[ÁCZ16] José Antonio Álvarez-Cubero and Pedro J. Zufiria. Algorithm 959: VBF: a library of C++ classes for vector Boolean functions in cryptography. *ACM Transactions on Mathematical Software*, 42(2):16:1–16:22, May 2016. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Ahrens:1985:SRS

[AD85] J. H. Ahrens and U. Dieter. Sequential random sampling. *ACM Transactions on Mathematical Software*, 11 (2):157–169, June 1985. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Adams:2008:ENE

[AD08] Michael D. Adams and R. Kent Dybvig. Efficient nondestructive equality checking for trees and graphs. *SIGPLAN Notices*, 43(9):179–188, September 2008. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Ashur:2011:LAR

[AD11] Tomer Ashur and Orr Dunkelman. Linear analysis of reduced-round CubeHash. *Lecture Notes in CS*, 6715:462–478, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-21554-4_27`.

Ayday:2012:DAA

[ADF12] Erman Ayday, Farshid Delgosha, and Faramarz Fekri. Data authenticity and availability in multihop wireless sensor networks. *ACM Transactions on Sensor Networks*, 8(2):10:1–10:??, March 2012. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Aceto:2008:ALPa

[ADG+08] Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors. *Automata, languages and programming: 35th international colloquium, ICALP 2008, Reykjavik, Iceland, July 7–11, 2008, proceedings, part I*, volume 5125 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 3-540-70574-0 (softcover). LCCN ???? URL `http://www.springerlink.com/content/7818221152674403/`; `http://www.springerlink.com/content/978-3-540-70574-1`.

Heide:1990:DHS

[adH90] Meyer auf der Heide. Dy-

namic hashing strategies. In Rovan [Rov90], page ?? ISBN 0-387-52953-5 (New York), 3-540-52953-5 (Berlin). LCCN QA76.9.M35 M386 1990.

Heide:1993:HSS

[adH93] Friedhelm Meyer auf der Heide. Hashing strategies for simulating shared memory on distributed memory machines. In auf der Heide et al. [adHMR93], page ?? ISBN 0-387-56731-3 (New York), 3-540-56731-3 (Berlin). LCCN QA76.58 .H45 1992. US$39.00, DM52.00.

Heide:1993:PAE

[adHMR93] Friedhelm Meyer auf der Heide, B. Monien, and Arnold L. Rosenberg, editors. *Parallel architectures and their efficient use: First Heinz Nixdorf Symposium, Paderborn, Germany, November 11–13, 1992: proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-56731-3 (New York), 3-540-56731-3 (Berlin). LCCN QA76.58 .H45 1992. US$39.00, DM52.00.

Adi:1988:DCC

[Adi88] W. Adi. Design criteria and complexity evaluation of a hash-based join processor. Technical report, Technischen Universität Carolo-Wilhelmina zu Braunschweig, Braunschweig, Germany, 1988. ?? pp.

Alon:1997:LHG

[ADM+97] Noga Alon, Martin Dietzfelbinger, Peter Bro Miltersen, Erez Petrank, and Gábor Tardos. Is linear hashing good? In ACM [ACM97b], pages 465–474. ISBN 0-89791-888-6. LCCN QA76.5 .A849 1997. URL `http://www.acm.org/pubs/articles/proceedings/stoc/258533/p465-alon/p465-alon.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/258533/p465-alon/`. ACM order no. 508970.

Alon:1999:LHF

[ADM+99] Noga Alon, Martin Dietzfelbinger, Peter Bro Miltersen, Erez Petrank, and Gábor Tardos. Linear hash functions. *Journal of the Association for Computing Machinery*, 46(5):667–683, September 1999. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/citations/journals/jacm/1999-46-5/p667-alon/`.

AlMahmoud:2019:SPP

[ADOAH19] A. AlMahmoud, E. Damiani, H. Otrok, and Y. Al-Hammadi. Spamdoop: a

privacy-preserving big data platform for collaborative spam detection. *IEEE Transactions on Big Data*, 5(3): 293–304, September 2019. ISSN 2332-7790.

Aumuller:2012:EEH

[ADW12] Martin Aumüller, Martin Dietzfelbinger, and Philipp Woelfel. Explicit and efficient hash families suffice for cuckoo hashing with a stash. In Epstein and Ferragina [EF12], pages 108–120. CODEN LNCSD9. ISBN 3-642-33089-4 (soft cover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL `http://www.springerlink.com/content/d7q7818203k8406t/`.

Aumuller:2014:EEH

[ADW14] Martin Aumüller, Martin Dietzfelbinger, and Philipp Woelfel. Explicit and efficient hash families suffice for cuckoo hashing with a stash. *Algorithmica*, 70(3):428–456, November 2014. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL `http://link.springer.com/article/10.1007/s00453-013-9840-x`.

Atighehchi:2009:EPA

[AEMR09] Kévin Atighehchi, Adriana Enache, Traian Muntean, and Gabriel Risterucci. An efficient parallel algorithm for Skein hash functions. Report, ERISCS Research Group, Université de la Méditerranée, Parc Scientifique de Luminy-Marseille, France, September 30, 2009. 11 pp.

Anagnostopoulos:2018:RES

[AEP18] Evangelos Anagnostopoulos, Ioannis Z. Emiris, and Ioannis Psarros. Randomized embeddings with slack and high-dimensional approximate nearest neighbor. *ACM Transactions on Algorithms*, 14(2):18:1–18:??, June 2018. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

AFIPS:1963:PSJ

[AFI63] *Proceedings 1963 Spring Joint Computer Conference*, volume 23 of *AFIPS conference proceedings*. Spartan Books, New York, NY, USA, 1963. LCCN TK7885.A1 J6 1963.

AFIPS:1969:ACP

[AFI69] *1969 Fall Joint Computer Conference, November 18–20, 1969, Las Vegas, Nevada*, volume 35 of *AFIPS conference proceedings*. AFIPS Press, Montvale, NJ, USA, 1969. LCCN TK7885.A1 J6 1969.

Ajtai:1983:HFP

[AFK83] M. Ajtai, M. Fredman, and J. Komlos. Hash functions for priority queues. *Annual Symposium on Foundations of*

Computer Science (Proceedings), pages 299–303, 1983. CODEN ASFPDV. ISBN 0-8186-0508-1. ISSN 0272-5428. IEEE Service Cent. Piscataway, NJ, USA.

Ajtai:1984:HFP

[AFK84] M. Ajtai, M. Fredman, and J. Komlòs. Hash functions for priority queues. *Information and Control*, 63(3):217–225, December 1984. CODEN IFCNA4. ISSN 0019-9958 (print), 1878-2981 (electronic).

Akl:1990:ACI

[AFK90] Selim G. Akl, F. Fiala, and Waldemar W. Koczkodaj, editors. *Advances in computing and information–ICCI '90 / International Conference on Computing and Information, Niagara Falls, Canada, May 23–26, 1990, proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. ISBN 0-387-53504-7 (New York), 3-540-53504-7 (Berlin). LCCN QA75.5 .I578 1990.

Appel:1993:HCG

[AG93] Andrew W. Appel and Marcelo J. R. Goncalves. Hash-consing garbage collection. Technical Report CS-TR-412-93, Princeton University, Computer Science Department, February 1993. ?? pp.

Alon:2010:BFP

[AG10] Noga Alon and Shai Gutner. Balanced families of perfect hash functions and their applications. *ACM Transactions on Algorithms*, 6(3): 54:1–54:??, June 2010. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

Aumasson:2017:SCP

[AG18] Jean-Philippe Aumasson and Matthew D. Green. *Serious Cryptography: a Practical Introduction to Modern Encryption*. No Starch Press, San Francisco, CA, USA, 2018. ISBN 1-59327-826-8 paperback. xxii + 282 pp. LCCN QA76.9.A25 A96 2018. URL `https://nostarch.com/seriouscrypto`.

Atighehchi:2019:GHC

[AGBR19] Kevin Atighehchi, Loubna Ghammam, Morgan Barbier, and Christophe Rosenberger. GREYC-Hashing: Combining biometrics and secret for enhancing the security of protected templates. *Future Generation Computer Systems*, 101(??): 819–830, December 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X1833125X`.

Agarwal:2006:AGA

[AGJA06] R. C. Agarwal, K. Gupta, S. Jain, and S. Amalapurapu. An approximation to the greedy algorithm for differential compression. *IBM Journal of Research and Development*, 50(1):149–??, January 2006. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL `http://www.research.ibm.com/journal/rd/501/agarwal.html`.

Abramsky:2010:ALP

[AGK+10] Samson Abramsky, Cyril Gavoille, Claude Kirchner, Friedhelm Meyer auf der Heide, and Paul G. Spirakis, editors. *Automata, languages and programming: 37th International Colloquium, ICALP 2010, Bordeaux, France, July 6–10, 2010, proceedings*, volume 6198–6199 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. CODEN LNCSD9. ISBN 3-642-14164-1 (vol. 1: paperback), 3-642-14161-7 (vol. 2: paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267 .I55 2010. URL `http://www.springerlink.com/content/978-3-642-14164-5/`.

Angelino:2011:EMM

[AGMT11] Elaine Angelino, Michael T. Goodrich, Michael Mitzenmacher, and Justin Thaler. External-memory multimaps. In Asano et al. [AiNOW11], pages 384–394. CODEN LNCSD9. ISBN 3-642-25590-6. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/g37344t4u5112706/`.

Alt:2003:SAS

[AH03] Helmut Alt and M. Habib, editors. *STACS 2003: 20th Annual Symposium on Theoretical Aspects of Computer Science, Berlin, Germany, February 27–March 1, 2003: Proceedings*, volume 2607 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-00623-0 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA75.5 .S956 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2607.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2607`. Also available via the World Wide Web.

Aumasson:2012:QLH

[AHMNP12] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and María Naya-Plasencia. QUARK: a lightweight hash. *Journal of Cryptology*, ?? (??):??, ???? 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/content/a310430665th50r4/`.

Aumasson:2013:QLH

[AHMNP13] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and María Naya-Plasencia. QUARK: a lightweight hash. *Journal of Cryptology*, 26(2): 313–339, April 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9125-6`.

Ahn:1986:AH

[Ahn86] Ilsoo Ahn. Adaptive hashing. Technical report, AT & T Bell Laboratories, Columbus, OH, USA, December 1986. 1–21 pp.

Ahn:1987:AH

[Ahn87] I. Ahn. Adaptive hashing. Technical report, ????, 1987. ?? pp.

Ahn:1993:FH

[Ahn93] Ilsoo Ahn. Filtered hashing. In Lomet [Lom93], pages 85–100. ISBN 0-387-57301-1 (New York), 3-540-57301-1 (Berlin). LCCN QA76.9.D3 I5535 1993.

Aldous:1992:MSD

[AHS92] David Aldous, Micha Hofri, and Wojciech Szpankowski. Maximum size of a dynamic data structure: Hashing with lazy deletion revisited. *SIAM Journal on Computing*, 21 (4):713–732, August 1992. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Aho:1983:DSA

[AHU83] Alfred V. Aho, John E. Hopcroft, and J. D. Ullman. *Data Structures and Algorithms*. Addison-Wesley, Reading, MA, USA, 1983. ISBN 0-201-00023-7. xi + 427 pp. LCCN QA76.9.D35 A38 1983.

Aiello:1998:NCS

[AHV98] William Aiello, Stuart Haber, and Ramarathnam Venkatesan. New constructions for secure hash functions. *Lecture Notes in CS*, 1372:150–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1372/13720150.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1372/13720150.pdf`.

Andoni:2006:NOH

[AI06] Alexandr Andoni and Piotr Indyk. Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions. In IEEE [IEE06], pages 459–468. ISBN 0-7695-2720-5, 0-7695-2362-5. ISSN 0272-5428. LCCN QA76 .S974 2006. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=4031329`. IEEE Computer Society Order Number P2720.

Andoni:2008:NOH

[AI08] Alexandr Andoni and Piotr Indyk. Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions. *Communications of the Association for Computing Machinery*, 51(1):117–122, January 2008. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Asano:1989:CPP

[AII89] Tetsuo Asano, H. Imai, and K. Imai. Clustering/hashing points in the plane with maxmin criteria. In CCCG '89 [CCC89], page 15. ISBN ???? LCCN ????

Asano:2011:ACI

[AiNOW11] Takao Asano, Shin ichi Nakano, Yoshio Okamoto, and Osamu Watanabe, editors. *Algorithms and Computation: 22nd International Symposium, ISAAC 2011, Yokohama, Japan, December 5–8. Proceedings*, volume 7074 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011. CODEN LNCSD9. ISBN 3-642-25590-6. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/978-3-642-25590-8`.

Amble:1974:OHT

[AK74] O. Amble and D. E. Knuth. Ordered hash tables. *The Computer Journal*, 17(2): 135–142, May 1974. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_17/Issue_02/tiff/135.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_17/Issue_02/tiff/136.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_17/Issue_02/tiff/137.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_17/Issue_02/tiff/138.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_17/Issue_02/tiff/139.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_17/Issue_02/tiff/140.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_`

17/Issue_02/tiff/141.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_17/Issue_02/tiff/142.tif.

Abdukhalikov:1998:SHS

[AK98] Kanat S. Abdukhalikov and Chul Kim. On the security of the hashing scheme based on SL_2. *Lecture Notes in CS*, 1372:93–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1372/13720093.htm; http://link.springer-ny.com/link/service/series/0558/papers/1372/13720093.pdf.

Ahn:2009:SLD

[AK09] Joon Ahn and Bhaskar Krishnamachari. Scaling laws for data-centric storage and querying in wireless sensor networks. *IEEE/ACM Transactions on Networking*, 17(4):1242–1255, August 2009. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Albutiu:2012:MPS

[AKN12] Martina-Cezara Albutiu, Alfons Kemper, and Thomas Neumann. Massively parallel sort-merge joins in main memory multi-core database systems. *Proceedings of the VLDB Endowment*, 5(10): 1064–1075, June 2012. CODEN ???? ISSN 2150-8097.

Ajtai:1978:TNF

[AKS78] Miklós Ajtai, János Komlós, and Endre Szemerédi. There is no fast single hashing algorithm. *Information Processing Letters*, 7(6):270–273, October 1978. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

AlTawy:2013:SOC

[AKY13] Riham AlTawy, Aleksandar Kircanski, and Amr Youssef. Second order collision for the 42-step reduced DHA-256 hash function. *Information Processing Letters*, 113(19–21):764–770, September/October 2013. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013002044.

Aho:1986:SDS

[AL86] Alfred V. Aho and David Lee. Storing a dynamic sparse table. *Annual Symposium on Foundations of Computer Science (Proceedings)*, pages 55–60, 1986. CODEN ASFPDV. ISBN 0-8186-0740-8. ISSN 0272-5428. IEEE Service Cent. Piscataway, NJ, USA.

Albeshri:2021:IHB

[Alb21] Aiiad Albeshri. An image hashing-based authenti-

cation and secure group communication scheme for IoT-enabled MANETs. *Future Internet*, 13(7):166, June 27, 2021. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/13/7/166.

Aldous:1987:HLP

[Ald87] David J. Aldous. Hashing with linear probing, under non-uniform probabilities. Technical Report TR-88, University of California, Berkeley. Dept. of Statistics, February 1987. 15 pp.

Aldous:1988:HLP

[Ald88] David Aldous. Hashing with linear probing under nonuniform probabilities. *Probability in the Engineering and Informational Sciences*, 2(1): 1–14, January 1988. CODEN ???? ISSN 0269-9648 (print), 1469-8951 (electronic). URL https://www.cambridge.org/core/product/9D2CACA7CC9B73AAEA021B85287BB2C7

Agrawal:2010:HLF

[ALS10] Kunal Agrawal, Charles E. Leiserson, and Jim Sukha. Helper locks for fork-join parallel programming. *SIGPLAN Notices*, 45(5):245–256, May 2010. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Aumasson:2007:AMH

[AM07] Jean-Philippe Aumasson and Willi Meier. Analysis of multivariate hash functions. *Lecture Notes in CS*, 4817: 309–323, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-76788-6_25.

Andreeva:2012:PFG

[AMP12] Elena Andreeva, Bart Mennink, and Bart Preneel. The parazoa family: generalizing the sponge hash functions. *International Journal of Information Security*, 11 (3):149–165, June 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0157-6.

Andreeva:2015:OPH

[AMP15] Elena Andreeva, Bart Mennink, and Bart Preneel. Open problems in hash function security. *Designs, Codes, and Cryptography*, 77(2–3):611–631, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-015-0096-0.

Aumasson:2014:HFB

[AMPH14] Jean-Philippe Aumasson, Willi Meier, Raphael C.-W.

Phan, and Luca Henzen. *The Hash Function BLAKE*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2014. ISBN 3-662-44756-8 (print), 3-662-44757-6 (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xviii + 228 + 18 pp. LCCN QA76.9.H36 A96 2014.

Albers:2009:ALP

[AMSM+09] Susanne Albers, Alberto Marchetti-Spaccamela, Yossi Matias, Sotiris Nikoletseas, and Wolfgang Thomas, editors. *Automata, languages and programming: 36th international colloquium, ICALP 2009, Rhodes, Greece, July 5–12, 2009; proceedings, part 1*, volume 5555 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 3-642-02926-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267 .I55 2009. URL `http://www.springerlink.com/content/978-3-642-02926-4`; `http://www.springerlink.com/content/978-3-642-02926-4/`.

Alon:1996:DWB

[AN96] Noga Alon and Moni Naor. Derandomization, witnesses for Boolean matrix multiplication and construction of perfect hash functions. *Algorithmica*, 16(4–5):434–449, 1996. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Araujo:2020:CHR

[AN20] Filipe Araujo and Samuel Neves. The circulant hash revisited. *Journal of Mathematical Cryptology*, 15(1): 250–257, December 3, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2018-0054/html`.

Anderson:1988:PHK

[And88] Paul B. Anderson. Parallel hashed key access on the connection machine. In *2nd Symposium on the Frontiers of Massively Parallel Computation (Oct 10–12 1988: Fairfax, VA, USA)*, pages 643–645. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. IEEE catalog number 88CH2649-2.

Anderson:1991:TFC

[And91] Ross J. Anderson. Tree functions and cipher systems. *Cryptologia*, 15(3): 194–202, July 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.`

`informaworld.com/smpp/content~content=a741902753~db=all~order=page`. encryption systems; plaintext bit; hash function; ciphertext errors; error extension; tree function; ciphertext attack; computable attack; connectivity; DES; RSA key selection; algorithm design.

Anderson:1993:CHF

[And93] R. Anderson. The classification of hash functions. In Farrell [Far93], pages 83–94. ISBN 0-905091-03-5. LCCN ????

Anderson:1994:FSE

[And94] R. Anderson, editor. *Fast software encryption: Security workshop — December 1993, Cambridge*, number 809 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. ISBN 0-387-58108-1, 3-540-58108-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C36 1993.

Anonymous:1983:MPM

[Ano83] Anonymous, editor. *Miconex '83: proceedings of a multi-national instrumentation conference convened in Shanghai, Peoples Republic of China, April 12–16, 1983*. ISA, Research Triangle Park, NC, USA, 1983. ISBN 0-87664-739-5. LCCN TA165.M52 1983. Two volumes.

Anonymous:1985:PFD

[Ano85a] Anonymous. Proceedings — foundations of data organization. In *Proceedings — Foundations of Data Organization*. Organizing Committee of the Int Conference on Foundations of Data Organization, Jpn, 1985. Kyoto Sangyo Univ. Computer Science Inst, Kyoto, Jpn.

Anonymous:1985:SS

[Ano85b] Anonymous. Software and services. *ComputerWorld*, 19 (38):50, September 23 1985. CODEN CMPWAB. ISSN 0010-4841.

Anon:1986:IRN

[Ano86] Anon. Integer random number generator. *IBM Technical Disclosure Bulletin*, 28(11): 4869–??, April 1986. CODEN IBMTAA. ISSN 0018-8689.

Anonymous:1989:TIC

[Ano89] Anonymous, editor. *Third International Conference on Data Engineering*, volume 48(2) of *Information Sciences*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, July 1989. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Anonymous:1992:PAW

[Ano92] Anonymous ???, editor. *Proceedings of the 1992 ACM Workshop on ML and its Applications*. ACM Press, New York, NY 10036, USA, June 1992.

Anonymous:1993:CSA

[Ano93a] Anonymous, editor. *Computer security, audit and control: 10th World conference — October 1993, London*, PROCEEDINGS OF COMPSEC INTERNATIONAL 1993; 10th. Elsevier Advanced Technology, Oxford, UK, 1993. ISBN 1-85617-211-2. LCCN ????

Anonymous:1993:FSH

[Ano93b] Anonymous. *FIPS 180, Secure Hash Standard*. NIST, US Department of Commerce, Washington, DC, USA, May 1993.

Anonymous:1993:TCC

[Ano93c] Anonymous, editor. *TENCON '93: computer, communication, control and power engineering: International conference — October 1993, Beijing*, volume 1 of *IEEE TENCON 1993*. International Academic Publishers, ????, 1993. ISBN 7-80003-285-X, 0-7803-1233-3, 0-87031-232-5, 0-87031-234-1. LCCN TK5105.5.I327 1993. Five volumes.

Anonymous:1993:SAD

[Ano93d] Anonymous, editor. *The Second Annual Dartmouth Institute on Advanced Graduate Studies in Parallel Computation*. Dartmouth College (??), Hanover, NH, USA, June 1993. ISBN ?? LCCN ?? I have been unable to locate this reference in several major libraries, including Dartmoth's, sigh. . . .

Anonymous:1994:WAM

[Ano94] Anonymous, editor. *Workshop: – April 1990, Milan, Italy*, PB REPORTS PB94-124997. NTIS, ????, 1994.

Anonymous:1995:AUC

[Ano95a] Anonymous. Algorithms update: Collisions in MD4; more developments with keyed hash functions; A linear protocol failure for RSA with exponent three. *CryptoBytes*, 1(3):4–6, Autumn 1995. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto1n3.pdf`.

Anonymous:1995:FSH

[Ano95b] Anonymous. *FIPS 180-1, Secure Hash Standard*. National Institute of Standards and Technology, US Department of Commerce, Washington, DC, USA, April 1995. ?? pp.

Anonymous:1995:NAF

[Ano95c] Anonymous, editor. *NATO ASI on Fractal Image En-*

coding and Analysis: July 1995, Trondheim, Norway. ????, ????, 1995. ISBN ???? LCCN ????

Anonymous:1995:SHS

[Ano95d] Anonymous. Super hash serves up super privacy on the Internet. *Computer Technology Review*, 15(4):1–??, April 1995. CODEN CTERES. ISSN 0278-9647.

Anonymous:1996:RF

[Ano96] Anonymous. Real fake. *Wired*, 4(6):156–??, June 1, 1996. CODEN WREDEM. ISSN 1059-1028 (print), 1078-3148 (electronic).

Anonymous:2002:SHS

[Ano02] Anonymous. Secure Hash Standard. Technical report, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, August 1, 2002. iv + 71 pp. URL `http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf`. FIPS Publication 180-2. Officially replaced by [Ano12], but that newer version is much shorter.

Anonymous:2008:SHS

[Ano08] Anonymous. Secure Hash Standard (SHS). Federal Information Processing Standards Publication FIPS Pub 180-3, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, October 2008. v + 27 pp. URL `http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf`. Superceded by FIPS 180-4 [Ano12].

Anonymous:2009:DSS

[Ano09a] Anonymous. Digital Signature Standard (DSS). Federal Information Processing Standards Publication FIPS Pub 186-3, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, June 2009. ix + 119 pp. URL `http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf`. Superceded by FIPS 186-4 [Ano13].

Anonymous:2009:PCA

[Ano09b] Anonymous. Proof of concept attack further discredits MD5. *Network Security*, 2009(1):2, January 2009. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485809700030`.

Anonymous:2010:NDS

[Ano10] Anonymous, editor. *17th Annual Network and Distributed System Symposium, NDSS '10, The Dana on Misson Bay, San Diego, California. February 28–March 3, 2010*. Internet Society, Reston, VA, USA,

2010. ISBN 1-891562-29-0, 1-891562-30-4. LCCN ???? URL http://www.isoc.org/isoc/conferences/ndss/10/proceedings.shtml.

Anonymous:2012:SHS

[Ano12] Anonymous. Secure Hash Standard (SHS). Federal Information Processing Standards Publication FIPS Pub 180-4, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, March 2012. v + 30 pp. URL http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf; http://csrc.nist.gov/publications/PubsFIPS.html#fips180-4.

Anonymous:2013:DSS

[Ano13] Anonymous. Digital Signature Standard (DSS). Federal Information Processing Standards Publication FIPS Pub 186-4, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, July 2013. vii + 121 pp. URL http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

ANSI:1997:AXP

[ANS97] ANSI. *ANSI X9.30-2:1997: Public Key Cryptography Using Irreversible Algorithms — Part 2: The Secure Hash Algorithm (SHA-1)*. American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, 1997. URL http://webstore.ansi.org/ansidocstore/product.asp?sku=ANSI+X9%2E30%2D2%3A1997.

ANSI:2005:AXP

[ANS05] ANSI. *ANSI X9.62:2005: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)*. American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, 2005. URL http://csrc.nist.gov/encryption/dss/ecdsa/NISTReCur.pdf; http://webstore.ansi.org/ansidocstore/product.asp?sku=ANSI+X9%2E62%3A2005.

Arbitman:2009:ACH

[ANS09] Yuriy Arbitman, Moni Naor, and Gil Segev. De-amortized cuckoo hashing: Provable worst-case performance and experimental results. In Albers et al. [AMSM+09], pages 107–118. ISBN 3-642-02926-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.I55 2009. URL http://www.springerlink.com/content/d5187mm887547j31/; http://www.wisdom.weizmann.ac.il/~naor/PAPERS/deamortized_cuckoo.pdf.

Arbitman:2010:BCH

[ANS10] Y. Arbitman, M. Naor,

and G. Segev. Backyard cuckoo hashing: Constant worst-case operations with a succinct representation. In IEEE [IEE10], pages 787–796. ISBN 1-4244-8525-8. LCCN ???? URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5669376`. IEEE Computer Society Order Number P4244.

Arnaurov:1985:ODF

[ANT85] D. D. Arnaurov, N. V. Naidenov, and A. G. Tasev. Organization of data files for document retrieval systems. *Programming and Computer Software; translation of Programmirovaniye, (Moscow, USSR) Plenum*, 11(3):??, June 1985. CODEN PCSODA. ISSN 0361-7688 (print), 1608-3261 (electronic).

Al-Odat:2020:SHA

[AOAAK20] Zeyad A. Al-Odat, Mazhar Ali, Assad Abbas, and Samee U. Khan. Secure hash algorithms and the corresponding FPGA optimization techniques. *ACM Computing Surveys*, 53(5):97:1–97:36, October 2020. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `https://dl.acm.org/doi/10.1145/3311724`.

Aluc:2019:BSC

[AÖD19] Günes Aluç, M. Tamer Özsu, and Khuzaima Daudjee. Building self-clustering RDF databases using Tunable-LSH. *VLDB Journal: Very Large Data Bases*, 28(2):173–195, April 2019. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Atkinson:1999:PTF

[AOV+99] Malcolm P. Atkinson, Maria E. Orlowska, Patrick Valduriez, Stanley B. Zdonik, and Michael L. Brodie, editors. *Proceedings of the Twenty-fifth International Conference on Very Large Databases, Edinburgh, Scotland, UK, 7–10 September, 1999*. Morgan Kaufmann Publishers, San Francisco, CA, 1999. ISBN 1-55860-615-7. LCCN QA76.9.D3 I559 1999. Also known as VLDB'99.

Analyti:1992:FSM

[AP92] Anastasia Analyti and Sakti Pramanik. Fast search in main memory databases. In Stonebraker [Sto92], pages 215–224. ISBN 0-89791-521-6. ISSN 0163-5808 (print), 1943-5835 (electronic). LCCN ???? URL `http://www.acm.org/pubs/articles/proceedings/mod/130283/p215-analyti/p215-analyti.pdf`; `http://www.acm.org/pubs/citations/proceedings/mod/130283/p215-analyti/`.

Analyti:1993:PAM

[AP93] Anastasia Analyti and Sakti Pramanik. Performance analysis of a main memory multi-directory hashing technique. *Information Processing Letters*, 45(4):191–197, March 22, 1993. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Aumasson:2008:HED

[AP08] Jean-Philippe Aumasson and Raphael C.-W. Phan. How (not) to efficiently dither blockcipher-based hash functions? *Lecture Notes in CS*, 5023:308–324, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-68164-9_21`.

Aumasson:2011:CHF

[AP11] Jean-Philippe Aumasson and Raphael C.-W. Phan. On the cryptanalysis of the hash function Fugue: Partitioning and inside-out distinguishers. *Information Processing Letters*, 111(11):512–515, May 15, 2011. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Akbarinia:2007:PTK

[APV07] Reza Akbarinia, Esther Pacitti, and Patrick Valduriez. Processing top-k queries in distributed hash tables. *Lecture Notes in CS*, 4641:489–502, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-74466-5_53`.

Areias:2016:LFH

[AR16] Miguel Areias and Ricardo Rocha. A lock-free hash trie design for concurrent tabled logic programs. *International Journal of Parallel Programming*, 44(3):386–406, June 2016. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic). URL `http://link.springer.com/article/10.1007/s10766-014-0346-1`.

Atighehchi:2017:OTM

[AR17] Kevin Atighehchi and Robert Rolland. Optimization of tree modes for parallel hash functions: A case study. *IEEE Transactions on Computers*, 66(9):1585–1598, September 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/document/7896557/`.

Areias:2021:CEN

[AR21] Miguel Areias and Ricardo Rocha. On the correctness and efficiency of a novel lock-free hash trie map design. *Journal of Parallel*

and Distributed Computing, 150(??):184–195, April 2021. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731521000010`.

Anger:1994:IEA

[ARA94] F. D. Anger, R. V. Rodriguez, and M. Ali, editors. *Industrial and engineering applications of artificial intelligence and expert systems: 7th International conference — May 1994, Austin, TX*, INDUSTRIAL AND ENGINEERING APPLICATIONS OF ARTIFICIAL INTELLIGENCE AND EXPERT SYSTEMS - INTERNATIONAL CONFERENCE-1994. Gordon and Breach, Langhorne, PA, USA, 1994. ISBN 2-88449-128-7. LCCN Q334.I556 1994.

Altawy:2018:SLT

[ARH+18] Riham Altawy, Raghvendra Rohit, Morgan He, Kalikinkar Mandal, Gangqiang Yang, and Guang Gong. SLISCP-light: Towards hardware optimized sponge-specific cryptographic permutations. *ACM Transactions on Embedded Computing Systems*, 17(4):81:1–81:??, August 2018. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Ariwasa:1968:RHM

[Ari68] Makota Ariwasa. Residue hash method. *Journal of the Information Processing Society of Japan*, 12(??):??, February 1968. CODEN JIPRDE. ISSN 0387-6101.

Arikan:1994:IGE

[Ari94] E. Arikan. An improved graph-entropy bound for perfect hashing. *IEEE International Symposium on Information Theory*, pages 314–??, 1994. CODEN PISTFZ. ISSN 0271-4655.

Aghili:1982:PGD

[AS82] Houtan Aghili and Dennis G. Severance. Practical guide to the design of differential files for recovery of on-line databases. *ACM Transactions on Database Systems*, 7(4):540–565, December 1982. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1982-7-4/p540-aghili/p540-aghili.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1982-7-4/p540-aghili/`.

Abdelguerfi:1989:EVA

[AS89] M. Abdelguerfi and A. K. Sood. External VLSI algorithm for the relational database projection operation. *International Jour-*

nal of Electronics Theoretical & Experimental, 66(3):339–347, March 1989. CODEN IJELA2. ISSN 0020-7217.

Atici:1996:UHM

[AS96] M. Atici and D. R. Stinson. Universal hashing and multiple authentication. *Lecture Notes in CS*, 1109:16–??, ???? 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Aspnes:2007:SG

[AS07] James Aspnes and Gauri Shah. Skip graphs. *ACM Transactions on Algorithms*, 3(4):37:1–37:??, November 2007. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

Agrawal:2009:HBN

[AS09] Banit Agrawal and Timothy Sherwood. High-bandwidth network memory system through virtual pipelines. *IEEE/ACM Transactions on Networking*, 17(4):1029–1041, August 2009. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Aysu:2016:PMH

[AS16] Aydin Aysu and Patrick Schaumont. Precomputation methods for hash-based signatures on energy-harvesting platforms. *IEEE Transactions on Computers*, 65(9): 2925–2931, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Alcantara:2009:RTP

[ASA+09] Dan A. Alcantara, Andrei Sharf, Fatemeh Abbasinejad, Shubhabrata Sengupta, Michael Mitzenmacher, John D. Owens, and Nina Amenta. Real-time parallel hashing on the GPU. *ACM Transactions on Graphics*, 28(5):154:1–154:9, December 2009. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Andrade:2016:LEP

[ASBdS16] Ewerton R. Andrade, Marcos A. Simplicio, Paulo S. L. M. Barreto, and Paulo C. F. dos Santos. Lyra2: Efficient password hashing with high security against time-memory trade-offs. *IEEE Transactions on Computers*, 65(10):3096–3108, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Askitis:2005:CCC

[Ask05] Justin Zobel Nikolas Askitis. Cache-conscious collision resolution in string hash tables. *Lecture Notes in CS*, 3772:91–102, 2005. CODEN LNCSD9. ISBN 3-540-29740-5. ISSN 0302-9743 (print), 1611-3349 (electronic).

Al-Ssulami:2017:FSM

[ASM17] Abdulrakeeb M. Al-Ssulami and Hassan Mathkour. Faster string matching based on hashing and bit-parallelism. *Information Processing Letters*, 123(??):51–55, July 2017. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019017300492`.

Astakhov:1980:OEA

[Ast80] A. D. Astakhov. Organization of efficient access by hashing. *Programming and Computer Software (English Translation of Programmirovanie)*, 6(3):141–144, May–June 1980. CODEN PCSODA.

Astrahan:1987:ANU

[ASW87] M. M. Astrahan, M. Schkolnick, and K. Y. Whang. Approximating the number of unique values of an attribute without sorting. *Information system*, 12(1):11, 1987. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Aspnas:2007:EAS

[ASW07] Mats Aspnäs, Artur Signell, and Jan Westerholm. Efficient assembly of sparse matrices using hashing. *Lecture Notes in CS*, 4699: 900–907, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-75755-9_107`.

Alrabaee:2018:FRE

[ASWD18] Saed Alrabaee, Paria Shirani, Lingyu Wang, and Mourad Debbabi. FOSSIL: A resilient and efficient system for identifying FOSS functions in malware binaries. *ACM Transactions on Privacy and Security (TOPS)*, 21(2):8:1–8:??, February 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3175492`.

Asano:1990:APP

[AT90] Tetsuo Asano and T. Tokuyama. Algorithms for projecting points to give the most uniform distribution with application to hashing. In Asano et al. [A$^+$90], pages 300–309. ISBN 0-387-52921-7. LCCN QA9.58 .I58 1990.

Azadegan:1991:PJA

[AT91] Shiva Azadegan and Anand Tripathi. Parallel join algorithms for SIMD models. In lin Wu (v.1) et al. [lWSS91], pages III–125–III–133. ISBN 0-8493-0190-4 (set), 0-8493-0191-2 (v. 1), 0-8493-0192-0 (v. 2), 0-8493-0193-9 (v. 3). LCCN QA76.58 .I55 1991. ????

Asano:1993:APP

[AT93] Tetsuo Asano and Takeshi Tokuyama. Algorithms for projecting points to give the most uniform distribution with applications to hashing. *Algorithmica*, 9(6): 572–590, June 1993. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). Selections from SIGAL International Symposium on Algorithms (Tokyo, 1990).

Abdulhayoglu:2018:ULS

[AT18] Mehmet Ali Abdulhayoglu and Bart Thijs. Use of locality sensitive hashing (LSH) algorithm to match Web of Science and Scopus. *Scientometrics*, 116(2):1229–1245, August 2018. CODEN SCNTDX. ISSN 0138-9130 (print), 1588-2861 (electronic). URL `http://link.springer.com/article/10.1007/s11192-017-2569-6`.

Al-Talib:2007:IMS

[ATAKS07] S. A. Al-Talib, B. M. Ali, S. Khatun, and S. Subramaniam. Improving the multicast state scalability in Internet routers by integrating hash algorithm with recursive unicast. *Journal of Network and Computer Applications*, 30(4): 1445–1454, November 2007. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804506000488`.

Atighehchi:2020:PNA

[Ati20] Kevin Atighehchi. A precise non-asymptotic complexity analysis of parallel hash functions without tree topology constraints. *Journal of Parallel and Distributed Computing*, 137(??): 246–251, March 2020. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731518308682`.

Atkinson:1975:HMS

[Atk75] L. V. Atkinson. Hashing matrix subscripts. *BIT (Nordisk tidskrift for informationsbehandling)*, 15(3): 328–330, 1975. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Aviv:2019:ELG

[ATS19] Nir Aviv and Amnon Ta-Shma. On the entropy loss and gap of condensers. *ACM Transactions on Computation Theory*, 11(3):15:1–15:??, June 2019. CODEN ???? ISSN 1942-3454 (print), 1942-3462 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3317691`.

Ang:1998:TLH

[ATT98] C. H. Ang, S. T. Tan, and T. C. Tan. Tried lin-

ear hashing. *Lecture Notes in CS*, 1538:86–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1538/15380086.htm; http://link.springer-ny.com/link/service/series/0558/papers/1538/15380086.pdf.

Aho:1979:OPM

[AU79] Alfred V. Aho and Jeffrey D. Ullman. Optimal partial-match retrieval when fields are independently specified. *ACM Transactions on Database Systems*, 4(2): 168–179, June 1979. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL http://www.acm.org/pubs/articles/journals/tods/1979-4-2/p168-aho/p168-aho.pdf; http://www.acm.org/pubs/citations/journals/tods/1979-4-2/p168-aho/.

Aumasson:2009:CHF

[Aum09] Jean-Philippe Aumasson. Cryptanalysis of a hash function based on norm form equations. *Cryptologia*, 33 (1):12–15, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Alvarez:2011:IME

[ÁVZ11] Rafael Álvarez, José-Francisco Vicent, and Antonio Zamora. Improving the message expansion of the Tangle hash function. *Lecture Notes in CS*, 6694:183–189, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-21323-6_23.

Apers:1989:VLD

[AW89] Peter M. G. Apers and Gio Wiederhold, editors. *Very Large Data Bases: Proceedings of the Fifteenth International Conference on Very Large Data Bases, August 22–25/1989, Amsterdam, the Netherlands*. Morgan Kaufmann Publishers, San Francisco, CA, 1989. ISBN 1-55860-101-5. LCCN QA 76.9 D3 I61 1989.

Ahmad:2014:RTN

[AY14] Tahir Ahmad and Usman Younis. Randomness testing of non-cryptographic hash functions for real-time hash table based storage and look-up of URLs. *Journal of Network and Computer Applications*, 41(??): 197–205, May 2014. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804513002853.

Askitis:2010:RSH

[AZ10] Nikolas Askitis and Justin

Zobel. Redesigning the string hash table, burst trie, and BST to exploit cache. *ACM Journal of Experimental Algorithmics*, 15(1):17:1–17:??, March 2010. ISSN 1084-6654.

Babb:1979:IRD

[Bab79] E. Babb. Implementing a relational database by means of specialized hardware. *ACM Transactions on Database Systems*, 4(1): 1–29, March 1979. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1979-4-1/p1-babb/p1-babb.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1979-4-1/p1-babb/`.

Back:2001:HC

[Bac01] A. Back. Hash cash. Web document., 2001. URL `https://web.archive.org/web/20010614013848/http://cypherspace.org/hashcash/`.

Back:2002:HDS

[Bac02] A. Back. Hashcash — a denial of service counter measure. Web document., 2002. URL `http://www.hashcash.org/papers/hashcash.pdf`..

Bailey:1981:CHP

[Bai81] Richard W. Bailey, editor. *Computing in the humanities: papers from the Fifth International Conference on Computing in the Humanities, Ann Arbor, Michigan, May 1981*. North-Holland, Amsterdam, The Netherlands, 1981. ISBN 0-444-86423-7. LCCN AZ105 .I57.1981.

Bakker:2009:MHT

[Bak09] Arno Bakker. Merkle hash torrent extension. Web document., August 2009. URL `http://www.bittorrent.org/beps/bep_0030.html`,.

Balakirsky:1996:HDB

[Bal96] V. B. Balakirsky. Hashing of databases based on indirect observations of Hamming distances. *IEEE Transactions on Information Theory*, 42 (2):664–671, March 1, 1996. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Balakirsky:2005:HDU

[Bal05] Vladimir B. Balakirsky. Hashing of databases with the use of metric properties of the Hamming space. *The Computer Journal*, 48 (1):4–16, January 2005. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_48/Issue_01/bxh059.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_48/Issue_01/pdf/bxh059.pdf`.

Bandypadhyay:1977:CWI

[Ban77] S. K. Bandypadhyay. Comment on weighted increment linear search for scatter tables. *Communications of the Association for Computing Machinery*, 20(4): 262–263, April 1977. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Burrows:1989:LAa

[BAN89] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. Technical Report 39, Digital Equipment Corporation, Systems Research Centre, February 28, 1989. 48 pp.

Barter:1983:ACS

[Bar83] C. J. Barter, editor. *Australian Computer Science Conference. Proceedings of the 7th Conference (Adelaide, Australia, Feb. 6–8, 1983)*. University of Adelaide, Computer Science Department, Adelaide, South Australia, Australia, 1983. Published as Australian Computer Science Communications; vol 6, no. 1.

Barequet:1997:UGH

[Bar97] Gill Barequet. Using geometric hashing to repair CAD objects. *IEEE Computational Science & Engineering*, 4(4):22–28, October/December 1997. CODEN ISCEE4. ISSN 1070-9924 (print), 1558-190X (electronic). URL `http://dlib.computer.org/cs/books/cs1997/pdf/c4022.pdf`; `http://www.computer.org/cse/cs1998/c4022abs.htm`.

Batson:1965:OST

[Bat65] A. Batson. The organization of symbol tables. *Communications of the Association for Computing Machinery*, 8(2): 111–112, February 1965. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Batagelj:1975:QHM

[Bat75] Vladimir Batagelj. Quadratic hash method when the table size is not a prime number. *Communications of the Association for Computing Machinery*, 18(4): 216–217, April 1975. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Batory:1980:OFD

[Bat80] D. S. Batory. Optimal file design and reorganisation points. Technical report, ????, Toronto, ON, Canada, 1980. ?? pp.

Batory:1981:AMP

[Bat81] D. S. Batory. An analytical model of physical databases. Technical report, ????, Toronto, ON, Canada, 1981. ?? pp.

Batory:1982:OFD

[Bat82] D. S. Batory. Optimal file designs and reorganization points. *ACM Transactions on Database Systems*, 7(1):??, March 1982. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). Also published in/as: University of Toronto, TR-CSRG-110, 1980.

Balkesen:2013:MCM

[BATÖ13] Cagri Balkesen, Gustavo Alonso, Jens Teubner, and M. Tamer Özsu. Multi-core, main-memory joins: sort vs. hash revisited. *Proceedings of the VLDB Endowment*, 7(1): 85–96, September 2013. CODEN ???? ISSN 2150-8097.

Bays:1973:STS

[Bay73a] C. Bays. Some techniques for structuring chained hash tables. *The Computer Journal*, 16(2):126–131, May 1973. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_16/Issue_02/160126.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_16/Issue_02/tiff/126.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_16/Issue_02/tiff/127.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_16/Issue_02/tiff/128.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_16/Issue_02/tiff/129.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_16/Issue_02/tiff/130.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_16/Issue_02/tiff/131.tif`.

Bays:1973:NWC

[Bay73b] Carter Bays. A note on when to chain overflow items within a direct-access table. *Communications of the Association for Computing Machinery*, 16(1):46–47, January 1973. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Bays:1973:RHC

[Bay73c] Carter Bays. The reallocation of hash-coded tables. *Communications of the Association for Computing Machinery*, 16(1):11–14, January 1973. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Bayer:1974:SCM

[Bay74] Rudolf Bayer. Storage characteristics and methods for searching and addressing. In Rosenfeld [Ros74], page ?? ISBN 0-444-10689-8. LCCN QA 76 I615.

Bohm:2007:FRA

[BB07] Klemens Böhm and Erik Buchmann. Free riding-aware forwarding in Content-Addressable Networks. *VLDB Journal: Very Large Data Bases*, 16(4):463–482, October 2007. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Berman:1982:CFP

[BBD+82] Francine Berman, Mary Ellen Bock, Eric Dittert, Michael J. O'Donnell, and Darrell Plank. Collections of functions for perfect hashing. Technical Report CSD-TR-408, Department of Computer Science, Purdue University, West Lafayette, IN, USA, 1982. ?? pp.

Berman:1986:CFP

[BBD+86] Francine Berman, Mary Ellen Bock, Eric Dittert, Michael J. O'Donnell, and Darrell Plank. Collections of functions for perfect hashing. *SIAM Journal on Computing*, 15(2):604–618, May 1986. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Belazzougui:2009:HDC

[BBD09a] Djamal Belazzougui, Fabiano C. Botelho, and Martin Dietzfelbinger. Hash, displace, and compress. In Fiat and Sanders [FS09], pages 682–693. CODEN LNCSD9. ISBN 3-642-04127-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A43 E83 2009. URL `http://www.springerlink.com/content/d41867w7r1236506/`.

Bernstein:2009:PQC

[BBD09b] Daniel J. (Daniel Julius) Bernstein, Johannes Buchmann, and Erik Dahmén, editors. *Post-quantum cryptography: [First International Workshop on Post-Quantum Cryptography ... at the Katholieke Universiteit Leuven in 2006]*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 3-540-88701-6 (hardcover), 3-642-10019-8 (softcover). LCCN QA76.9.A25 P67 2009.

Bellare:2001:OCH

[BBKN01] Mihir Bellare, Alexandra Boldyreva, Lars Knudsen, and Chanathip Namprempre. Online ciphers and the hash-CBC construction. *Lecture Notes in CS*, 2139:292–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390292.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2139/21390292.pdf`.

Bellare:2012:LCH

[BBKN12] M. Bellare, A. Boldyreva, L. Knudsen, and C. Namprempre. On-line ciphers and the hash-CBC constructions. *Journal of Cryptology*, 25(4):640–679, October 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=4&spage=640`.

Bernstein:1988:OCE

[BBP88] D. Bernstein, H. Boral, and R. Y. Pinter. Optimal chaining in expression trees. *IEEE Transactions on Computers*, 37(11):1366–1374, November 1988. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Belazzougui:2011:TPM

[BBPV11] Djamal Belazzougui, Paolo Boldi, Rasmus Pagh, and Sebastiano Vigna. Theory and practice of monotone minimal perfect hashing. *ACM Journal of Experimental Algorithmics*, 16(1):32:1–32:??, 2011. ISSN 1084-6654.

Bennett:1988:PAP

[BBR88] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Applies hash functions to problems of error correction in messages.

Bollobas:1990:CDC

[BBS90] Béla Bollobás, Andrei Z. Broder, and Istvan Simon. The cost distribution of clustering in random probing. *Journal of the Association for Computing Machinery*, 37(2):224–237, April 1990. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Ball:1939:MRE

[BC39] W. W. Rouse (Walter William Rouse) Ball and H. S. M. (Harold Scott MacDonald [“Donald”]) Coxeter. *Mathematical recreations and essays*. Macmillan Publishing Company, New York, NY, USA, 11th edition, 1939. 45 pp. LCCN QA95 .B3 1939. According to Knuth [Knu73, p. 507], this is one of two papers that first discuss the birthday paradox: “if 23 or more people are present in the same room, chances are good that two of them will have the same month and day of birth! In other words, if we select a random function which maps 23 keys into a table of size

365, the probability that no two keys map into the same location is only 0.4927 (less than one-half)." The discovery is credited to unpublished work of H. Davenport (1927). See also [vM39].

Burkowski:1990:UPH

[BC90] F. J. Burkowski and G. V. Cormack. Use of perfect hashing in a paged memory management unit. In Wah (v.1) et al. [WPY90], pages 96–100. ISBN 0-271-00728-1. LCCN QA 76.58 I58 1990. Three volumes.

Bird:2006:BSE

[BC06] Steven Bird and James R. Curran. Building a search engine to drive problem-based learning. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 38(3):153–157, September 2006. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Balachandran:2008:SHC

[BC08] S. Balachandran and C. Constantinescu. Sequence of hashes compression in data de-duplication. In Storer and Marcellin [SM08], page 505. ISBN 0-7695-3121-0. ISSN 1068-0314. LCCN QA76.9.D33 D372 2008; QA76.9.D33 INTERNET. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4483332`.

Bu:2010:SHF

[BCCL10] Tian Bu, Jin Cao, Aiyou Chen, and Patrick P. C. Lee. Sequential hashing: a flexible approach for unveiling significant patterns in high speed networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 54(18):3309–3326, December 20, 2010. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Boldyreva:2009:FNM

[BCFW09] Alexandra Boldyreva, David Cash, Marc Fischlin, and Bogdan Warinschi. Foundations of non-malleable hash and one-way functions. *Lecture Notes in CS*, 5912: 524–541, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-10366-7_31`.

Boneh:2016:BHP

[BCGS16] Dan Boneh, Henry Corrigan-Gibbs, and Stuart Schechter. Balloon hashing: Provably space-hard hash functions with data-independent access patterns, January 14, 2016. URL `https://pdfs.semanticscholar.org/f49f/8e135695937bfe03e467e215177eec79d7c pdf`. Cryptology ePrint Archive Report 2016/027 Version: 20160601:225540. See [AB17].

Berra:1987:CAS

[BCH87] P. B. Berra, Soon M. Chung, and Nabil I. Hachem. Computer architecture for a surrogate file to a very large data/knowledge base. *Computer*, 20(3):25–32, March 1987. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Biham:2015:CSR

[BCJ15] Eli Biham, Rafi Chen, and Antoine Joux. Cryptanalysis of SHA-0 and reduced SHA-1. *Journal of Cryptology*, 28(1):110–160, January 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-014-9179-8`.

Bellare:1996:KHF

[BCK96a] M. Bellare, R. Canetti, and H. Krawczyk. Keying hash functions for message authentication. *Lecture Notes in CS*, 1109:1–15, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.research.ibm.com/security/`.

Bellare:1996:MAU

[BCK96b] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Message authentication using hash functions: the HMAC construction. *CryptoBytes*, 2 (1):12–15, Spring 1996. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto2n1.pdf`.

Bedau:2004:CHF

[BCR04] M. Bedau, R. E. Crandall, and M. Raven. Cryptographic hash functions based on Artificial Life. Report, Reed College, Portland, OR, USA, 2004. 20 pp. URL `http://people.reed.edu/~crandall/papers/crypto8.pdf`.

Barr:2010:TCS

[BCR10] Thomas W. Barr, Alan L. Cox, and Scott Rixner. Translation caching: skip, don't walk (the page table). *ACM SIGARCH Computer Architecture News*, 38 (3):48–59, June 2010. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Bardin:1989:IUI

[BCS89] B. Bardin, C. Colket, and D. Smith. Implementation of unsigned integers in Ada. *Ada Letters*, 9(1):47–70, January–February 1989. CODEN AALEE5.

Black:2009:IHE

[BCS09] J. Black, M. Cochran, and T. Shrimpton. On the impossibility of highly-efficient blockcipher-based hash functions. *Journal of Cryptology*, 22(3):311–329, July 2009. CODEN JOCREQ. ISSN

0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=3&spage=311`.

Bell:1982:KSC

[BD82] D. A. Bell and S. M. Deen. Key space compression and hashing in PRECI. *The Computer Journal*, 25(4): 486–492, November 1982. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Bell:1984:HTV

[BD84] D. A. Bell and S. M. Deen. Hash trees versus B-Trees. *The Computer Journal*, 27 (3):218–224, August 1984. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Bancilhon:1988:PFI

[BD88] Francois Bancilhon and David J. DeWitt, editors. *Proceedings of the Fourteenth International Conference on Very Large Data Bases, Los Angeles, USA, Aug. 29/Sept. 1, 1988*. Morgan Kaufmann Publishers, San Francisco, CA, 1988. ISBN 0-934613-75-3. LCCN QA76.9.D3 I559 1988.

Bauspiess:1992:RCH

[BD92] Fritz Bauspiess and Frank Damm. Requirements for cryptographic hash functions. *Computers and Security*, 11(5):427–437, September 1, 1992. CODEN CPSEDU. ISSN 0167-4048.

Buchmann:2008:PQC

[BD08] Johannes Buchmann and Jintai Ding, editors. *Post-Quantum Cryptography: Second International Workshop, PQCrypto 2008 Cincinnati, OH, USA, October 17–19, 2008 Proceedings*, volume 5299 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 3-540-88403-3. LCCN QA76.9.A25 P63 2008. URL `http://www.springer.com/computer/security+and+cryptology/book/978-3-540-88402-6`.

Blin:2010:ARS

[BDD+10] Guillaume Blin, Alain Denise, Serge Dulucq, Claire Herrbach, and Heleene Touzet. Alignments of RNA structures. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 7 (2):309–322, April 2010. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Bao:2020:GAH

[BDG+20] Zhenzhen Bao, Itai Dinur, Jian Guo, Gaëtan Leurent, and Lei Wang. Generic attacks on hash combiners.

Journal of Cryptology, 33(3): 742–823, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-019-09328-w`.

Biryukov:2016:ANG

[BDK16] Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich. Argon2: new generation of memory-hard functions for password hashing and other applications. In IEEE, editor, *2016 IEEE European Symposium on Security and Privacy (EURO S&P 2016). 21–24 March 2016 Saarbruecken, Germany*, pages 292–302. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2016. ISBN 1-5090-1751-8. LCCN ???? URL `https://ieeexplore.ieee.org/document/7467361`. IEEE Computer Society Order Number P5776. See [AB17].

Berger:2012:GFL

[BDM+12] Thierry P. Berger, Joffrey D'Hayer, Kevin Marquet, Marine Minier, and Gaël Thomas. The GLUON family: a lightweight hash function family based on FCSRs. *Lecture Notes in CS*, 7374:306–323, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31410-0_19/`.

Bussi:2019:MHF

[BDMD19] Khushboo Bussi, Dhananjoy Dey, P. R. Mishra, and B. K. Dass. MGR hash functions. *Cryptologia*, 43 (5):372–390, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1596995`.

Bosselaers:1997:RCH

[BDP97] Antoon Bosselaers, Hans Dogbbertin, and Bart Preneel. The RIPEMD-160 cryptographic hash function. *Dr. Dobbs Journal*, 22(1):24, 26, 28, 78, 80, January 1997. CODEN DDJOEB. ISSN 1044-789X.

Bertoni:2011:CSF

[BDP11] Guido Bertoni, Joan Daemen, and Michaël Peeters. Cryptographic sponge functions. Report, STMicroelectronics, Antwerp, Belgium (??), January 14, 2011. 93 pp. URL `http://sponge.noekeon.org/CSF-0.1.pdf`.

Bertoni:2012:KIO

[BDP+12] Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. Keccak implementation overview. Report, STMicroelectronics,

Antwerp, Belgium (??), May 29, 2012. 59 pp. URL http://keccak.noekeon.org/Keccak-implementation-3.2.pdf.

Baraani-Dastjerdi:1997:UCH

[BDPSNG97] A. Baraani-Dastjerdi, J. Pieprzyk, R. Safavi-Naini, and J. R. Getta. Using cryptographic hash functions for discretionary access control in object-oriented databases. *J.UCS: Journal of Universal Computer Science*, 3 (6):730–??, June 28, 1997. ISSN 0948-6968. URL http://medoc.springer.de:8000/jucs_3_6/using_cryptographic_functions_for; internal&sk=05460486.

Bertoni:2006:RBM

[BDPV06] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. RadioGatún, a belt-and-mill hash function. Report, STMicroelectronics, Antwerp, Belgium (??), 2006. URL http://radiogatun.noekeon.org/. Presented at the Second Cryptographic Hash Workshop, Santa Barbara, August 2006.

Bertoni:2007:SF

[BDPV07] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Sponge functions. Report, STMicroelectronics, Antwerp, Belgium (??), 2007. URL http://www.csrc.nist.gov/pki/HashWorkshop/Public_Comments/2007_May.html. Presented at the Ecrypt Hash Workshop 2007, May 2007.

Bertoni:2008:ISC

[BDPV08] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. On the indifferentiability of the sponge construction. *Lecture Notes in Computer Science*, 4965:181–197, 2008. ISBN ???? URL http://sponge.noekeon.org.

Bertoni:2009:RPK

[BDPV09] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The road from Panama to Keccak via RadioGatún. In Helena Handschuh, Stefan Lucks, Bart Preneel, and Phillip Rogaway, editors, *Symmetric Cryptography*, number 09031 in Dagstuhl Seminar Proceedings, page ?? Schloss Dagstuhl — Leibniz-Zentrum für Informatik, Germany, Dagstuhl, Germany, 2009. ISSN 1862-4405. URL http://drops.dagstuhl.de/opus/volltexte/2009/1958.

Bertoni:2012:KSF

[BDPV12] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The Keccak sponge function family. Web site, October 24, 2012. URL http://keccak.noekeon.org/.

Bertoni:2014:SCS

[BDPV14] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Sufficient conditions for sound tree and sequential hashing modes. *International Journal of Information Security*, 13(4):335–353, August 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-013-0220-y`.

Beeri:1988:PTI

[BDS88] Catriel Beeri, Umeshwar Dayal, and Joachim W. Schmidt, editors. *Proceedings of the third International Conference on Data and Knowledge Bases–Improving Usability and Responsiveness: June 28–30, 1988, Jerusalem, Israel*. Morgan Kaufmann Publishers, San Francisco, CA, 1988. ISBN 0-934613-95-8. LCCN QA76.9.D3 I5541 1988.

Buchmann:2009:HBD

[BDS09] Johannes Buchmann, Erik Dahmen, and Michael Szydlo. Hash-based digital signature schemes. In Bernstein et al. [BBD09b], pages 35–94. ISBN 3-540-88701-6 (hardcover), 3-642-10019-8 (softcover). LCCN QA76.9.A25 P67 2009.

Beeton:TB4-1-36

[Bee83] Barbara Beeton. Determining hashtable size and other quantities. *TUGboat*, 4(1): 36–37, April 1983. ISSN 0896-3207.

Beebe:1999:HTL

[Bee99] Nelson H. F. Beebe. The hash table library. Report, Center for Scientific Computing and Department of Mathematics, University of Utah, Salt Lake City, UT 84112, USA, March 12, 1999. 10 pp. URL `https://www.math.utah.edu/pub/emacs/`; `https://www.math.utah.edu/pub/emacs/hash-1.00.tar.gz`.

Bell:1970:QQM

[Bel70] James R. Bell. The quadratic quotient method: a hash code eliminating secondary clustering. *Communications of the Association for Computing Machinery*, 13(2):107–109, February 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Bell:1972:QQM

[Bel72] James R. Bell. The quadratic quotient method: a hash code eliminating secondary clustering. *Communications of the Association for Computing Machinery*, 13(2):107–109, February 1972. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Bell:1983:QQM

[Bel83] J. R. Bell. The quadratic quotient method: a hash code eliminating secondary clustering. *Communications of the Association for Computing Machinery*, 26(1):62–63, January 1983. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Bellare:2000:ACC

[Bel00] Mihir Bellare, editor. *Advances in cryptology — CRYPTO 2000: 20th annual International Cryptology Conference, Santa Barbara, California, USA, August 20–24, 2000: proceedings*, volume 1880 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar.

Benzinger:1998:SCB

[Ben98] Mike Benzinger. STL containers based on hash tables. *C/C++ Users Journal*, 16 (2):??, February 1998. CODEN CCUJEX. ISSN 1075-2838.

Bell:1983:MCS

[BF83] R. Charles Bell and Bryan Floyd. Monte Carlo study of Cichelli hash-function solvability. *Communications of the Association for Computing Machinery*, 26(11):924–925, November 1983. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Boral:1989:DMS

[BF89] Haran Boral and Pascal Faudemay, editors. *Database Machines: Sixth International Workshop, IWDM '89, Deauville, France, June 1989: Proceedings*, volume 368 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1989. ISBN 0-387-51324-8. LCCN QA76.9.D3 D3576 1989.

Bouillaguet:2008:ACR

[BF08] C. Bouillaguet and P.-A. Fouque. Analysis of the collision resistance of Radio-Gatún using algebraic techniques. *Lecture Notes in CS*, 4876:??, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL ????.

Bender:2012:DTH

[BFCJ+12] Michael A. Bender, Martin Farach-Colton, Rob Johnson, Russell Kraner, Bradley C. Kuszmaul, Dzejla Medjedovic, Pablo Montes, Pradeep Shetty, Richard P. Spillane, and Erez Zadok.

Don't thrash: how to cache your hash on flash. *Proceedings of the VLDB Endowment*, 5(11):1627–1637, July 2012. CODEN ???? ISSN 2150-8097.

Barn:1995:ODP

[BFG+95] C. Barn, G. Fecteau, A. Goyal, H. i. Hsiao, A. Jhingran, S. Padmanabhan, and W. Wilson. An overview of DB2 parallel edition. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 24(2): 460–462, May 1995. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Battiato:2011:RFH

[BFMP11] Sebastiano Battiato, Giovanni Maria Farinella, Enrico Messina, and Giovanni Puglisi. A robust forensic hash component for image alignment. *Lecture Notes in CS*, 6978:473–483, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-24085-0_49`.

Boeker:1987:SAG

[BFR87] Michael Boeker, Dietmar Fox, and Elisabeth Rueter. Setl in action: a gallery of data structures. Technical report, ????, Hildesheim, Germany, 1987. ?? pp.

Batory:1980:UMP

[BG80] D. S. Batory and C. C. Gotlieb. A unifying model of physical databases. Technical report, ????, Toronto, ON, Canada, 1980. ?? pp.

Batory:1982:UMP

[BG82] D. S. Batory and C. C. Gotlieb. A unifying model of physical databases. *ACM Transactions on Database Systems*, 7(4):509–539, December 1982. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1982-7-4/p509-batory/p509-batory.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1982-7-4/p509-batory/`.

Becker:1992:RBO

[BG92] Ludger Becker and Ralf Hartmut Güting. Rule-based optimization and query processing in an extensible geometric database system. *ACM Transactions on Database Systems*, 17(2): 247–303, June 1992. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1992-17-2/p247-becker/p247-becker.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1992-17-2/p247-becker/`

; http://www.acm.org/pubs/toc/Abstracts/tods/128905.html.

Baritaud:1993:FHCb

[BG93] T. Baritaud and H. Gilbert. FFT hashing is not collision-free. In Rueppel [Rue93], pages 31–40. ISBN 0-387-56413-6 (New York), 3-540-56413-6 (Berlin). LCCN QA76.9.A25 E964 1992.

Blelloch:2007:SHI

[BG07] G. E. Blelloch and D. Golovin. Strongly history-independent hashing with applications. In IEEE [IEE07], pages 272–282. ISBN 0-7695-3010-9. ISSN 0272-5428. LCCN QA76 .S974 2007. URL http://ieeexplore.ieee.org/servlet/opac?punumber=4389466. IEEE Computer Society order number P3010.

Broadbery:1995:IDE

[BGDW95] P. A. Broadbery, T. Gómez-Díaz, and S. M. Watt. On the implementation of dynamic evaluation. In Levelt [Lev95], pages 77–84. ISBN 0-89791-699-9. LCCN QA 76.95 I59 1995. URL http://www.acm.org:80/pubs/citations/proceedings/issac/220346/p77-broadbery/. ACM order number: 505950.

Barak:1988:HFS

[BGF88] Amnon Barak, Bernard A. Galler, and Yaron Farber. A holographic file system for a multicomputer with many disk nodes. Technical Report 88-6, Dept. of Computer Science, Hebrew University of Jerusalem, May 1988. ?? pp.

Baritaud:1993:FHCa

[BGG93] T. Baritaud, H. Gilbert, and M. Girault. FFT hashing is not collision-free. *Lecture Notes in CS*, 658:35–44, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580035.htm; http://link.springer-ny.com/link/service/series/0558/papers/0658/06580035.pdf.

Bellare:1994:ICC

[BGG94] M. Bellare, O. Goldreich, and S. Goldwasser. Incremental cryptography: the case of hashing and signing. *Lecture Notes in CS*, 839:216–233, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brun:2012:LLS

[BGG12] Emmanuel Brun, Arthur Guittet, and Frédéric Gibou. A local level-set method using a hash table data structure. *Journal of Computational Physics*, 231(6): 2528–2536, March 20, 2012. CODEN JCTPAH. ISSN

0021-9991 (print), 1090-2716 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0021999111006991.

Barthe:2012:VIH

[BGH12] Gilles Barthe, Benjamin Grégoire, and Sylvain Heraud. Verified indifferentiable hashing into elliptic curves. *Lecture Notes in CS*, 7215:209–228, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28641-4_12/.

Barthe:2013:VIH

[BGH+13] Gilles Barthe, Benjamin Grégoire, Sylvain Heraud, Federico Olmedo, and Santiago Zanella-Béguelin. Verified indifferentiable hashing into elliptic curves. *Journal of Computer Security*, 21(6):881–917, ???? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bagheri:2012:SFP

[BGKZ12] Nasour Bagheri, Praveen Gauravaram, Lars R. Knudsen, and Erik Zenner. The suffix-free-prefix-free hash function construction and its indifferentiability security analysis. *International Journal of Information Security*, 11(6):419–434, November 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0175-4.

Bierbrauer:1996:OAR

[BGS96] Jürgen Bierbrauer, K. Gopalakrishnan, and D. R. Stinson. Orthogonal arrays, resilient functions, error-correcting codes, and linear programming bounds. *SIAM Journal on Discrete Mathematics*, 9(3):424–452, August 1996. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Bosselaers:1996:FHP

[BGV96] A. Bosselaers, R. Govaerts, and J. Vandewalle. Fast hashing on the Pentium. *Lecture Notes in CS*, 1109:298–312, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Berkovich:1985:MSP

[BH85] Simon Y. Berkovich and Abd El Fatah A. Hegazy. *Matching String Patterns in Large Textual Files*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1985. ISBN 0-8186-0639-8. 122–127 pp. LCCN QA75.5 .I6351 1985. IEEE Service Cent. Piscataway, NJ, USA.

Bruckner:1986:MPH

[BH86] Jared A. Bruckner and James Harp. Minimal perfect hashing functions for Modula-2 word lists. *Journal of Pascal, Ada and Modula-2*, 5(6): 39–40, November–December 1986. CODEN JPAME8. ISSN 0747-1351, 0735-1232.

Banieqbal:1990:RMH

[BH90] B. Banieqbal and S. Hilditch. The random matrix hashing algorithm. Technical Report UMCS-90-9-1, Department of Computer Science, University of Manchester, Manchester, UK, 1990. ?? pp.

Bast:1991:FRP

[BH91] Holger Bast and Torben Hagerup. Fast and reliable parallel hashing. In ACM-PAA'91 [ACM91c], pages 50–61. ISBN 0-89791-438-4. LCCN QA76.58 .A27 1991.

Ban-Hashemi:1993:FAC

[BH93] A. Ban-Hashemi. A Fourier approach to camera orientation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(11): 1197, 1993. CODEN ITPIDJ. ISSN 0162-8828.

Bernstein:2015:SPS

[BHH+15] Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn. SPHINCS: Practical stateless hash-based signatures. *Lecture Notes in CS*, 9056:368–397, 2015. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `https://link.springer.com/chapter/10.1007/978-3-662-46800-5_15`.

Ben-Haim:2012:PHC

[BHIMM12] Yael Ben-Haim, Alexander Ivrii, Oded Margalit, and Arie Matsliah. Perfect hashing and CNF encodings of cardinality constraints. *Lecture Notes in CS*, 7317:397–409, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-31612-8_30`.

Berman:2013:HPR

[BHKN13] Itay Berman, Iftach Haitner, Ilan Komargodski, and Moni Naor. Hardness preserving reductions via cuckoo hashing. *Lecture Notes in CS*, 7785:40–59, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-36594-2_3/`.

Berman:2019:HPR

[BHKN19] Itay Berman, Iftach Haitner, Ilan Komargodski, and

Moni Naor. Hardness-preserving reductions via cuckoo hashing. *Journal of Cryptology*, 32(2):361–392, April 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9293-0`.

Brassard:1997:QCH

[BHT97] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. *ACM SIGACT News*, 28(2):14–19, June 1997. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Brassard:1998:QCH

[BHT98] G. Brassard, P. Hoyer, and A. Tapp. Quantum cryptanalysis of hash and claw-free functions. *Lecture Notes in CS*, 1380:163–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bohm:1987:BQK

[BI87] Alexander Böhm and Jannis Iliadis. Ein Beitrag zu den quadratischen Kollisionsstrategien in Hash-Tabellen—Ein neuer Algorithmus. (German) [on quadratic strategies for handling collisions in hash tables — a new algorithm]. *Angewandte Informatik*, 29(3): 111–118, March 1987. CODEN AWIFA7.

Bozas:2012:LSS

[BI12] Konstantinos Bozas and Ebroul Izquierdo. Large scale sketch based image retrieval using patch hashing. *Lecture Notes in CS*, 7431:210–219, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-33179-4_21`.

Bierbrauer:1995:CUH

[Bie95] J. Bierbrauer. A^2-codes from universal hash classes. In Guillou and Quisquater [GQ95], pages 311–318. ISBN 3-540-59409-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C794 1995. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0921/09210311.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0921/09210311.pdf`.

Bierbrauer:1997:UHG

[Bie97] Jürgen Bierbrauer. Universal hashing and geometric codes. *Designs, Codes, and Cryptography*, 11(3): 207–221, July 1997. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http:`

//www.wkap.nl/oasis.htm/131331.

Biham:2008:NTC

[Bih08] Eli Biham. New techniques for cryptanalysis of hash functions and improved attacks on Snefru. *Lecture Notes in CS*, 5086: 444–461, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-71039-4_28.

Binstock:1996:HR

[Bin96] Andrew Binstock. Hashing rehashed. *Dr. Dobbs Journal*, 21(4):24–??, April 1, 1996. CODEN DDJOEB. ISSN 1044-789X.

Belkin:1992:PAI

[BIP92] Nicholas Belkin, Peter Ingwersen, and Annelise Mark Pejtersen, editors. *Proceedings of the 15th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, Copenhagen, Denmark, June 21–24, 1992*. ACM Press, New York, NY 10036, USA, 1992. ISBN 0-89791-523-2 (paperback), 0-89791-524-0 (hardcover). LCCN Z699.A1 I659 1992.

Biryukov:2007:FSE

[Bir07] Alex Biryukov, editor. *Fast software encryption: 14th international workshop, FSE 2007, Luxembourg, Luxembourg, March 26–28, 2007, revised selected papers*, volume 4593 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-74617-X (softcover). LCCN QA76.9.A25 F77 2007. URL http://www.springerlink.com/openurl.asp?genre=book\%26isbn=978-3-540-74617-1.

Biscani:2012:PSP

[Bis12] Francesco Biscani. Parallel sparse polynomial multiplication on modern hardware architectures. In van der Hoeven and van Hoeij [vdHvH12], pages 83–90. ISBN 1-4503-1269-1. LCCN QA76.95 .I59 2012.

Buneman:1993:PAS

[BJ93] Peter Buneman and Sushil Jajodia, editors. *Proceedings of the 1993 ACM SIGMOD International Conference on Management of Data: SIGMOD '93, Washington, DC, May 26–28, 1993*. ACM Press, New York, NY 10036, USA, 1993. ISBN 0-89791-592-5. LCCN QA76.A1 A1135 v.22:2.

Barwick:2007:SAL

[BJ07] Susan G. Barwick and Wen-Ai Jackson. A sequence approach to linear perfect hash families. *Designs,*

Codes, and Cryptography, 45 (1):95–121, October 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=1&spage=95`.

Bierbrauer:1993:FHF

[BJKS93] J. Bierbrauer, T. Johansson, G. Kabatianskii, and B. Smeets. On families of hash functions via geometric codes and concatenation. In Stinson [Sti93], pages 331–342. ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). LCCN QA76.9.A25 C79 1993.

Bierbrauer:1994:FHF

[BJKS94] Jurgen Bierbrauer, Thomas Johansson, Gregory Kabatianskii, and Ben Smeets. On families of hash functions via geometric codes and concatenation. *Lecture Notes in CS*, 773:331–342, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Benhamouda:2016:NFP

[BJL16] Fabrice Benhamouda, Marc Joye, and BenoîT Libert. A new framework for privacy-preserving aggregation of time-series data. *ACM Transactions on Information and System Security*, 18(3): 10:1–10:??, April 2016. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Braibant:2014:IRA

[BJM14] Thomas Braibant, Jacques-Henri Jourdan, and David Monniaux. Implementing and reasoning about hash-consed data structures in Coq. *Journal of Automated Reasoning*, 53(3):271–304, October 2014. CODEN JAREEW. ISSN 0168-7433 (print), 1573-0670 (electronic). URL `http://link.springer.com/article/10.1007/s10817-014-9306-0`.

Benouamer:1994:HST

[BJMM94a] M. O. Benouamer, P. Jaillon, D. Michelucci, and J.-M. Moreau. Hash-Speicherung von ,,tragen" Zahlen. (German) [Hashing "lazy" numbers]. *Computing*, 53(3–4):205–217, 1994. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics (Vienna, 1993).

Benouamer:1994:HLN

[BJMM94b] M. O. Benouamer, P. Jaillon, D. Michelucci, and J.-M. Moreau. Hashing lazy numbers: Hash-Speicherung von ,,tragen" Zahlen. *Computing*, 53(3 / 4):205–??, 1994.

CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Bocca:1994:ICV

[BJZ94] Jorge Bocca, Matthias Jarke, and Carlo Zaniolo, editors. *20th International Conference on Very Large Data Bases, September 12th–15th 1994, Santiago, Chile proceedings*, PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON VERY LARGE DATA BASES 1994; EDIT 20. Morgan Kaufmann Publishers, San Francisco, CA, 1994. ISBN 1-55860-153-8. ISSN 0730-9317. LCCN QA76.9 D3 I61 1994.

Bell:1970:LQH

[BK70] James R. Bell and Charles H. Kaman. The linear quotient hash code. *Communications of the Association for Computing Machinery*, 13(11): 675–677, November 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Independent discovery of technique of secondary hash functions first proposed by [de 69].

Bechtold:1984:UEH

[BK84] Ulrich Bechtold and Klaus Küspert. On the use of extendible hashing without hashing. *Information Processing Letters*, 19(1): 21–26, July 1984. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Brassard:1988:GRP

[BK88] Gilles Brassard and Sampath Kannan. The generation of random permutations on the fly. *Information Processing Letters*, 28 (4):207–212, July 1988. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Broder:1990:MAH

[BK90] Andrei Z. Broder and Anna R. Karlin. Multilevel adaptive hashing. In SDA'90 [SDA90], pages 43–53. ISBN 0-89871-251-3. LCCN QA76.6 .A278 1990.

Barker:2007:RRN

[BK07a] Elaine Barker and John Kelsey. *Recommendation for random number generation using deterministic random bit generators (revised)*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, March 2007. viii + 124 pp. URL `http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90revised_March2007.pdf`.

Bradford:2007:PSC

[BK07b] Phillip G. Bradford and Michael N. Katehakis. A probabilistic study on combinatorial expanders and

hashing. *SIAM Journal on Computing*, 37(1):83–111, ???? 2007. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Boldyreva:2012:NPG

[BK12] Alexandra Boldyreva and Virendra Kumar. A new pseudorandom generator from collision-resistant hash functions. Report, School of Computer Science, Georgia Institute of Technology, Atlanta, GA, USA, February 6, 2012. URL `http://eprint.iacr.org/2012/056`.

Bogdanov:2011:SLH

[BKL+11] Andrey Bogdanov, Miroslav Knežević, Gregor Leander, Deniz Toz, and Kerem Varıcı. `spongent`: a lightweight hash function. *Lecture Notes in CS*, 6917:312–325, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-23951-9_21`.

Brier:2009:LFC

[BKMP09] Eric Brier, Shahram Khazaei, Willi Meier, and Thomas Peyrin. Linearization framework for collision attacks: Application to CubeHash and MD6. *Lecture Notes in CS*, 5912:560–577, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-10366-7_33`.

Bibak:2018:AUH

[BKST18] Khodakhast Bibak, Bruce M. Kapron, Venkatesh Srinivasan, and László Tóth. On an almost-universal hash function family with applications to authentication and secrecy codes. *International Journal of Foundations of Computer Science*, 29(3): 357–??, April 2018. CODEN IFCSEN. ISSN 0129-0541.

Boral:1988:SIC

[BL88] Haran Boral and Per-Åke Larson, editors. *SIGMOD International Conference on Management of Data, Chicago, Illinois, June 1–3: 1988 Proceedings*. ACM Press, New York, NY 10036, USA, 1988. ISBN 0-89791-268-3. LCCN QA 76.9 D3 S53 v.17 no.3 1988. US$33.00.

Barkley:1989:PRH

[BL89] Ronald E. Barkley and T. Paul Lee. Point representation and hashing of an interval. *Information Processing Letters*, 30(4):201–203, February 1989. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Blasius:1995:GRR

[Bla95] Arlene Blasius. Generating a rotation reduction perfect hashing function. *Mathematics Magazine*, 68(1):35–??, February 1, 1995. CODEN MAMGA8. ISSN 0025-570X.

Blackburn:2000:PHF

[Bla00] S. R. Blackburn. Perfect hash families: Probabilistic methods and explicit constructions. *Journal of Combinatorial Theory (Series A)*, 92(1): 54–60, October 2000. CODEN JCBTA7. ISSN 0097-3165.

Bando:2012:FBG

[BLC12] Masanori Bando, Yi-Li Lin, and H. Jonathan Chao. FlashTrie: beyond 100-Gb/s IP route lookup using hash-based prefix-compressed trie. *IEEE/ACM Transactions on Networking*, 20(4):1262–1275, August 2012. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Bloom:1970:STT

[Blo70] Burton H. Bloom. Space/time trade-offs in hash coding with allowable errors. *Communications of the Association for Computing Machinery*, 13(7):422–426, July 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Barber:2014:MEH

[BLP+14] R. Barber, G. Lohman, I. Pandis, V. Raman, R. Sidle, G. Attaluri, N. Chainani, S. Lightstone, and D. Sharpe. Memory-efficient hash joins. *Proceedings of the VLDB Endowment*, 8(4):353–364, December 2014. CODEN ???? ISSN 2150-8097.

Blustein:1995:IBV

[Blu95] James Blustein. Implementing bit vectors in C. *Dr. Dobbs Journal*, 20(8):42, 44, 46, 96, 98–100, August 1, 1995. CODEN DDJOEB. ISSN 1044-789X.

Battulga:2020:HTP

[BLY20] Lkhagvadorj Battulga, Sang-Hyun Lee, and Kwan-Hee Yoo. Hash-tree PCA: accelerating PCA with hash-based grouping. *The Journal of Supercomputing*, 76(10):8248–8264, October 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-019-02947-x`.

Bayer:1976:EST

[BM76] R. Bayer and J. K. Metzger. On the encipherment of search trees and random access files. *ACM Transactions on Database Systems*, 1 (1):37–52, March 1976. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (elec-

tronic). Also published in [Ker75, p. 508–510].

Barklund:1987:HTL

[BM87] J. Barklund and H. Millroth. Hash tables in logic programming. In Lassez [Las87], pages 411–427. ISBN 0-262-12125-5 (ensemble) 0-262-12129-8 (vol. 2). LCCN QA76.6 .L589 1987 v. 1-2.

Blakeley:1989:JIM

[BM89] J. A. Blakeley and N. L. Martin. Join index, materialized view, and hybrid-hash join: a performance analysis. Technical Report T, Indiana University, Computer Science Department, June 1989. ?? pp.

Blakeley:1990:JIM

[BM90a] Jose A. Blakeley and Nancy L. Martin. Join index, materialized view, and hybrid-hash join: a performance analysis. In Blakeley & Martin [ICD90], pages 256–263. ISBN 0-8186-2025-0 (paperback), 0-8186-9025-9 (hardcover), 0-8186-6025-2 (microfiche). LCCN QA76.9.D3 I5582 1990.

Bourdon:1990:ORU

[BM90b] Olivier Bourdon and Gérard Medioni. Object Recognition Using Geometric Hashing on the Connection Machine. In Freeman [Fre90], pages 596–600. ISBN 0-8186-2062-5 (v.1, paperback), 0-8186-2063-3 (v.2, paperback), 0-8186-6062-7 (v.1, microfiche), 0-8186-6063-5 (v.2, microfiche), 0-8186-9062-3 (v.1, hardcover), 0-8186-9063-1 (v.2, hardcover). LCCN TK7882.P3 I58 1990. Two volumes.

Bellare:1997:NPC

[BM97] M. Bellare and D. Micciancio. A new paradigm for collision-free hashing: Incrementality at reduced cost. *Lecture Notes in CS*, 1233:163–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brodnik:1999:MCT

[BM99] Andrej Brodnik and J. Ian Munro. Membership in constant time and almost-minimum space. *SIAM Journal on Computing*, 28(5): 1627–1640, October 1999. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/29416`.

Broder:2001:UMH

[BM01] Andrei Broder and Michael Mitzenmacher. Using multiple hash functions to improve IP lookups. In IEEE [IEE01], pages 1454–1463. ISBN 0-7803-7016-3 (softbound), 0-7803-7017-1 (microfiche), 0-7803-7018-X (CD-ROM). LCCN TK5105.5 .I48 2001.

URL http://ieeexplore.ieee.org/servlet/opac?punumber=7321.

Beyer:1968:LEC

[BMB68] J. D. Beyer, W. D. Maurer, and Frank K. Bamberger. Letter to the Editor: Comments on "an improved hash code for scatter storage". *Communications of the Association for Computing Machinery*, 11 (5):378, May 1968. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Bustio-Martinez:2019:UHL

[BMLLC+19] Lázaro Bustio-Martínez, Martín Letras-Luna, René Cumplido, Raudel Hernández-León, Claudia Feregrino-Uribe, and José M. Bande-Serrano. Using hashing and lexicographic order for Frequent Itemsets Mining on data streams. *Journal of Parallel and Distributed Computing*, 125(??): 58–71, March 2019. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731518308244.

Black:1998:GHA

[BMQ98] John R. Black, Jr., Charles U. Martel, and Hongbin Qi. Graph and hashing algorithms for modern architectures: Design and performance. In Kurt Mehlhorn, editor, *Proceedings of the 2nd Workshop on Algorithm Engineering (WAE'98), Saarbrücken, Germany, August 1998*, page ?? Max-Planck-Institut für Informatik, Saarbrücken, Germany, 1998. ISBN ???? LCCN ???? Report number MPI-I-98-1-019.

Buhrman:2002:BO

[BMRV02] H. Buhrman, P. B. Miltersen, J. Radhakrishnan, and S. Venkatesh. Are bitvectors optimal? *SIAM Journal on Computing*, 31(6): 1723–1744, December 2002. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/40529.

Barthels:2017:DJA

[BMS+17] Claude Barthels, Ingo Müller, Timo Schneider, Gustavo Alonso, and Torsten Hoefler. Distributed join algorithms on thousands of cores. *Proceedings of the VLDB Endowment*, 10(5):517–528, January 2017. CODEN ???? ISSN 2150-8097.

Barth:1985:SSS

[BN85] Wilhelm Barth and Heinrich Nirschl. Sichere Sinnentsprechende Silbentrennung für die Deutsche Sprache. *Angewandte Informatik, Applied Informatics*, 27(4):152–159, April 1985. CODEN AWIFA7.

Barreto:2010:WNC

[BNN+10] Paulo Barreto, Ventzislav Nikov, Svetla Nikova, Vincent Rijmen, and Elmar Tischhauser. Whirlwind: a new cryptographic hash function. *Designs, Codes, and Cryptography*, 56(2–3):141–162, August 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=56&issue=2&spage=141`.

Bobrow:1975:NHL

[Bob75] Daniel G. Bobrow. A note on hash linking. *Communications of the Association for Computing Machinery*, 18 (7):413–415, July 1975. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Bolour:1979:OPM

[Bol79] Azad Bolour. Optimality properties of multiple-key hashing functions. *Journal of the Association for Computing Machinery*, 26(2):196–210, April 1979. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Bookstein:1972:DH

[Boo72] Abraham Bookstein. Double hashing. *Journal of the American Society for Information Science*, 23(6):402–405, November 1972. CODEN AISJB6. ISSN 0002-8231 (print), 1097-4571 (electronic).

Bookstein:1973:HST

[Boo73] Abraham Bookstein. On Harrison's substring testing technique. *Communications of the Association for Computing Machinery*, 16(3):180–181, March 1973. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Bookstein:1974:HCN

[Boo74] Abraham Bookstein. Hash coding with a non-unique search key. *Journal of the American Society for Information Science*, 25(4):232–236, July–August 1974. CODEN AISJB6. ISSN 0002-8231 (print), 1097-4571 (electronic).

Borman:1981:PSP

[Bor81] Lorraine Borman, editor. *Proceedings: selected papers from the Conference on Easier and More Productive Use of Computer Systems, May 20–22, 1981, Ann Arbor, Michigan. Part 2. Human interaction and the user interface*, volume 12(4), 13(1–3) of *SIGSOC Bulletin*. ACM Press, New York, NY 10036, USA, 1981. CODEN SGBLDB. ISBN 0-89791-056-7

(pt. 1), 0-89791-064-8 (pt. 2). ISSN 0163-5794. LCCN H61 .S53 v.12 no.4-v.13 no.1-3.

Borgwardt:1984:PPU

[Bor84] P. Borgwardt. Parallel Prolog using stack segments on shared-memory multiprocessors. In IEEE-ISLP'84 [IEE84], page ?? ISBN 0-8186-0522-7 (paperback), 0-8186-8522-0 (hardcover), 0-8186-4522-9 (microfiche). LCCN QA76.6 .I5735 1984. CH2007-3/84/0002$01.00.

Bosselaers:19xx:EFH

[Bosxx] A. Bosselaers. Even faster hashing on the Pentium. In *????*, page ???? ????, ????, 19xx. URL `ftp://ftp.esat.kuleuven.ac.be/pub/COSIC/bosselae/pentiumplus.ps.gz`. Presented at the rump session of Eurocrypt'97, Konstanz, Germany, May 12-15, 1997, and updated on November 13, 1997.

Bos:2011:EHU

[BÖS11] Joppe W. Bos, Onur Özen, and Martijn Stam. Efficient hashing using the AES instruction set. *Lecture Notes in CS*, 6917: 507–522, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-23951-9_33`.

Boukliev:1995:NTL

[Bou95] I. G. Boukliev. New ternary linear codes. *IEEE International Symposium on Information Theory*, ????(????): 500–??, ???? 1995. CODEN PISTFZ. ISSN 0271-4655.

Boutin:2012:NSW

[Bou12] Chad Boutin. NIST selects winner of Secure Hash Algorithm (SHA-3) Competition. Press release., October 2, 2012. URL `http://csrc.nist.gov/groups/ST/hash/sha-3/index.html`; `http://csrc.nist.gov/groups/ST/hash/sha-3/winner_sha-3.html`; `http://www.nist.gov/itl/csd/sha-100212.cfm`.

Boyd:1995:CCC

[Boy95a] C. Boyd, editor. *Cryptography and coding: 5th Conference — December 1995, Cirencester*, number 1025 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. ISBN 3-540-60693-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .C76 1995.

Boyd:1995:CCI

[Boy95b] Colin Boyd, editor. *Cryptography and coding: 5th IMA conference, Cirencester, UK, December 18–20, 1995, pro-*

ceedings, volume 1025 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. CODEN LNCSD9. ISBN 3-540-60693-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .C76 1995. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1025.htm`; `http://www.springerlink.com/content/978-3-540-60693-2`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1025`. Papers from the 5th IMA Conference on Cryptography and Coding.

Boyer:1998:AAR

[Boy98] John Boyer. Algorithm alley: Resizable data structures. *Dr. Dobbs Journal*, 23(1):115–116, 118, 129, January 1998. CODEN DDJOEB. ISSN 1044-789X. Discusses some deficiencies of the Java library hash table support, and compares it with his algorithm and that used in the C++ Standard Template Library. Also compares the Jenkins hash function [Jen97] with the one proposed in this paper.

Beuchat:2011:LAU

[BOY11] Jean-Luc Beuchat, Eiji Okamoto, and Teppei Yamazaki. A low-area unified hardware architecture for the AES and the cryptographic hash function ECHO. *Journal of Cryptographic Engineering*, 1(2): 101–121, August 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-011-0009-8`.

Biliris:1994:EEO

[BP94] Alexandros Biliris and Euthimios Panagos. EOS: An Extensible Object Store. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 23(2): 517, June 1994. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Barbour:1997:DMH

[BP97] A. D. Barbour and R. M. Phatarfod. Dimensioning a multiple hashing scheme. *Journal of Applied Probability*, 34(2):477–486, June 1997. CODEN JPRBAM. ISSN 0021-9002 (print), 1475-6072 (electronic). URL `http://www.jstor.org/stable/3215386`.

Brier:2009:CC

[BP09] Eric Brier and Thomas Peyrin. Cryptanalysis of CubeHash. *Lecture Notes in CS*, 5536:354–368, 2009. CODEN LNCSD9. ISSN 0302-

9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-01957-9_22.

Budroni:2018:HGB

[BP18] Alessandro Budroni and Federico Pintore. Hashing to G2 on BLS pairing-friendly curves. *ACM Communications in Computer Algebra*, 52(3):63–66, September 2018. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Ben-Porat:2012:VHH

[BPBBLP12] Udi Ben-Porat, Anat Bremler-Barr, Hanoch Levy, and Bernhard Plattner. On the vulnerability of hardware hash tables to sophisticated attacks. *Lecture Notes in CS*, 7289:135–148, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-30045-5_11/.

Bakhtiari:1997:WGC

[BPSN97] S. Bakhtiari, J. Pieprzyk, and R. Safavi-Naini. On the weaknesses of Gong's collisionful hash function. *J.UCS: Journal of Universal Computer Science*, 3(3):185–??, March 28, 1997. ISSN 0948-6968. URL http://www.iicm.edu/jucs_3_3/hash_function.

Buehrer:2010:DPS

[BPT10] Gregory Buehrer, Srinivasan Parthasarathy, and Shirish Tatikonda. A distributed placement service for graph-structured and tree-structured data. *SIGPLAN Notices*, 45(5):355–356, May 2010. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Botelho:2007:SSE

[BPZ07] Fabiano C. Botelho, Rasmus Pagh, and Nivio Ziviani. Simple and space-efficient minimal perfect hash functions. In Dehne et al. [DSZ07b], pages 139–150. CODEN LNCSD9. ISBN 3-540-73948-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/content/12165xq21248x275/; http://www.springerlink.com/content/978-3-540-73948-7/.

Banerjee:1975:DLD

[BR75] J. Banerjee and V. Rajaraman. A dual link data structure for random file organization. *Information Processing Letters*, 4(3):64–69, December ??, 1975. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Bellare:1994:OAEa

[BR94] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. Research report RC 19610 (86198), IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, June 16, 1994. 19 pp. Appears in Advances in Cryptology — Eurocrypt 94 Proceedings, 1994.

Bellare:1997:CRH

[BR97] Mihir Bellare and Phillip Rogaway. Collision-resistant hashing: Towards making UOWHFs practical. *Lecture Notes in CS*, 1294:470–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940470.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1294/12940470.pdf`.

Bellare:2006:MPP

[BR06] Mihir Bellare and Thomas Ristenpart. Multi-property-preserving hash domain extension and the EMD transform. *Lecture Notes in CS*, 4284:299–314, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/11935230_20.pdf`.

Bellare:2014:CCH

[BR14] Mihir Bellare and Todor Ristov. A characterization of chameleon hash functions and new, efficient designs. *Journal of Cryptology*, 27(4): 799–823, October 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9155-8`.

Bradley:1984:UMD

[Bra84a] James Bradley. Use of mean distance between overflow records to compute average search lengths in hash files with open addressing. Technical Report 84/154/12, University of Calgary, May 1984. ?? pp. (email parin@cpsc.ucalgary.ca).

Bratbergsengen:1984:HMR

[Bra84b] Kjell Bratbergsengen. Hashing methods and relational algebra operations. In *Proceedings of the 10th Conference on Very Large Databases, Singapore*, pages 323–333. Morgan Kaufmann Publishers, San Francisco, CA, August 1984.

Bradley:1985:UMD

[Bra85] James Bradley. Use of mean distance between overflow records to compute average search lengths in hash files with open adressing. *The Computer Journal (to*

appear), ??(??):??, August 1985.

Bradley:1986:UMD

[Bra86] J. Bradley. Use of mean distance between overflow records to compute average search lengths in hash files with open addressing. *The Computer Journal*, 29 (2):167–170, April 1986. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Bradley:1988:BFP

[Bra88] James Bradley. *Business file processing!: COBOL, CICS, and SQL*. Mitchell Publishing, Inc., Santa Cruz, CA, USA, 1988. ISBN 0-394-39217-5. 400 pp. LCCN QA76.9.F5 B725 1988. US$28.00. Includes two chapters on hash file processing.

Brassard:1990:ACC

[Bra90] Gilles Brassard, editor. *Advances in cryptology: CRYPTO '89: proceedings*, volume 435 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. CODEN LNCSD9. ISBN 0-387-97317-6, 3-540-97317-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1989. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0435.htm`; `http://www.springerlink.com/content/978-0-387-97317-3`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=435`. Conference held Aug. 20–24, 1989 at the University of California, Santa Barbara.

Brass:2009:UHF

[Bra09] Peter Brass. Universal hash functions for an infinite universe and hash trees. *Information Processing Letters*, 109(10):461–462, April 30, 2009. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Brent:1973:RRT

[Bre73] Richard P. Brent. Reducing the retrieval time of scatter storage techniques. *Communications of the Association for Computing Machinery*, 16 (2):105–109, February 1973. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Modification of open addressing with double hashing to reduce the average number of probes for a successful search.

Bremers:1991:HPP

[Bre91] H. L. Bremers. Hash partitioning performance improved by exploiting skew and dealing with duplicates. M.s. thesis, Univ. of Colorado at Boulder, Boulder, CO, USA, 1991. ?? pp.

Brickell:1992:ACC

[Bri92] Ernest F. Brickell, editor. *Advances in Cryptology–CRYPTO '92: 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992: Proceedings*, volume 740 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992. ISBN 0-387-57340-2 (New York), 3-540-57340-2 (Berlin). LCCN QA76.9.A25 C79 1992. DM104.00.

Brickell:1993:ACC

[Bri93] Ernest F. Brickell, editor. *Advances in Cryptology — CRYPTO '92: 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992: Proceedings*, volume 740 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. CODEN LNCSD9. ISBN 0-387-57340-2 (New York), 3-540-57340-2 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1992. DM104.00. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0740.htm`; `http://www.springerlink.com/content/978-0-387-57340-3`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=740`.

Bauer:2009:FSA

[BRM+09] Raphael André Bauer, Kristian Rother, Peter Moor, Knut Reinert, Thomas Steinke, Janusz M. Bujnicki, and Robert Preissner. Fast structural alignment of biomolecules using a hash table, N-grams and string descriptors. *Algorithms (Basel)*, 2(2):692–709, June 2009. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL `https://www.mdpi.com/1999-4893/2/2/692`.

Blundell:2010:RTR

[BRM10] Colin Blundell, Arun Raghavan, and Milo M. K. Martin. RETCON: transactional repair without replay. *ACM SIGARCH Computer Architecture News*, 38(3): 258–269, June 2010. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Black:2002:BBA

[BRS02] John Black, Phillip Rogaway, and Thomas Shrimpton. Black-box analysis of the block-cipher-based hash-function constructions from PGV. In Yung [Yun02], pages 320–335. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (elec-

tronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420320.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420320.pdf.

Black:2010:ABB

[BRSS10] J. Black, P. Rogaway, T. Shrimpton, and M. Stam. An analysis of the blockcipher-based hash functions from PGV. *Journal of Cryptology*, 23(4):519–545, October 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=4&spage=519.

Bode:1993:PPA

[BRW93] Arndt Bode, Mike Reeve, and Gottfried Wolf, editors. *PARLE '93, Parallel Architectures and Languages Europe: 5th International PARLE Conference, Munich, Germany, June 14–17, 1993, Proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-56891-3 (New York), 3-540-56891-3 (Berlin). LCCN QA76.58 .I564 1993.

Bryant:1984:EHL

[Bry84] R. M. Bryant. Extendible hashing for line-oriented paging stores. *IBM Technical Disclosure Bulletin*, 26(11): 6046–6049, April 1984. CODEN IBMTAA. ISSN 0018-8689.

Biham:1991:DCFb

[BS91a] E. Biham and A. Shamir. Differential cryptanalysis of Feal and N-hash. In Davies [Dav91], pages 1–?? ISBN 0-387-54620-0 (New York), 3-540-54620-0 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1991.

Biham:1991:DCFa

[BS91b] Eli Biham and Adi Shamir. Differential cryptanalysis of Feal and N-hash. Technical report CS91-17, Department of Applied Mathematics and Computer Science, Weizmann Institute of Science, Rehovot, Israel, October 1991. 34 pp.

Biham:1991:DCS

[BS91c] Eli Biham and Adi Shamir. Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer. Technical report CS91-18, Department of Applied Mathematics and Computer Science, Weizmann Institute of Science, Rehovot, Israel, October 1991. 36 pp.

Bhatia:1994:FPH

[BS94a] S. Bhatia and C. Sabharwal. A fast perfect hash function for image databases. In

Anger et al. [ARA94], pages 337–346. ISBN 2-88449-128-7. LCCN Q334.I556 1994.

Bhatia:1994:FIP

[BS94b] Sanjiv K. Bhatia and Chaman L. Sabharwal. A fast implementation of a perfect hash function for picture objects. *Pattern Recognition*, 27(3): 365–376, March 1994. CODEN PTNRA8. ISSN 0031-3203 (print), 1873-5142 (electronic).

Bjatia:1994:FIP

[BS94c] S. K. Bjatia and C. L. Sabharwal. A fast implementation of a perfect hash function for picture objects. *Pattern Recognition*, 27(3):365–??, 1994. CODEN PTNRA8. ISSN 0031-3203 (print), 1873-5142 (electronic).

Bentley:1997:FAS

[BS97] Jon L. Bentley and Robert Sedgewick. Fast algorithms for sorting and searching strings. In ACM [ACM97a], pages 360–369. CODEN PAAAF2. ISBN 0-89871-390-0. LCCN ???? URL `http://www.cs.princeton.edu/~rs/strings/paper.pdf`.

Balkic:2012:GUI

[BŠH12] Zoran Balkić, Damir Šoštarić, and Goran Horvat. GeoHash and UUID identifier for multi-agent systems. *Lecture Notes in CS*, 7327: 290–298, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-30947-2_33`.

Bakhtiari:1996:KHF

[BSNP96a] S. Bakhtiari, R. Safavi-Naini, and J. Pieprzyk. Keyed hash functions. In Dawson and Golic [DG96], pages 201–214. ISBN 3-540-60759-5. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C844 1996.

Bakhtiari:1996:PBA

[BSNP96b] S. Bakhtiari, R. Safavi-Naini, and J. Pieprzyk. On password-based authenticated key exchange using collisionful hash functions. *Lecture Notes in CS*, 1172:299–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bakhtiari:1996:SCH

[BSNP96c] S. Bakhtiari, R. Safavi-Naini, and J. Pieprzyk. On selectable collisionful hash functions. *Lecture Notes in CS*, 1172:287–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blackburn:2012:CHA

[BSU12] Simon R. Blackburn, Douglas R. Stinson, and Jalaj

Upadhyay. On the complexity of the herding attack and some related attacks on hash functions. *Designs, Codes, and Cryptography*, 63(1):??, April 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=0&issue=0&spage=??`.

Brain:1989:NPH

[BT89] Marshall D. Brain and Alan L. Tharp. Near-perfect hashing for large word sets. *Software—Practice and Experience*, 19(10):967–978, October 1, 1989. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Brain:1990:PHU

[BT90] Marshall D. Brain and Alan L. Tharp. Perfect hashing using sparse matrix packing. *Information system*, 15(3):281–290, 1990. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Briggs:1993:ERS

[BT93] Preston Briggs and Linda Torczon. An efficient representation for sparse sets. *ACM Letters on Programming Languages and Systems*, 2(4):59–69, March 1993. CODEN ALPSE8. ISSN 1057-4514 (print), 1557-7384 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/1057-4514/176484.html`.

Brain:1994:UTE

[BT94a] Marshall D. Brain and Alan L. Tharp. Using tries to eliminate pattern collisions in perfect hashing. *IEEE Transactions on Knowledge and Data Engineering*, 6(2):239–247, April 1994. CODEN ITKEEH. ISSN 1041-4347.

Brian:1994:UTE

[BT94b] M. D. Brian and A. L. Tharp. Using tries to eliminate pattern collisions in perfect hashing. *IEEE Transactions on Knowledge and Data Engineering*, 6(2):239–??, April 1, 1994. CODEN ITKEEH. ISSN 1041-4347.

Bouabana-Tebibel:2012:HCB

[BT12a] Thouraya Bouabana-Tebibel. Hash chains at the basis of a secure reactive routing protocol. *Lecture Notes in CS*, 7222:258–270, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32298-3_17/`.

Brown:2012:FPT

[BT12b] Daniel G. Brown and Jakub Truszkowski. Fast phylogenetic tree reconstruction us-

ing locality-sensitive hashing. *Lecture Notes in CS*, 7534:14–29, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33122-0_2/.

Buchholz:1963:FOA

[Buc63] Werner Buchholz. File organization and addressing. *IBM Systems Journal*, 2(1): 86–111, June 1963. CODEN IBMSA7. ISSN 0018-8670. Comprehensive survey of hashing, with a good discussion of hash functions.

Buckhart:1982:AII

[Buc82] Walter A. Buckhart. Advances in interpolation-based index maintenance. In *Proceedings of the 1982 Conference on Information Sciences and Systems.*, pages 488–491. Princeton University Press, Princeton, NJ, USA, 1982.

Burkhard:1975:FTQ

[Bur75a] W. A. Burkhard. Full table quadratic quotient searching. *The Computer Journal*, 18(2):161–163, May 1975. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/18/2/161.full.pdf+html; http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_02/tiff/161.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_02/tiff/162.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_02/tiff/163.tif.

Burkhard:1975:PMQ

[Bur75b] Walter A. Burkhard. Partial-match queries and file designs. In Kerr [Ker75], page ?? ISBN ???? ISSN 0278-2596. LCCN QA76.9.D3 I55 1975. US$15.00.

Burkhard:1976:ART

[Bur76a] Walter A. Burkhard. Associative retrieval trie hashcoding. In ACM-TOC'76 [ACM76], pages 211–219.

Burkhard:1976:HTA

[Bur76b] Walter A. Burkhard. Hashing and trie algorithms for partial-match retrieval. *ACM Transactions on Database Systems*, 1(2):175–187, 1976. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). Also published in/as: UCSD, Appl. Physics and Inf. Sc, CS TR.2, Jun. 1975.

Burkhard:1976:PMR

[Bur76c] Walter A. Burkhard. Partial match retrieval. *BIT (Nordisk tidskrift for informationsbehandling)*, 16(1): 13–31, 1976. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Burkhard:1977:ART

[Bur77] Walter A. Burkhard. Associative retrieval trie hashcoding. *Journal of Computer and System Sciences*, 15(3): 280–299, December 1977. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic).

Burkhard:1978:PMH

[Bur78] W. A. Burkhard. Partial-match hash coding projection functions. *Proceedings of the Hawaii International Conference on System Science*, 1 (??):99–105, ???? 1978. CODEN PHISD7.

Burkhard:1979:PMH

[Bur79] Walter A. Burkhard. Partial-match hash coding: Benefits of redundancy. *ACM Transactions on Database Systems*, 4(2):228–239, June 1979. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1979-4-2/p228-burkhard/p228-burkhard.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1979-4-2/p228-burkhard/`.

Burkowski:1981:PHH

[Bur81] F. J. Burkowski. Parallel hashing hardware for text scanning applications. *Proceedings of the International Conference on Parallel Processing*, pages 282–286, 1981. CODEN PCPADL. ISSN 0190-3918.

Burkowski:1982:HHS

[Bur82] Forbes J. Burkowski. A hardware hashing scheme in the design of a multiterm string comparator. *IEEE Transactions on Computers*, C-31(9): 825–834, September 1982. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Burkhard:1983:IBI

[Bur83a] Walter A. Burkhard. Interpolation-based index maintenance. *BIT (Nordisk tidskrift for informationsbehandling)*, 23 (3):274–294, 1983. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). Discusses construction of order-preserving hash functions for use in range queries.

Burkhard:1983:IIM

[Bur83b] Walter A. Burkhard. Interpolation-based index maintenance. In ACM-PODS'83 [ACM83b], pages 76–89. ISBN 0-89791-097-4. LCCN QA76.9.D3 A15 1983. US$25.00.

Burkhard:1983:PRI

[Bur83c] Walter A. Burkhard. Performance results for interpolation-based index maintenance. In *Proceedings of the 17th Annual Conference on Information Sciences and Systems.*, pages 484–489. Johns Hop-

kins Univ, Baltimore, Md, USA, 1983.

Burkowski:1984:CHH

[Bur84] F. J. Burkowski. Correction to "A Hardware Hashing Scheme in the Design of a Multiterm String Comparator". *IEEE Transactions on Computers*, C-33 (4):375, April 1984. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1676447`. See [Bur82].

Burk:1992:HGP

[Bur92] Ron L. Burk. Hashing: From good to perfect. *C Users Journal*, 10(2):41–??, February 1992. ISSN 0898-9788.

Burkhard:2005:DHP

[Bur05] Walter A. Burkhard. Double hashing with passbits. *Information Processing Letters*, 96(5):162–166, December 16, 2005. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Burr:2006:CHS

[Bur06] William E. Burr. Cryptographic hash standards: Where do we go from here? *IEEE Security & Privacy*, 4 (2):88–91, March/April 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Burr:2008:NHC

[Bur08] William E. Burr. A new hash competition. *IEEE Security & Privacy*, 6(3):60–62, May/June 2008. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Buttner:1986:UDM

[Büt86] Wolfram Büttner. Unification in datastructure multisets. *Journal of Automated Reasoning*, 2(1):75–88, March 1986. CODEN JAREEW. ISSN 0168-7433 (print), 1573-0670 (electronic). URL `http://link.springer.com/article/10.1007/BF00246024`. Discusses generalization of extendible hashing to handle partial match retrieval efficiently.

Butin:2017:HBS

[But17] Denis Butin. Hash-based signatures: State of play. *IEEE Security & Privacy*, 15 (4):37–43, July/August 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `https://www.computer.org/csdl/mags/sp/2017/04/msp2017040037-abs.html`.

Belkin:1989:SPT

[BV89] Nicholas J. Belkin and C. J. Van Rijsbergen, editors. *SIGIR '89: Proceedings of the Twelfth Annual International*

ACM SIGIR Conference on Research and Development in Information Retrieval: Cambridge, Massachusetts, June 25–28, 1989, Information Access Methods. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-321-3. LCCN Z699.A1 I571 1989.

Barreto:2012:HCS

[BVF12] João Barreto, Luís Veiga, and Paulo Ferreira. Hash challenges: Stretching the limits of compare-by-hash in distributed data deduplication. *Information Processing Letters*, 112(10): 380–385, May 31, 2012. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019012000385`.

Bazrafshan:2013:IBS

[BvT13] Marjan Bazrafshan and Tran van Trung. Improved bounds for separating hash families. *Designs, Codes, and Cryptography*, 69(3):369–382, December 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9673-7`.

Breen:1989:HFP

[BW89] Edmond J. Breen and Keith L. Williams. Hash function performance on different biological databases. *Computer Methods and Programs in Biomedicine*, 28(2): 87–91, February 1989. CODEN CMPBEK. ISSN 0169-2607 (print), 1872-7565 (electronic).

Bruynooghe:1992:PLI

[BW92] Maurice Bruynooghe and Martin Wirsing, editors. *Programming language implementation and logic programming: 4th International Symposium, PLILP '92, Leuven, Belgium, August 26–28, 1992: proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992. ISBN 0-387-55844-6 (New York), 3-540-55844-6 (Berlin). LCCN QA76.7 .I5773 1992.

Blackburn:1998:OLP

[BW98] S. R. Blackburn and P. R. Wild. Optimal linear perfect hash families. *Journal of Combinatorial Theory (Series A)*, 83(2):233–250, August 1998. CODEN JCBTA7. ISSN 0097-3165.

Baeza-Yates:1989:MSF

[BY89] Ricardo A. Baeza-Yates. Modeling splits in file structures. *Acta Informatica*, 26 (4):349–362, February 1989. CODEN AINFA2. ISSN 0001-5903 (print), 1432-0525 (electronic).

Baeza-Yates:1998:ALH

[BYSP98] Ricardo A. Baeza-Yates and Héctor Soza-Pollman. Anal-

ysis of linear hashing revisited. *Nordic Journal of Computing*, 5(1):70–85, Spring 1998. CODEN NJCOFR. ISSN 1236-6064. URL `http://www.cs.helsinki.fi/njc/References/baeza-yatess1998:70.html`.

Barnes:2015:PEP

[BZL+15] Connelly Barnes, Fang-Lue Zhang, Liming Lou, Xian Wu, and Shi-Min Hu. PatchTable: efficient patch queries for large datasets and applications. *ACM Transactions on Graphics*, 34(4): 97:1–97:??, August 2015. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Bao:2012:WBS

[BZZ12] Tao Bao, Yunhui Zheng, and Xiangyu Zhang. White box sampling in uncertain data processing enabled by program analysis. *SIGPLAN Notices*, 47(10):897–914, October 2012. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Czumaj:2000:CRH

[CadHS00] Artur Czumaj, Friedhelm Meyer auf der Heide, and Volker Stemann. Contention resolution in hashing based shared memory simulations. *SIAM Journal on Computing*, 29 (5):1703–1739, October 2000. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/29564`.

Chen:2007:IHJ

[CAGM07] Shimin Chen, Anastassia Ailamaki, Phillip B. Gibbons, and Todd C. Mowry. Improving hash join performance through prefetching. *ACM Transactions on Database Systems*, 32 (3):17:1–17:??, August 2007. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Cain:1984:MAD

[Cai84] Peter Cain. Mixing analogue and digital circuitry in a signal generator. *IEE Colloquium (Digest)*, 1984/1:4.1–4.4, 1984. CODEN DCILDN.

Canetti:1997:TRR

[Can97] Ran Canetti. Towards realizing random oracles: Hash functions that hide all partial information. *Lecture Notes in CS*, 1294:455–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940455.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1294/12940455.pdf`.

Coelkesen:1994:MCV

[CBA94] R. Coelkesen, K. Balasubramanian, and Z. G. Altun. A microprocessor-controlled versatile 3D motion control system incorporating a dynamic hash function command interpreter. *Laboratory microcomputer*, 13(1):3–??, 1994. CODEN LMICDI. ISSN 0262-2955.

Challal:2005:HHC

[CBB05] Yacine Challal, Abdelmadjid Bouabdallah, and Hatem Bettahar. H_2A: Hybrid hash-chaining scheme for adaptive multicast source authentication of media-streaming. *Computers and Security*, 24(1):57–68, February 2005. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404804001816`.

Cercone:1983:SIS

[CBK83] Nick Cercone, John Boates, and Max Krause. A semi-interactive system for finding perfect hash functions. Technical report CMPT TR 83-4, Simon Fraser University, Burnaby, BC, Canada, 1983. ?? pp. (email `library@cs.sfu.ca`).

Cercone:1985:ISF

[CBK85] Nick Cercone, John Boates, and Max Krause. An interactive system for finding perfect hash functions. *IEEE Software*, 2(6):38–53, November 1985. CODEN IESOEG. ISSN 0740-7459 (print), 0740-7459 (electronic).

Chang:1987:PAG

[CC87] C. C. Chang and C. Y. Chen. Performance analysis of the generalised disc modulo allocation method for multiple key hashing files on multi-disc systems. *The Computer Journal*, 30(6):535–540, December 1987. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Chan:1988:OMP

[CC88a] M. Y. Chan and W. L. Chung. Optimal multidisk partial match file designs. *Information Processing Letters*, 28(3):149–155, July 4, 1988. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chang:1988:OMP

[CC88b] C. C. Chang and C. H. Chang. An ordered minimal perfect hashing scheme with single parameter. *Information Processing Letters*, 27(2):79–83, February 1988. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chang:1991:NAA

[CC91] C. C. Chang and C. Y. Chen. A note on allocating k-ary multiple key hashing files among multiple disks. *Information Sciences*, 55(1 / 3): 69–??, June 1, 1991. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Coburn:2012:NHM

[CCA+12] Joel Coburn, Adrian M. Caulfield, Ameen Akel, Laura M. Grupp, Rajesh K. Gupta, Ranjit Jhala, and Steven Swanson. NV-Heaps: making persistent objects fast and safe with next-generation, non-volatile memories. *SIGPLAN Notices*, 47(4):105–118, April 2012. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

CCCG:1989:CCC

[CCC89] *Canadian Conference on Computational Geometry (1st: 1989: McGill University, Montréal)*. North-Holland, Amsterdam, The Netherlands, 1989. ISBN ???? LCCN ????

Cai:2004:PPR

[CCF04] Min Cai, Ann Chervenak, and Martin Frank. A peer-to-peer replica location service based on a distributed hash table. In ACM [ACM04], page 56. ISBN 0-7695-2153-3. LCCN ????

Chang:2009:HTF

[CCH09] Ye-In Chang, Jiun-Rung Chen, and Min-Tze Hsu. A hash trie filter approach to approximate string matching for genomic databases. *Lecture Notes in CS*, 5579: 816–825, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-02568-6_83`.

Cho:2008:DNX

[CCHK08] Sung-Jin Cho, Un-Sook Choi, Yoon-Hee Hwang, and Han-Doo Kim. Design of new XOR-based hash functions for cache memories. *Computers and Mathematics with Applications*, 55 (9):2005–2011, May 2008. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122107006682`.

Chang:1991:DMI

[CCJ91] C. C. Chang, C. Y. Chen, and J. K. Jan. On the design of a machine-independent perfect hashing scheme. *The Computer Journal*, 34(5): 469–474, October 1991. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.`

org/content/34/5/469.full.pdf+html; http://www3.oup.co.uk/computer_journal/hdb/Volume_34/Issue_05/tiff/469.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_34/Issue_05/tiff/470.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_34/Issue_05/tiff/471.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_34/Issue_05/tiff/472.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_34/Issue_05/tiff/473.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_34/Issue_05/tiff/474.tif.

Chen:1991:DMK

[CCL91] C. Y. Chen, C. C. Chang, and R. C. T. Lee. On the design of multiple key hashing files for concurrent orthogonal range retrieval between two disks. *Information system*, 16(6):613–626, 1991. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Chen:2017:FMT

[CCW+17] Haibo Chen, Rong Chen, Xingda Wei, Jiaxin Shi, Yanzhe Chen, Zhaoguo Wang, Binyu Zang, and Haibing Guan. Fast in-memory transaction processing using RDMA and HTM. *ACM Transactions on Computer Systems*, 35(1): 3:1–3:??, July 2017. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Chen:1991:HNT

[CCY91] Tung-Shou Chen, Arbee L. P. Chen, and Wei-Pang Yang. Hash-semijoin: a new technique for minimizing distributed query time. In *Proceedings of the Third Workshop on Future Trends of Distributed Computing Systems, Taipei, Taiwan, April 14–16, 1991*, pages 325–330 (of xiii + 426). IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1991. ISBN 0-8186-2755-7. LCCN QA76.9.D5 I335 1992.

Chang:1984:CHC

[CD84a] S. K. Chang and J. C. Dorng. Concatenated hash code selection. *International Journal of Computer and Information Sciences*, 13(5):395–412, October 1984. CODEN IJCIAH. ISSN 0091-7036.

Cleary:1984:FCR

[CD84b] John G. Cleary and John J. Darragh. A fast compact representation of trees using hash tables. Technical Report 84/162/20, University of Calgary, September 1984. ?? pp. (email parin@cpsc.ucalgary.ca).

Colbourn:2019:DHF

[CDH19] Charles J. Colbourn, Ryan E. Dougherty, and Daniel Horsley. Distributing hash families with few rows. *Theoret. Comput. Sci.*, 800(??): 31–41, December 31, 2019. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397519306437`.

Cheiney:1989:PTC

[CdM89] J.-P. Cheiney and C. de Maindreville. A parallel transitive closure algorithm using hash-based clustering. In Boral and Faudemay [BF89], page 301. ISBN 0-387-51324-8. LCCN QA76.9.D3 D3576 1989.

Cheiney:1990:PST

[CdM90] J. P. Cheiney and C. de Maindreville. A parallel strategy for transitive closure using double hash-based clustering. In McLeod et al. [MSDS90], page 347. ISBN 1-55860-149-X. LCCN ???

Coron:2005:MDR

[CDMP05] Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, and Prashant Puniya. Merkle–Damgård revisited: How to construct a hash function. In Shoup [Sho05], pages 430–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621`.

Castryck:2020:HFS

[CDS20] Wouter Castryck, Thomas Decru, and Benjamin Smith. Hash functions from superspecial genus-2 curves using Richelot isogenies. *Journal of Mathematical Cryptology*, 14 (1):268–292, August 7, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0021/html`.

Cui:2019:STA

[CDW+19] Wanqiu Cui, Junping Du, Dawei Wang, Xunpu Yuan, Feifei Kou, Liyan Zhou, and Nan Zhou. Short text analysis based on dual semantic extension and deep hashing in microblog. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 10 (4):38:1–38:??, August 2019. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3326166`.

Coffman:1970:FSU

[CE70] E. G. Coffman, Jr. and J. Eve. File structures using

hashing functions. *Communications of the Association for Computing Machinery*, 13 (7):427–432, 436, July 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Camurati:1995:CHD

[CE95] P. E. Camurati and H. Eveking, editors. *Correct hardware design and verification methods: Advanced research working conference on correct hardware design methodologies — October 1995, Frankfurt am Main, Germany*, number 987 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. ISBN 3-540-60385-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7874.75 .A39 1995.

Celis:1986:RHHa

[Cel86] Pedro Celis. *Robin Hood Hashing*. PhD thesis, Department of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, 1986. ?? pp. See also [CLM86].

Cercone:1981:PHFa

[Cer81] N. Cercone. Perfect hash function search with application to natural language systems. Technical report TR81-6, Simon Fraser University, Burnaby, BC, Canada, 1981.

Cercone:1983:CL

[Cer83] N. Cercone. *Computational Linguistics*. International Series in Modern Applied Mathematics and Computer Science, vol. 5. Pergamon Press, Oxford, UK, 1983. ISBN 0-08-030253-X. xi + 245 pp. LCCN P98 .C612 1983. US$37.50.

Cercone:1985:AAA

[Cer85] N. Cercone. The Automated Academic Advisor, LCCR working paper #2. an interactive system for finding perfect hash functions. Technical report LCCR TR85-3, Simon Fraser University, Burnaby, BC, Canada, 1985.

Cercone:1987:FAP

[Cer87] Nick Cercone. Finding and applying perfect hash functions. *Applied Mathematics Letters*, 0(1):21–24, 1987. CODEN AMLEEL. ISSN 0893-9659 (print), 1873-5452 (electronic).

Cercone:1988:FAP

[Cer88] Nick Cercone. Finding and applying perfect hash functions. *Applied Mathematics Letters*, 1(1):25–28, 1988. CODEN AMLEEL. ISSN 0893-9659 (print), 1873-5452 (electronic).

Christodoulakis:1989:FOA

[CF89a] S. Christodoulakis and D. A. Ford. File organizations and

access methods for CLV optical discs. In Belkin and Van Rijsbergen [BV89], page 152. ISBN 0-89791-321-3. LCCN Z699.A1 I571 1989.

Christodoulakis:1989:RPV

[CF89b] Stavros Christodoulakis and Daniel Alexander Ford. Retrieval performance versus disc space utilization on WORM optical discs. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 18(2): 306–314, June 1989. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Celis:1992:AHL

[CF92] Pedro Celis and John Franco. The analysis of hashing with lazy deletions. *Information Sciences*, 62(1 / 2):13–26, July 1, 1992. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Catalano:2018:HSS

[CFN18] Dario Catalano, Dario Fiore, and Luca Nizzardo. Homomorphic signatures with sublinear public keys via asymmetric programmable hash functions. *Designs, Codes, and Cryptography*, 86(10): 2197–2246, October 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0444-3`.

Cantone:2019:LES

[CFP19] Domenico Cantone, Simone Faro, and Arianna Pavone. Linear and efficient string matching algorithms based on weak factor recognition. *ACM Journal of Experimental Algorithmics*, 24(1):1.8:1–1.8:??, October 2019. CODEN ???? ISSN 1084-6654. URL `https://dl.acm.org/ft_gateway.cfm?id=3301295`.

Cooperman:1994:CPR

[CFYT94] Gene Cooperman, Larry Finkelstein, Bryant York, and Michael Tselman. Constructing permutation representations for large matrix groups. In ACM [ACM94b], pages 134–138. ISBN 0-89791-638-7. LCCN QA76.95.I59 1994. URL `http://www.acm.org:80/pubs/citations/proceedings/issac/190347/p134-cooperman/`.

Cowan:1979:HKR

[CG79] Richard M. Cowan and Martin L. Griss. Hashing – the key to rapid pattern matching. In Ng [Ng79], pages 266–278. ISBN 0-387-09519-5. LCCN QA155.7.E4 I57 1979.

Cotter:1992:CTK

[CG92] N. E. Cotter and T. J. Guillerm. The CMAC

and a theorem of Kolmogorov. *Neural Networks*, 5 (??):221–228, 1992. CODEN NNETEB. ISSN 0893-6080.

Chen:2020:PPM

[CGLC20] T. Chen, X. Gao, T. Liao, and G. Chen. Pache: a packet management scheme of cache in data center networks. *IEEE Transactions on Parallel and Distributed Systems*, 31(2):253–265, February 2020. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Chu:1986:VLD

[CGO86] Wesley Chu, Georges Gardarin, and Setsuo Ohsuga, editors. *Very Large Data Bases: Proceedings Twelfth International Conference on Very Large Data Bases, Kyoto, Japan, August 15–18, 1986*. Morgan Kaufmann Publishers, San Francisco, CA, 1986. ISBN 0-934613-18-4. LCCN QA76.9.D3 I559 1986.

Cousin:1994:PIS

[CH94] B. Cousin and J. Helary. Performance improvement of state space exploration by regular and differential hashing functions. *Lecture Notes in CS*, 818:364–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cormode:2009:FFI

[CH09] Graham Cormode and Marios Hadjieleftheriou. Finding the frequent items in streams of data. *Communications of the Association for Computing Machinery*, 52(10):97–105, October 2009. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Ceglarek:2012:FPD

[CH12] Dariusz Ceglarek and Konstanty Haniewicz. Fast plagiarism detection by sentence hashing. *Lecture Notes in CS*, 7268:30–37, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-29350-4_4/`.

Chang:1984:OIR

[Cha84a] C. C. Chang. Optimal information retrieval when queries are not random. *Information Sciences*, 34 (3):199–223, 1984. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic). Discusses the Multiple Key Hashing method of Rothnie and Lozano [RL74].

Chang:1984:OMP

[Cha84b] C. C. Chang. An ordered minimal perfect hashing scheme based upon Euler's theorem. *Information Sciences*, 32(3):165–172, June

1984. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Chang:1984:SOM

[Cha84c] C. C. Chang. The study of an ordered minimal perfect hashing scheme. *Communications of the Association for Computing Machinery*, 27 (4):384–387, April 1984. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). The English translation of Ref. 6 of this paper appears in [Hua82]; that book contains the fundamental prime number functions needed for the ordered minimal perfect hash functions described here.

Chang:1985:SLO

[Cha85] C. C. Chang. Study of a letter oriented minimal perfect hashing scheme. In *Proceedings — Foundations of Data Organization.*, pages 61–65. Organizing Committee of the Int Conference on Foundations of Data Organization, Japan, 1985. Kyoto Sangyo Univ. Computer Science Inst, Kyoto, Jpn.

Chang:1986:LOR

[Cha86a] C. C. Chang. Letter-oriented reciprocal hashing scheme. *Information Sciences*, 38(3): 243–255, June 1986. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Chang:1986:SCO

[Cha86b] C. C. Chang. A scheme for constructing ordered minimal perfect hashing functions. *Information Sciences*, 39(2):187–195, September 1986. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Chang:1988:APC

[Cha88] C. C. Chang. Application of principal component analysis to multi-disk concurrent accessing. *BIT (Copenhagen)*, 28(2):205–214, 1988. CODEN NBITAB.

Chapman:1991:QSS

[Cha91] Rob Chapman. QuikFind string search. *Forth Dimensions*, 13(4):21–??, November 1, 1991. CODEN FODMD5. ISSN 0884-0822.

Chaudhuri:1994:TBO

[Cha94] Shiva Chaudhuri. Tight bounds on oblivious chaining. *SIAM Journal on Computing*, 23(6):1253–1265, December 1994. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/23027`.

Chang:2012:HCM

[Cha12] Chao-Tsun Chang. Hash caching mechanism in source-based routing for wireless ad hoc networks. *Journal of Network and Com-*

puter Applications, 35(1): 447–458, January 2012. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804511001858`.

Chen:1984:DACa

[Che84a] Wen-Chin Chen. *The Design and Analysis of Coalesced Hashing*. PhD thesis, Department of Computer Science, Brown University, Providence, RI, USA, November 1984. ?? pp. See also [Che84b].

Chen:1984:DACb

[Che84b] Wen-Chin Chen. The design and analysis of coalesced hashing. Technical Report CS-84-22, Department of Computer Science, Brown University, Providence, RI, USA, November 1984. ?? pp. This is the author's Ph.D. thesis, [Che84a].

Chin:1991:LPH

[Chi91] A. Chin. Locality-preserving hash functions for general purpose parallel computation. Technical Report PRG-TR-9-91, Programming Research Group, Oxford University, 1991. ?? pp.

Chin:1993:LPH

[Chi93] Andrew Chin. Locality-preserving hashing. In Anonymous [Ano93d], pages 87–98. ISBN ?? LCCN ?? I have been unable to locate this reference in several major libraries, including Dartmoth's, sigh. . . .

Chin:1994:LPHb

[Chi94] A. Chin. Locality-preserving hash functions for general purpose parallel computation. *Algorithmica*, 12(2–3):170–181, 1994. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Cormack:1985:PPH

[CHK85] G. V. Cormack, R. N. S. Horspool, and M. Kaiserwerth. Practical perfect hashing. *The Computer Journal*, 28(1):54–58, February 1985. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Correa:2006:LTI

[CHK06] José R. Correa, Alejandro Hevia, and Marcos Kiwi, editors. *LATIN 2006: Theoretical Informatics: 7th Latin American Symposium, Valdivia, Chile, March 20–24, 2006. Proceedings*, volume 3887 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. CODEN LNCSD9. ISBN 3-540-32755-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL

http://www.springerlink.com/content/978-3-540-32755-4/; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3887.

Camacho:2008:SAC

[CHKO08] Philippe Camacho, Alejandro Hevia, Marcos Kiwi, and Roberto Opazo. Strong accumulators from collision-resistant hashing. *Lecture Notes in CS*, 5222: 471–486, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-85886-7_32.

Camacho:2012:SAC

[CHKO12] Philippe Camacho, Alejandro Hevia, Marcos Kiwi, and Roberto Opazo. Strong accumulators from collision-resistant hashing. *International Journal of Information Security*, 11(5):349–363, October 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-012-0169-2.

Chen:2007:TPB

[CHL07] Hsiang-Yang Chen, Ting-Wei Hou, and Chun-Liang Lin. Tamper-proofing basis path by using oblivious hashing on Java. *SIGPLAN Notices*, 42(2):9–16, February 2007. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Czech:1992:OAGa

[CHM92a] Zbigniew J. Czech, George Havas, and Bohdan S. Majewski. An optimal algorithm for generating minimal perfect hash functions. Technical Report 92-24, Center for Discrete Mathematics and Theoretical Computer Science (DIMACS) at Rutgers University, New Jersey, 1992. ?? pp.

Czech:1992:OAGb

[CHM92b] Zbigniew J. Czech, George Havas, and Bohdan S. Majewski. An optimal algorithm for generating minimal perfect hash functions. *Information Processing Letters*, 43 (5):257–264, October 5, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Czech:1997:PH

[CHM97] Z. J. Czech, G. Havas, and B. S. Majewski. Perfect hashing. *Theoret. Comput. Sci.*, 182(1-2):1–43, August 15, 1997. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Choudhury:2021:HLS

[Cho21] Hiten Choudhury. HashXor: a lightweight scheme for iden-

tity privacy of IoT devices in 5G mobile network. *Computer Networks (Amsterdam, Netherlands: 1999)*, 186(??): Article 107753, February 26, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128620313335`.

Christodoulakis:1984:ICA

[Chr84] S. Christodoulakis. Implications of certain assumptions in data base performance evaluation. *ACM Transactions on Database Systems*, 9(2):??, June 1984. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). Also published in/as: rcvd 1983.

Chen:2018:CHT

[CHS+18] Zhiwen Chen, Xin He, Jianhua Sun, Hao Chen, and Ligang He. Concurrent hash tables on multicore machines: Comparison, evaluation and implications. *Future Generation Computer Systems*, 82(??):127–141, May 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X17317715`.

Chen:2018:YCE

[CHSC18] Zhiwen Chen, Xin He, Jianhua Sun, and Hao Chen. Have your cake and eat it (too): a concurrent hash table with hardware transactions. *International Journal of Parallel Programming*, 46(4):699–709, August 2018. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic).

Chung:1990:BCW

[Chu90] S. Chung. Block code words for partial match retrieval in very large databases. Technical Report WSU-CS-90-10, Washington State University, 1990. ?? pp.

Chung:1991:IEH

[Chu91] Soon M. Chung. Indexed extendible hashing for databases. Technical Report WSU-CS-91-02, Washington State University, 1991. ?? pp.

Chung:1992:IEH

[Chu92] Soon M. Chung. Indexed extendible hashing. *Information Processing Letters*, 44 (1):1–6, November 9, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chen:1993:AHF

[CHY93] M.-S. Chen, H.-I. Hsiao, and P. S. Yu. Applying hash filters to improving the execution of bushy trees. In Agrawal et al. [ABB93], pages 505–516. ISBN 1-55860-152-X. ISSN 0730-9317. LCCN QA76.9.D3 I61 1993.

Chen:1997:AHF

[CHY97] Ming-Syan Chen, Hui-I Hsiao, and Philip S. Yu. On applying hash filters to improving the execution of multi-join queries. *VLDB Journal: Very Large Data Bases*, 6(2):121–131, August 1997. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic). URL `http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/c/Chen:Ming=Syan.html`; `http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/h/Hsiao:Hui=I.html`; `http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/y/Yu:Philip_S=.html`; `http://link.springer.de/link/service/journals/00778/bibs/7006002/70060121.htm`; `http://link.springer.de/link/service/journals/00778/papers/7006002/70060121.pdf`; `http://link.springer.de/link/service/journals/00778/papers/7006002/70060121.ps.gz`. Electronic edition.

Cichelli:1980:CMP

[Cic80a] R. J. Cichelli. On Cichelli's minimal perfect hash functions method. *Communications of the Association for Computing Machinery*, 23(12):728–729, December 1980. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). This is the author's response to the comments in [JO80] about [Cic80b]. See also [Sag85a].

Cichelli:1980:MPH

[Cic80b] Richard J. Cichelli. Minimal perfect hash functions made simple. *Communications of the Association for Computing Machinery*, 23(1):17–19, January 1980. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See remarks in [JO80], and the author's response in [Cic80a]. A simple improvement giving dramatic speedups is described in [Tro95].

Caires:2005:ALP

[CIM+05] Luís Caires, Guiseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors. *Automata, languages and programming: 32nd international colloquium, ICALP 2005, Lisbon, Portugal, July 11–15, 2005: proceedings*, volume 3580 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. ISBN 3-540-27580-0. LCCN ???? EUR 130.54. URL `http://www.gbv.de/dms/bowker/toc/9783540275800.pdf`; `http://www.springerlink.com/content/978-3-540-27580-0/`; `http://www.`

zentralblatt-math.org/zmath/en/search/?an=1078.68001.

Cipra:1993:ETS

[Cip93] Barry Cipra. Electronic time-stamping: The notary public goes digital: All the hash that's fit to print. *Science*, 261(5118): 162–163, July 9, 1993. CODEN SCIEAS. ISSN 0036-8075 (print), 1095-9203 (electronic).

Colomb:1986:CIS

[CJ86] R. M. Colomb and Jayasooriah. A clause indexing system for PROLOG based on superimposed coding. *Australian Computer Journal*, 18(1):18–25, 1986. CODEN ACMJB2. ISSN 0004-8917. Compares clause indexing with hashing.

Cormode:2019:STA

[CJ19] Graham Cormode and Hossein Jowhari. L_p samplers and their applications: a survey. *ACM Computing Surveys*, 52(1):16:1–16:??, February 2019. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3297715.

Choi:2009:DSC

[CJC+09] Myung Geol Choi, Eunjung Ju, Jung-Woo Chang, Jehee Lee, and Young J. Kim. Data structure and collision detection: Linkless octree using multi-level perfect hashing. *Computer Graphics Forum*, 28(7):1773–1780, October 2009. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Choi:2019:RDR

[CJKK19] Kyu Hyun Choi, Jaeyung Jun, Minseong Kim, and Seon Wook Kim. Reducing DRAM refresh rate using retention time aware universal hashing redundancy repair. *ACM Transactions on Design Automation of Electronic Systems.*, 24(5):53:1–53:31, October 2019. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3339851.

Chang:2019:CTM

[CJMS19] Donghoon Chang, Arpan Jati, Sweta Mishra, and Somitra Kumar Sanadhya. Cryptanalytic time-memory trade-off for password hashing schemes. *International Journal of Information Security*, 18(2):163–180, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0405-5.

Cheng:2020:RUC

[CJN20] Miaomiao Cheng, Liping Jing, and Michael K. Ng. Robust unsupervised cross-modal hashing for multimedia retrieval. *ACM Transactions on Information Systems*, 38(3):30:1–30:25, June 2020. CODEN ATISET. ISSN 1046-8188. URL `https://dl.acm.org/doi/abs/10.1145/3389547`.

Cho:2012:CBF

[CJP12] Jung-Sik Cho, Young-Sik Jeong, and Sang Oh Park. Consideration on the brute-force attack cost and retrieval cost: a hash-based radio-frequency identification (RFID) Tag Mutual Authentication Protocol. *Computers and Mathematics with Applications*, 69(1):58–65, January 2012. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122112001393`. See cryptanalysis [SPLHCB14].

Cho:2015:CBF

[CJP15] Jung-Sik Cho, Young-Sik Jeong, and Sang Oh Park. Consideration on the brute-force attack cost and retrieval cost: a hash-based radio-frequency identification (RFID) tag mutual authentication protocol. *Computers and Mathematics with Applications*, 69(1):58–65, January 2015. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122112001393`.

Cercone:1989:IAP

[CK89] N. Cercone and M. Krause. An informal analysis of perfect hash function search. *Applied Mathematics Letters*, 2(3):287–291, 1989. CODEN AMLEEL. ISSN 0893-9659 (print), 1873-5452 (electronic).

Chu:1994:ASH

[CK94] Jiang-Hsing Chu and Gary D. Knott. An analysis of spiral hashing. *The Computer Journal*, 37(8):715–719, ???? 1994. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/Volume_37/Issue_08/Vol37_08.body.html#AbstractChu`.

Chase:2012:NHS

[CK12] Melissa Chase and Markulf Kohlweiss. A new hash-and-sign approach and structure-preserving signatures from DLIN. *Lecture Notes in CS*, 7485:131–148, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32928-9_8/`.

Chierichetti:2015:LPF

[CK15] Flavio Chierichetti and Ravi Kumar. LSH-preserving functions and their applications. *Journal of the Association for Computing Machinery*, 62(5):33:1–33:??, November 2015. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Cercone:1981:LDU

[CKB81] Nick Cercone, Max Krause, and John Boates. Lexicon design using perfect hash functions. In Borman [Bor81], pages 69–78. CODEN SGBLDB. ISBN 0-89791-056-7 (pt. 1), 0-89791-064-8 (pt. 2). ISSN 0163-5794. LCCN H61 .S53 v.12 no.4-v.13 no.1-3.

Cercone:1983:MAMa

[CKB83a] N. Cercone, M. Krause, and J. Boates. Minimal and almost minimal perfect hash function search with application to natural language lexicon design. In *Computational Linguistics* [Cer83], pages 215–232. ISBN 0-08-030253-X. LCCN P98 .C612 1983. US$37.50.

Cercone:1983:MAMb

[CKB83b] Nick Cercone, Max Krause, and John Boates. Minimal and almost minimal perfect hash function search with application to natural language lexicon design. *Computers and Mathematics with Applications*, 9(1): 215–231, ???? 1983. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0898122183900160`.

Cercone:1985:ESL

[CKB85] N. Cercone, M. Krause, and J. Boates. Efficient search of large lexicons using perfect hash functions. In *1983 International Conference on Data Bases in the Humanities Social Sciences, New Brunswick, NJ*, pages 359–373. Paradigm Press, ????, 1985.

Choi:2009:SPC

[CKKK09] Lynn Choi, Hyogon Kim, Sunil Kim, and Moon Hae Kim. Scalable packet classification through rulebase partitioning using the maximum entropy hashing. *IEEE/ACM Transactions on Networking*, 17(6):1926–1935, December 2009. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Claussen:2000:EES

[CKKW00] J. Claussen, A. Kemper, D. Kossmann, and C. Wiesner. Exploiting early sorting and early partitioning for decision support query processing. *VLDB Journal: Very Large Data Bases*, 9

(3):190–213, December 2000. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Chierichetti:2014:CLF

[CKM14] Flavio Chierichetti, Ravi Kumar, and Mohammad Mahdian. The complexity of LSH feasibility. *Theoret. Comput. Sci.*, 530(??): 89–101, April 17, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397514001467`.

Cygan:2018:FHC

[CKN18] Marek Cygan, Stefan Kratsch, and Jesper Nederlof. Fast Hamiltonicity checking via bases of perfect matchings. *Journal of the Association for Computing Machinery*, 65 (3):12:1–12:??, March 2018. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Chierichetti:2019:DLS

[CKPT19] Flavio Chierichetti, Ravi Kumar, Alessandro Panconesi, and Erisa Terolli. On the distortion of locality sensitive hashing. *SIAM Journal on Computing*, 48(2): 350–372, ???? 2019. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Chang:1993:RCO

[CKW93] Chin-Chen Chang, Huey-Cheue Kowng, and Tzong-Chen Wu. A refinement of a compression-oriented addressing scheme. *BIT (Nordisk tidskrift for informationsbehandling)*, 33(4): 529–535, December 1993. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.mai.liu.se/BIT/contents/bit33.html`; `http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=33&issue=4&spage=529`.

Coetser:2009:REH

[CKW09] Wikus Coetser, Derrick G. Kourie, and Bruce W. Watson. On regular expression hashing to reduce FA size. *International Journal of Foundations of Computer Science*, 20(6):1069–1086, December 2009. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Cook:1983:STA

[CL83] R. P. Cook and T. J. LeBlanc. A symbol table abstraction to implement languages with explicit scope control. *IEEE Transactions on Software Engineering*, SE-9(1):8–12, January 1983. CODEN IESEDJ. ISSN

0098-5589 (print), 1939-3520 (electronic).

Chang:1985:PAK

[CL85] Chin-Chen Chang and Jenn Liang. Performance analysis of a k-nearest neighbor searching technique. *Chungkuo Kung Ch'eng Hsueh K'an/Journal of the Chinese Institute of Engineers*, 8(2): 157–169, April 1985. CODEN CKCKDZ.

Chang:1986:LOM

[CL86] C. C. Chang and R. C. T. Lee. A letter-oriented minimal perfect hashing scheme. *The Computer Journal*, 29 (3):277–281, June 1986. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Chang:1995:CHE

[CL95] Ye-In Chang and Chien-I Lee. Climbing hashing for expansible files. *Information Sciences*, 86(1 / 3):77–??, September 1, 1995. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Chang:2005:PHS

[CL05] Chin-Chen Chang and Chih-Yang Lin. Perfect hashing schemes for mining association rules. *The Computer Journal*, 48(2):168–179, March 2005. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_48/Issue_02/bxh074.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_48/Issue_02/pdf/bxh074.pdf`.

Colbourn:2009:LHF

[CL09a] Charles J. Colbourn and Alan C. H. Ling. Linear hash families and forbidden configurations. *Designs, Codes, and Cryptography*, 52(1):25–55, July 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=52&issue=1&spage=25`.

Colbourn:2009:RCP

[CL09b] Charles J. Colbourn and Alan C. H. Ling. A recursive construction for perfect hash families. *Journal of Mathematical Cryptology*, 3(4):291–306, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Clapson:1977:IAT

[Cla77] Philip Clapson. Improving the access time for random access files. *Communications of the Association for Computing Machinery*, 20(3):127–135, March 1977. CODEN CACMA2. ISSN 0001-

0782 (print), 1557-7317 (electronic).

Chang:1992:OPD

[CLC92] C. C. Chang, H. F. Lin, and C. Y. Chen. Optimality properties of the disc modulo allocation method for k-ary multiple key hashing files. *The Computer Journal*, 35 (4):390–394, August 1, 1992. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Chang:2006:PHS

[CLC06] Chin-Chen Chang, Chih-Yang Lin, and Henry Chou. Perfect hashing schemes for mining traversal patterns. *Fundamenta Informaticae*, 70(3):185–202, May 2006. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Chang:1982:SGC

[CLD82] C. C. Chang, R. C. T. Lee, and M. W. Du. Symbolic gray code as a perfect multiattribute hashing scheme for partial match queries. *IEEE Transactions on Software Engineering*, SE-8(3): 235–249, May 1982. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic).

Cleary:1984:CHT

[Cle84] John G. Cleary. Compact hash tables using bidirectional linear probing. *IEEE Transactions on Computers*, C-33(9):828–834, September 1984. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1676499`.

Charles:2009:CHF

[CLG09] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22 (1):93–113, January 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=1&spage=93`.

Click:1995:GCM

[Cli95] Cliff Click. Global code motion: global value numbering. *SIGPLAN Notices*, 30(6):246–257, June 1995. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). URL `http://www.acm.org:80/pubs/citations/proceedings/pldi/207110/p246-click/`.

Cheng:2014:SSM

[CLL+14] Jian Cheng, Cong Leng, Peng Li, Meng Wang, and Hanqing Lu. Semi-supervised multi-graph hashing for scalable similarity search. *Com-*

puter vision and image understanding: CVIU, 124(??): 12–21, July 2014. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic). URL http://www.sciencedirect.com/science/article/pii/S1077314214000794.

Celis:1985:RHH

[CLM85] Pedro Celis, Per-Åke Larson, and J. Ian Munro. Robin Hood hashing. In IEEE-FOCS'85 [IEE85a], pages 281–288. ISBN 0-8186-0644-4 (paperback), 0-8186-4644-6 (microfiche), 0-8186-8644-8 (hardcover). LCCN QA 76 S979 1985.

Celis:1986:RHHb

[CLM86] P. Celis, P. Å. Larson, and J. I. Munro. Robin Hood hashing. Technical Report CS-86-14, Department of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, April 1986. ?? pp. See also [Cel86].

Clifford:1989:AIC

[CLM89] James Clifford, Bruce Lindsay, and David Maier, editors. *Proceedings of the 1989 ACM SIGMOD International Conference on the Management of Data, Portland, Oregon*. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-317-5. LCCN QA 76.9 D3 S53 v.18 no.2 1989.

Li:2007:RNH

[cLmL07] Jun cao Li and Chun ming Li. Research on a novel hashing stream cipher. *Lecture Notes in CS*, 4456: 481–490, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-74377-4_51.

Chang:2006:ISA

[CLNY06] Donghoon Chang, Sangjin Lee, Mridul Nandi, and Moti Yung. Indifferentiable security analysis of popular hash functions with prefix-free padding. *Lecture Notes in CS*, 4284:283–298, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11935230_19.pdf.

Canetti:2013:PCC

[CLP13] Ran Canetti, Huijia Lin, and Omer Paneth. Public-coin concurrent zero-knowledge in the global hash model. *Lecture Notes in CS*, 7785: 80–99, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_5/.

Chiu:2017:AAS

[CLP17] Chih-Yi Chiu, Yu-Cyuan

Liou, and Amorntip Prayoonwong. Approximate asymmetric search for binary embedding codes. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 13 (1):3:1–3:??, January 2017. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Chen:1995:STP

[CLS95] Tzer-Shyong Chen, Feipei Lai, and Rung-Ji Shang. A simple tree pattern matching algorithm for code generator. In IEEE [IEE95], pages 162–167. ISBN 0-8186-7119-X. LCCN ???? IEEE Catalog No. 95CB35838.

Chen:2012:EDI

[CLS12] Long Chen, Banglan Liu, and Wei Song. An efficient data integrity verification method supporting multi-granular operation with commutative hash. *Lecture Notes in CS*, 7413:132–141, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32115-3_15/`.

Colbourn:2018:ACM

[CLS18] Charles J. Colbourn, Erin Lanus, and Kaushik Sarkar. Asymptotic and constructive methods for covering perfect hash families and covering arrays. *Designs, Codes, and Cryptography*, 86 (4):907–937, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0369-x`.

Chu:1998:EHB

[CLW98] K. W. Chu, S. K. Lam, and M. H. Wong. An efficient hash-based algorithm for sequence data searching. *The Computer Journal*, 41(6):402–415, ???? 1998. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/Volume_41/Issue_06/Vol41_06.body.html#AbstractChu`.

Chen:1992:USR

[CLYY92] M-S. Chen, M. L. Lo, P. S. Yu, and H. C. Young. Using segmented right-deep trees for the execution of pipelined hash joins. In Yuan [Yua92], page 15. ISBN 1-55860-151-1. LCCN QA76.9.D3 I61 1992.

Chen:1995:ASR

[CLYY95] Ming-Syan Chen, Mingling Lo, Philip S. Yu, and Honesty C. Young. Applying segmented right-deep trees to pipelining multiple hash joins. *IEEE Transactions on Knowledge and Data Engineering*, 7(4):656–??, August 1, 1995. CODEN ITKEEH. ISSN 1041-4347.

Czech:1993:LTA

[CM93] Zbigniew J. Czech and Bohdan S. Majewski. A linear time algorithm for finding minimal perfect hash functions. *The Computer Journal*, 36(6):579–587, December 1993. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/36/6/579.full.pdf+html`; `http://www3.oup.co.uk/computer_journal/Volume_36/Issue_06/Vol36_06.body.html#AbstractCzech`.

Christophi:2001:DSR

[CM01] C. A. Christophi and H. M. Mahmoud. Distribution of the size of random hash trees, pebbled hash trees and N-trees. *Statistics & Probability Letters*, 53(3):277–282, June 15, 2001. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic).

Chen:2013:LSM

[CML+13] Xiangyu Chen, Yadong Mu, Hairong Liu, Shuicheng Yan, Yong Rui, and Tat-Seng Chua. Large-scale multi-label propagation based on efficient sparse graph construction. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 10(1):6:1–6:??, December 2013. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Contini:2007:EFA

[CMP07] Scott Contini, Krystian Matusiewicz, and Josef Pieprzyk. Extending FORK-256 attack to the full hash function. *Lecture Notes in CS*, 4861:296–305, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-77048-0_23`.

Canetti:1998:POW

[CMR98] Ran Canetti, Daniele Micciancio, and Omer Reingold. Perfectly one-way probabilistic hash functions (preliminary version). In ACM [ACM98], pages 131–140. ISBN 0-89791-962-9. LCCN QA75.5 .A14 1998. URL `http://www.acm.org/pubs/articles/proceedings/stoc/276698/p131-canetti/p131-canetti.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/276698/p131-canetti/`. ACM order number 508980.

Carter:1983:CEI

[CMW83] J. L. Carter, G. Markowsky, and M. N. Wegman. Class of easily implemented hash functions. *IBM Technical Disclosure Bulletin*, 26(2): 515–516, July 1983. CODEN IBMTAA. ISSN 0018-8689.

Cheng:2007:DHL

[CN07] James Cheng and Wilfred Ng. A development of hash-lookup trees to support querying streaming XML. *Lecture Notes in CS*, 4443: 768–780, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-71703-4_64`.

Chang:2008:IIS

[CN08] Donghoon Chang and Mridul Nandi. Improved indifferentiability security analysis of chopMD hash function. *Lecture Notes in CS*, 5086:429–443, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-71039-4_27`.

Comer:1982:GPA

[CO82a] Douglas Comer and Michael J. O'Donnell. Geometric problems with application to hashing. *SIAM Journal on Computing*, 11(2):217–226, ???? 1982. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Cook:1982:LOM

[CO82b] Curtis R. Cook and R. R. Oldehoeft. A letter oriented minimal perfect hashing function. *SIGPLAN Notices*, 17(9):18–27, September 1982. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). A simple improvement giving dramatic speedups is described in [Tro95].

Coburn:1994:ISH

[Cob94] T. K. Coburn. An introduction to the SSPIN hash function: Making more out of the multidimensional array. In IEEE [IEE94b], pages 919–925. ISBN 0-7803-1893-5, 0-7803-1894-3, 0-7803-1895-1. ISSN 0547-3578. LCCN TL 693 N37 1994. Two volumes.

Cohen:1984:MSP

[Coh84] Shimon Cohen. *Multi-Version Structures in Prolog*. Ohmsha, Ltd., 3-1 Kanda Nishiki-cho, Chiyoda-ku, Tokyo 101, Japan, 1984. ISBN 4-274-07221-5. 229–234 pp. LCCN ????

Cohen:1994:ACF

[Coh94] G. Cohen, editor. *Algebraic coding: 1st French-Israeli workshop — July 1993, Paris*, number 781 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. ISBN 3-540-57843-9. ISSN 0302-9743 (print), 1611-3349 (elec-

tronic). LCCN QA268 .A397 1994.

Cohen:1997:RHF

[Coh97] Jonathan D. Cohen. Recursive hashing functions for n-grams. *ACM Transactions on Information Systems*, 15(3): 291–320, July 1997. CODEN ATISET. ISSN 1046-8188. URL `http://www.acm.org:80/tois/abstracts/cohen.html`.

Cohen:1998:GHS

[Coh98] Jonathan D. Cohen. An n-gram hash and skip algorithm for finding large numbers of keywords in continuous text streams. *Software—Practice and Experience*, 28(15):1605–1635, December 25, 1998. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic). URL `http://www3.interscience.wiley.com/cgi-bin/abstract?ID=10050312`; `http://www3.interscience.wiley.com/cgi-bin/fulltext?ID=10050312&PLACEBO=IE.pdf`.

Coleman:1993:PTI

[Col93] Samuel S. Coleman, editor. *Proceedings: Twelfth IEEE Symposium on Mass Storage Systems: putting all that data to work, April 26–29, 1993, Monterey, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1993. ISBN 0-8186-3462-6. LCCN TK7895.M4 I5 1993.

Constantin:2017:SHF

[Con17] Lucian Constantin. The SHA1 hash function is now completely unsafe: Researchers have achieved the first practical SHA-1 collision, generating two PDF files with the same signature. *ComputerWorld*, ?? (??):??, February 23, 2017. CODEN CMPWAB. ISSN 0010-4841. URL `https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-unsafe.html`.

Coppersmith:1995:ACA

[Cop95a] D. Coppersmith, editor. *Advances in cryptology: 15th Annual international conference — August 1995, Santa Barbara, CA*, number 963 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. ISBN 3-540-60221-6. LCCN QA76.9.A25 C79 1995.

Coppersmith:1995:ACC

[Cop95b] Don Coppersmith, editor. *Advances in cryptology, CRYPTO '95: 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27–31, 1995: proceedings*, volume 963 of *Lecture Notes in*

Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. CODEN LNCSD9. ISBN 3-540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1995. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0963.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=963. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy.

Coron:2000:ESF

[Cor00] Jean-Sébastien Coron. On the exact security of full domain hash. In Bellare [Bel00], pages 229–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800229.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800229.pdf.

Coron:2002:SPP

[Cor02] Jean-Sébastien Coron. Security proof for partial-domain hash signature schemes. In Yung [Yun02], pages 613–626. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL http://link.springer.de/link/service/series/0558/bibs/2442/24420613.htm; http://link.springer.de/link/service/series/0558/papers/2442/24420613.pdf.

Chaum:1987:ACE

[CP87] David Chaum and Wyn L. Price, editors. *Advances in Cryptology–EUROCRYPT '87: Workshop on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, April 13–15, 1987: Proceedings*, volume 304 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). LCCN QA76.9.A25 E963 1987.

Chaum:1988:ACE

[CP88] David Chaum and Wyn L. Price, editors. *Advances in cryptology — EUROCRYPT '87: Workshop on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, April 13–15, 1987: proceedings*, volume 304 of *Lecture Notes*

in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. CODEN LNCSD9. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E9631 1987; QA267.A1 L43 no.304. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0304.htm`; `http://www.springerlink.com/content/978-0-387-19102-7`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=304`. Sponsored by the International Association for Cryptologic Research.

Cai:1991:MNH

[CP91a] Jiazhen Cai and Robert Paige. "Look Ma, no hashing, and no arrays neither". In ACM-POPL'91 [ACM91d], pages 143–154. ISBN 0-89791-419-8. LCCN QA76.7 .A15 1991.

Cai:1991:LMN

[CP91b] Jiazhen Cai and Robert A. Paige. Look ma, no hashing, and no arrays neither. In ACM [ACM91a], pages 143–154. ISBN ???? LCCN ???? URL `http://www.acm.org:80/pubs/citations/proceedings/plan/99583/p143-cai/`.

Camion:1991:KHF

[CP91c] P. Camion and J. Patarin. The knapsack hash function proposed at Crypto '89 can be broken. In Davies [Dav91], pages 39–53. ISBN 0-387-54620-0 (New York), 3-540-54620-0 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1991.

Cai:1995:UMD

[CP95a] Jiazhen Cai and R. Paige. Using multiset discrimination to solve language processing problems without hashing. *Theoret. Comput. Sci.*, 145(1-2):189–228, July 10, 1995. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Charnes:1995:ASH

[CP95b] C. Charnes and J. Pieprzyk. Attacking the SL2 hashing scheme. *Lecture Notes in CS*, 917:322–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Claessen:2013:SPN

[CP13] Koen Claessen and Michał H. Pałka. Splittable pseudorandom number generators using cryptographic hashing. *SIGPLAN Notices*, 48 (12):47–58, December 2013. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867

(print), 1558-1160 (electronic). Haskell '14 conference proceedings.

Chaudhuri:2008:LCF

[CPP08] Kaustuv Chaudhuri, Frank Pfenning, and Greg Price. A logical characterization of forward and backward chaining in the inverse method. *Journal of Automated Reasoning*, 40(2–3): 133–177, March 2008. CODEN JAREEW. ISSN 0168-7433 (print), 1573-0670 (electronic). URL `http://link.springer.com/article/10.1007/s10817-007-9091-0`.

Chen:2008:IRS

[CQW08] Guihai Chen, Tongqing Qiu, and Fan Wu. Insight into redundancy schemes in DHTs. *The Journal of Supercomputing*, 43(2):183–198, February 2008. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=43&issue=2&spage=183`.

Chung:1989:DSH

[CR89] Yunmo Chung and M. V. Ramakrishna. Dynamic signature hashing. In Knafl [Kna89], pages 257–262. ISBN 0-8186-1964-3. LCCN QA76.6 .C62951 1989.

Crammond:1985:CSU

[Cra85] Jim Crammond. A comparative study of unification algorithms for OR-parallel execution of logic languages. *IEEE Transactions on Computers*, C-34(1): 911–917, October 1985. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). Compares directory trees, hash windows, and variable importation.

Carreras-Riudavets:2012:MAU

[CRdPHF12] Francisco J. Carreras-Riudavets, Juan C. Rodríguez del Pino, and Zenón Hernández-Figueroa. A morphological analyzer using hash tables in main memory (MAHT) and a lexical knowledge base. *Lecture Notes in CS*, 7181:80–91, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-28604-9_7/`.

Cromwell:1998:PBD

[Cro98] Jeff Cromwell. Programmer's bookshelf: The dawning of the age of multithreading. *Dr. Dobbs Journal*, 23(9): 127, 129, September 1998. CODEN DDJOEB. ISSN 1044-789X.

Collom:2018:FMM

[CRR18] Gerald Collom, Colin Redman, and Robert W. Robey.

Fast mesh-to-mesh remaps using hash algorithms. *SIAM Journal on Scientific Computing*, 40(4):C450–C476, ???? 2018. CODEN SJOCE3. ISSN 1064-8275 (print), 1095-7197 (electronic).

Chaum:1983:ACP

[CRS83a] David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors. *Advances in Cryptology: Proceedings of CRYPTO '83 (21–24 August 1983: University of California, Santa Barbara)*. Plenum Press, New York, NY, USA, 1983. ISBN 0-306-41637-9, 1-4757-0604-9 (print), 1-4757-0602-2. LCCN QA76.9.A25 C791 1983.

Chung:1983:PSR

[CRS83b] F. R. K. Chung, A. L. Rosenberg, and Lawrence Snyder. Perfect storage representations for families of data structures. *SIAM Journal of Algebraic Discrete Methods*, 4 (4):548–565, December 1983. CODEN SJAMDU. ISSN 0196-5212 (print), 2168-345X (electronic).

Celis:2011:BBS

[CRSW11] L. E. Celis, O. Reingold, G. Segev, and U. Wieder. Balls and bins: Smaller hash families and faster evaluation. In IEEE [IEE11b], pages 599–608. ISBN 1-4577-1843-X. LCCN ????

Celis:2013:BBS

[CRSW13] L. Elisa Celis, Omer Reingold, Gil Segev, and Udi Wieder. Balls and bins: Smaller hash families and faster evaluation. *SIAM Journal on Computing*, 42 (3):1030–1050, ???? 2013. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Comer:1982:HBS

[CS82] Douglas Comer and Vincent Yun Shen. Hash-bucket search — a fast technique for searching an English spelling dictionary. *Software—Practice and Experience*, 12(7):669–682, July 1982. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Chang:1983:DOM

[CS83a] C. C. Chang and J. C. Shieh. On the design of ordered minimal perfect hashing functions and join dependencies. Was to appear in J. ACM, but did not. Where was it finally published?, 1983.

Chang:1983:PMF

[CS83b] C. C. Chang and D. H. Su. Properties of multi-attribute file systems based upon multiple key hashing functions. *Proceedings — Annual Allerton Conference on Communication, Control, and Computing*, pages 675–682, 1983.

CODEN PCCCDU. ISSN 0732-6181.

Chang:1985:FAC

[CS85a] C. C. Chang and J. C. Shieh. *Fast Algorithm for Constructing Reciprocal Hashing Functions*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1985. ISBN 0-8186-0639-8. 232–236 pp. LCCN ???? IEEE Service Cent. Piscataway, NJ, USA.

Chang:1985:DLO

[CS85b] C.-C. Chang and J.-C. Shieh. On the design of letter oriented minimal perfect hashing functions (in Chinese). *Journal of Chinese Institute of Engineers*, 8(3):285–297, July 1985. CODEN CKCKDZ. ISSN 0368-7058.

Chang:1985:DLM

[CS85c] Chin-Chen Chang and Jiann-Cherng Shieh. On the design of letter-oriented minimal perfect hashing functions. *Chung-kuo Kung Ch'eng Hsueh K'an/Journal of the Chinese Institute of Engineers*, 8(3):285–297, July 1985. CODEN CKCKDZ.

Chang:1986:DOM

[CS86] C. C. Chang and J. C. Shieh. On the design of ordered minimal perfect hashing functions. In ICDE'86 [ICD86], pages 112–115. ISBN 0-8186-0655-X (paperback), 0-8186-8655-3 (hardcover), 0-8186-4655-1 (microfiche). LCCN QA 76.9 D3 I5582 1986.

Chang:1987:PAM

[CS87] Chin-Chen Chang and Don-Hsin Su. Performance analyses of multi-attribute files based upon multiple key hashing functions and haphazard files. *Chung-kuo Kung Ch'eng Hsueh K'an/Journal of the Chinese Institute of Engineers*, 10(1):99–105, January 1987. CODEN CKCKDZ.

Cesarini:1991:DHM

[CS91] F. Cesarini and G. Soda. A dynamic hash method with signature. *ACM Transactions on Database Systems*, 16(2):309–337, June 1, 1991. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Cesarini:1993:SAH

[CS93a] F. Cesarini and G. Soda. Single access hashing with overflow separators for dynamic files. *BIT (Nordisk tidskrift for informationsbehandling)*, 33(1):15–28, 1993. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.mai.liu.se/BIT/contents/bit33.html`.

Cooper:1993:TTA

[CS93b] Robert B. Cooper and Martin K. Solomon. Teletraffic theory applied to the analysis of hash-structured files. *AEU: Archiv für Elektronik und Ubertragungstech*, 47(5 / 6):336–341, September 1, 1993. CODEN AEUTAH. ISSN 0001-1096.

Cramer:2002:UHP

[CS02] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. *Lecture Notes in CS*, 2332:45–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320045.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2332/23320045.pdf`.

Chakrabarti:2015:BPL

[CSSP15] Aniket Chakrabarti, Venu Satuluri, Atreya Srivathsan, and Srinivasan Parthasarathy. A Bayesian perspective on locality sensitive hashing with extensions for kernel methods. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 10(2):19:1–19:??, October 2015. CODEN ???? ISSN 1556-4681 (print), 1556-472X (electronic).

Cooperman:1996:NSP

[CT96] Gene Cooperman and Michael Tselman. New sequential and parallel algorithms for generating high dimension Hecke algebras using the condensation technique. In Lakshman Y.N. [Lak96], pages 155–160. ISBN 0-89791-796-0. LCCN QA 76.95 I59 1996. URL `http://www.acm.org:80/pubs/citations/proceedings/issac/236869/p155-cooperman/`.

Cormode:2010:ANG

[CT10] Graham Cormode and Marina Thottan, editors. *Algorithms for next generation networks*. Computer Communications and Networks. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 1-84882-764-4. xx + 462 pp. LCCN TK5105.5 .A39523 2010. URL `http://www.springerlink.com/content/978-1-84882-764-6/`.

Chiou:2012:IMA

[CT12] Chuang-Kai Chiou and Judy C. R. Tseng. An incremental mining algorithm for association rules based on minimal perfect hashing and pruning. *Lecture Notes in CS*, 7234:106–113, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-

tronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29426-6_14/.

IEEE:1990:FAS

[CTC90] *Fifth Annual Structure in Complexity Theory Conference Proceedings: July 8–11 1990, Universitat Politecnica de Catalunya, Barcelona, Spain*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. ISBN 0-8186-2072-2 (paper), 0-8186-6072-4 (microfiche), 0-8186-9072-0 (case). LCCN QA267.7 .S75 1990.

Chen:2011:CIK

[CTZD11] Xiaofeng Chen, Haibo Tian, Fangguo Zhang, and Yong Ding. Comments and improvements on key-exposure free Chameleon hashing based on factoring. *Lecture Notes in CS*, 6584: 415–426, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-21518-6_29.

Chen:1983:AEI

[CV83a] Wen Chin Chen and Jeffrey Scott Vitter. Analysis of early-insertion standard coalesced hashing. *SIAM Journal on Computing*, 12 (4):667–676, November 1983. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Chen:1983:NVC

[CV83b] Wen-Chin Chen and Jeffrey Scott Vitter. New variants of coalesced hashing. *Proceedings — Annual Allerton Conference on Communication, Control, and Computing*, pages 683–692, 1983. CODEN PCCCDU. ISSN 0732-6181.

Chen:1984:ANV

[CV84] Wen-Chin Chen and Jeffrey Scott Vitter. Analysis of new variants of coalesced hashing. *ACM Transactions on Database Systems*, 9 (4):616–645, December 1984. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Chen:1985:AAS

[CV85] W.-C. Chen and J. S. Vitter. Addendum to *Analysis of Some New Variants of Coalesced Hashing*. *ACM Transactions on Database Systems*, 10(1):127, March 1985. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Chen:1986:DAC

[CV86] W. C. Chen and J. S. Vitter. Deletion algorithms for coalesced hashing. *The Computer Journal*, 29(5):436–450, October 1986. CO-

DEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Castro:2005:NRG

[CV05] Julio César Hernández Castro and Pedro Isasi Viñuela. New results on the genetic cryptanalysis of TEA and reduced-round versions of XTEA. *New Generation Computing*, 23(3): 233–243, 2005. CODEN NGCOE5. ISSN 0288-3635 (print), 1882-7055 (electronic). URL `http://www.springerlink.com/content/e018uh040400kh87/`.

Chung:2008:TBH

[CV08] Kai-Min Chung and Salil Vadhan. Tight bounds for hashing block sources. *Lecture Notes in CS*, 5171: 357–370, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-85363-3_29`.

Carrea:2014:OHN

[CVR14] Laura Carrea, Alexei Vernitski, and Martin Reed. Optimized hash for network path encoding with minimized false positives. *Computer Networks (Amsterdam, Netherlands: 1999)*, 58(??):180–191, January 15, 2014. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128613003046`.

Carter:1977:UCHa

[CW77a] I. L. Carter and M. N. Wegman. Universal classes of hash functions. In Carter & Wegman [ACM77b], pages 106–112.

Carter:1977:UCHb

[CW77b] J. L. Carter and M. N. Wegman. Universal classes of hash functions. Technical report, ????, Yorktown Heights, NY, USA, 1977. ?? pp.

Carter:1979:UCH

[CW79] J. Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2): 143–154, April 1979. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic).

Chang:1991:LOP

[CW91] Chin-Chen Chang and Tzong-Chen Wu. A letter-oriented perfect hashing scheme based upon Sparse table compression. *Software—Practice and Experience*, 21(1):35–49, January 1991. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Chang:1993:HON

[CW93] C. C. Chang and T. C. Wu. A hashing oriented nearest neighbor searching scheme. *Pattern Recognition Letters*, 14(8):625–??, August 1, 1993. CODEN PRLEDG. ISSN 0167-8655 (print), 1872-7344 (electronic).

Chen:2009:SHA

[CW09] Ning Chen and Wang-Gen Wan. Speech hashing algorithm based on short-time stability. *Lecture Notes in CS*, 5769:426–434, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-04277-5_43`.

Chiu:2010:FMH

[CWC10] Chih-Yi Chiu, Hsin-Min Wang, and Chu-Song Chen. Fast min-hashing indexing and robust spatio-temporal matching for detecting video copies. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 6(2):10:1–10:??, March 2010. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Chandramouli:2019:FFI

[CXLK19] Badrish Chandramouli, Dong Xie, Yinan Li, and Donald Kossmann. FishStore: fast ingestion and indexing of raw data. *Proceedings of the VLDB Endowment*, 12(12):1922–1925, August 2019. CODEN ???? ISSN 2150-8097.

Contini:2006:FPK

[CY06] Scott Contini and Yiqun Lisa Yin. Forgery and partial key-recovery attacks on HMAC and NMAC using hash collisions. *Lecture Notes in CS*, 4284:37–53, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/11935230_3.pdf`.

Cobb:1991:SIP

[CyWM91] Jorge A. Cobb, Shiow yang Wu, and Daniel P. Miranker. Skew insensitive parallel join with sampling. Technical Report TR-91-35, University of Texas, Austin, Austin, TX, USA, November 1991. 18 pp.

Chen:2014:MLC

[CZ14] Long Chen and Zhao Zhang. MemGuard: a low cost and energy efficient design to support and enhance memory system reliability. *ACM SIGARCH Computer Architecture News*, 42(3):49–60, June 2014. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Chi:2017:HTS

[CZ17] Lianhua Chi and Xingquan Zhu. Hashing techniques: a survey and taxonomy. *ACM Computing Surveys*, 50(1): 11:1–11:36, April 2017. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Czech:1998:QPH

[Cze98] Zbigniew J. Czech. Quasi-perfect hashing. *The Computer Journal*, 41(6): ??, ???? 1998. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/Volume_41/Issue_06/Vol41_06.body.html#AbstractCzech`.

Chu:2012:TMP

[CZL12] Xiaowen Chu, Kaiyong Zhao, and Zongpeng Li. Tsunami: massively parallel homomorphic hashing on many-core GPUs. *Concurrency and Computation: Practice and Experience*, 24(17):2028–2039, December 10, 2012. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Chen:2012:AIB

[CZLC12a] Yu Chen, Zongyang Zhang, Dongdai Lin, and Zhenfu Cao. Anonymous identity-based hash proof system and its applications. *Lecture Notes in CS*, 7496: 143–160, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-33272-2_10/`.

Chen:2012:IBE

[CZLC12b] Yu Chen, Zongyang Zhang, Dongdai Lin, and Zhenfu Cao. Identity-based extractable hash proofs and their applications. *Lecture Notes in CS*, 7341: 153–170, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31284-7_10/`.

Chen:2014:CSI

[CZLC14] Yu Chen, Zongyang Zhang, Dongdai Lin, and Zhenfu Cao. CCA-secure IB–KEM from identity-based extractable hash proof system. *The Computer Journal*, 57(10):1537–1556, October 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/57/10/1537`.

Dolev:1992:NPH

[D+92] D. Dolev et al. On neighborhood preserving hashing. Technical report 92-31, Hebrew University of

Jerusalem, Department of Computer Science, 1992. ?? pp.

Dietzfelbinger:1993:OPD

[DA93] M. Dietzfelbinger and F. M. Aufderheide. An optimal parallel dictionary. *Information and Computation*, 102 (2):196–217, February 1993. CODEN INFCEC. ISSN 0890-5401 (print), 1090-2651 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0890540183710072`.

Crescenzo:2012:DFC

[DA12] Giovanni Di Crescenzo and Gonzalo Arce. Data forensics constructions from cryptographic hashing and coding. *Lecture Notes in CS*, 7128:494–509, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-32205-1_39`.

Diaz:2013:TLH

[DAC+13] Antonio F. Díaz, Mancia Anguita, Hugo E. Camacho, Erik Nieto, and Julio Ortega. Two-level hash/table approach for metadata management in distributed file systems. *The Journal of Supercomputing*, 64(1): 144–155, April 2013. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://link.springer.com/article/10.1007/s11227-012-0801-y`.

Dietzfelbinger:1990:NUC

[DadH90] M. Dietzfelbinger and Meyer auf der Heide. A new universal class of hash functions and dynamic hashing in real time. In Paterson [Pat90], pages 6–19. ISBN 0-387-52826-1 (New York), 3-540-52826-1 (Berlin). LCCN QA267.A1 L43 no.443.

Dietzfelbinger:1992:HPU

[DadH92] Martin Dietzfelbinger and Friedhelm Meyer auf der Heide. High performance universal hashing, with applications to shared memory simulations. In Monien and Ottmann [MO92a], pages 250–269. ISBN 0-387-55488-2 (New York), 3-540-55488-2 (Berlin). LCCN QA76.9.D35D36 1992. Papers presented at a symposium held at the Freie Universität Berlin, Sept. 23–26, 1991.

Daemen:1995:HFC

[Dae95] Joan Daemen. *Hash Function and Cipher Design: Strategies Based on Linear and Differential Cryptanalysis*. Ph.D. thesis, Katholieke Universiteit Leuven, Leuven, Belgium, March 1995. 280 pp. URL `http://wwwlib.umi.com/dissertations/fullcit/f548867`.

Damgaard:1987:CFH

[Dam87] I. B. Damgård. Collision free hash functions and public key signature schemes. In Chaum and Price [CP87], pages 203–216. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). LCCN QA76.9.A25 E963 1987.

Damgaard:1990:ACE

[Dam90a] I. B. Damgård, editor. *Advances in Cryptology–EUROCRYPT '90: Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, May 21–24, 1990: proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. ISBN 0-387-53587-X (New York), 3-540-53587-X (Berlin). LCCN QA76.9.A25 E964 1990. DM69.00.

Damgaard:1990:DPH

[Dam90b] I. B. Damgård. A design principle for hash functions. In Brassard [Bra90], pages 416–427. CODEN LNCSD9. ISBN 0-387-97317-6, 3-540-97317-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1989. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0435.htm`; `http://www.springerlink.com/content/978-0-387-97317-3`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=435`. Conference held Aug. 20–24, 1989 at the University of California, Santa Barbara.

Damgaard:1991:ACE

[Dam91] I. B. Damgård, editor. *Advances in cryptology — EUROCRYPT '90: Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, May 21–24, 1990: proceedings*, volume 473 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1991. CODEN LNCSD9. ISBN 0-387-53587-X (New York), 3-540-53587-X (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1990. DM69.00.

Damgaard:1993:IHC

[Dam93] I. B. Damgård. Interactive hashing can simplify zero-knowledge protocol design without complexity assumptions. In Stinson [Sti93], page ?? ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). LCCN QA76.9.A25 C79 1993.

Damgaard:1994:IHC

[Dam94] Ivan B. Damgård. Interactive hashing can simplify zero-knowledge protocol design without computational

assumptions. *Lecture Notes in CS*, 773:100–109, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730100.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0773/07730100.pdf`.

Dang:2013:CFI

[Dan13] Quynh Dang. Changes in Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard. *Cryptologia*, 37(1):69–73, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Datta:1988:IPH

[Dat88] S. Datta. Implementation of a perfect hashing function scheme. M.s. thesis, Department of Computer Science, Virginia Polytechnic Institute and State University, Blacksburg, VA 24061-0106, USA, March 1988. ?? pp.

Davison:1973:RSC

[Dav73] G. A. Davison. Rapidly searching for character string matches using hash coding. *IBM Technical Disclosure Bulletin*, 16(1):??, June 1973. CODEN IBMTAA. ISSN 0018-8689.

Davies:1991:ACE

[Dav91] Donald Watts Davies, editor. *Advances in Cryptology–EUROCRYPT '91: Workshop on the Theory and Application of Cryptographic Techniques, Brighton, UK, April 8–11, 1991: Proceedings*, volume 547 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1991. ISBN 0-387-54620-0 (New York), 3-540-54620-0 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1991.

Day:1970:FTQ

[Day70] A. C. Day. Full table quadratic searching for scatter storage. *Communications of the Association for Computing Machinery*, 13(8):481–482, August 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Drechsler:2012:IEH

[DB12] Chris Drechsler and Thomas Bauschert. Improving the efficiency of HTTP caching by hash based resource identifiers. *Lecture Notes in CS*, 7479:362–371, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/`

10.1007/978-3-642-32808-4_33.

Daemen:1993:CSH

[DBGV93] Joan Daemen, Antoon Bosselaers, Rene Govaerts, and Joos Vandewalle. Collisions for Schnorr's hash function FFT-Hash presented at Crypto'91. In Imai et al. [IRM93], pages 477–480. ISBN 0-387-57332-1 (New York), 3-540-57332-1 (Berlin). LCCN QA76.9.A25 I555 1991. DM96.00.

Bakker:1980:ALP

[dBvL80] J. W. de Bakker and J. van Leeuwen, editors. *Automata, Languages, and Programming: Seventh Colloquium, Noordwijkerhout, the Netherlands, July 14–18, 1980*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1980. ISBN 0-387-10003-2. LCCN QA267.A1 L43 no.85.

Dorng:1981:CHC

[DC81] J. C. Dorng and S. K. Chang. Concatenated hash code selection. *Proceedings - IEEE Computer Society's International Computer Software & Applications Conference 5th.*, pages 245–256, 1981. CODEN PSICD2. IEEE Serv Cent. Piscataway, NJ, USA.

Du:1994:ADV

[DC94] M.-W. Du and S. C. Chang. Approach to designing very fast approximate string matching algorithms. *IEEE Transactions on Knowledge and Data Engineering*, 6(4): 620–633, August 1994. CODEN ITKEEH. ISSN 1041-4347.

Daemen:1998:FHS

[DC98a] J. Daemen and C. S. K. Clapp. Fast hashing and stream encryption with PANAMA. *Lecture Notes in CS*, 1372:60–74, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1372/13720060.htm; http://link.springer-ny.com/link/service/series/0558/papers/1372/13720060.pdf.

Daemen:1998:PCF

[DC98b] Joan Daemen and Craig Clapp. The Panama cryptographic function. *Dr. Dobbs Journal*, 23(12):42, 44, 46, 48–49, December 1998. CODEN DDJOEB. ISSN 1044-789X. URL http://www.ddj.com/ddj/1998/1998_12/../../../ftp/1998/1998_12/panama.zip.

Ding:2018:NPH

[DCM18] Kaimeng Ding, Shiping Chen, and Fan Meng. A novel perceptual hash algorithm for multispectral im-

age authentication. *Algorithms (Basel)*, 11(1), January 2018. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL `https://www.mdpi.com/1999-4893/11/1/6`.

Darragh:1991:BCR

[DCW91] John J. Darragh, John G. Cleary, and Ian H. Witten. Bonsai: a compact representation of trees predictive interfaces: What will they think of next? oriented database definitions. Technical Report 91/447/31, University of Calgary, October 1991. ?? pp. (email parin@cpsc.ucalgary.ca).

DeBonis:2011:CGT

[DD11] Annalisa De Bonis and Giovanni Di Crescenzo. Combinatorial group testing for corruption localizing hashing. *Lecture Notes in CS*, 6842:579–591, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-22685-4_50`.

Dhawan:2015:AEN

[DD15] Udit Dhawan and André Dehon. Area-efficient near-associative memories on FPGAs. *ACM Transactions on Reconfigurable Technology and Systems*, 7(4):3:1–3:??, January 2015. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Danezis:2007:END

[DDF+07] George Danezis, Claudia Diaz, Sebastian Faust, Emilia Käsper, and Carmela Troncoso. Efficient negative databases from cryptographic hash functions. *Lecture Notes in CS*, 4779:423–436, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-75496-1_28`.

Dalal:2005:TWC

[DDMM05] Ketan Dalal, Luc Devroye, Ebrahim Malalla, and Erin McLeish. Two-way chaining with reassignment. *SIAM Journal on Computing*, 35 (2):327–340, ???? 2005. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Dinur:2014:IPA

[DDS14] Itai Dinur, Orr Dunkelman, and Adi Shamir. Improved practical attacks on round-reduced Keccak. *Journal of Cryptology*, 27(2): 183–209, April 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9142-5`.

deBalbine:1969:CAR

[de 69] Guy de Balbine. *Computational Analysis of the Random Components Induced by a Binary Equivalence Relation*. Ph.d. thesis, California Institute of Technology, Pasadena, CA, USA, 1969. 168 pp. First use of second hash function for computing next hash table location after a collision. See also [BK70].

DeSantis:1995:ACE

[De 95] A. De Santis, editor. *Advances in cryptology: EUROCRYPT '94: Workshop on the theory and application of cryptographic techniques — May 1994, Perugia, Italy*, number 950 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. ISBN 3-540-60176-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E965 1995.

Debnath:2003:CTA

[Deb03] Narayan C. Debnath, editor. *Computers and Their Applications: proceedings of the ISCA 18th international conference, Honolulu, Hawaii, USA March 26–28, 2003*. ISCA, Carey, NC, USA, 2003. ISBN 1-880843-46-3 (paperback). LCCN QA75.5 I76 2003; QA76.76.A65 I83 2003.

Deen:1982:IIS

[Dee82] S. M. Deen. Implementation of impure surrogates. *Very Large Data Bases, International Conference on Very Large Data Bases*, pages 245–256, 1982. CODEN VLDBDP.

Devroye:1986:LNB

[Dev86] Luc Devroye. *Lecture Notes on Bucket Algorithms*. Birkhäuser, Cambridge, MA, USA; Berlin, Germany; Basel, Switzerland, 1986. ISBN 0-8176-3328-6. 148 pp. LCCN QA76.9.D35 D48 1986.

Devine:1993:DID

[Dev93] Robert Devine. Design and implementation of DDH: a distributed dynamic hashing algorithm. *Lecture Notes in CS*, 730:101–114, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Devroye:1999:HSR

[Dev99] Luc Devroye. The height and size of random hash trees and random pebbled hash trees. *SIAM Journal on Computing*, 28(4): 1215–1224, August 1999. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/32617`.

Denert:1977:D

[DF77] Ernst Denert and Reinhold Franxk. *Datenstrukturen*. Bibliographisches Institut, Mannheim, Germany, 1977. ISBN 3-411-01524-1. 362 pp. LCCN QA76.9.D35 D46.

Datta:1989:IPH

[DF89] S. Datta and E. A. Fox. Implementation of a perfect hash function scheme. Technical Report TR 89-9, Department of Computer Science, Virginia Polytechnic Institute and State University, Blacksburg, VA 24061-0106, USA, 1989. ?? pp.

Domingo-Ferrer:2001:MAR

[DF01] J. Domingo-Ferrer. Mobile agent route protection through hash-based mechanisms. *Lecture Notes in CS*, 2247:17–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470017.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2247/22470017.pdf`.

DellAmico:2015:UAP

[DFMR15] Matteo Dell'Amico, Maurizio Filippone, Pietro Michiardi, and Yves Roudier. On user availability prediction and network applications. *IEEE/ACM Transactions on Networking*, 23(4):1300–1313, August 2015. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

DeWitt:1985:MHBa

[DG85a] D. J. DeWitt and R. Gerber. Multiprocessor hash-based join algorithms. Technical report, University of Wisconsin–Madison, Madison, WI, USA, 1985. ?? pp.

DeWitt:1985:MHBb

[DG85b] D. J. DeWitt and R. H. Gerber. Multiprocessor hash-based join algorithms. In Pirotte and Vassiliou [PV85], page 151. ISBN 0-934613-17-6. LCCN QA 76.9 D3 I61 1985.

Davison:1993:MCR

[DG93] D. L. Davison and G. Graefe. Memory-contention responsive hash joins. Technical Report CU-CS-682-93, University of Colorado Computer Science Department, Boulder, CO, USA, 1993. ?? pp.

Davison:1994:MRH

[DG94] D. L. Davison and G. Graefe. Memory-contention responsive hash joins. In Bocca et al. [BJZ94], pages 379–390. ISBN 1-55860-153-8. ISSN 0730-9317. LCCN QA76.9 D3 I61 1994. URL `http://www.vldb.org/dblp/db/conf/vldb/vldb94-379.html`.

Dawson:1996:CPA

[DG96] E. Dawson and J. Golic, editors. *Cryptography: policy and algorithms: International conference — July 1995, Brisbane, Australia*, number 1029 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1996. ISBN 3-540-60759-5. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C844 1996.

Desmet:2002:IHC

[DGD02] V. Desmet, B. Goeman, and K. De Bosschere. Independent hashing as confidence mechanism for value predictors in microprocessors. *Lecture Notes in CS*, 2400:458–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2400/24000458.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2400/24000458.pdf`.

DeWitt:1986:GHP

[DGG+86] D. J. DeWitt, R. H. Gerber, G. Graefe, M. L. Heytens, K. B. Kumar, and M. Muralikrishna. GAMMA — a high performance dataflow database machine. In Chu et al. [CGO86], page 228. ISBN 0-934613-18-4. LCCN QA76.9.D3 I559 1986. Reprinted in M. Stonebraker, Readings in Database Sys., Morgan Kaufmann, San Mateo, CA, 1988.

Dantras:2016:OIB

[DGGL16] Amanieu D'antras, Cosmin Gorgovan, Jim Garside, and Mikel Luján. Optimizing indirect branches in dynamic binary translators. *ACM Transactions on Architecture and Code Optimization*, 13 (1):7:1–7:??, April 2016. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic).

Durvaux:2012:IPP

[DGKK12] François Durvaux, Benoît Gérard, Stéphanie Kerckhof, and François Koeune. Intellectual property protection for integrated systems using soft physical hash functions. *Lecture Notes in CS*, 7690:208–225, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-35416-8_15/`.

Du:1989:EFS

[DGM89] D. H. C. Du, S. Ghanta, and K. J. Maly. An efficient file structure for document retrieval in the automated office environment. *IEEE Transactions on Knowledge*

and Data Engineering, 1(2): ??, June 1989. CODEN ITKEEH. ISSN 1041-4347. Also published in [ICD87].

Dietzfelbinger:1992:PHF

[DGMP92] M. Dietzfelbinger, J. Gil, Y. Matias, and N. Pippenger. Polynomial hash functions are reliable. In Kuich [Kui92], pages 235–246. ISBN 0-387-55719-9 (New York), 3-540-55719-9 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.623.

DeWitt:1990:GDMb

[DGS+90a] David J. DeWitt, Shaharm Ghandeharizadeh, Donovan A. Schneider, Allan Bricker, Hui i Hsiao, and Rick Rasmusen. The gamma database machine project. *IEEE Transactions on Knowledge and Data Engineering*, 2(1):44–62, March 1990. CODEN ITKEEH. ISSN 1041-4347.

DeWitt:1990:GDMa

[DGS+90b] David J. DeWitt, Shahram Ghandeharizadeh, Donovan Schneider, Allan Bricker, Hui-I Hsiao, and Rick Rasmussen. The gamma database machine project. Technical Report TR 921, University of Wisconsin, March 1990. ?? pp.

Daemen:1993:FDO

[DGV93] Joan Daemen, Rene Govaerts, and Joos Vandewalle. A framework for the design of one-way hash functions including cryptanalysis of damgård's one-way function based on a cellular automaton. In Imai et al. [IRM93], pages 82–96. ISBN 0-387-57332-1 (New York), 3-540-57332-1 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I555 1991. DM96.00.

Donaldson:1984:CMV

[DH84] Val Donaldson and Lois W. Hawkes. Cyclic multiple-valued filing schemes for higher-order queries. *Information Sciences*, 32(1):47–74, February 1984. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic). Combinatorial filing schemes are a class of file organizations for formatted records which are based on multiattribute hashing.

Dietzfelbinger:2001:SMP

[DH01] Martin Dietzfelbinger and Torben Hagerup. Simple minimal perfect hashing in less space. *Lecture Notes in CS*, 2161:109–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2161/21610109.htm`; `http://link.springer-ny.com/link/service/series/`

0558/papers/2161/21610109.pdf.

Du:1983:SNP

[DHJS83] M. W. Du, T. M. Hsieh, K. F. Jea, and D. W. Shieh. The study of a new perfect hash scheme. *IEEE Transactions on Software Engineering*, SE-9(3):305–313, May 1983. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic).

Debnath:2015:RHT

[DHK+15] Biplob Debnath, Alireza Haghdoost, Asim Kadav, Mohammed G. Khatib, and Cristian Ungureanu. Revisiting hash table design for phase change memory. *Operating Systems Review*, 49 (2):18–26, December 2015. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Dietzfelbinger:1997:RRA

[DHKP97] Martin Dietzfelbinger, Torben Hagerup, Jyrki Katajainen, and Martti Penttonen. A reliable randomized algorithm for the closest-pair problem. *Journal of Algorithms*, 25(1):19–51, ???? 1997. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic).

Dolev:1994:NPH

[DHL+94] Danny Dolev, Yuval Harari, Nathan Linial, Noam Nisan, and Michal Parnas. Neighborhood preserving hashing and approximate queries. In ACM-SIAM-SDA'94 [ACM94d], pages 73–85. ISBN 0-89871-329-3. LCCN QA76.6 .A278 1994.

Dolev:2002:NPH

[DHL+02] Danny Dolev, Yuval Harari, Nathan Linial, Noam Nisan, and Michal Parnas. Neighborhood preserving hashing and approximate queries. *SIAM Journal on Discrete Mathematics*, 15(1):73–85, 2002. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/31809.

Do:2019:SDC

[DHT+19] Thanh-Toan Do, Tuan Hoang, Dang-Khoa Le Tan, Huu Le, Tam V. Nguyen, and Ngai-Man Cheung. From selective deep convolutional features to compact binary representations for image retrieval. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 15(2):43:1–43:??, June 2019. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3314051.

Dietzfelbinger:2008:DIB

[DHW08] Martin Dietzfelbinger, Martin Hühne, and Christoph

Weidling. A dictionary implementation based on dynamic perfect hashing. *ACM Journal of Experimental Algorithmics*, 12:1.11:1–1.11:??, June 2008. CODEN ???? ISSN 1084-6654.

Dietzfelbinger:1990:HDD

[Die90] Martin Dietzfelbinger. How to distribute a dictionary in a complete network. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (May 14–16 1990: Baltimore, MD, USA)*, pages 117–127. ACM Press, New York, NY 10036, USA, 1990. ISBN 0-89791-361-2. LCCN QA 76.6 A13 1990.

Dietzfelbinger:1996:UHW

[Die96] M. Dietzfelbinger. Universal hashing and k-wise independent random variables via integer arithmetic without primes. *Lecture Notes in CS*, 1046:569–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dietzfelbinger:2007:DSM

[Die07] Martin Dietzfelbinger. Design strategies for minimal perfect hash functions. In Hromkovič et al. [HKNW07], pages 2–17. CODEN LNCSD9. ISBN 3-540-74870-9 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA9.58 .S24 2007. URL `http://www.springerlink.com/content/y48k83u127014207/`.

Dittmer:1976:IEP

[Dit76] Ingo Dittmer. Implementation eines Einschrittcompilers für die Programmiersprache PASCAL auf der Rechenanlage IBM/360 der Universität Münster. (English title: Implementation of a one-step compiler for the programming language PASCAL on the IBM/360 of the University of Muenster). Master's thesis, Universität Münster, Münster, Germany, 1976. ?? pp. Diplomearbeit Münster 1976 und doert angegebene Literatur (English: Muenster diploma work 1976 and the literature cited therein). The hashing method was rediscovered fourteen years later by Pearson [Pea90], and then commented on by several authors [Dit91, Sav91, Lit91, Pea91].

Dittmer:1991:NFH

[Dit91] I. Dittmer. Note on fast hashing of variable length text strings. *Communications of the Association for Computing Machinery*, 34(11):118, November 1991. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Points out that Pearson's hashing algorithm [Pea90] was discovered fourteen years earlier by

this author [Dit76]. See also comments in [Sav91, Lit91, Pea91].

Dinur:2009:ARC

[DJNR09] Irit Dinur, Klaus Jansen, Joseph Naor, and José Rolim, editors. *Approximation, randomization, and combinatorial optimization: algorithms and techniques: 12th International Workshop, APPROX 2009, and 13th International Workshop, RANDOM 2009, Berkeley, CA, USA, August, 21–23, 2009: proceedings*, volume 5687 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 3-642-03684-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA75.5 .I643 2009. URL `http://www.loc.gov/catdir/enhancements/fy1208/2009932147-d.html`; `http://www.springerlink.com/content/978-3-642-03684-2/`.

Diaz:2006:ARC

[DJRZ06] J. (Josep) Díaz, Klaus Jansen, José D. P. Rolim, and Uri Zwick, editors. *Approximation, randomization and combinatorial optimization: algorithms and techniques: 9th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2006, and 10th International Workshop on Randomization and Computation, RANDOM 2006, Barcelona, Spain, August 28–30, 2006: proceedings*, volume 4110 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. CODEN LNCSD9. ISBN 3-540-38044-2 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA75.5 .I643 2006. URL `http://www.loc.gov/catdir/enhancements/fy0825/2006931401-d.html`; `http://www.loc.gov/catdir/toc/fy0703/2006931401.html`; `http://www.springerlink.com/content/978-3-540-38044-3/`; `http://www.springerlink.com/openurl.asp?genre=issue\%26issn=0302-9743\%26volume=4110`.

Du:1980:SNP

[DJS80] Min Wen Du, Kuen Fang Jea, and Den Wey Shieh. Study of a new perfect hash scheme. In IEEE-COMPSAC'80 [IEE80a], pages 341–347. LCCN QA 75.5 C586 1980.

DiCrescenzo:2009:CLH

[DJSN09] Giovanni Di Crescenzo, Shaoquan Jiang, and Reihaneh Safavi-Naini. Corruption-localizing hashing. *Lecture Notes in CS*, 5789: 489–504, 2009. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-04444-1_30.

Damgaard:1994:BAH

[DK94] I. B. Damgård and L. R. Knudsen. The breaking of the AR hash function. In Helleseth [Hel94], pages 286–292. ISBN 0-387-57600-2 (New York), 3-540-57600-2 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1993.

Delfs:2002:ICP

[DK02] Hans Delfs and Helmut Knebl. *Introduction to Cryptography: Principles and Applications*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. ISBN 3-642-87126-7 (e-book), 3-642-87128-3. ISSN 1619-7100 (print), 2197-845X (electronic). xiv + 310 pp. LCCN QA76.9.A25. URL http://www.springerlink.com/content/978-3-642-87126-9.

De:2007:IAS

[DK07] Debapratim De and Abishek Kumarasubramanian. Inversion attacks on secure hash functions using sat solvers. *Lecture Notes in CS*, 4501:377–382, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-72788-0_36.

Dahmen:2009:SHB

[DK09] Erik Dahmen and Christoph Krauß. Short hash-based signatures for wireless sensor networks. *Lecture Notes in CS*, 5888:463–476, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-10433-6_31.

Drmota:2012:PAC

[DK12] Michael Drmota and Reinhard Kutzelnigg. A precise analysis of Cuckoo hashing. *ACM Transactions on Algorithms*, 8(2):11:1–11:36, April 2012. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

Delfs:2015:ICP

[DK15] Hans Delfs and Helmut Knebl. *Introduction to Cryptography : Principles and Applications*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., third edition, 2015. ISBN 3-662-47973-7 (paper), 3-662-47974-5 (e-book). ISSN

1619-7100 (print), 2197-845X (electronic). xx + 508 + 5 pp. LCCN QA76.9.A25; QA76.9.D35. URL `http://link.springer.com/book/10.1007/978-3-662-47974-2`.

deKergommeaux:1994:PLP

[dKC94] Jacques Chassin de Kergommeaux and Philippe Codognet. Parallel logic programming systems. *ACM Computing Surveys*, 26(3): 295–336, September 1994. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0360-0300/185453.html`.

Dietzfelbinger:1988:DPH

[DKM+88] M. Dietzfelbinger, A. Karlin, K. Mehlhorn, F. Meyer auf der Heide, H. Rohnert, and R. E. Tarjan. Dynamic perfect hashing: Upper and lower bounds. In IEEE-FOCS'88 [IEE88c], pages 524–531. ISBN 0-8186-0877-3 (paperback), 0-8186-4877-5 (microfiche), 0-8186-8877-7 (hardcover). LCCN QA 76 S979 1988.

Dietzfelbinger:1991:DPH

[DKM+91] M. Dietzfelbinger, A. Karlin, K. Mehlhorn, F. Meyer auf def Heide, H. Rohnert, and Robert E. Tarjan. Dynamic perfect hashing: upper and lower bounds. Technical Report CS-TR-310-91, Department of Computer Science, Princeton University, Princeton, NJ, USA, March 1991. ?? pp.

Dietzfelbinger:1994:DPH

[DKM+94] Martin Dietzfelbinger, Anna Karlin, Kurt Mehlhorn, Friedhelm Meyer auf der Heide, Hans Rohnert, and Robert E. Tarjan. Dynamic perfect hashing: Upper and lower bounds. *SIAM Journal on Computing*, 23(4): 738–761, ???? 1994. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

DeWitt:1984:ITMc

[DKO84a] D. J. DeWitt, H. R. Katz, and F. Olken. Implementation techniques for main memory database systems. Technical report, University of Wisconsin–Madison, Madison, WI, USA, 1984. ?? pp.

DeWitt:1984:ITMa

[DKO+84b] D. J. DeWitt, R. Katz, F. Olken, L. Shapiro, M. Stonebraker, and D. Wood. Implementation techniques for main memory database systems. In *Proc. ACM SIGMOD Conf*, page 1. ACM Press, New York, NY 10036, USA, June 1984.

DeWitt:1984:ITMb

[DKO+84c] D. J. DeWitt, R. H. Katz, F. Olken, L. D. Shapiro,

M. R. Stonebraker, and D. Wood. Implementation techniques for main memory database systems. Technical Report UCB/ERL 84/5, Electronics Research Laboratory, University of California, Berkeley, CA, USA, January 1984. 1–23 pp.

DeWitt:1984:ITMd

[DKO+84d] David J. DeWitt, Randy H. Katz, Frank Olken, Leonard D. Shapiro, Michael R. Stonebraker, and David Wood. Implementation techniques for main memory database systems. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 14(2):1–8, 1984. CODEN SRECD8. ISBN 0-89791-128-8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Dahlgaard:2015:HSP

[DKRT15] Søren Dahlgaard, Mathias Bæk Tejs Knudsen, Eva Rotenberg, and Mikkel Thorup. Hashing for statistics over k-partitions. In IEEE, editor, *2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1292–1310. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2015. ISBN 1-4673-8191-8. ISSN 0272-5428.

Dahlgaard:2016:PTC

[DKRT16] Søren Dahlgaard, Mathias Bæk Tejs Knudsen, Eva Rotenberg, and Mikkel Thorup. The power of two choices with simple tabulation. In Robert Krauthgamer, editor, *Proceedings of the 27th SODA (2016)*, pages 1631–1642. ACM Press, New York, NY 10036, USA, 2016. URL `http://dl.acm.org/citation.cfm?id=2884435.2884546`.

Dharmapurikar:2006:LPM

[DKT06] Sarang Dharmapurikar, Praveen Krishnamurthy, and David E. Taylor. Longest prefix matching using Bloom filters. *IEEE/ACM Transactions on Networking*, 14(2): 397–409, April 2006. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Devillers:1979:HTG

[DL79] R. Devillers and G. Louchard. Hashing techniques, a global approach. *BIT (Copenhagen)*, 19(3):302–311, ???? 1979. CODEN NBITAB.

Du:1980:SGC

[DL80] H. C. Du and R. C. T. Lee. Symbolic Gray code as a multikey hashing function. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, PAMI-2(1):83–90, January 1980. CODEN ITPIDJ. ISSN 0162-8828.

Denielou:2006:APS

[DL06] Pierre-Malo Deniélou and James J. Leifer. Abstraction preservation and subtyping in distributed languages. *SIGPLAN Notices*, 41(9):286–297, September 2006. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Dong:2012:UAS

[DL12] Qi Dong and Donggang Liu. Using auxiliary sensors for pairwise key establishment in WSN. *ACM Transactions on Embedded Computing Systems*, 11(3):59:1–59:??, September 2012. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Dinur:2017:IGA

[DL17] Itai Dinur and Gaëtan Leurent. Improved generic attacks against hash-based MACs and HAIFA. *Algorithmica*, 79(4):1161–1195, December 2017. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

DeRemer:1979:SCS

[DLH+79] Frank DeRemer, Philip Levy, Steve Hanson, Philip Jackson, Richard Jullig, and Tom Pittman. Summary of the characteristics of several 'modern' programming languages. *SIGPLAN Notices*, 14(5):28–45, May 1979. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Dolev:2009:BAU

[DLH09] Shlomi Dolev, Limor Lahiani, and Yinnon Haviv. Brief announcement: Unique permutation hashing. *Lecture Notes in CS*, 5873: 777–778, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-05118-0_56`.

Dolev:2013:UPH

[DLH13] Shlomi Dolev, Limor Lahiani, and Yinnon Haviv. Unique permutation hashing. *Theoret. Comput. Sci.*, 475 (??):59–65, March 4, 2013. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397513000133`.

Durand:2007:SPP

[DLM07] Arnaud Durand, Clemens Lautemann, and Malika More. A simple proof of the polylog counting ability of first-order logic: guest column. *ACM SIGACT News*, 38(4):40–45, December 2007. CODEN SIGNDM. ISSN

0163-5700 (print), 1943-5827 (electronic).

Duan:2018:EGS

[DLN+18] Weiwei Duan, Jianxin Luo, Guiqiang Ni, Bin Tang, Qi Hu, and Yi Gao. Exclusive grouped spatial hashing. *Computers and Graphics*, 70 (??):71–79, February 2018. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0097849317301474`.

Damiani:1998:EDH

[DLT98] Ernesto Damiani, Valentino Liberali, and Andrea G. B. Tettamanzi. Evolutionary design of hashing function circuits using an FPGA. *Lecture Notes in CS*, 1478:36–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1478/14780036.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1478/14780036.pdf`.

Davie:1981:RDC

[DM81] A. J. T. Davie and R. Morrison. *Recursive Descent Compiling*. Ellis Horwood Series in Computers and their Applications, Editor: Brian Meek. Ellis Horwood, New York, NY, USA, 1981. ISBN 0-470-27270-8 (Halstead Press), 0-85312-386-1 (Ellis Horwood). 195 pp. LCCN QA76.6 .D373. US$34.95. Discusses handling of clustering in hash tables.

Diby:1990:DDK

[DM90] K. Diby and P. Mateti. Design documentation of Knuth's solution to the common words problem. Technical Report WSU-CS-90-08, Washington State University, 1990. ?? pp.

Devroye:2003:CHF

[DM03] Luc Devroye and Pat Morin. Cuckoo hashing: Further analysis. *Information Processing Letters*, 86(4):215–219, May 31, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ducournau:2011:PCH

[DM11] Roland Ducournau and Floréal Morandat. Perfect class hashing and numbering for object-oriented implementation. *Software—Practice and Experience*, 41(6):661–694, May 2011. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Doukas:2019:HFD

[DMB19] Nikolaos Doukas, Oleksandr P. Markovskyi, and Nikolaos G. Bardis. Hash function design for cloud

storage data auditing. *Theoret. Comput. Sci.*, 800(??): 42–51, December 31, 2019. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397519306449`.

Ducournau:2009:EAO

[DMP09] Roland Ducournau, Floréal Morandat, and Jean Privat. Empirical assessment of object-oriented implementations with multiple inheritance and static typing. *SIGPLAN Notices*, 44(10):41–60, October 2009. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Demaine:2006:DDP

[DMPP06] E. D. Demaine, F. Meyer auf der Heide, R. Pagh, and M. Pătraşcu. De dictionariis dynamicis pauco spatio utentibus. (latin) [On dynamic dictionaries using little space]. In Correa et al. [CHK06], pages 349–361. CODEN LNCSD9. ISBN 3-540-32755-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL `http://www.springerlink.com/content/978-3-540-32756-1`.

Dietzfelbinger:2011:CHP

[DMR11] Martin Dietzfelbinger, Michael Mitzenmacher, and Michael Rink. Cuckoo hashing with pages. *Lecture Notes in CS*, 6942:615–627, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-23719-5_52`.

Devroye:2004:WCR

[DMV04] Luc Devroye, Pat Morin, and Alfredo Viola. On worst-case Robin Hood hashing. *SIAM Journal on Computing*, 33 (4):923–936, August 2004. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/40337`.

DeWitt:1992:PSH

[DNSS92] David J. DeWitt, Jeffrey F. Naughton, Donovan A. Schneider, and S. Seshadri. Practical skew handling in parallel joins. Technical Report TR 1098, Computer Sciences Department, University of Wisconsin–Madison, July 1992. ?? pp.

Deen:1981:DCD

[DNV81] S. M. Deen, D. Nikodem, and A. Vashishta. Design of a canonical database system (PRECI). *The Computer Journal*, 24(3):200–209, August 1981. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Dodds:1982:PRD

[Dod82] D. J. Dodds. Pracniques: Reducing dictionary size by using a hashing technique. *Communications of the Association for Computing Machinery*, 25(6): 368–370, June 1982. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Donovan:1991:PSM

[Don91] Kevin Donovan. Performance of shared memory in a parallel computer. *IEEE Transactions on Parallel and Distributed Systems*, 2(2): 253–256, April 1991. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Dodis:2005:GIF

[DOP05] Yevgeniy Dodis, Roberto Oliveira, and Krzysztof Pietrzak. On the generic insecurity of the full domain hash. In Shoup [Sho05], pages 449–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621`.

Diegues:2014:OHH

[DOP+14] Nuno Diegues, Muhammet Orazov, João Paiva, Luís Rodrigues, and Paolo Romano. Optimizing hyperspace hashing via analytical modelling and adaptation. *ACM SIGAPP Applied Computing Review*, 14 (2):23–35, June 2014. CODEN ???? ISSN 1559-6915 (print), 1931-0161 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/2656864.2656866`.

Doster:1978:AHG

[Dos78a] Wolfgang Doster. Auswahl eines Hashverfahrens bei grosser Anzahl von speziellen Schluesselwoertern (Postortsnamen). [Selection of a hash-coding method for a large number of special key words (postal place names)]. *Wissenschaftliche Berichte AEG-Telefunken*, 51(2-3): 104–114, ???? 1978. CODEN WBATB3. ISSN 0043-6801.

Doszkocs:1978:AAI

[Dos78b] Tamas E. Doszkocs. AID, an associative interactive dictionary for online searching. *Online Review*, 2(2): 163–165, June 1978. CODEN OLREDR.

Dietzfelbinger:2008:SDS

[DP08] Martin Dietzfelbinger and Rasmus Pagh. Succinct data structures for retrieval and approximate member-

ship (extended abstract). In Aceto et al. [ADG+08], pages 385–396. ISBN 3-540-70574-0 (softcover). LCCN ???? URL http://www.springerlink.com/content/r124235788213548/.

Das:2008:DHS

[DPH08] Saumitra M. Das, Himabindu Pucha, and Y. Charlie Hu. Distributed hashing for scalable multicast in wireless ad hoc networks. *IEEE Transactions on Parallel and Distributed Systems*, 19(3): 347–362, March 2008. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Delis:1992:PSC

[DR92] A. Delis and N. Roussopoulos. Performance and scalability of client-server architectures. In *Proceedings of the 18th Conference on Very Large Databases, Vancouver*, page ?? Morgan Kaufmann Publishers, San Francisco, CA, August 1992.

DeCanniere:2006:FSC

[DR06] Christophe De Cannière and Christian Rechberger. Finding SHA-1 characteristics: General results and applications. *Lecture Notes in CS*, 4284:1–20, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11935230_1.pdf; http://link.springer.com/content/pdf/bfm:978-3-540-49476-8/1.pdf.

Dietzfelbinger:2009:AST

[DR09] Martin Dietzfelbinger and Michael Rink. Applications of a splitting trick. In Albers et al. [AMSM+09], pages 354–365. CODEN LNCSD9. ISBN 3-642-02926-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267 .I55 2009. URL http://www.springerlink.com/content/27w12p275w8njju3/.

Doyoddorj:2011:NSI

[DR11] Munkhbaatar Doyoddorj and Kyung-Hyune Rhee. A novel secure image hashing based on reversible watermarking for forensic analysis. *Lecture Notes in CS*, 6908:286–294, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-23300-5_22.

Drescher:2017:BB

[Dre17a] Daniel Drescher. *Blockchain Basics*. Apress, Berkeley, CA, USA, 2017. ISBN 1-4842-2603-8 (print), 1-4842-2604-6 (e-book). xv + 255 pp. LCCN HG1710 .D74 2017. URL http://link.springer.com/book/

10.1007/978-1-4842-2604-9.

Drescher:2017:HD

[Dre17b] Daniel Drescher. Hashing data. In *Blockchain Basics* [Dre17a], pages 71–79. ISBN 1-4842-2603-8 (print), 1-4842-2604-6 (e-book). LCCN HG1710 .D74 2017. URL http://link.springer.com/chapter/10.1007/978-1-4842-2604-9_10.

Drescher:2017:HRW

[Dre17c] Daniel Drescher. Hashing in the real world. In *Blockchain Basics* [Dre17a], pages 81–92. ISBN 1-4842-2603-8 (print), 1-4842-2604-6 (e-book). LCCN HG1710 .D74 2017. URL http://link.springer.com/chapter/10.1007/978-1-4842-2604-9_11.

Dodis:2012:HHA

[DRS12] Yevgeniy Dodis, Thomas Ristenpart, and John Steinberger. To hash or not to hash again? (in)differentiability results for H^2 and HMAC. *Lecture Notes in CS*, 7417: 348–366, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-32009-5_21.

Dertmann:1984:SBI

[DS84a] M. Dertmann and G. Saake. Simulation von Bounded Index Exponential Hashing im Vergleich mit Anderen Dynamischen Speicherverfahren. Studienarbeit, 1984.

Devine:1984:DFO

[DS84b] K. Devine and F. J. Smith. Direct file organization for lemmatized text retrieval. *Inf. Tech. Res. Dev. Appl.*, 3(1):25–32, January 1984. CODEN ITRDDE. ISSN 0144-817X.

Dixon:1997:HPS

[DS97] Brandon Dixon and John Swallow. High-performance sorting algorithms for the CRAY T3D parallel computer. *The Journal of Supercomputing*, 10(4):371–395, December 1997. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=10&issue=4&spage=371; http://www.wkap.nl/oasis.htm/134570.

Deepthi:2009:DIA

[DS09a] P. P. Deepthi and P. S. Sathidevi. Design, implementation and analysis of hardware efficient stream ciphers using LFSR based hash functions. *Computers and Security*, 28(3–4):

229–241, May/June 2009. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404808001193.

Dietzfelbinger:2009:RUC

[DS09b] M. Dietzfelbinger and U. Schellbach. On risks of using cuckoo hashing with simple universal hash classes. In Mathieu [Mat09], pages 795–804. ISBN 0-89871-680-2. LCCN QA76.6 A849 2009. URL http://dl.acm.org/citation.cfm?id=1496857.

Dietzfelbinger:2009:WCH

[DS09c] Martin Dietzfelbinger and Ulf Schellbach. Weaknesses of cuckoo hashing with a simple universal hash class: The case of large universes. *Lecture Notes in CS*, 5404:217–228, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-95891-8_22.

Du:1995:RMQ

[DSD95] Weimin Du, Ming-Chien Shan, and Umeshwar Dayal. Reducing multidatabase query response time by tree balancing. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 24 (2):293–303, May 1995. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Dachman-Soled:2020:TRA

[DSGKS20] Dana Dachman-Soled, Huijing Gong, Mukul Kulkarni, and Aria Shahverdi. Towards a ring analogue of the leftover hash lemma. *Journal of Mathematical Cryptology*, 15(1):87–110, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL https://www.degruyter.com/document/doi/10.1515/jmc-2020-0076/html.

Dayal:1984:VLD

[DSS84] Umeshwar Dayal, G. Schlageter, and Lim Huat Seng, editors. *Very Large Data Bases: Proceedings: Tenth International Conference on Very Large Data Bases, Singapore, August 27–31, 1984*. Very Large Data Bases Endowment, Saratoga, CA, USA, 1984.

Dalessandro:2010:NSS

[DSS10] Luke Dalessandro, Michael F. Spear, and Michael L. Scott. NOrec: streamlining STM by abolishing ownership records. *SIGPLAN Notices*, 45(5):67–78, May 2010. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Dhayal:2017:MMP

[DSS17] Anant Dhayal, Jayalal Sarma, and Saurabh Sawlani. Min/max-poly weighting schemes and the NL versus UL problem. *ACM Transactions on Computation Theory*, 9(2): 10:1–10:??, May 2017. CODEN ???? ISSN 1942-3454 (print), 1942-3462 (electronic).

Dontas:1990:FTHa

[DSSW90a] K. Dontas, J. Sarma, P. Srinivasan, and H. Wechsler. Fault tolerant hashing and information retrieval using back propagation. In *Proceedings of HICCS-90*, pages 345–352. ????, ????, 1990.

Dontas:1990:FTHb

[DSSW90b] Kejitan Dontas, Jayshree Sarma, Padmini Srinivasan, and Harry Wechsler. Fault-tolerant hashing and information retrieval using back propagation. *Proceedings of the Hawaii International Conference on System Science*, 4:345–352, 1990. CODEN PHISD7. ISBN 0-8186-2011-0. ISSN 0073-1129. IEEE catalog number 90TH0294-9.

Dehne:2007:ADS

[DSZ07a] Frank Dehne, Jörg-Rüdiger Sack, and Norbert Zeh, editors. *Algorithms and Data Structures. 10th International Workshop, WADS 2007, Halifax, Canada, August 15–17, 2007. Proceedings*, volume 4619. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. CODEN LNCSD9. ISBN 3-540-73948-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL `http://www.springerlink.com/content/978-3-540-73948-7`.

Dehne:2007:PAI

[DSZ07b] Frank Dehne, Jörg-Rüdiger Sack, and Norbert Zeh, editors. *Algorithms and Data Structures. 10th International Workshop, WADS 2007, Halifax, Canada, August 15–17, 2007. Proceedings*, volume 4619. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. CODEN LNCSD9. ISBN 3-540-73948-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ????

Dubost:1975:SIN

[DT75] P. Dubost and J.-M. Trousse. Software implementation of a new method of combinatorial hashing. Technical Report STAN-CS-75-511, Stanford University Computer Science Department, September 1975. ?? pp.

Dayal:1987:PAC

[DT87] Umeshwar Dayal and Irv Traiger, editors. *Proceed-*

ings of Association for Computing Machinery Special Interest Group on Management of Data 1987 annual conference, San Francisco, May 27–29, 1987. ACM Press, New York, NY 10036, USA, 1987. ISBN 0-89791-236-5. LCCN QA 76.9 D3 P76 1987. ACM order number 472870.

Du:1991:MEH

[DT91a] D. H. C. Du and S.-R. Tong. Multilevel extendible hashing: a file structure for very large databases. *IEEE Transactions on Knowledge and Data Engineering*, 3(3):357–370, September 1, 1991. CODEN ITKEEH. ISSN 1041-4347.

Du:1991:PDD

[DT91b] D. H. C. Du and S.-R. Tong. Physical database design multilevel extendible hashing: a file structure for very large databases. *IEEE Transactions on Knowledge and Data Engineering*, 3 (3):357–??, September 1991. CODEN ITKEEH. ISSN 1041-4347.

Dahlgaard:2014:AMI

[DT14] Søren Dahlgaard and Mikkel Thorup. Approximately minwise independence with twisted tabulation. In R. Ravi and Inge Li Gørtz, editors, *Algorithm Theory — SWAT 2014: 14th Scandinavian Symposium and Workshops, Copenhagen, Denmark, July 2–4, 2014. Proceedings*, pages 134–145. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2014. URL `https://link.springer.com/content/pdf/10.1007/978-3-319-08404-6_12.pdf`.

Daloze:2018:PDL

[DTM+18] Benoit Daloze, Arie Tal, Stefan Marr, Hanspeter Mössenböck, and Erez Petrank. Parallelization of dynamic languages: synchronizing built-in collections. *Proceedings of the ACM on Programming Languages (PACMPL)*, 2(OOPSLA): 108:1–108:30, October 2018. URL `https://dl.acm.org/doi/abs/10.1145/3276478`.

Deutscher:1975:CSD

[DTS75] R. F. Deutscher, R. P. Tremblay, and P. G. Sorenson. A comparative study of distribution-dependent and distribution-independent hashing functions. In ACM-DUOM'75 [ACM75b], page ?? Also published in/as: Dept. Computational Science, Report 75.4, Mar. 1975.

Du:1986:DAM

[Du86] H. C. Du. Disk allocation mehods for binary Cartesian product files. *BIT (Copenhagen)*, 26(2):138–147, 1986. CODEN NBITAB.

Ducournau:2008:PHA

[Duc08] Roland Ducournau. Perfect hashing as an almost perfect subtype test. *ACM Transactions on Programming Languages and Systems*, 30(6): 33:1–33:56, October 2008. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic).

Dumey:1956:IRR

[Dum56] Arnold I. Dumey. Indexing for rapid random access memory systems. *Computers and Automation*, 5(12): 6–9, December 1956. CODEN CPAUAJ. ISSN 0010-4795, 0887-4549. First paper in open literature on hashing. First use of hashing by taking the modulus of division by a prime number. Mentions chaining for collision handling, but not open addressing. See [Ers58b] for the latter.

Duncan:1989:PPU

[Dun89a] Ray Duncan. Power programming — understanding hashing techniques. *PC Magazine*, 8(8):297–??, April 25, 1989. CODEN PCMGEP. ISSN 0888-8507.

Duncan:1989:UHT

[Dun89b] Ray Duncan. Understanding hashing techniques. *PC Magazine*, 8(8):297–??, April 17, 1989. CODEN PCMGEP. ISSN 0888-8507.

Daemen:2007:PCP

[DV07] J. Daemen and G. Van Assche. Producing collisions for PANAMA, instantaneously. In Biryukov [Bir07], pages 1–18. ISBN 3-540-74617-X (softcover). LCCN QA76.9.A25 F77 2007. URL `http://www.springerlink.com/openurl.asp?genre=book\%26isbn=978-3-540-74617-1`.

Deligiannis:2014:PRW

[DVS+14] Nikos Deligiannis, Frederik Verbist, Jürgen Slowack, Rik van de Walle, Peter Schelkens, and Adrian Munteanu. Progressively refined Wyner–Ziv video coding for visual sensors. *ACM Transactions on Sensor Networks*, 10(2):21:1–21:??, January 2014. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

DaSilva:1983:PAS

[DW83a] J. Da Silva and I. Watson. Pseudo-associative store with hardware hashing. *IEEE Proceedings*, Pt. E(1):19–24, 1983.

daSilva:1983:PSH

[dW83b] J. G. D. da Silva and I. Watson. Pseudo-associative store with hardware hashing. *IEE Proceedings, Part E: Computers and Digital Techniques*, 130(1):19–24, Jan-

uary 1983. CODEN IPETD3. ISSN 0143-7062.

Dietzfelbinger:2003:ARG

[DW03] Martin Dietzfelbinger and Philipp Woelfel. Almost random graphs with simple hash functions. In ACM [ACM03a], pages 629–638. ISBN ???? LCCN QA75.5 .A22 2003. ACM order number 508030.

Dietzfelbinger:2005:BAD

[DW05] Martin Dietzfelbinger and Christoph Weidling. Balanced allocation and dictionaries with tightly packed constant size bins. In Caires et al. [CIM+05], pages 166–178. ISBN 3-540-27580-0. LCCN ???? EUR 130.54. URL `http://www.springerlink.com/content/39gwr5b5hp6dl5hw/`; `http://www.tuilmenau.de/fakia/mdpapers.html`.

Dietzfelbinger:2007:BAD

[DW07] Martin Dietzfelbinger and Christoph Weidling. Balanced allocation and dictionaries with tightly packed constant size bins. *Theoret. Comput. Sci.*, 380(1–2): 47–68, June 21, 2007. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

DeSantis:1990:DPS

[DY90] A. De Santis and M. Yung. On the design of provably-secure cryptographic hash functions. In Damgård [Dam90a], pages 377–397. ISBN 0-387-53587-X (New York), 3-540-53587-X (Berlin). LCCN QA76.9.A25 E964 1990. DM69.00.

DeSantis:1991:DPS

[DY91] A. De Santis and M. Yung. On the design of provably-secure cryptographic hash functions. In Damgård [Dam91], pages 377–397. CODEN LNCSD9. ISBN 0-387-53587-X (New York), 3-540-53587-X (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1990. DM69.00.

Ding:2008:MPH

[DY08] Jintai Ding and Bo-Yin Yang. Multivariates polynomials for hashing. *Lecture Notes in CS*, 4990: 358–371, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-79499-8_28`.

Ehdaie:2016:HCR

[EAA+16] Mohammad Ehdaie, Nikos Alexiou, Mahmoud Ahmadian, Mohammad Reza Aref, and Panos Papadimitratos. 2D hash chain robust random key distribution scheme. *Information Processing Letters*, 116(5):367–372, May 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119

(electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019015002239`.

Esmat:2022:PHB

[EASR22] Aghaee-Meybodi Esmat, Nezarat Amin, Emadi Sima, and Ghaffari Mohammad Reza. A parallel hash-based method for local sequence alignment. *Concurrency and Computation: Practice and Experience*, 34(3):e6568:1–e6568:??, February 1, 2022. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Elleithy:1991:VIS

[EBD91] K. M. Elleithy, M. A. Bayoumi, and L. M. Delcambre. VLSI implementation of a systolic database machine for relational algebra and hashing. *Integration, the VLSI journal*, 11(2):169–??, April 1, 1991. CODEN IVJODL. ISSN 0167-9260.

Ecker:1974:BRG

[Eck74a] A. Ecker. Eine Bemerkung zum Restklassenhash. (German) [Remark on the division hash code]. *Angewandte Informatik/Applied Informatics*, 16(6):253–256, June 1974. CODEN AWIFA7.

Ecker:1974:PSQ

[Eck74b] A. Ecker. Period of search for the quadratic and related hash methods. *The Computer Journal*, 17(4):340–343, November 1974. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Enbody:1988:DHS

[ED88] R. J. Enbody and H. C. Du. Dynamic hashing schemes. *ACM Computing Surveys*, 20 (2):85–113, June 1988. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Ege:1986:DIG

[EE86] A. Ege and C. A. Ellis. Design and implementation of GORDION, an object base management system. Technical Report STP-172-86, Software Technology Program, MCC, Austin, TX, USA, May 1986. 1–22 pp.

Epstein:2012:AEA

[EF12] Leah Epstein and Paolo Ferragina, editors. *Algorithms – ESA 2012: 20th Annual European Symposium, Ljubljana, Slovenia, September 10–12, 2012. Proceedings*, volume 7501 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. CODEN LNCSD9. ISBN 3-642-33089-4 (soft cover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL `http://www.springerlink.`

com/content/978-3-642-33089-6/.

Eiras-Franco:2020:FDN

[EFMRK+20] Carlos Eiras-Franco, David Martínez-Rego, Leslie Kanthan, César Piñeiro, Antonio Bahamonde, Bertha Guijarro-Berdiñas, and Amparo Alonso-Betanzos. Fast distributed k NN graph construction using auto-tuned locality-sensitive hashing. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 11(6):71:1–71:18, November 2020. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic). URL https://dl.acm.org/doi/10.1145/3408889.

Essex:2012:HTE

[EH12] Aleksander Essex and Urs Hengartner. Hover: Trustworthy elections with hash-only verification. *IEEE Security & Privacy*, 10(5):18–24, September/October 2012. ISSN 1540-7993 (print), 1558-4046 (electronic).

Elghamrawy:2017:PFC

[EH17] Sally M. Elghamrawy and Aboul Ella Hassanien. A partitioning framework for Cassandra NoSQL database using Rendezvous hashing. *The Journal of Supercomputing*, 73(10):4444–4465, October 2017. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Ehrig:1980:AIA

[EjKMP80] Hartmut Ehrig, H. j. Kreowski, B. Mahr, and P. Padawitz. Algebraic implementation of abstract data types. Technical report, ????, Berlin, Germany, 1980. ?? pp.

Engelmann:1993:SBC

[EK93] Curd Engelmann and Jörg Keller. Simulation-based comparison of hash functions for emulated shared memory. In Bode et al. [BRW93], pages 1–11. ISBN 0-387-56891-3 (New York), 3-540-56891-3 (Berlin). LCCN QA76.58 .I564 1993.

Elder:1984:CDP

[Eld84] John Elder. *Construction of Data Processing Software*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1984. ISBN 0-13-168675-5. xiv + 432 pp. LCCN QA76.6 .E434 1984. US$22.95. Presents code in Pascal Plus and COBOL for a wide variety of algorithms, including hashing.

Ellzey:1982:DSC

[Ell82] Roy S. Ellzey. *Data Structures for Computer Information Systems*. Science Research Associates, Inc., Chicago, IL, USA, 1982. ISBN 0-574-21400-3. xii + 270 pp. LCCN QA 76.9 D35

E44 1982. US$22.95. Undergraduate textbook treatment of hashing.

Ellis:1983:EHC

[Ell83] Carla Schlatter Ellis. Extendible hashing for concurrent operations and distributed data. In ACM-PODS'83 [ACM83b], pages 106–116. ISBN 0-89791-097-4. LCCN QA76.9.D3 A15 1983. US$25.00. ACM (order n 475830). Baltimore, MD, USA.

Ellis:1985:CLH

[Ell85a] C. Ellis. Concurrency and linear hashing. In ACM-PODS'85 [ACM85b], page 1. ISBN 0-89791-153-9. LCCN QA 76.9 D3 A296 1985.

Ellis:1985:DDS

[Ell85b] Carla Schlatter Ellis. Distributed data structures: a case study. *IEEE Transactions on Computers*, C-34(12):1178–1185, December 1985. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Ellis:1987:CLH

[Ell87] Carla Schlatter Ellis. Concurrency in linear hashing. *ACM Transactions on Database Systems*, 12(2): 195–217, June 1987. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). Also published in [ACM85b].

Ellis:1988:CEH

[Ell88] Carla Schlatter Ellis. Concurrency in extendible hashing. *Information system*, 13(1):97–109, January 1988. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Erlingsson:2007:CPA

[EMM07] Ulfar Erlingsson, Mark Manasse, and Frank McSherry. A cool and practical alternative to traditional hash tables. Report, Microsoft Research, Mountain View, CA, USA, March 27, 2007. URL `http://www.ru.is/faculty/ulfar/CuckooHash.pdf`.

Englert:1994:NSS

[Eng94] Susanne Englert. NonStop SQL: Scalability and availability for decision support. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 23(2): 491, June 1994. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Etzel:1999:SHF

[EPR99] M. Etzel, S. Patel, and Z. Ramzan. Square hash: Fast message authentication via optimized universal hash functions. In Wiener [Wie99], pages 234–251. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar. URL

http://link.springer-ny.com/link/service/series/0558/bibs/1666/16660234.htm; http://link.springer-ny.com/link/service/series/0558/papers/1666/16660234.pdf.

[Ers58b]

Er:1986:UTI

[Er86] M. C. Er. The use of termination indicators in computer programming. *The Computer Journal*, 29(5): 430–433, October 1986. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_05/tiff/430.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_05/tiff/431.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_05/tiff/432.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_29/Issue_05/tiff/433.tif.

Ershov:1958:PAO

[Ers58a] Andrei P. Ershov. On programming of arithmetic operations. *Communications of the Association for Computing Machinery*, 1(8): 3–6, August 1958. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). English translation of [Ers58b].

Ershov:1958:PPB

Andrei P. Ershov. Programming programs for the BESM [Moscow]. *Doklady Adak. Nauk SSSR*, 118 (??):427–430, 1958. CODEN DANKAS. ISSN 0002-3264. Rediscovery and first publication of linear open addressing. See [ABRS53, Dum56]. English translation in [Ers58a].

Estebanez:2014:PMC

[ESRI14] César Estébanez, Yago Saez, Gustavo Recio, and Pedro Isasi. Performance of the most common non-cryptographic hash functions. *Software—Practice and Experience*, 44(6):681–698, June 2014. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Eugenides:1990:ESM

[Eug90] J. G. Eugenides. Easier strings for the Mac. Get a handle on Mac strings with this C++ class. *Byte Magazine*, 15(13):349–350, 352, December 1990. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Estan:2006:BAC

[EVF06] Cristian Estan, George Varghese, and Michael Fisk. Bitmap algorithms for counting active flows on high-speed

links. *IEEE/ACM Transactions on Networking*, 14(5): 925–937, October 2006. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Fotakis:2003:SEH

[F+03] D. Fotakis et al. Space efficient hash tables with worst case constant access time. In Alt and Habib [AH03], pages 271–283. CODEN LNCSD9. ISBN 3-540-00623-0 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA75.5 .S956 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2607.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2607`. Also available via the World Wide Web.

Fabry:1974:CBA

[Fab74] Robert S. Fabry. Capability-based addressing. *Communications of the Association for Computing Machinery*, 17 (7):403–412, July 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Fairouz:2021:HAH

[FAFK21] Abbas A. Fairouz, Monther Abusultan, Viacheslav V. Fedorov, and Sunil P. Khatri. Hardware acceleration of hash operations in modern microprocessors. *IEEE Transactions on Computers*, 70(9):1412–1426, September 2021. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Fahlman:1980:HIS

[Fah80] S. E. Fahlman. The hashnet interconnection scheme. Technical Report CMU-CS-80-125, Department of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 1980. ?? pp.

Faloutsos:1985:MHU

[Fal85a] C. Faloutsos. Multiattribute hashing using gray codes. *ACM Computing Surveys*, 17 (1):??, March 1985. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). Also published in/as: ACM SIGMOD, 1986.

Faloutsos:1985:AMT

[Fal85b] Christos Faloutsos. Access methods for text. *ACM Computing Surveys*, 17(1): 49–74, March 1985. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). Also published in/as: "Multiattribute Hashing Using Gray Codes", ACM SIGMOD, 1986.

Faloutsos:1986:MHU

[Fal86] Christos Faloutsos. Multiattribute hashing using Gray codes. *SIGMOD Record (ACM Special Interest Group*

on Management of Data), 15 (2):227–238, June 1986. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Faloutsos:1988:GCP

[Fal88] Christos Faloutsos. Gray codes for partial match and range queries. *IEEE Transactions on Software Engineering*, 14(10):1381–1393, October 1988. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6184`.

Farrell:1993:CCC

[Far93] P. G. Farrell, editor. *Codes and cyphers: cryptography and coding IV: 4th Conference — December 1993, Cirencester*. International Academic Publishers, ????, 1993. ISBN 0-905091-03-5. LCCN ????

Farashahi:2014:HHC

[Far14] Reza Rezaeian Farashahi. Hashing into Hessian curves. *International Journal of Applied Cryptography. IJACT*, 3(2):139–147, 2014. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Fontayne:1987:MSR

[FB87] Yves D. Fontayne and Robert J. Bowman. *Multiple Storage Radix Hash Tree: an Improved Region Query Data Structure*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. ISBN 0-8186-0814-5. 302–305 pp. LCCN TK 7874 I3235 1987. IEEE Service Cent. Piscataway, NJ, USA.

Frakes:1992:IRD

[FBY92] William B. Frakes and Ricardo Baeza-Yates, editors. *Information Retrieval: Data Structures and Algorithms*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1992. ISBN 0-13-463837-9. viii + 504 pp. LCCN QA76.9.D351543 1992. US$56.00.

Faloutsos:1987:DPA

[FC87a] Christos Faloutsos and Stavros Christodoulakis. Description and performance analysis of signature file methods for office filing. *ACM Transactions on Office Information Systems*, 5(3):237–257, July 1987. CODEN ATOSDO. ISSN 0734-2047. URL `http://www.acm.org:80`.

Faloutsos:1987:OSE

[FC87b] Christos Faloutsos and Stavros Christodoulakis. Optimal signature extraction and information loss. *ACM Transactions on Database Systems*, 12(3):395–428, September 1987. CODEN ATDSD3. ISSN 0362-5915 (print),

1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1987-12-3/p395-faloutsos/p395-faloutsos.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1987-12-3/p395-faloutsos/`; `http://www.acm.org/pubs/toc/Abstracts/tods/214285.html`.

Fox:1990:OPM

[FCDH90] E. A. Fox, Q. F. Chen, A. M. Daoud, and L. S. Heath. Order preserving minimal perfect hash functions and information retrieval. In Vidick [Vid90], page 279. ISBN 0-89791-408-2. LCCN QA76.9.D3I5588 1990, Z 699 A1 I582 1990.

Fox:1991:OPM

[FCDH91] Edward A. Fox, Qi Fan Chen, Amjad M. Daoud, and Lenwood S. Heath. Order preserving minimal perfect hash functions and information retrieval. *ACM Transactions on Information Systems*, 9(3):281–308, July 1991. CODEN ATISET. ISSN 1046-8188. URL `http://www.acm.org:80`. Special Issue on Research and Development in Information Retrieval.

Fox:1992:FAC

[FCH92] E. A. Fox, Q. F. Chen, and L. S. Heath. A faster algorithm for constructing minimal perfect hash functions. In Belkin et al. [BIP92], pages 266–273. ISBN 0-89791-523-2 (paperback), 0-89791-524-0 (hardcover). LCCN Z699.A1 I659 1992.

Fox:1988:MCE

[FCHD88] Edward A. Fox, Qi-Fan Chen, Lenwood Heath, and Sanjeev Datta. A more cost effective algorithm for finding perfect hash functions. Technical Report TR 88-30, Department of Computer Science, Virginia Polytechnic Institute and State University, Blacksburg, VA 24061-0106, USA, 1988. 11 pp. Electronic mail to `fox@fox.cs.vt.edu`.

Fox:1989:MCE

[FCHD89] Edward A. Fox, Qi-Fan Chen, Lenwood Heath, and Sanjeev Datta. A more cost effective algorithm for finding perfect hash functions. In Riehl [Rie89], pages 114–122. ISBN 0-89791-299-3. LCCN QA75.5 .A1371 1989. US$36.00.

Fondrat:1986:PCQ

[FDL86] C. Fondrat, P. Dessen, and P. Le Beux. Principle of codification for quick comparisons with the entire biomolecule databanks and associated programs in FORTRAN 77. *Nucleic Acids Research*, 14(1):197–204, January 10, 1986. CODEN NARHAD. ISSN 0305-1048.

Feigenbaum:1991:ACC

[Fei91] Joan Feigenbaum, editor. *Advances in Cryptology–CRYPTO '91: Proceedings*, volume 576 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1991. ISBN 0-387-55188-3 (New York), 3-540-55188-3 (Berlin). LCCN QA76.9.A25 C79 1991.

Feller:1950:IPT

[Fel50] W. Feller. *An Introduction to Probability Theory and its Applications*. John Wiley, New York, NY, USA, 1950. ??? pp. LCCN QA273 .F37. See the discussion of the birthday paradox in Section 2.3.

Felician:1987:LHI

[Fel87] Leonardo Felician. Linked hashing: an improvement of open addressing techniques for large secondary storage files. *Information system*, 12(4):385–390, 1987. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Feldman:1988:DSM

[Fel88] Michael B. Feldman. *Data Structures with Modula-2*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1988. ISBN 0-13-197344-4. xvii + 301 pp. LCCN QA76.73.M63 F45 1988. US$40.00. Includes chapter on hash tables.

Forman:2009:EDL

[FES09] George Forman, Kave Eshghi, and Jaap Suermondt. Efficient detection of large-scale redundancy in enterprise file systems. *Operating Systems Review*, 43(1):84–91, January 2009. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Franco:1990:TFL

[FF90] John Franco and Daniel P. Friedman. Towards a facility for lexically scoped, dynamic mutual recursion in Scheme. *Computer Languages*, 15(1): 55–64, ???? 1990. CODEN COLADA. ISSN 0096-0551 (print), 1873-6742 (electronic).

Fleischmann:2009:TFS

[FFGL09] Ewan Fleischmann, Christian Forler, Michael Gorski, and Stefan Lucks. Twister — a framework for secure and fast hash functions. *Lecture Notes in CS*, 5451:257–273, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-00843-6_23`.

Fleischmann:2010:TFS

[FFGL10] Ewan Fleischmann, Christian Forler, Michael Gorski, and Stefan Lucks. TWISTERπ

— a framework for secure and fast hash functions. *International Journal of Applied Cryptography. IJACT*, 2(1):68–81, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Freire:2007:BHB

[FFGOG07] Manuel R. Freire, Julian Fierrez, Javier Galbally, and Javier Ortega-Garcia. Biometric hashing based on genetic selection and its application to on-line signatures. *Lecture Notes in CS*, 4642:1134–1143, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-74549-5_118`.

Figini:1984:ACH

[FFPV84] E. Figini, C. A. Folda, M. Panti, and S. Valenti. An algorithm for constructing hash tables (in Italian). *Rivista di Informatica (Milano)*, 14(2):185–196, April–June 1984. ISSN 0390-668X.

Farashahi:2013:IDH

[FFS+13] Reza R. Farashahi, Pierre-Alain Fouque, Igor E. Shparlinski, Mehdi Tibouchi, and J. Felipe Voloch. Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. *Mathematics of Computation*, 82(281): 491–512, January 2013. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/journals/mcom/2013-82-281/S0025-5718-2012-02606-8; http://www.ams.org/journals/mcom/2013-82-281/S0025-5718-2012-02606-8/S0025-5718-2012-02606-8.pdf`.

Fisteus:2010:HCN

[FGFK10] Jesus Arias Fisteus, Norberto Fernández García, Luis Sánchez Fernández, and Carlos Delgado Kloos. Hashing and canonicalizing notation 3 graphs. *Journal of Computer and System Sciences*, 76(7):663–685, November 2010. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0022000010000048`.

Files:1969:IRS

[FH69] John R. Files and Harry D. Huskey. An information retrieval system based on superimposed coding. In AFIPS FJCC '69 [AFI69], page ?? LCCN TK7885.A1 J6 1969.

Fortune:1979:NRN

[FH79] Steve Fortune and John Hopcroft. A note on Rabin's nearest-neighbor algorithm. *Information Processing Letters*, 8(1):20–23, January 2, 1979. CO-

DEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Fateman:1996:SLB

[FH96] Richard J. Fateman and Mark Hayden. Speeding up Lisp-Based symbolic mathematics. *SIGSAM Bulletin (ACM Special Interest Group on Symbolic and Algebraic Manipulation)*, 30(1): 25–30, March 1996. CODEN SIGSBZ. ISSN 0163-5824 (print), 1557-9492 (electronic).

Fuji-Hara:2015:PHF

[FH15] Ryoh Fuji-Hara. Perfect hash families of strength three with three rows from varieties on finite projective geometries. *Designs, Codes, and Cryptography*, 77(2–3):351–356, December 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-015-0052-z`.

Fox:1989:LAF

[FHC89] E. A. Fox, L. Heath, and Q. Chen. An O(n log n) algorithm for finding minimal perfect hash functions. Technical Report TR 89-10, Department of Computer Science, Virginia Polytechnic Institute and State University, Blacksburg, VA 24061-0106, USA, 1989. ?? pp.

Fox:1992:MPH

[FHCD92a] Edward A. Fox, Lenwood S. Heath, Qi Fan Chen, and Amjad M. Daoud. Minimal perfect hash functions for large databases. *Communications of the Association for Computing Machinery*, 35 (1):105–121, January 1992. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). This is the first published algorithm for computing minimal perfect hash functions for lists of millions of words; previous algorithms were computationally infeasible for more than a few hundred words.

Fox:1992:PMP

[FHCD92b] Edward A. Fox, Lenwood S. Heath, Qi Fan Chen, and Amjad M. Daoud. Practical minimal perfect hash functions for large databases. *Communications of the Association for Computing Machinery*, 35(1):105–121, January 1992. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/129623.html`. This is the first published algorithm for computing minimal perfect hash functions for lists of millions of words; previous algorithms were computationally infeasible for more than a few hundred words.

Fan:2019:DSP

[FHL+19] Wenfei Fan, Chunming Hu, Muyang Liu, Ping Lu, Qiang Yin, and Jingren Zhou. Dynamic scaling for parallel graph computations. *Proceedings of the VLDB Endowment*, 12(8):877–890, April 2019. CODEN ???? ISSN 2150-8097.

Frieder:1985:LSP

[FHMU85] Gideon Frieder, Gabor T. Herman, Craig Meyer, and Jayaram Udupa. Large software problems for small computers: an example from medical imaging. *IEEE Software*, 2(5):37–47, September 1985. CODEN IESOEG. ISSN 0740-7459 (print), 0740-7459 (electronic).

Filiol:2002:NST

[Fil02] Eric Filiol. A new statistical testing for symmetric ciphers and hash functions. Technical report, ESAT — Virology and Cryptology Lab, B.P. 18 35998 Rennes, FRANCE, July 23, 2002. 14 pp. URL `http://eprint.iacr.org/2002/099/`. Cryptology ePrint Archive, Report 2002/099.

FIPS:1993:SHS

[FIP93] FIPS (Federal Information Processing Standards Publication). *Secure Hash Standard: FIPS PUB 180, May 11, 1993*. United States Government Printing Office, Washington, DC, USA, May 11 1993. ?? pp.

FIPS:2002:KHM

[FIP02a] FIPS. *The Keyed-Hash Message Authentication Code (HMAC)*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, March 6, 2002. vii + 13 pp. URL `http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf`.

FIPS:2002:SHS

[FIP02b] FIPS. *Secure Hash Standard*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, August 1, 2002. iv + 79 pp. URL `http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf`.

Fischer:1987:FMP

[Fis87] James R. Fischer, editor. *Frontiers of massively parallel scientific computation: proceedings of the first symposium sponsored by the National Aeronautics and Space Administration, Washington, DC., and the Goodyear Aerospace Corporation, Akron, Ohio, and held at NASA Goddard Space Flight Center, Greenbelt, MD, September 24–25, 1986*. National Aeronautics and Space Administration,

Washington, DC, USA, 1987. LCCN QA76.5 .F755 1987.

Field:2013:UCT

[FJ13] Rebecca E. Field and Brant C. Jones. Using carry-truncated addition to analyze add-rotate-xor hash algorithms. *Journal of Mathematical Cryptology*, 7(2):97–110, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Fredman:1984:SSS

[FK84] M. L. Fredman and J. Komlòs. On the size of separating systems and families of perfect hash functions. *SIAM Journal of Algebraic Discrete Methods*, 5(1):61–68, March 1984. CODEN SJAMDU. ISSN 0196-5212 (print), 2168-345X (electronic).

Fu:1989:CCN

[FK89] A. Fu and T. Kameda. Concurrency control of nested transactions accessing B-trees. In ACM [ACM89a], pages 270–285. ISBN 0-89791-308-6. LCCN QA 76.9 D3 A26 1989. URL `http://www.acm.org/pubs/articles/proceedings/pods/73721/p270-fu/p270-fu.pdf`; `http://www.acm.org/pubs/citations/proceedings/pods/73721/p270-fu/`; `http://www.acm.org:80/pubs/citations/proceedings/pods/73721/p270-fu/`.

Fujiwara:2021:FAA

[FKI+21] Yasuhiro Fujiwara, Sekitoshi Kanai, Yasutoshi Ida, Atsutoshi Kumagai, and Naonori Ueda. Fast algorithm for anchor graph hashing. *Proceedings of the VLDB Endowment*, 14(6):916–928, February 2021. CODEN ???? ISSN 2150-8097. URL `https://dl.acm.org/doi/10.14778/3447689.3447696`.

Fredman:1984:SST

[FKS84] Michael L. Fredman, János Komlós, and Endre Szemerédi. Storing a sparse table with $O(1)$ worst case access time. *Journal of the Association for Computing Machinery*, 31(3):538–544, July 1984. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). Extends the work of Tarjan and Yao [TY79], using a two-level data structure, the first containing pointers to the second, and the second containing blocks accessible by a perfect hashing function.

Feldman:1973:CBS

[FL73] J. A. Feldman and J. R. Low. Comment on Brent's scatter storage algorithm. *Communications of the Association for Computing Machinery*, 16 (11):??, November 1973. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Fan:2004:DBS

[FL04] C. I. Fan and C. L. Lei. Divisible blind signatures based on hash chains. *International Journal of Computer Applications*, 26(1):1–9, 2004. CODEN IJCAFW. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.1080/1206212X.2004.11441718`.

Fischlin:2008:MPP

[FL08] Marc Fischlin and Anja Lehmann. Multi-property preserving combiners for hash functions. *Lecture Notes in CS*, 4948:375–392, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-78524-8_21`.

Flajolet:1981:PEE

[Fla81] P. Flajolet. On the performance evaluation of extendible hashing and trie searching. Technical report, International Business Machines (IBM), San Jose, Research Laboratory (CA), October 1981. ?? pp.

Flajolet:1983:PEE

[Fla83a] Philippe Flajolet. On the performance evaluation of extendible hashing and trie searching. *Acta Informatica*, 20(4):345–369, ???? 1983. CODEN AINFA2. ISSN 0001-5903 (print), 1432-0525 (electronic).

Flajolet:1983:PC

[Fla83b] Philippe Flajolet. Probabilistic counting. *Annual Symposium on Foundations of Computer Science (Proceedings)*, pages 76–82, 1983. CODEN ASFPDV. ISBN 0-8186-0508-1. ISSN 0272-5428. IEEE Service Cent. Piscataway, NJ, USA.

Fernandez:2011:HWS

[FLF11] David Fernández, Josep Lladós, and Alicia Fornés. Handwritten word spotting in old manuscript images using a pseudo-structural descriptor organized in a hash structure. *Lecture Notes in CS*, 6669:628–635, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-21257-4_78`.

Flores:1977:DSM

[Flo77] Ivan Flores. *Data Structure and Management*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, second edition, 1977. ISBN 0-13-197335-5. ix + 390 pp. LCCN QA76.9.D35 F57 1977. US$17.50.

Floyd:1987:HHP

[Flo87] Edwin T. Floyd. Hashing for high-performance searching.

Dr. Dobbs Journal, 12(2):34–??, February 1987. CODEN DDJTEQ. ISSN 0888-3076.

Fischlin:2008:RMP

[FLP08] Marc Fischlin, Anja Lehmann, and Krzysztof Pietrzak. Robust multi-property combiners for hash functions revisited. *Lecture Notes in CS*, 5126:655–666, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-70583-3_53.

Fischlin:2014:RMP

[FLP14] Marc Fischlin, Anja Lehmann, and Krzysztof Pietrzak. Robust multi-property combiners for hash functions. *Journal of Cryptology*, 27(3): 397–428, July 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9148-7.

Ferguson:2010:SHF

[FLS+10] Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein hash function family. Report, (various), October 1, 2010. ii + vi + 92 pp. URL http://en.wikipedia.org/wiki/Skein_(hash_function); http://www.skein-hash.info/sites/default/files/skein1.3.pdf.

Flynn:1992:ORU

[Fly92] P. J. Flynn. 3D object recognition using invariant feature indexing of interpretation tables. *Computer Vision, Graphics, and Image Processing. Image Understanding*, 55(2):119–129, March 1992. CODEN CIUNEJ. ISSN 1049-9660.

Flajolet:1985:PCA

[FM85] Philippe Flajolet and G. N. Martin. Probabilistic counting algorithms for data base applications. *Journal of Computer and System Sciences*, 31(2):182–209, September 1985. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic).

Faloutsos:1989:DUE

[FM89] C. Faloutsos and D. Metaxas. Declustering using error correcting codes. In ACM [ACM89a], pages 253–258. ISBN 0-89791-308-6. LCCN QA 76.9 D3 A26 1989. URL http://www.acm.org/pubs/articles/proceedings/pods/73721/p253-faloutsos/p253-faloutsos.pdf; http://www.acm.org/pubs/citations/proceedings/pods/73721/p253-faloutsos/; http://www.acm.org:80/pubs/citations/proceedings/pods/73721/p253-faloutsos/.

Faudemay:1991:AAL

[FM91] Pascal Faudemay and Mongia Mhiri. An associative accelerator for large databases. *IEEE Micro*, 11(6):22–34, November/December 1991. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Farach:1996:PHS

[FM96] M. Farach and S. Muthukrishnan. Perfect hashing for strings: Forrealization and algorithms. *Lecture Notes in CS*, 1075:130–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Franklin:2002:PAS

[FMA02] Michael Franklin, Bongki Moon, and Anastassia Ailamaki, editors. *Proceedings of the ACM SIGMOD International Conference on Management of Data, June 3–6, 2002, Madison, WI, USA*. ACM Press, New York, NY 10036, USA, 2002. ISBN ???? LCCN ???? ACM order number 475020.

Frieze:2009:ARW

[FMM09] Alan Frieze, Páll Melsted, and Michael Mitzenmacher. An analysis of random-walk cuckoo hashing. In Dinur et al. [DJNR09], pages 490–503. ISBN 3-642-03684-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA75.5 .I643 2009. URL `http://www.springerlink.com/content/vr67337v41pn1055/`.

Frieze:2011:ARW

[FMM11] Alan Frieze, Páll Melsted, and Michael Mitzenmacher. An analysis of random-walk cuckoo hashing. *SIAM Journal on Computing*, 40 (2):291–308, ???? 2011. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sicomp/resource/1/smjcat/v40/i2/p291_s1`.

Faezipour:2009:HPE

[FNP09] Miad Faezipour, Mehrdad Nourani, and Rina Panigrahy. A hardware platform for efficient worm outbreak detection. *ACM Transactions on Design Automation of Electronic Systems.*, 14 (4):49:1–49:??, August 2009. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Fagin:1979:EHF

[FNPS79] Ronald Fagin, Jurg Nievergelt, Nicholas Pippenger, and H. Raymond Strong. Extendible hashing — a fast access method for dynamic files. *ACM Transactions on Database Systems*, 4(3): 315–344, September 1979. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644

(electronic). Also published in/as: IBM Research Report RJ2305, Jul. 1978. See also [Reg85].

Fiat:1988:NOH

[FNSS88] A. Fiat, M. Naor, J. P. Schmidt, and A. Siegel. Nonoblivious hashing. In ACM-TOC'88 [ACM88b], pages 367–376. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988.

Fiat:1992:NH

[FNSS92] Amos Fiat, Moni Naor, Jeanette P. Schmidt, and Alan Siegel. Nonoblivious hashing. *Journal of the Association for Computing Machinery*, 39 (4):764–782, October 1, 1992. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Finin:1992:IKM

[FNY92] Timothy W. Finin, Charles K. Nicholas, and Yelena Yesha, editors. *Information and knowledge management: expanding the definition of 'database': First International Conference, CIKM '92, Baltimore, Maryland, USA, November 8–11, 1992: select papers*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992. ISBN 0-387-57419-0 (New York), 3-540-57419-0 (Berlin). LCCN QA76.9.D3 I5586 1992.

Forte:2009:DM

[For09] Dario Forte. The death of MD5. *Network Security*, 2009 (2):18–20, February 2009. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485809700200`.

Fox:1991:GEI

[Fox91] Edward A. Fox. Guest Editor's introduction: Standards and the emergence of digital multimedia systems. *Communications of the Association for Computing Machinery*, 34(4):26–29, April 1991. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/103086.html`. See [FHCD92b].

Frost:1982:FGN

[FP82] R. A. Frost and M. M. Peterson. A function for generating nearly balanced binary search trees from sets of non-random keys. *Software—Practice and Experience*, 12 (2):163–168, February 1982. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Fateman:1989:SDS

[FP89a] R. J. Fateman and C. G. Ponder. Speed and data structures in computer algebra systems. *SIGSAM*

Bulletin (ACM Special Interest Group on Symbolic and Algebraic Manipulation), 23 (2):8–11, April 1989. CODEN SIGSBZ. ISSN 0163-5824 (print), 1557-9492 (electronic).

Fotouhi:1989:OSS

[FP89b] F. Fotouhi and S. Pramanik. Optimal secondary storage access sequence for performing relational join. *IEEE Transactions on Knowledge and Data Engineering*, 1(3): 318–328, September 1989. CODEN ITKEEH. ISSN 1041-4347.

Fountoulakis:2010:ORH

[FP10] Nikolaos Fountoulakis and Konstantinos Panagiotou. Orientability of random hypergraphs and the power of multiple choices. In Abramsky et al. [AGK+10], pages 348–359. CODEN LNCSD9. ISBN 3-642-14164-1 (vol. 1: paperback), 3-642-14161-7 (vol. 2: paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267 .I55 2010. URL `http://www.springerlink.com/content/e8r0t858j8217141/`.

Fountoulakis:2013:ITC

[FPS13] Nikolaos Fountoulakis, Konstantinos Panagiotou, and Angelika Steger. On the insertion time of cuckoo hashing. *SIAM Journal on Computing*, 42(6):2156–2181, ???? 2013. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Feigenblat:2017:MWI

[FPS17] Guy Feigenblat, Ely Porat, and Ariel Shiftan. *d-k*-min-wise independent family of hash functions. *Journal of Computer and System Sciences*, 84(??):171–184, March 2017. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0022000016300848`.

Fotakis:2005:SEH

[FPSS05] D. Fotakis, R. Pagh, P. Sanders, and P. G. Spirakis. Space efficient hash tables with worst case constant access time. *Theory of Computing Systems*, 38(2):229–248, ???? 2005. CODEN TCSYFI. ISSN 1432-4350 (print), 1433-0490 (electronic). URL `????`.

Flajolet:1998:ALP

[FPV98] Philippe Flajolet, Patricio V. Poblete, and Alfredo Viola. On the analysis of linear probing hashing. *Algorithmica*, 22(4): 490–515, December 1998. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL `http://link.springer.de/link/`

service/journals/00453/bibs/22n4p490.html; http://www.springerlink.com/openurl.asp?genre=article&issn=0178-4617&volume=22&issue=4&spage=490. Average-case analysis of algorithms.

Feldman:1969:ABA

[FR69] Jerome A. Feldman and Paul D. Rovner. An Algol-based associative language. *Communications of the Association for Computing Machinery*, 12(8):439–449, August 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Franklin:2004:ACC

[Fra04] Matt Franklin, editor. *Advances in Cryptology — CRYPTO 2004: 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15–19, 2004. Proceedings*, volume 3152 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Ferreira:2011:LHB

[FRB11] Kurt B. Ferreira, Rolf Riesen, and Ron Brighwell. libhashckpt: Hash-based incremental checkpointing using GPU's. *Lecture Notes in CS*, 6960: 272–281, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-24449-0_31.

Freeman:1990:ICP

[Fre90] Herbert Freeman, editor. *10th International Conference on Pattern Recognition: 16–21 June 1990, Atlantic City, New Jersey, USA: Proceedings*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. ISBN 0-8186-2062-5 (v.1, paperback), 0-8186-2063-3 (v.2, paperback), 0-8186-6062-7 (v.1, microfiche), 0-8186-6063-5 (v.2, microfiche), 0-8186-9062-3 (v.1, hardcover), 0-8186-9063-1 (v.2, hardcover). LCCN TK7882.P3 I58 1990. Two volumes.

Friemel:1986:DM

[Fri86] Andrea Friemel. Dateistrukturen fuer mehrschluesselzugriff. Studienarbeit, 1986.

Frost:1981:ADI

[Fro81] R. A. Frost. Algorithm 112: Dumping the index of a dynamic hash table. *The Computer Journal*, 24 (4):383–384, November 1981. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_24/Issue_04/tiff/383.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_24/Issue_04/tiff/384.tif`. Discusses the dynamic hashing scheme used by ASDAS, under development at Strathclyde University.

Frost:1982:BRS

[Fro82] R. A. Frost. Binary-relational storage structures. *The Computer Journal*, 25 (3):358–367, August 1982. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_25/Issue_03/tiff/358.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_25/Issue_03/tiff/359.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_25/Issue_03/tiff/360.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_25/Issue_03/tiff/361.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_25/Issue_03/tiff/362.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_25/Issue_03/tiff/363.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_25/Issue_03/tiff/364.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_25/Issue_03/tiff/365.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_25/Issue_03/tiff/366.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_25/Issue_03/tiff/367.tif`. Discusses the dynamic hashing scheme used by ASDAS, under development at Strathclyde University.

Fraenkel:1994:EMD

[FRS94] Aviezri S. Fraenkel, Edward M. Reingold, and Prashant Saxena. Efficient management of dynamic tables. *Information Processing Letters*, 50(1):25–30, April 8, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Flajolet:1982:BPA

[FS82] P. Flajolet and J.-M. Steyaert. A branching process arising in dynamic hashing, trie searching and polynomial factorization. In Nielsen and Schmidt [NS82], pages 239–251. ISBN 0-387-11576-5. LCCN QA267.A1 L43 no.140.

Fortnow:2008:IIC

[F08] Lance Fortnow and Rahul Santhanam. Infeasibility of instance compression and

succinct PCPs for NP. In ACM [ACM08b], pages 133–142. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Fiat:2009:AEA

[FS09] Amos Fiat and Peter Sanders, editors. *Algorithms, ESA 2009: 17th annual European symposium, Copenhagen, Denmark, September 7–9: proceedings*, volume 5757 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. CODEN LNCSD9. ISBN 3-642-04127-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A43 E83 2009. URL `http://www.loc.gov/catdir/enhancements/fy1208/2009933188-d.html`; `http://www.springerlink.com/content/978-3-642-04127-3/`.

Farashahi:2009:HEC

[FSV09] Reza R. Farashahi, Igor E. Shparlinski, and José Felipe Voloch. On hashing into elliptic curves. *Journal of Mathematical Cryptology*, 3 (4):353–360, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Fouque:2012:IHB

[FT12] Pierre-Alain Fouque and Mehdi Tibouchi. Indifferentiable hashing to Barreto–Naehrig curves. *Lecture Notes in CS*, 7533: 1–17, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-33481-8_1/`.

Fuerer:1988:UHV

[Für88] M. Fürer. Universal hashing in VLSI. In Reif [Rei88], pages 312–318. ISBN 0-387-96818-0. LCCN TK7874 .A338 1988. Lecture notes in computer science # 319.

Fusco:2012:RTC

[FVS12] Francesco Fusco, Michail Vlachos, and Marc Ph. Stoecklin. Real-time creation of bitmap indexes on streaming network data. *VLDB Journal: Very Large Data Bases*, 21(3):287–307, June 2012. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Friedman:1976:GCH

[FW76] Daniel P. Friedman and David S. Wise. Garbage collecting a heap which includes a scatter table. *Information Processing Letters*, 5(6):161–164, December ??, 1976. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See erratum [FW77].

Friedman:1977:EGC

[FW77] Daniel P. Friedman and David S. Wise. Erra-

tum: "Garbage Collecting a Heap Which Includes a Scatter Table". *Information Processing Letters*, 6(2): 72, April ??, 1977. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [FW76].

Feldhofer:2009:HIS

[FW09] Martin Feldhofer and Johannes Wolkerstorfer. Hardware implementation of symmetric algorithms for RFID security. In Paris Kitsos and Yan Zhang, editors, *RFID Security: Techniques, Protocols and System-on-Chip Design*, pages 373–415. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 0-387-76481-X (e-book), 0-387-76480-1 (hardcover). LCCN TK6553 .R45 2008eb. URL `http://www.springerlink.com/content/q1160h1036371331/`.

Fan:2018:HCS

[FWG18] Jingzhe Fan, Yan Wang, and Lei Guo. Hierarchical coherency sensitive hashing and interpolation with RANSAC for large displacement optical flow. *Computer vision and image understanding: CVIU*, 175(??):1–10, October 2018. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1077314218304223`.

Fang:2017:OHT

[FXWW17] Jianwu Fang, Hongke Xu, Qi Wang, and Tianjun Wu. Online hash tracking with spatio-temporal saliency auxiliary. *Computer vision and image understanding: CVIU*, 160(??):57–72, July 2017. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1077314217300565`.

Folk:1987:FSC

[FZ87] Michael J. Folk and Bill Zoellick. *File Structures: a Conceptual Toolkit*. Addison-Wesley, Reading, MA, USA, 1987. ISBN 0-201-12003-8. xxi + 538 pp. LCCN QA76.9.F5 F651 1987. US$32.95. *Computing Reviews*: "A surprisingly thorough discussion of hashing algorithms, collision resolution, and the use and performance of hashed files completes the text with chapter 11.".

Gil:1996:TMH

[GadHW96] Joseph Gil, Friedhelm Meyer auf der Heide, and Avi Wigderson. The tree model for hashing: Lower and upper bounds. *SIAM Journal on Computing*, 25(5): 936–955, ???? 1996. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Gait:1982:AEC

[Gai82] J. Gait. An algorithm for an efficient command interpreter. *Software—Practice and Experience*, 12(10):981–982, October 1982. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Gutierrez:2016:IDO

[GAS+16] Christopher N. Gutierrez, Mohammed H. Almeshekah, Eugene H. Spafford, Mikhail J. Atallah, and Jeff Avery. Inhibiting and detecting offline password cracking using ErsatzPasswords. *ACM Transactions on Privacy and Security (TOPS)*, 19(3):9:1–9:??, December 2016. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Guillemot:2010:FPT

[GB10] Sylvain Guillemot and Vincent Berry. Fixed-parameter tractability of the maximum agreement supertree problem. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 7 (2):342–353, April 2010. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Garg:2017:RMR

[GB17] Neenu Garg and Seema Bawa. RITS–MHT: Relative indexed and time stamped Merkle hash tree based data auditing protocol for cloud computing. *Journal of Network and Computer Applications*, 84 (??):1–13, April 15, 2017. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804517300668`.

Graefe:1998:HJH

[GBC98] Goetz Graefe, Ross Bunker, and Shaun Cooper. Hash joins and hash teams in Microsoft SQL server. In Gupta et al. [GSW98], pages 86–97. ISBN 1-55860-566-5. LCCN QA76.9.D3 I559 1998. URL `http://www.vldb.org/dblp/db/conf/vldb/GraefeBC98.html`. Also known as VLDB.

Gong:1994:AKD

[GBL94] Li Gong, T. A. (Thomas A.) Berson, and T. Mark A. Lomas. Authentication, key distribution, and secure broadcast in computer networks using no encryption or decryption. Technical report SRI-CSL-94-08, SRI International, Computer Science Laboratory, Menlo Park, CA, USA, 1994. 13 + 4 + 10 pp.

Gonnet:1990:AKR

[GBY90] Gaston H. Gonnet and Ricardo A. Baeza-Yates. Analysis of the Karp-Rabin string matching algorithm. *Information Processing Letters*, 34

(5):271–274, May 1990. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Gonnet:1991:HAD

[GBY91] Gaston H. Gonnet and Ricardo Baeza-Yates. *Handbook of Algorithms and Data Structures: in Pascal and C*. Addison-Wesley, Reading, MA, USA, second. edition, 1991. ISBN 0-201-41607-7. xiv + 424 pp. LCCN QA76.73.P2 G66 1991. UK£18.95.

Guh:1990:PPS

[GC90] Keh-Chang Guh and Jose Chavarria. Parallel processing strategy for computing transitive closure of a database relation. In *Proceedings — Parbase-90 International Conference on Databases, Parallel Architectures, and Their Applications (Mar 7–9 1990: Miami Beach, FL, USA)*, pages 37–43. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. IEEE catalog number 90CH2728-4.

Graefe:1995:FAU

[GC95] Goetz Graefe and Richard L. Cole. Fast algorithms for universal quantification in large databases. *ACM Transactions on Database Systems*, 20(2):187–236, June 1995. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1995-20-2/p187-graefe/p187-graefe.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1995-20-2/p187-graefe/`; `http://www.acm.org/pubs/toc/Abstracts/tods/210202.html`.

Gollapalli:2015:IRH

[GCMG15] Sujatha Das Gollapalli, Cornelia Caragea, Prasenjit Mitra, and C. Lee Giles. Improving researcher homepage classification with unlabeled data. *ACM Transactions on the Web (TWEB)*, 9(4):17:1–17:??, October 2015. CODEN ???? ISSN 1559-1131 (print), 1559-114X (electronic).

Gerber:1987:IHS

[GD87] R. H. Gerber and D. J. DeWitt. The impact of hardware and software alternatives on the performance of the gamma database machine. Technical Report CS TR 708, University of Wisconsin–Madison, Madison, WI, USA, July 1987. ?? pp.

Girdzijauskas:2010:SOH

[GDA10] Šarūnas Girdzijauskas, Anwitaman Datta, and Karl Aberer. Structured overlay for heterogeneous envi-

ronments: Design and evaluation of Oscar. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 5 (1):2:1–2:??, February 2010. CODEN ???? ISSN 1556-4665 (print), 1556-4703 (electronic).

Giatrakos:2020:OOD

[GDGK20] Nikos Giatrakos, Antonios Deligiannakis, Minos Garofalakis, and Yannis Kotidis. Omnibus outlier detection in sensor networks using windowed locality sensitive hashing. *Future Generation Computer Systems*, 110(??): 587–609, September 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X17319180`.

Gedik:2014:PFS

[Ged14] Bugra Gedik. Partitioning functions for stateful data parallelism in stream processing. *VLDB Journal: Very Large Data Bases*, 23 (4):517–539, August 2014. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Geiselmann:1995:NHF

[Gei95] W. Geiselmann. A note on the hash function of Tillich and Zemor. In Boyd [Boy95a], pages 257–263. ISBN 3-540-60693-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .C76 1995.

Geiselmann:1996:NHF

[Gei96] W. Geiselmann. A note on the hash function of Tillich and Zemor. *Lecture Notes in CS*, 1039:51–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gerber:1986:DQPa

[Ger86a] R. H. Gerber. *Dataflow Query Processing using Multiprocessor Hash-Partitioned Algorithms*. Ph.d. thesis, University of Wisconsin–Madison, Madison, WI, USA, October 1986. ?? pp.

Gerber:1986:DQPb

[Ger86b] Robert H. Gerber. Dataflow query processing using multiprocessor hash-partitioned algorithms. Technical report, University of Wisconsin–Madison, Madison, WI, USA, 1986. ?? pp.

Gerber:1995:IOX

[Ger95] Bob Gerber. Informix online XPS. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 24 (2):463, May 1995. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Gettys:2001:AAG

[Get01] Thomas Gettys. Algorithm alley: Generating perfect

hash functions. *Dr. Dobbs Journal*, 26(2):151, 153, 155, February 2001. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/ftp/2001/2001_02/aa0201.txt`.

Groner:1974:CHF

[GG74] L. H. Groner and A. L. Goel. Concurrency in hashed file access. In Rosenfeld [Ros74], page ?? ISBN 0-444-10689-8. LCCN QA 76 I615.

Gunji:1980:SHC

[GG80] Takao Gunji and Eiichi Goto. Studies on hashing — 1. a comparison of hashing algorithms with key deletion. *Journal of the Information Processing Society of Japan*, 3(1):1–12, ???? 1980. CODEN JIPRDE. ISSN 0387-6101.

Garg:1986:OPK

[GG86a] Anil K. Garg and C. C. Gotlieb. Order-preserving key transformations. *ACM Transactions on Database Systems*, 11(2):213–234, June 1986. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1986-11-2/p213-garg/p213-garg.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1986-11-2/p213-garg/`; `http://www.acm.org/pubs/toc/Abstracts/tods/5923.html`.

Griswold:1986:IIP

[GG86b] Ralph E. Griswold and Madge T. Griswold. *The Implementation of the Icon Programming Language*. Princeton University Press, Princeton, NJ, USA, 1986. ISBN 0-691-08431-9. x + 336 pp. LCCN QA76.73.I19 G76 1986. US$39.50. The hashing algorithms used in the Icon compiler are described on pp. 97–107.

Gavrila:1992:ORI

[GG92] D. M. Gavrila and F. C. A. Groen. 3D object recognition from 2D images using geometric hashing. *Pattern Recognition Letters*, 13 (4):263–278, April 1992. CODEN PRLEDG. ISSN 0167-8655 (print), 1872-7344 (electronic).

Ganguly:2004:TSE

[GGR04] Sumit Ganguly, Minos Garofalakis, and Rajeev Rastogi. Tracking set-expression cardinalities over continuous update streams. *VLDB Journal: Very Large Data Bases*, 13(4):354–369, December 2004. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Gao:2019:ERB

[GGY+19] Y. Gao, X. Gao, X. Yang, J. Liu, and G. Chen. An efficient ring-based metadata management policy for

large-scale distributed file systems. *IEEE Transactions on Parallel and Distributed Systems*, 30(9):1962–1974, September 2019. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Guo:2007:CBI

[GH07] Xin C. Guo and Dimitrios Hatzinakos. Content based image hashing via wavelet and Radon transform. *Lecture Notes in CS*, 4810:755–764, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-77255-2_91`.

Ghandeharizadeh:1993:ILS

[GHJ+93] S. Ghandeharizadeh, R. Hull, D. Jacobs, J. Castillo, M. Escobar-Molano, S. Lu, J. Luo, C. Tsang, and G. Zhou. On implementing a language for specifying active database execution models. In Agrawal et al. [ABB93], page 441. ISBN 1-55860-152-X. ISSN 0730-9317. LCCN QA76.9.D3 I61 1993.

Goldsmith:1991:SCIa

[GHK91a] Judy Goldsmith, Lane A. Hemachandra, and Kenneth Kunen. On the structure and complexity of infinite sets with minimal perfect hash functions. *Foundations of Software Technology and Theoretical Computer Science*, 11(??):??, 1991.

Goldsmith:1991:SCIb

[GHK91b] Judy Goldsmith, Lane A. Hemachandra, and Kenneth Kunen. On the structure and complexity of infinite sets with minimal perfect hash functions. *Lecture Notes in CS*, 560:212–223, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gal:2012:TBC

[GHK+12] Anna Gál, Kristoffer Arnsfelt Hansen, Michal Koucký, Pavel Pudlák, and Emanuele Viola. Tight bounds on computing error-correcting codes by bounded-depth circuits with arbitrary gates. In ACM [ACM12], pages 479–494. ISBN 1-4503-1245-4. LCCN ???? URL `http://www.gbv.de/dms/tib-ub-hannover/63314455x`..

Ghosh:1977:DBO

[Gho77] Sakti P. Ghosh. *Data Base Organization For Data Management*. Academic Press, New York, NY, USA, 1977. ISBN 0-12-281850-4. xi + 376 pp. LCCN QA76.9.F5 G47.

Ghosh:1986:DBO

[Gho86] Sakti P. Ghosh. *Data Base Organization For Data Management*. Academic Press,

New York, NY, USA, second edition, 1986. ISBN 0-12-281852-0. xiii + 487 pp. LCCN QA76.9.F5 G47 1986.

Gennaro:1999:SHS

[GHR99] R. Gennaro, S. Halevi, and T. Rabin. Secure hash-and-sign signatures without the random oracle. *Lecture Notes in CS*, 1592:123–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ghodsi:2007:ESB

[GHW07] Ali Ghodsi, Seif Haridi, and Hakim Weatherspoon. Exploiting the synergy between gossiping and structured overlays. *Operating Systems Review*, 41(5):61–66, October 2007. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Goto:1977:PHA

[GI77] E. Goto and T. Ida. Parallel hashing algorithms. *Information Processing Letters*, 6(1):8–13, 1977. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Godor:2012:HBM

[GI12] Győző Gódor and Sándor Imre. Hash-based mutual authentication protocol for low-cost RFID systems. *Lecture Notes in CS*, 7479:76–87, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32808-4_8/`.

Gibson:1990:SCD

[Gib90] J. K. Gibson. Some comments on Damgård's hashing principle. *Electronics Letters*, 26(15):1178–1179, July 19, 1990. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic).

Gibson:1991:DLH

[Gib91] J. K. Gibson. Discrete logarithm hash function that is collision free and one way. *IEE proceedings, E: Computers and digital techniques*, 138(6):407–410, November 1, 1991. CODEN IPETD3. ISSN 0143-7062.

Gilchrist:1977:IPP

[Gil77] Bruce Gilchrist, editor. *Information Processing 77: Proceedings of IFIP Congress 77, Toronto, August 8–12, 1977*. North-Holland, Amsterdam, The Netherlands, 1977. ISBN 0-7204-0755-9. LCCN ????

Gionis:1999:SSH

[GIM99] Aristides Gionis, Piotr Indyk, and Rajeev Motwani. Similarity search in high dimensions via hashing. In Atkinson

et al. [AOV+99], pages 518–529. ISBN 1-55860-615-7. LCCN QA76.9.D3 I559 1999. URL `http://www.vldb.org/dblp/db/conf/vldb/GionisIM99.html`. Also known as VLDB'99.

Grassl:2011:CTZ

[GIMS11] Markus Grassl, Ivana Ilić, Spyros Magliveras, and Rainer Steinwandt. Cryptanalysis of the Tillich–Zémor hash function. *Journal of Cryptology*, 24(1):148–156, January 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=1&spage=148`.

Girault:1987:HFU

[Gir87] Mark Girault. Hash-functions using modulo-N operations. In Chaum and Price [CP87], pages 217–226. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). LCCN QA76.9.A25 E963 1987.

Gebhardt:2005:NPV

[GIS05] M. Gebhardt, G. Illies, and W. Schindler. A note on the practical value of single hash function collisions for special file formats. In *NIST Cryptographic Hash Workshop 2005*, page ?? ????, ????, 2005. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/pki/HashWorkshop/2005/Oct31_Presentations/Illies_NIST_05.pdf`. 18 slides + 15-page paper.

Goldwasser:2002:DSN

[GJM02] Michael H. Goldwasser, David S. Johnson, and Catherine C. McGeoch, editors. *Data structures, near neighbor searches, and methodology: fifth and sixth DIMACS implementation challenges: papers related to the DIMACS challenge on dictionaries and priority queues (1995–1996) and the DIMACS challenge on near neighbor searches (1998–1999)*, volume 59 of *DIMACS series in discrete mathematics and theoretical computer science*. American Mathematical Society, Providence, RI, USA, 2002. ISBN 0-8218-2892-4 (hardcover). LCCN QA76.9.D35 D385 2002.

Graham:1979:HST

[GJR79] Susan L. Graham, William N. Joy, and O. Roubine. Hashed symbol tables for languages with explicit scope control. In ACM SIGPLAN SCC '79 [ACM79], pages 50–57. LCCN QA 76.7 A1095 v.14 pt.2.

Goto:1976:HLT

[GK76] E. Goto and Y. Kanada. Hashing lemmas on time complexities with applica-

tion to formula manipulation. In Jenks [Jen76], page ?? LCCN QA155.7.E4 A15 1976. US$20.00.

Greene:1981:MAA

[GK81] Daniel H. Greene and Donald E. Knuth. *Mathematics For the Analysis of Algorithms*. Birkhäuser, Cambridge, MA, USA; Berlin, Germany; Basel, Switzerland, 1981. ISBN 3-7643-3046-5. 107 pp. LCCN QA76.6 .G7423 1981. US$10.00.

Greene:1982:MAA

[GK82] Daniel H. Greene and Donald E. Knuth. *Mathematics for the Analysis of Algorithms*. Birkhäuser, Cambridge, MA, USA; Berlin, Germany; Basel, Switzerland, second edition, 1982. ISBN 3-7643-3102-X. 123 pp. LCCN QA76.6 .G7423 1982.

Grewe:1994:ILM

[GK94] Lynne Grewe and Avi Kak. Interactive learning of multiple attribute hash table for fast 3D object recognition. In Kak and Ikeuchi [KI94], pages 17–27. ISBN 0-8186-5310-8, 0-8186-5311-6. LCCN TA1632 .C33 1994.

Grewe:1995:ILM

[GK95] Lynne Grewe and Avinash C. Kak. Interactive learning of a multiple-attribute hash table classifier for fast object recognition. *Computer vision and image understanding: CVIU*, 61(3):387–416, May 1995. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic).

Garcia:2005:HJA

[GK05] P. Garcia and H. F. Korth. Hash-join algorithms on modern multithreaded computer architectures. Report LUCSE-05-001, Lehigh University, Bethlehem, PA, USA, ???? 2005.

Gueron:2008:VNF

[GK08] Shay Gueron and Michael E. Kounavis. Vortex: a new family of one-way hash functions based on AES rounds and carry-less multiplication. *Lecture Notes in CS*, 5222:331–340, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-85886-7_23`.

Gauravaram:2012:SAR

[GK12a] Praveen Gauravaram and Lars R. Knudsen. Security analysis of Randomize-Hash-then-Sign digital signatures. *Journal of Cryptology*, 25 (4):748–779, October 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&`

volume=25&issue=4&spage=748.

Gueron:2012:PMS

[GK12b] Shay Gueron and Vlad Krasnov. Parallelizing message schedules to accelerate the computations of hash functions. *Journal of Cryptographic Engineering*, 2(4): 241–253, November 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-012-0037-z.

Gauravaram:2010:HFU

[GKKT10] Praveen Gauravaram, John Kelsey, Lars R. Knudsen, and Søren S. Thomsen. On hash functions using checksums. *International Journal of Information Security*, 9(2): 137–151, April 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-009-0100-7.

Graham:1989:CM

[GKP89] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics*. Addison-Wesley, Reading, MA, USA, 1989. ISBN 0-201-14236-8. xiii + 625 pp. LCCN QA39.2 .G7331 1989.

Graham:1994:CM

[GKP94] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics*. Addison-Wesley, Reading, MA, USA, second edition, 1994. ISBN 0-201-55802-5. xiii + 657 pp. LCCN QA39.2 .G733 1994.

Ghosh:1973:ACW

[GL73] S. P. Ghosh and V. Y. Lum. An analysis of collisions when hashing by division. Technical Report RJ-1218, IBM Corporation, San Jose, CA, USA, May 1973.

Gonnet:1982:EHL

[GL82] G. H. Gonnet and P.-A. Larson. External hashing with limited internal storage. In ACM-PODS'82 [ACM82], pages 256–261. ISBN 0-89791-070-2. LCCN QA76.9.D3 A33 1982. US$24.00.

Gonnet:1988:EHL

[GL88] Gaston H. Gonnet and Per-Åke Larson. External hashing with limited internal storage. *Journal of the Association for Computing Machinery*, 35(1):161–184, January 1988. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Gennaro:2006:FPB

[GL06] Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange. *ACM Transactions on Information*

and System Security, 9(2): 181–234, May 2006. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Gubner:2021:OCH

[GLB21] Tim Gubner, Viktor Leis, and Peter Boncz. Optimistically compressed hash tables & strings in the USSR. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 50(1): 60–67, June 2021. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic). URL `https://dl.acm.org/doi/10.1145/3471485.3471500`.

Gong:2008:SIA

[GLC08] Zheng Gong, Xuejia Lai, and Kefei Chen. A synthetic indifferentiability analysis of some block-cipher-based hash functions. *Designs, Codes, and Cryptography*, 48(3):293–305, September 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=48&issue=3&spage=293`.

Grembowski:2002:CAH

[GLG+02] Tim Grembowski, Roar Lien, Kris Gaj, Nghi Nguyen, Peter Bellows, Jaroslav Flidr, Tom Lehman, and Brian Schott. Comparative analysis of the hardware implementations of hash functions SHA-1 and SHA-512. *Lecture Notes in CS*, 2433:75–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330075.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2433/24330075.pdf`.

Garcia:2011:CPH

[GLHL11] Ismael García, Sylvain Lefebvre, Samuel Hornus, and Anass Lasram. Coherent parallel hashing. *ACM Transactions on Graphics*, 30(6):161:1–161:??, December 2011. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Goodman:2011:SHS

[GLJ11] Eric Goodman, M. Nicole Lemaster, and Edward Jimenez. Scalable hashing for shared memory supercomputers. In Lathrop et al. [LCK11], pages 41:1–41:11. ISBN 1-4503-0771-X. LCCN ????

Gong:2017:TMR

[GLLL17] Wei Gong, Jiangchuan Liu, Kebin Liu, and Yunhao Liu. Toward more rigorous and practical cardinality estimation for large-scale RFID sys-

tems. *IEEE/ACM Transactions on Networking*, 25(3): 1347–1358, June 2017. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Rehak:2008:IAD

[GLM+10] Praveen Gauravaram, Gaëtan Leurent, Florian Mendel, María Naya-Plasencia, and Thomas Peyrin. Cryptanalysis of the 10-round hash and full compression function of SHAvite-3-512. *Lecture Notes in CS*, 6055: 419–436, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-12678-9_25`.

Graefe:1991:SVH

[GLS91] G. Graefe, A. Linville, and L. D. Shapiro. Sort versus hash revisited. Technical report CU-CS-534-91, University of Colorado at Boulder, July 1991. 25 pp.

Graefe:1994:SVH

[GLS94] G. Graefe, A. Linville, and L. D. Shapiro. Sort vs. hash revisited. *IEEE Transactions on Knowledge and Data Engineering*, 6(6):934–??, December 1, 1994. CODEN ITKEEH. ISSN 1041-4347.

Gonnet:1977:AIH

[GM77] G. Gonnet and I. Munro. The analysis of an improved hashing technique. In ACM-TOC'77 [ACM77b], pages 113–121.

Gonnet:1979:EOH

[GM79] Gaston H. Gonnet and J. Ian Munro. Efficient ordering of hash tables. *SIAM Journal on Computing*, 8(3):463–478, ???? 1979. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Gil:1991:FHP

[GM91] Joseph Gil and Yossi Matias. Fast hashing on a PRAM – designing by expectation. In SDA'91 [SDA91], pages 271–280. LCCN QA76.9.A43 A34 199. Symposium held Jan. 28–30, 1991, San Francisco, CA, USA.

Gil:1994:SFP

[GM94] J. Gil and Y. Matias. Simple fast parallel hashing. *Lecture Notes in CS*, 820: 239–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gil:1998:SFP

[GM98] Joseph Gil and Yossi Matias. Simple fast parallel hashing by oblivious execution. *SIAM Journal on Computing*, 27 (5):1348–1375, October 1998. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/29158`.

Ghaffari:2018:MSV

[GM18] Mohammad Hossein Ghaffari and Zohreh Mostaghim. More secure version of a Cayley hash function. *Groups. Complexity. Cryptology*, 10 (1):29–??, May 2018. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL `https://www.degruyter.com/view/j/gcc.2018.10.issue-1/gcc-2018-0002/gcc-2018-0002.xml`.

Garcia-Molina:1990:ASI

[GMJ90] Hector Garcia-Molina and H. V. Jagadish, editors. *Proceedings of the 1990 ACM SIGMOD International Conference on Management of Data, May 23–25, 1990, Atlantic City, NJ.* ACM Press, New York, NY 10036, USA, 1990. ISBN 0-89791-365-5. LCCN QA 76.9 D3 S53 v.19 no.2 1990.

Gardarin:1995:OFE

[GMP95] Georges Gardarin, Fernando Machuca, and Philippe Pucheral. OFL: a functional execution model for object query languages. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 24(2): 59–70, May 1995. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Gil:1990:AKC

[GMW90] Joseph Gil, Friedhelm Meyer auf der Heide, and Avi Wigderson. Not all keys can be hashed in constant time. In ACM-TOC'90 [ACM90], pages 244–253. ISBN 0-89791-361-2. LCCN ????

Gall:1980:SIA

[GN80] R. Gall and Manfred Nagl. Software-implementation assoziativer speicher. Technical report, ????, Koblenz, Germany, 1980. ?? pp.

Gutmann:2005:WHC

[GNP05] P. Gutmann, D. Naccache, and C. C. Palmer. When hashes collide [applied cryptography]. *IEEE Security & Privacy*, 3(3):68–71, May/June 2005. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `http://ieeexplore.ieee.org/iel5/8013/31002/01439506.pdf`; `http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=31002&arnumber=1439506&count=20&index=13`.

Gauravaram:2007:USC

[GO07] Praveen Gauravaram and Katsuyuki Okeya. An update on the side channel cryptanalysis of MACs based on cryptographic hash functions. *Lecture Notes in CS*, 4859:393–403, 2007. CODEN LNCSD9. ISSN 0302-

9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-77026-8_31.

Grossi:2015:FCT

[GO15] Roberto Grossi and Giuseppe Ottaviano. Fast compressed tries through path decompositions. *ACM Journal of Experimental Algorithmics*, 19(??):1.8:1–1.8:??, February 2015. CODEN ???? ISSN 1084-6654.

Goble:1975:FTR

[Gob75] C. E. Goble. A free-text retrieval system using hash codes. *The Computer Journal*, 18(1):18–20, February 1975. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/18/1/18.full.pdf+html; http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_01/tiff/18.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_01/tiff/19.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_01/tiff/20.tif.

Golshani:1992:EIC

[Gol92] Forouzan Golshani, editor. *Eighth International Conference on Data Engineering: February 2–3, 1992, Tempe, Arizona*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. ISBN 0-8186-2545-7 (paper) 0-8186-2546-5 (microfiche) 0-8186-2547-3 (hardcover). LCCN QA76.9.D3 I5582 1992.

Goldwasser:1994:P

[Gol94] Shafi Goldwasser, editor. *Proceedings: 35th Annual Symposium on Foundations of Computer Science, November 20–22, 1994, Santa Fe, New Mexico*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. CODEN ASFPDV. ISBN 0-8186-6582-3. ISSN 0272-5428. LCCN QA 76 S979 1994. IEEE catalog number 94CH35717. IEEE Computer Society Press Order Number 6580-02.

Gollmann:1996:FSE

[Gol96] Dieter Gollmann, editor. *Fast software encryption: third international workshop Cambridge, UK, February 21–23, 1996: proceedings*, volume 1039 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1996. CODEN LNCSD9. ISBN 3-540-60865-6 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 F38 1996.

Gonnet:1977:ALB

[Gon77] Gaston H. Gonnet. Average lower bounds for open-addressing hash coding. In *Proceedings of a Conference on Theoretical Computer Science*, page ?? ????, ????, 1977. Is this [TWW77]????

Gonnet:1980:OAH

[Gon80] Gaston H. Gonnet. Open-addressing hashing with unequal-probability keys. *Journal of Computer and System Sciences*, 21(??):??, 1980. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic).

Gonnet:1981:ELL

[Gon81] Gaston H. Gonnet. Expected length of the longest probe sequence in hash code searching. *Journal of the Association for Computing Machinery*, 28(2):289–304, April 1981. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Gonnet:1983:UDB

[Gon83] Gaston H. Gonnet. Unstructured data bases or very efficient text searching. In ACM-PODS'83 [ACM83b], pages 117–124. ISBN 0-89791-097-4. LCCN QA76.9.D3 A15 1983. US$25.00.

Gonnet:1984:HAD

[Gon84] Gaston H. Gonnet. *Handbook of Algorithms and Data Structures*. International Computer Science Series. Editors: A. D. McGettrick and J. van Leeuwen. Addison-Wesley, Reading, MA, USA, 1984. ISBN 0-201-14218-X. xi + 286 pp. LCCN QA76.6 .G636 1984. US$12.95.

Gong:1995:CKH

[Gon95] Li Gong. Collisionful keyed hash functions with selectable collisions. *Information Processing Letters*, 55(3):167–170, August 11, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Goto:1983:RSS

[Got83] Eiichi Goto, editor. *RIMS Symposia on Software Science and Engineering. Proceedings of the Symposia. (Kyoto, Japan, 1982)*, volume 147 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1983. ISBN 0-387-11980-9 (New York), 3-540-11980-9 (Berlin). LCCN QA76.6 .R55 1983.

Gollapudi:2008:PTM

[GP08] Sreenivas Gollapudi and Rina Panigrahy. The power of two min-hashes for similarity search among hierarchical data objects. In Lenzerini and Lembo [LL08], pages 211–220. ISBN 1-59593-685-X. LCCN ????

Gueziec:1997:MIR

[GPA97] André P. Guéziec, Xavier Pennec, and Nicholas Ayache. Medical image registration using geometric hashing. *IEEE Computational Science & Engineering*, 4(4):29–41, October/December 1997. CODEN ISCEE4. ISSN 1070-9924 (print), 1558-190X (electronic). URL `http://dlib.computer.org/cs/books/cs1997/pdf/c4029.pdf`; `http://www.computer.org/cse/cs1998/c4029abs.htm`.

Gomez-Perez:2016:CCT

[GPGO16] Domingo Gómez-Pérez, Jaime Gutierrez, and Alina Ostafe. Common composites of triangular polynomial systems and hash functions. *Journal of Symbolic Computation*, 72(??):182–195, January/February 2016. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0747717115000140`.

Gentry:2008:THL

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In ACM [ACM08b], pages 197–206. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Greene:1994:MIHa

[GPY94a] D. Greene, M. Parnas, and F. Yao. Multi-index hashing for information retrieval. In Goldwasser [Gol94], pages 722–731. CODEN ASFPDV. ISBN 0-8186-6582-3. ISSN 0272-5428. LCCN QA 76 S979 1994. IEEE catalog number 94CH35717. IEEE Computer Society Press Order Number 6580-02.

Greene:1994:MIHb

[GPY94b] D. Greene, M. Parnas, and F. Yao. Multi-index hashing for information retrieval. *Annual Symposium on Foundations of Computer Science [papers]*, 35(??):722–??, 1994. ISSN 0272-5428.

Guillou:1995:ACE

[GQ95] L. C. Guillou and J.-J. Quisquater, editors. *Advances in cryptology: EUROCRYPT '95: Workshop on the theory and application of cryptographic techniques — May 1995, Saint-Malo, France*, number 921 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. ISBN 3-540-59409-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C794 1995.

Gray:1986:IJH

[Gra86] P. M. D. Gray. Implement-

ing joins by hashing on Codasyl DBMS. In Oxborrow [Oxb86], pages 187–199. ISBN 0-521-33260-5. LCCN QA76.9.D3 B75 1986.

Graefe:1988:RDF

[Gra88] Goetz Graefe. Relational division: Four algorithms and their performance. Technical report, ????, Beaverton, OR, USA, 1988. ?? pp.

Graefe:1989:RDF

[Gra89] Goetz Graefe. Relational division: Four algorithms and their performance. In *Proceedings of the Fifth International Conference on Data Engineering*, pages 94–101. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, February 1989. ISBN 0-8186-1915-5. LCCN QA 76.9 D3 I5582 1989. Available from IEEE Service Cent. Piscataway.

Graefe:1992:QPT

[Gra92] G. Graefe. Query processing techniques for large databases. Technical Report CU-CS-579-92, Department of Computer Science, University of Colorado at Boulder, January 1992. 87 pp.

Graefe:1993:PEHa

[Gra93a] G. Graefe. Performance enhancements for hybrid hash join. Technical report, ????, 1993. ?? pp.

Graefe:1993:PEHb

[Gra93b] G. Graefe. A performance evaluation of histogram-driven recursive hybrid hash join. Technical report, ????, August 1993. ?? pp.

Graefe:1993:QET

[Gra93c] Goetz Graefe. Query evaluation techniques for large databases. *ACM Computing Surveys*, 25(2):73–170, June 1993. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Graefe:1994:DAE

[Gra94a] G. Graefe. Disk arrays for external sorting and hybrid hash join. Technical report, ????, 1994. ?? pp.

Graefe:1994:SIW

[Gra94b] G. Graefe. Sort-merge-join: An idea whose time has(h) passed? In IEEE [IEE94a], pages 406–417. ISBN 0-8186-5402-3, 0-8186-5400-7, 0-8186-5401-5. LCCN QA76.9.D3 I5582 1994.

Graefe:1994:VEP

[Gra94c] G. Graefe. Volcano, an extensible and parallel dataflow query processing system. *IEEE Transactions on Knowledge and Data Engineering (to appear)*, ??(??):??, 1994.

Graefe:1999:VMJ

[Gra99] Goetz Graefe. The value of merge-join and hash-join

in SQL server. In Atkinson et al. [AOV+99], pages 250–253. ISBN 1-55860-615-7. LCCN QA76.9.D3 I559 1999. URL `http://www.vldb.org/dblp/db/conf/vldb/Graefe99.html`. Also known as VLDB'99.

Garcia-Retuerta:2019:CTV

[GRBCC19] David García-Retuerta, Álvaro Bartolomé, Pablo Chamoso, and Juan Manuel Corchado. Counter-terrorism video analysis using hash-based algorithms. *Algorithms (Basel)*, 12(5), May 2019. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL `https://www.mdpi.com/1999-4893/12/5/110`.

Gregg:1995:HFT

[Gre95] X. Gregg. Hashing Forth: It's a topic discussed so nonchalantly that neophytes hesitate to ask how it works. *Forth Dimensions*, 17(4):13–??, 1995. CODEN FODMD5. ISSN 0884-0822.

Green:2021:HSH

[Gre21] Oded Green. HashGraph — scalable hash tables using a sparse graph data structure. *ACM Transactions on Parallel Computing (TOPC)*, 8(2):11:1–11:17, June 2021. CODEN ???? ISSN 2329-4949 (print), 2329-4957 (electronic). URL `https://dl.acm.org/doi/10.1145/3460872`.

Grech:2011:JGE

[GRF11] Neville Grech, Julian Rathke, and Bernd Fischer. JEqualityGen: generating equality and hashing methods. *SIGPLAN Notices*, 46(2):177–186, February 2011. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Grimson:1974:PSS

[Gri74] J. B. Grimson. A performance study of some directory structures for large data files. *Information Storage and Retrieval*, 10(11):??, 1974.

Griss:1977:EEE

[Gri77] Martin L. Griss. Efficient expression evaluation in sparse minor expansion, using hashing and deferred evaluation. In Sprague and Chattergy [SC77], pages 169–172. LCCN ??

Griss:1979:HKR

[Gri79] M. L. Griss. Hashing—the key to rapid pattern matching. Technical Report UUCS-79-108, Computer Science Department, University of Utah, 1979. ?? pp.

Griebel:1998:ASG

[Gri98] M. Griebel. Adaptive sparse grid multilevel methods for elliptic PDEs based on finite differences. *Computing*, 61(2):151–179, 1998. CODEN CMPTA2. ISSN

0010-485X (print), 1436-5057 (electronic). URL http://www.springer.at/journals/pdf/3571.pdf; http://www.springer.at/journals/pdf/3815.pdf.

Grosshans:1986:FSD

[Gro86] Daniel Grosshans. *File Systems: Design and Implementation*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1986. ISBN 0-13-314568-9. xiv + 482 pp. LCCN QA76.9.F5 G76 1986. US$38.95.

Gopal:1993:CCH

[GRZ93] R. D. Gopal, R. Ramesh, and S. Zionts. Criss-cross hashing by page map zoning: An efficient system for binary view generation. Technical Report Working Paper 851, SUNY Buffalo School of Management, Buffalo, NY, USA, March 1993. ?? pp.

Guibas:1976:ADH

[GS76] L. J. Guibas and E. Szemerédi. The analysis of double hashing. In Guibas & Szemeredi [ACM76], pages 187–191. Extended abstract.

Guibas:1978:ADH

[GS78] L. J. Guibas and E. Szemerédi. The analysis of double hashing. *Journal of Computer and System Sciences*, 16(2):226–274, April 1978. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic).

Gori:1989:AAC

[GS89] M. Gori and G. Soda. An algebraic approach to Cichelli's perfect hashing. *BIT (Nordisk tidskrift for informationsbehandling)*, 29(1):2–13, March 1989. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=29&issue=1&spage=2.

Girault:1994:LCH

[GS94] M. Girault and J. Stern. On the length of cryptographic hash-values used in identification schemes. *Lecture Notes in CS*, 839:202–215, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gupta:1994:RSD

[GSB94] Rajiv Gupta, Scott A. Smolka, and Shaji Bhaskar. On randomization in sequential and distributed algorithms. *ACM Computing Surveys*, 26(1):7–86, March 1994. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Goi:2001:IHF

[GSC01] B.-M. Goi, M. U. Siddiqi, and H.-T. Chuah. Incremental hash function based on pair chaining & modular

arithmetic combining. *Lecture Notes in CS*, 2247:50–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470050.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2247/22470050.pdf`.

Goto:1982:DLM

[GSI+82] E. Goto, T. Soma, N. Inada, M. Idesawa, K. Hiraki, M. Suzuki, K. Shimizu, and B. Philipov. Design of a Lisp machine – FLATS. In LFP82 [LFP82], pages 208–215. ISBN 0-89791-082-6. LCCN QA76.73.L23 A26 1982. US$26.00. The papers were not formally refereed but were accepted on the bases of extended abstracts.

Gope:2017:ASS

[GSL17] Dibakar Gope, David J. Schlais, and Mikko H. Lipasti. Architectural support for server-side PHP processing. *ACM SIGARCH Computer Architecture News*, 45 (2):507–520, May 2017. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Galli:2001:THO

[GSS01] N. Galli, B. Seybold, and K. Simon. Tetris-hashing or optimal table compression. *Discrete Applied Mathematics*, 110(1):41–58, June 1, 2001. CODEN DAMADU. ISSN 0166-218X (print), 1872-6771 (electronic).

Ganguly:1990:FPP

[GST90] Sumit Ganguly, Avi Silberschatz, and Shalom Tsur. A framework for the parallel processing of Datalog queries. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 19 (2):143–152, June 1990. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Gupta:1998:PTF

[GSW98] Ashish Gupta, Oded Shmueli, and Jennifer Widom, editors. *Proceedings of the Twenty-fourth International Conference on Very Large Databases, New York, NY, USA, 24–27 August, 1998.* Morgan Kaufmann Publishers, San Francisco, CA, 1998. ISBN 1-55860-566-5. LCCN QA76.9.D3 I559 1998. Also known as VLDB.

Greniewski:1963:ELK

[GT63] M. Greniewski and W. Turski. The external language KLIPA for the URAL-2 digital computer. *Communications of the Association for Computing Machinery*, 6(6):322–324, June 1963. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (elec-

tronic). Early work on derivation of hash functions.

Goto:1980:SHM

[GT80] Eiichi Goto and Motoaki Terashima. Studies on hashing — 3. MTAC — Mathematical Tabulative Automatic Computing. *Journal of the Information Processing Society of Japan*, 3(1): 23–30, ???? 1980. CODEN JIPRDE. ISSN 0387-6101.

Griswold:1993:DID

[GT93] William G. Griswold and Gregg M. Townsend. The design and implementation of dynamic hashing for sets and tables in Icon. *Software—Practice and Experience*, 23(4):351–367, April 1993. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Guerraoui:2016:OCO

[GT16] Rachid Guerraoui and Vasileios Trigonakis. Optimistic concurrency with OPTIK. *SIGPLAN Notices*, 51(8):18:1–18:??, August 2016. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Gaikwad:2021:PSL

[GTL21] Vishesh P. Gaikwad, Jitendra V. Tembhurne, and Cheng-Chi Lee. Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function. *The Journal of Supercomputing*, 77(8):8281–8304, August 2021. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-020-03553-y`.

Guibas:1975:HTE

[Gui75] Leo J. Guibas. Hashing techniques that exhibit secondary or tertiary clustering. In *USA-Jpn Comput Conf, 2nd, Proc*, pages 324–328. AFIPS, Montvale, NJ, 1975.

Guibas:1976:AHAa

[Gui76a] Leo J. Guibas. *The Analysis of Hashing Algorithms*. PhD thesis, Stanford University, Stanford, CA, USA, August 1976. ?? pp. See [Gui76b].

Guibas:1976:AHAb

[Gui76b] Leo J. Guibas. The analysis of hashing algorithms. Technical Report TR STAN-CS-76-556, Stanford University, Stanford, CA, USA, August 1976. ?? pp. This is the author's Ph.D. thesis, [Gui76a].

Guibas:1976:AHAc

[Gui76c] Leo J. Guibas. The analysis of hashing algorithms that exhibit k-ary clustering. In IEEE-FOCS'76 [IEE76], pages 183–196.

Guibas:1978:AHT

[Gui78] Leo J. Guibas. The analysis of hashing techniques that exhibit k-ary clustering. *Journal of the Association for Computing Machinery*, 25 (4):544–555, October 1978. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Guinier:1989:FUA

[Gui89] Daniel Guinier. A fast uniform 'astronomical' random number generator. *SIGSAC Review*, 7(1):1–13, Spring 1989. CODEN SSARE7. ISSN 0277-920X (print), 1558-0261 (electronic).

Gupta:1989:SHI

[Gup89] Govind Gupta. Sorting by hashing and inserting. In *Computing Trends in the 1990's. Proceedings 1989 ACM Seventeenth Annual Computer Science Conference (Feb 21–23 1989: Louisville, KY, USA)*, pages 409–?? ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-299-3. LCCN ????

Gurski:1973:NAK

[Gur73] Aaron Gurski. A note on analysis of keys for use in hashing. *BIT (Nordisk tidskrift for informationsbehandling)*, 13(1):120–122, 1973. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Garcia:2008:SCC

[GvR08] Flavio D. Garcia and Peter van Rossum. Sound and complete computational interpretation of symbolic hashes in the standard model. *Theoret. Comput. Sci.*, 394(1–2):112–133, March 31, 2008. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Goldreich:1994:TFF

[GW94] O. Goldreich and A. Wigderson. Tiny families of functions with random properties: a quality-size trade-off for hashing. *Proceedings of the ... annual ACM Symposium on Theory of Computing*, 26(??):574–??, 1994. ISSN 0737-8017.

Gadia:1991:IIT

[GY91] Shashi K. Gadia and Chuen-Sing Yeung. Inadequacy of interval timestamps in temporal databases. *Information Sciences*, 54(1/2):1–??, 1991. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Guo:2019:EER

[GYW+19] Y. Guo, X. Yuan, X. Wang, C. Wang, B. Li, and X. Jia. Enabling encrypted rich queries in distributed key–value stores. *IEEE Transactions on Parallel and Dis-*

tributed Systems, 30(6):1283–1297, June 2019. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Griebel:1999:PMA

[GZ99] M. Griebel and G. Zumbusch. Parallel multigrid in an adaptive PDE solver based on hashing and space-filling curves. *Parallel Computing*, 25(7):827–843, July 1999. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Guo:2014:CHS

[GZX14] Song Guo, Deze Zeng, and Yang Xiang. Chameleon hashing for secure and privacy-preserving vehicular communications. *IEEE Transactions on Parallel and Distributed Systems*, 25(11):2794–2803, November 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL `http://www.computer.org/csdl/trans/td/2014/11/06654169-abs.html`.

Hachem:1993:AAP

[Hac93] Nabil I. Hachem. An approximate analysis of the performance of extendible hashing with elastic buckets. *Information Processing Letters*, 48(1):13–20, October 1993. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Harbi:2016:ASQ

[HAK+16] Razen Harbi, Ibrahim Abdelaziz, Panos Kalnis, Nikos Mamoulis, Yasser Ebrahim, and Majed Sahli. Accelerating SPARQL queries by exploiting hash-based locality and adaptive partitioning. *VLDB Journal: Very Large Data Bases*, 25(3):355–380, June 2016. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Harbi:2015:ESQ

[HAKM15] Razen Harbi, Ibrahim Abdelaziz, Panos Kalnis, and Nikos Mamoulis. Evaluating SPARQL queries on massive RDF datasets. *Proceedings of the VLDB Endowment*, 8(12):1848–1851, August 2015. CODEN VLDBFR. ISSN 2150-8097.

Halunen:2012:MGB

[Hal12] Kimmo Halunen. Multicollisions and graph-based hash functions. *Lecture Notes in CS*, 7222:156–167, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32298-3_11/`.

Hamer:2002:HR

[Ham02] John Hamer. Hashing revisited. *SIGCSE Bulletin (ACM Special Interest Group on Computer Sci-*

ence Education), 34(3):80–83, September 2002. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Hanson:1990:PMAa

[Han90] E. N. Hanson. A predicate matching algorithm for database rule systems. Technical Report WSU-CS-90-01, Washington State University, 1990. ?? pp.

Han:2017:CPW

[Han17] Yijie Han. Construct a perfect word hash function in time independent of the size of integers. *Information Processing Letters*, 128 (??):5–10, December 2017. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019017301266`.

Harrison:1971:IST

[Har71a] M. C. Harrison. Implementation of the substring test by hashing. *Communications of the Association for Computing Machinery*, 14(12):777–779, December 1971. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See also [TT82].

Harrison:1971:DSP

[Har71b] Malcolm C. Harrison. *Data Structures and Programming*. Courant Institute of Mathematical Sciences, New York University, New York, NY, USA, April 1971. xii + 381 pp. LCCN QA76.5 .H37. See also [Har73].

Harrison:1973:DSP

[Har73] Malcolm C. Harrison. *Datastructures and Programming*. Scott, Foresman and Company, Glenview, IL, USA, 1973. ISBN 0-673-05964-2. 322 pp. LCCN QA76.6 .H37. See [Har71b].

Harris:1985:INL

[Har85] Mary Dee Harris. *Introduction to Natural Language Processing*. Reston Publishing Co. Inc., Reston, VA, USA, 1985. ISBN 0-8359-3254-0. xv + 368 pp. LCCN QA76.9.I58 H37 1985. US$27.95. Hashing is discussed in Part II.

Harbron:1988:FSS

[Har88] Thomas R. Harbron. *File Systems: Structures and Algorithms*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1988. ISBN 0-13-314709-6. xv + 254 pp. LCCN QA76.9.F5 H37 1988. US$33.00.

Harari:1997:HHF

[Har97] S. Harari. HCC: a hash function using error correcting codes. *Lecture Notes in CS*, 1355:110–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hashida:1972:AM

[Has72] O. Hashida. Analysis of multiqueue. *Rev. of the El. Commun. Lab.*, 20(??):189–199, 1972.

Hachem:1989:KSA

[HB89a] N. I. Hachem and B. P. Berra. Key-sequential access methods for very large files derived from linear hashing. In *Proceedings of the Fifth International Conference on Data Engineering*, pages 305–312. ????, Los Angeles, CA, USA, February 1989.

Hachem:1989:KAM

[HB89b] Nabil I. Hachem and P. Bruce Berra. Key-sequential access methods for very large files derived from linear hashing. In *FIFTH INTERNATIONAL CONFERENCE ON DATA ENGINEERING (Feb 6–10 1989: Los Angeles, CA, USA)*, pages 305–2. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. ISBN 0-8186-1915-5. LCCN ???? Available from IEEE Service Cent. Piscataway.

Hecker:1989:IGH

[HB89c] Yaron C. Hecker and Ruud M. Bolle. Is Geometric Hashing a Hough Transform? Technical Report RC 15202(#67767). IBM Research Division, T. J. Watson Research Center, 1989. ?? pp.

Hachem:1992:NOP

[HB92] N. I. Hachem and P. B. Berra. New order preserving access methods for very large files derived from linear hashing. *IEEE Transactions on Knowledge and Data Engineering*, 4(1):68–82, February 1, 1992. CODEN ITKEEH. ISSN 1041-4347.

Hariri:1993:PIC

[HB93] Salim Hariri and P. Bruce Berra, editors. *Proceedings of the 1993 International Conference on Parallel Processing, August 16–20, 1993/ sponsored by the Pennsylvania State University. Boca Raton, FL*, volume 3. Algorithms and applications. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 1993. ISBN 0-8493-8983-6 (set), 0-8493-8984-4 (vol. 1), 0-8493-8985-2 (vol. 2), 0-8493-8986-0 (vol. 3). LCCN QA76.58 .I55 1993.

Hecker:1994:GHG

[HB94] Y. C. Hecker and R. M. Bolle. On geometric hashing and the generalized Hough transform. *IEEE Trans. Systems, Man, and Cybernetics*, 24(9): 1328–??, September 1, 1994. CODEN ISYMAW. ISSN 0018-9472, 1083-4427.

Hulsing:2017:XEH

[HBG+17] A. Hülsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen. XMSS: Extended hash-based signatures. Web document, July 24, 2017. URL `http://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signature`.

Hoang:2010:CAN

[HBL+10] Giang Hoang, Chang Bae, John Lange, Lide Zhang, Peter Dinda, and Russ Joseph. A case for alternative nested paging models for virtualized systems. *IEEE Computer Architecture Letters*, 9(1):17–20, January/June 2010. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Horspool:1987:HCT

[HC87] R. Nigel Horspool and Gordon V. Cormack. Hashing as a compaction technique for LR parser tables. *Software—Practice and Experience*, 17(6):413–416, June 1987. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Holt:2002:MAR

[HC02] John D. Holt and Soon M. Chung. Mining association rules using inverted hashing and pruning. *Information Processing Letters*, 83(4):211–220, August 31, 2002. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Holt:2007:PMA

[HC07] John D. Holt and Soon M. Chung. Parallel mining of association rules from text databases. *The Journal of Supercomputing*, 39(3):273–299, March 2007. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=39&issue=3&spage=273`.

Hedayatpour:2011:HFB

[HC11] S. Hedayatpour and S. Chuprat. Hash functions-based random number generator with image data source. In *2011 IEEE Conference on Open Systems (ICOS)*, pages 69–73. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6079248`.

Hsiao:2013:SLB

[HC13] Hung-Chang Hsiao and Che-Wei Chang. A symmetric load balancing algorithm with performance guarantees for distributed hash tables. *IEEE Transactions on Computers*, 62(4):662–675, April 2013. CO-

DEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Healy:2014:AKM

[HC14] John Healy and Desmond Chambers. Approximate k-mer matching using fuzzy hash maps. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 11(1):258–264, January 2014. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Hart:1995:SHC

[HCF95] John C. Hart, Wayne O. Cochran, and Patrick J. Flynn. Similarity hashing: a computer vision solution to the inverse problem of linear fractals. In Anonymous [Ano95c], page ???? ISBN ???? LCCN ????

Hasan:2006:CSE

[HCJC06] Jahangir Hasan, Srihari Cadambi, Venkatta Jakkula, and Srimat Chakradhar. Chisel: a storage-efficient, collision-free hash-based network processing architecture. *ACM SIGARCH Computer Architecture News*, 34 (2):203–215, 2006. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Hanson:1990:PMAb

[HCKW90] Eric N. Hanson, Moez Chaabouni, Chang-Ho Kim, and Yu-Wang Wang. A predicate matching algorithm for database rule systems. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 19(2): 271–280, June 1990. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic). URL `http://www.acm.org/pubs/articles/proceedings/mod/93597/p271-hanson/p271-hanson.pdf`; `http://www.acm.org/pubs/citations/proceedings/mod/93597/p271-hanson/`.

Hernandez-Castro:2012:AFH

[HCPLSB12] Julio Cesar Hernandez-Castro, Pedro Peris-Lopez, Masoumeh Safkhani, and Nasour Bagheri. Another fallen hash-based RFID authentication protocol. *Lecture Notes in CS*, 7322:29–37, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-30955-7_4/`.

Hu:2021:PMH

[HCW+21] Daokun Hu, Zhiwen Chen, Jianbing Wu, Jianhua Sun, and Hao Chen. Persistent memory hash indexes: an experimental evaluation. *Proceedings of the VLDB Endowment*, 14(5): 785–798, January 2021. CODEN ???? ISSN 2150-8097. URL `https://`

dl.acm.org/doi/10.14778/3446095.3446101.

Hsiao:1994:PEM

[HCY94] Hui-I Hsiao, Ming-Syan Chen, and Philip S. Yu. On parallel execution of multiple pipelined hash joins. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 23(2): 185–196, June 1994. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Hsiao:1997:PEH

[HCY97] Hui-I Hsiao, Ming-Syan Chen, and P. S. Yu. Parallel execution of hash joins in parallel databases. *IEEE Transactions on Parallel and Distributed Systems*, 8(8): 872–883, August 1997. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL http://dlib.computer.org/td/books/td1997/pdf/l0872.pdf; http://www.computer.org/tpds/td1997/l0872abs.htm.

Hopgood:1972:QHM

[HD72] F. R. A. Hopgood and J. Davenport. The quadratic hash method when the table size is a power of 2. *The Computer Journal*, 15 (4):314–315, November 1972. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_15/Issue_04/150314.sgm.abs.html; http://www3.oup.co.uk/computer_journal/hdb/Volume_15/Issue_04/tiff/314.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_15/Issue_04/tiff/315.tif. See correspondence [PH73].

Hanna:2009:CEE

[HDCM09] Michel Hanna, Socrates Demetriades, Sangyeun Cho, and Rami Melhem. CHAP: Enabling efficient hardware-based multiple hash schemes for IP lookup. *Lecture Notes in CS*, 5550: 756–769, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-01399-7_59.

Hanna:2011:AHS

[HDCM11] Michel Hanna, Socrates Demetriades, Sangyeun Cho, and Rami Melhem. Advanced hashing schemes for packet forwarding using set associative memory architectures. *Journal of Parallel and Distributed Computing*, 71 (1):1–15, January 2011. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic).

He:1987:PAS

[He87] Guo He. *Pipelined Array Sys-*

tem for Relational Database Operations. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. ISBN 0-8186-0780-7. 795–801 pp. LCCN QA75.5 .I5761 1987. IEEE Service Cent. Piscataway, NJ, USA.

Healey:1972:CEP

[Hea72] M. J. R. Healey. Checking the execution of programs by hashing. *IBM Technical Disclosure Bulletin*, 15(7):??, December 1972. CODEN IBMTAA. ISSN 0018-8689.

Headrick:1982:HRS

[Hea82] R. Wayne Headrick. Hashing routine selection: a quantitative methodology. *Proceedings — Annual Meeting of the American Institute for Decision Sciences*, 2:401–??, 1982. CODEN PAMSED.

Hejlsberg:1989:COT

[Hej89] Anders Hejlsberg. Container object types in Turbo Pascal. *Dr. Dobbs Journal*, 14(11): 56–??, November 1, 1989. CODEN DDJOEB. ISSN 1044-789X.

Hekmatpour:1989:LPI

[Hek89] Sharam Hekmatpour. *LISP: a Portable Implementation*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1989. ISBN 0-13-537490-1. viii + 177 pp. LCCN QA 76.73 L23 H47 1989. US$54.80. Describes a hashed symbol table.

Heller:1989:EH

[Hel89] Steve Heller. Extensible hashing. *Dr. Dobbs Journal*, 14(11):66, 69–70, 116, 118, 120–121, November 1, 1989. CODEN DDJOEB. ISSN 1044-789X.

Heller:1991:MHY

[Hel91] Steve Heller. Making a hash of your data. *Computer Language Magazine*, 8(8):47–??, August 1, 1991. CODEN COMLEF. ISSN 0749-2839.

Helleseth:1994:ACE

[Hel94] Tor Helleseth, editor. *Advances in Cryptology, EUROCRYPT '93: Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, May 1993: Proceedings*, volume 765 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. ISBN 0-387-57600-2 (New York), 3-540-57600-2 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1993.

Herbert:2007:WHP

[Her07] Andrew Herbert. What happened to Pastry. *Operating Systems Review*, 41(2): 10–16, April 2007. CODEN OSRED8. ISSN 0163-5980

(print), 1943-586X (electronic).

Heuer:1987:WRD

[Heu87] Andreas Heuer, editor. *Workshop on Relational Databases and Their Extensions*. ??, Clausthal-Zellerfeld, 1987.

Herrin:1991:ADF

[HF91] Erin H. Herrin II and Raphael Finkel. An ASCII database for fast queries of relatively stable data. *Computing Systems*, 4(2):127–155, Spring 1991. CODEN CMSYE2. ISSN 0895-6340.

Hull:2013:SPC

[HF13] Richard Hull and Wenfei Fan, editors. *SIGMOD/PODS'13: compilation proceedings of the 2013 ACM Symposium on Principles of Database Systems, ACM SIGMOD international conference on management of data, and SIGMOD/PODS 2013 PhD symposium: June 22–27, 2013, New York, New York, USA*. ACM Press, New York, NY 10036, USA, 2013. ISBN 1-4503-2066-X, 1-4503-2037-6. LCCN ???? URL `http://dl.acm.org/citation.cfm?id=2463664`; `http://www.sigmod.org/2013/`.

Huang:2017:QAL

[HFF+17] Qiang Huang, Jianlin Feng, Qiong Fang, Wilfred Ng, and Wei Wang. Query-aware locality-sensitive hashing scheme for l_p norm. *VLDB Journal: Very Large Data Bases*, 26(5):683–708, October 2017. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Huang:2015:QAL

[HFZ+15] Qiang Huang, Jianlin Feng, Yikai Zhang, Qiong Fang, and Wilfred Ng. Query-aware locality-sensitive hashing for approximate nearest neighbor search. *Proceedings of the VLDB Endowment*, 9(1):1–12, September 2015. CODEN ???? ISSN 2150-8097.

Hikita:1977:AFP

[HG77] R. Hikita and E. Goto. An $O(N)$ algorithm for finding periodicity of a sequence using hash coding. *Information Processing Letters*, 6(2):69–71, 1977. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lai:2009:CCD

[HGH+12] Jiao Hui, Xiongzi Ge, Xiaoxia Huang, Yi Liu, and Qiangjun Ran. E-HASH: an energy-efficient hybrid storage system composed of one SSD and multiple HDDs. *Lecture Notes in CS*, 7332:527–534, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.`

springer.com/content/pdf/10.1007/978-3-642-31020-1_63.

Hendricks:2007:LOB

[HGR07] James Hendricks, Gregory R. Ganger, and Michael K. Reiter. Low-overhead Byzantine fault-tolerant storage. *Operating Systems Review*, 41 (6):73–86, December 2007. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Hester:1985:SOL

[HH85] J. H. Hester and D. S. Hirschberg. Self-organizing linear search. *ACM Computing Surveys*, 17(3):295, September 1985. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Harn:2010:ELL

[HHL10] Lein Harn, Wen-Jung Hsin, and Changlu Lin. Efficient on-line/off-line signature schemes based on multiple-collision trapdoor hash families. *The Computer Journal*, 53(9):1478–1484, November 2010. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/53/9/1478.full.pdf+html.

Haitner:2010:UOW

[HHR+10] Iftach Haitner, Thomas Holenstein, Omer Reingold, Salil Vadhan, and Hoeteck Wee. Universal one-way hash functions via inaccessible entropy. *Lecture Notes in CS*, 6110:616–637, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-13190-5_31.

Hill:1978:CSVb

[Hil78a] Edward Hill, Jr. *A Comparative Study of Very Large Data Bases*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1978. ISBN 0-387-08653-6. x + 140 pp. LCCN QA76.9.D3 H54 1978. A revision of the author's thesis, George Washington University, 1977.

Hill:1978:CSVa

[Hil78b] Edward Hill.Jr. A comparative study of very large data bases. Technical report, ????, Berlin, Germany, 1978. ?? pp.

Hildebrandt:1982:VBD

[Hil82] F. Hildebrandt. Vergleichende bewertung dynamischer hash-verfahren durch simulation. Master's thesis, Technischen Universität Carolo-Wilhelmina

zu Braunschweig, Braunschweig, Germany, 1982. ?? pp.

Hille:1988:DAP

[Hil88] Reinhold F. Hille. *Data Abstraction and Program Development using Pascal*. Advances in Computer Science Series. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1988. ISBN 0-13-196552-2. xi + 259 pp. LCCN QA76.9.A23 H55 1988. US$42.00. Chapter 6 discusses hash tables.

Hilley:2005:CRM

[Hil05] Sarah Hilley. Crypto race for mathematical infinity. *Network Security*, 2005(4): 10–11, April 2005. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485805702233`.

Hinsen:2020:MCA

[Hin20] K. Hinsen. The magic of content-addressable storage. *Computing in Science and Engineering*, 22 (3):113–119, 2020. CODEN CSENFA. ISSN 1521-9615 (print), 1558-366X (electronic).

Herschel:1975:WHC

[HJ75] R. Herschel and B. Jonsson. Was ist Hash-coding? (German) [what is hash-coding?]. *Elektronische Rechenanlagen mit Computer Praxis*, 17(4): 131–138, June 1975. CODEN ERCPDJ.

Helleseth:1996:UHF

[HJ96] T. Helleseth and T. Johansson. Universal hash functions from exponential sums over finite fields and Galois rings. *Lecture Notes in CS*, 1109:31–??, ???? 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hopcroft:1983:HCG

[HK83] J. E. Hopcroft and M. S. Krishnamoorthy. On the harmonious coloring of graphs. *SIAM Journal of Algebraic Discrete Methods*, 4(3):306–311, September 1983. CODEN SJAMDU. ISSN 0196-5212 (print), 2168-345X (electronic). Work related to minimal perfect hash functions.

Haggard:1986:FMP

[HK86] Gary Haggard and Kevin Karplus. Finding minimal perfect hash functions. In Little and Cassel [LC86b], pages 191–193. ISBN 0-89791-178-4. LCCN QA76.27.A79 v.18 no.1. US$28.00.

Hofri:1987:PLR

[HK87] Micha Hofri and Alan G. Konheim. Padded lists revisited. *SIAM Journal on Computing*, 16(6):1073–1114, December 1987. CO-

DEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Hagerup:1995:FPP

[HK95] Torben Hagerup and Jörg Keller. Fast parallel permutation algorithms. *Parallel Processing Letters*, 5(2):139–148, June 1995. CODEN PPLTEE. ISSN 0129-6264 (print), 1793-642X (electronic).

Halevi:2012:SPH

[HK12a] Shai Halevi and Yael Tauman Kalai. Smooth projective hashing and two-message oblivious transfer. *Journal of Cryptology*, 25 (1):158–193, January 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=1&spage=158`.

Hofheinz:2012:PHF

[HK12b] Dennis Hofheinz and Eike Kiltz. Programmable hash functions and their applications. *Journal of Cryptology*, 25(3):484–527, July 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=3&spage=484`.

Hong:2010:PAR

[HKKK10] Deukjo Hong, Bonwook Koo, Woo-Hwan Kim, and Daesung Kwon. Preimage attacks on reduced steps of ARIRANG and PKC98-hash. *Lecture Notes in CS*, 5984:315–331, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-14423-3_21`.

Hong:2013:HOE

[HKKK13] Deukjo Hong, Dong-Chan Kim, Woo-Hwan Kim, and Jongsung Kim. Higher order eTCR hash functions. *Computers and Mathematics with Applications*, 65 (9):1396–1402, May 2013. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122112000430`.

Hao:2004:ARF

[HKL04] Fang Hao, Murali Kodialam, and T. V. Lakshman. ACCEL-RATE: a faster mechanism for memory efficient per-flow traffic estimation. *ACM SIGMETRICS Performance Evaluation Review*, 32(1):155–166, June 2004. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Hao:2007:BHA

[HKL07] Fang Hao, Murali Kodialam, and T. V. Lakshman. Building high accuracy Bloom filters using partitioned hashing. *ACM SIGMETRICS Performance Evaluation Review*, 35(1):277–288, June 2007. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Hao:2012:FDM

[HKLS12] Fang Hao, Murali Kodialam, T. V. Lakshman, and Haoyu Song. Fast dynamic multiple-set membership testing using combinatorial Bloom filters. *IEEE/ACM Transactions on Networking*, 20(1): 295–304, February 2012. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Hromkovic:2007:SAF

[HKNW07] Juraj Hromkovič, Richard Královic, Marc Nunkesser, and Peter Widmayer, editors. *Stochastic algorithms: foundations and applications: 4th international symposium, SAGA 2007, Zurich, Switzerland, September 13–14, 2007: proceedings*, volume 4665 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-74870-9 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA9.58 .S24 2007. URL `http://www.springerlink.com/content/978-3-540-74870-0`; `http://www.springerlink.com/openurl.asp?genre=issue\%26issn=0302-9743\%26volume=4665`.

Hsiao:2005:TMD

[HKW05] Hung-Chang Hsiao, Chung-Ta King, and Chia-Wei Wang. TYPHOON: mobile distributed hash tables. *Journal of Parallel and Distributed Computing*, 65(2): 191–206, February 2005. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic).

Hirose:2012:CFU

[HKY12] Shoichi Hirose, Hidenori Kuwakado, and Hirotaka Yoshida. Compression functions using a dedicated block-cipher for lightweight hashing. *Lecture Notes in CS*, 7259:346–364, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-31912-9_23`.

Hsu:1991:IAI

[HL91] W. L. Hsu and R. C. T. Lee, editors. *ISA '91 Algorithms: 2nd International Symposium on Algorithms, Taipei, Republic of China, December 16–18, 1991: proceedings*, volume 557 of *Lec-*

ture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1991. ISBN 0-387-54945-5 (New York), 3-540-54945-5 (Berlin). LCCN QA76.9.A43 I57 1991.

Horton:1994:MLS

[HL94] Graham Horton and Scott T. Leutenegger. A multilevel solution algorithm for steady-state Markov chains. *ACM SIGMETRICS Performance Evaluation Review*, 22 (1):191–200, May 1994. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Hsu:2003:NCS

[HL03] Ching-Hung Hsu and Ming-Chih Lai. A new cipher scheme based on one-way hash function and IDEA. *Journal of Discrete Mathematical Sciences and Cryptography*, 7(1):111–120, 2003. CODEN ???? ISSN 0972-0529.

Heileman:2005:HCA

[HL05] Gregory L. Heileman and Wenbin Luo. How caching affects hashing. In Camil Demetrescu, Robert Sedgewick, and Roberto Tamassia, editors, *Proceedings of the Seventh Workshop on Algorithm Engineering and Experiments and the Second Workshop on Analytic Algorithmics and Combinatorics, ALENEX/ANALCO 2005, Sheraton Vancouver Wall Center Hotel, Vancouver, British Columbia, Canada, 22 January 2005*, pages 141–154. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2005. ISBN 0-89871-596-2. LCCN QA76.9.A43.W69 2005. URL `http://www.siam.org/meetings/alenex05/papers/13gheileman.pdf`.

Hsieh:2012:EHF

[HL12] Wen-Bin Hsieh and Jenq-Shiou Leu. Exploiting hash functions to intensify the remote user authentication scheme. *Computers and Security*, 31(6): 791–798, September 2012. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404812000910`.

Huang:2010:DHT

[HLC10] Chung-Ming Huang, Jian-Wei Li, and Chun-Ta Chen. Distributed hash table-based interrogating-call session control function network in the Internet protocol multimedia subsystem for efficient query services. *The Computer Journal*, 53(7): 918–933, September 2010. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.`

org/cgi/content/abstract/53/7/918; http://comjnl.oxfordjournals.org/cgi/reprint/53/7/918.

He:2013:RCP

[HLH13] Jiong He, Mian Lu, and Bingsheng He. Revisiting co-processing for hash joins on the coupled CPU–GPU architecture. *Proceedings of the VLDB Endowment*, 6 (10):889–900, August 2013. CODEN ???? ISSN 2150-8097.

Han:2018:SSR

[HLL18a] Shuai Han, Shengli Liu, and Lin Lyu. Super-strong RKA secure MAC, PKE and SE from tag-based hash proof system. *Designs, Codes, and Cryptography*, 86(7): 1411–1449, July 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-017-0404-y.

Han:2018:NRA

[HLL18b] Zhijie Han, Yaqiong Li, and Jie Li. A novel routing algorithm for IoT cloud based on hash offset tree. *Future Generation Computer Systems*, 86(??): 456–463, September 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17324512.

Hohl:1993:SIH

[HLMW93] W. Hohl, X. Lai, T. Meier, and C. Waldvogel. Security of iterated hash functions based on block ciphers. In Stinson [Sti93], pages 379–390. ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). LCCN QA76.9.A25 C79 1993.

Havas:1993:GTO

[HM93] George Havas and Bohdan Majewski. Graph theoretic obstacles to perfect hashing. *Congressus Numerantium*, 98:81–??, 1993. ISSN 0384-9864.

Halevi:1996:PPS

[HM96] S. Halevi and S. Micali. Practical and provably-secure commitment schemes from collision-free hashing. *Lecture Notes in CS*, 1109: 201–??, ???? 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1109/11090201.htm; http://link.springer-ny.com/link/service/series/0558/papers/1109/11090201.pdf.

Helmer:2003:PSF

[HM03] Sven Helmer and Guido Moerkotte. A performance study of four index structures for set-valued attributes of low cardinality. *VLDB Journal:*

Very Large Data Bases, 12 (3):244–261, October 2003. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Halperin:2008:AEA

[HM08] Dan Halperin and Kurt Mehlhorn, editors. *Algorithms — ESA 2008: 16th annual European symposium, Karlsruhe, Germany, September 15–17, 2008, proceedings*, volume 5193 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 3-540-87744-4, 3-540-87743-6 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A43 E83 2008. URL `http://www.springerlink.com/content/978-3-540-87743-1/`.

Hanaoka:2012:ICE

[HM12] Goichiro Hanaoka and Takahiro Matsuda. On the impossibility of constructing efficient key encapsulation and programmable hash functions in prime order groups. *Lecture Notes in CS*, 7417: 812–831, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-32009-5_47`.

Hwang:2019:BBR

[HM19] S. O. Hwang and A. Mehmood. Blockchain-based resource syndicate. *Computer*, 52 (5):58–66, May 2019. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Ha:2007:SAE

[HMNB07] JeaCheol Ha, SangJae Moon, Juan Manuel Gonzalez Nieto, and Colin Boyd. Security analysis and enhancement of One-Way Hash Based Low-Cost Authentication Protocol (OHLCAP). *Lecture Notes in CS*, 4819: 574–583, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-77018-3_57`.

Hagerup:2001:DD

[HMP01] T. Hagerup, P. B. Miltersen, and R. Pagh. Deterministic dictionaries. *Journal of Algorithms*, 41(1):69–85, ???? 2001. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic). URL `????`.

Havas:1994:GHH

[HMWC94] G. Havas, B. S. Majewski, N. C. Wormald, and Z. J. Czech. Graphs, hypergraphs and hashing. In van Leeuwen [vL94], pages 153–165. CO-

DEN LNCSD9. ISBN 0-86636-292-4 (New York), 3-540-57899-4 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA75.5 .I647 1993. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0790.htm`; `http://www.springerlink.com/content/978-0-86636-292-4`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=790`.

Hassanzadeh-Nazarabadi:2020:DUL

[HNKO20] Y. Hassanzadeh-Nazarabadi, A. Küpçü, and O. Ozkasap. Decentralized utility- and locality-aware replication for heterogeneous DHT-based P2P cloud storage systems. *IEEE Transactions on Parallel and Distributed Systems*, 31(5):1183–1193, May 2020. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Hiraki:1984:EAM

[HNS84] Kei Hiraki, Kenji Nishida, and Toshio Shimada. Evaluation of associative memory using parallel chained hashing. *IEEE Transactions on Computers*, C-33(9):851–855, September 1984. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Hashida:1972:LAC

[HO72] O. Hashida and K. Ohara. Line accommodation capacity of a communication control unit. *Rev. of the El. Commun. Lab.*, 20(??):231–239, 1972.

Holub:1987:NHE

[Hol87] Allen Holub. Nroff: Hashing, expressions, and roman numerals. *Dr. Dobbs Journal*, 12(2):90–??, February 1987. CODEN DDJTEQ. ISSN 0888-3076.

Holden:2013:GHF

[Hol13] Joshua Holden. A good hash function is hard to find, and vice versa. *Cryptologia*, 37(2):107–119, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hopgood:1968:xxx

[Hop68a] F. R. A. Hopgood. ??? *The Computer Bulletin*, 11(??): 297–300, 1968. Presents algorithms for expanding and rehashing nearly full hash tables.

Hopgood:1968:STO

[Hop68b] F. R. A. Hopgood. A solution for the table overflow problem for hash tables. *The Computer Bulletin*, ??(??): ??, March 1968.

Hanan:1963:ACT

[HP63] M. Hanan and F. P. Palermo. An application of coding theory to a file address problem. *IBM Journal of Research and Development*, 7

(2):127–129, April 1963. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Halatsis:1978:PHT

[HP78] Constantine Halatsis and George Philokyprou. Pseudochaining in hash tables. *Communications of the Association for Computing Machinery*, 21(7):554–557, July 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Han:2002:CMV

[HPC02] Daewan Han, Sangwoo Park, and Seongtaek Chee. Cryptanalysis of the modified version of the hash function proposed at PKC'98. *Lecture Notes in CS*, 2365:252–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650252.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2365/23650252.pdf`.

Harris:1993:ODM

[HR93] Evan P. Harris and Kotagiri Ramamohanarao. Optimal dynamic multi-attribute hashing for range queries. *BIT (Nordisk tidskrift for informationsbehandling)*, 33 (4):561–579, 1993. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.mai.liu.se/BIT/contents/bit33.html`.

Harris:1996:JAC

[HR96] Evan P. Harris and Kotagiri Ramamohanarao. Join algorithm costs revisited. *VLDB Journal: Very Large Data Bases*, 5(1):64–84, January 1996. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic). URL `http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/h/Harris:Evan_P=.html`; `http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/r/Ramamohanarao:Kotagiri.html`; `http://link.springer.de/link/service/journals/00778/bibs/6005001/60050064.htm`; `http://link.springer.de/link/service/journals/00778/papers/6005001/60050064.pdf`; `http://link.springer.de/link/service/journals/00778/papers/6005001/60050064.ps.gz`. Electronic edition.

Hsiao:2004:FCP

[HR04] Chun-Yuan Hsiao and Leonid Reyzin. Finding collisions on a public road, or do secure hash functions need secret coins? In Franklin [Fra04], pages 92–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/`

openurl.asp?genre=issue&issn=0302-9743&volume=3152; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099.

Haitner:2007:SHC

[HR07] Iftach Haitner and Omer Reingold. Statistically-hiding commitment from any one-way function. In ACM [ACM07], pages 1–10. ISBN 1-59593-631-9. LCCN ????

Haitner:2014:NIH

[HR14] Iftach Haitner and Omer Reingold. A new interactive hashing theorem. *Journal of Cryptology*, 27(1):109–138, January 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-012-9139-0.

Hulsing:2013:OPX

[HRB13] Andreas Hülsing, Lea Rausch, and Johannes Buchman. Optimal parameters for XMSS^{MT}. *Lecture Notes in CS*, 8128:194–208, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL https://link.springer.com/chapter/10.1007/978-3-642-40588-4_14.

Hulsing:2016:MMT

[HRS16] Andreas Hülsing, Joost Rijneveld, and Fang Song. Mitigating multi-target attacks in hash-based signatures. *Lecture Notes in CS*, 9614:387–416, 2016. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL https://link.springer.com/chapter/10.1007/978-3-662-49384-7_15.

Horowitz:1978:FCA

[HS78] Ellis Horowitz and Sartaj Sahni. *Fundamentals of Computer Algorithms*. Computer Science Press, 11 Taft Court, Rockville, MD 20850, USA, 1978. ISBN 0-914894-22-6. xiv + 626 pp. LCCN QA76.6 .H67 1978. A standard textbook treatment of well-known hashing algorithms appears on pp. 82–93.

Horowitz:1984:FDS

[HS84] Ellis Horowitz and Sartaj Sahni. *Fundamentals of Data Structures in Pascal*. Computer Science Press, 11 Taft Court, Rockville, MD 20850, USA, 1984. ISBN 0-914894-94-3. xiv + 542 pp. LCCN QA76.9.D35 H67 1984. US$29.95. Textbook treatment of hashing algorithms.

Hoch:2008:SCH

[HS08] Jonathan J. Hoch and Adi Shamir. On the strength of the concatenated hash combiner when all the hash functions are weak. *Lecture Notes in CS*, 5126:

616–630, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-70583-3_50`.

Hsiao:1983:ADM

[Hsi83] David K. Hsiao. *Advanced Database Machine Architecture*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1983. ISBN 0-13-011262-3. xxii + 394 pp. LCCN QA76.9.D3 A343 1983.

Hernandez:2002:GCT

[HSIR02] Julio César Hernández, José María Sierra, Pedro Isasi, and Arturo Ribagorda. Genetic cryptoanalysis of two rounds TEA. *Lecture Notes in CS*, 2331:1024–1031, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/0pa8nj982jewn9ev/`.

Hoshi:1988:AHF

[HSK88] Mamoru Hoshi, Hajime Sato, and Kingo Kobayashi. Arithmetic hash functions. In *IEEE 1988 International Symposium on Information Theory — Abstracts of papers*, volume 25 n 13, pages 156–157. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. Available from IEEE Service Cent (catalog number 88CH2621-1). Piscataway, NJ, USA.

Hirano:1995:IEH

[HSM95] Yasuhiro Hirano, Tetsuji Satoh, and Fumiaki Miura. Improved extendible hashing with high concurrency. *Systems and computers in Japan*, 26(13):1–??, 1995. CODEN SCJAEP. ISSN 0882-1666 (print), 1520-684X (electronic).

Hiranandani:1991:PHC

[HSMB91] Seema Hiranandani, Joel Saltz, Piyush Mehrotra, and Harry Berryman. Performance of hashed cache data migration schemes on multicomputers. *Journal of Parallel and Distributed Computing*, 12(4):415–422, August 1991. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic).

Hafiane:2008:RIH

[HSPZ08] Adel Hafiane, Guna Seetharaman, Kannappan Palaniappan, and Bertrand Zavidovique. Rotationally invariant hashing of median binary patterns for texture classification. *Lecture Notes in CS*, 5112:619–629, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/`

10.1007/978-3-540-69812-8_61.

Hernandez:2001:DTR

[HSR+01] Julio César Hernández, José María Sierra, Arturo Ribagorda, Benjamín Ramos, and J. C. Mex-Perera. Distinguishing TEA from a random permutation: Reduced round versions of TEA do not have the SAC or do not generate random numbers. *Lecture Notes in CS*, 2260:374–377, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600374.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600374.pdf.

Herlihy:2008:HH

[HST08] Maurice Herlihy, Nir Shavit, and Moran Tzafrir. Hopscotch hashing. *Lecture Notes in CS*, 5218:350–364, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-87779-0_24.

Hutflesz:1988:GOP

[HSW88] Andreas Hutflesz, Hans-Werner Six, and Peter Widmayer. Globally order preserving multidimensional linear hashing. In ICDE'88 [ICD88], pages 572–579. ISBN 0-8186-0827-7 (paperback), 0-8186-8827-0 (hardcover), 0-8186-4827-9 (microfiche). LCCN QA76.9.D3 I5582 1988. IEEE Service Cent. Piscataway, NJ, USA.

Hsiao:1988:AH

[HT88] Yeong-Shiou S. Hsiao and Alan L. Tharp. Adaptive hashing. *Information system*, 13(1):111–127, 1988. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Hagerup:2001:EMP

[HT01] Torben Hagerup and Torsten Tholey. Efficient minimal perfect hashing in nearly minimal space. *Lecture Notes in CS*, 2010:317–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2010/20100317.htm; http://link.springer-ny.com/link/service/series/0558/papers/2010/20100317.pdf.

Hsu:1990:COL

[HTY90] Meichun Hsu, Shang-Sheng Tung, and Wei-Pang Yang. Concurrent operations in linear hashing. *Information Sciences*, 51(2):193–??, July 1, 1990. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Hua:1982:INT

[Hua82] Lo-Keng Hua. *Introduction to number theory.* Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1982. ISBN 0-387-10818-1. xviii + 572 pp. LCCN QA241 .H7513 1982. Translated from the 1975 Chinese edition *Shu lun tao yin* by Peter Shiu. This is the English edition of Ref. 6 of [Cha84c], the book that contains the fundamental prime number functions needed for Chang's ordered minimal perfect hash functions.

Huang:1985:MEH

[Hua85] S.-H. S. Huang. Multidimensional extendible hashing for partial-match queries. *International Journal of Computer and Information Sciences*, 14(2):73–82, April 1985. CODEN IJCIAH. ISSN 0091-7036.

Hughes:1985:LMF

[Hug85] John Hughes. Lazy memo-functions. In Jouannaud [Jou85], pages 129–146. ISBN 0-387-15975-4. LCCN QA76.7 .F861 1985. Uses hashing in the implementation of memo functions, which keep track of all their past arguments and corresponding results.

Huisman:1990:SEM

[Hui90] Leendert M. Huisman. Simulation of embedded memories by defective hashing. *IBM Journal of Research and Development*, 34(2/3): 289–298, March/May 1990. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Hulsing:2013:WOS

[Hül13] Andreas Hülsing. W-OTS+ — shorter signatures for hash-based signature scheme. *Lecture Notes in CS*, 7918: 173–188, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `https://link.springer.com/chapter/10.1007/978-3-642-38553-7_10`.

Hong:1988:IMB

[HW88] Jiawei Hong and Haim Wolfson. Improved model-based matching method using footprints. *Proceedings — International Conference on Pattern Recognition*, pages 72–78, 1988. CODEN PICREG. ISBN 0-8186-0878-1. Available from IEEE Service Cent (catalog number 88CH2614-6). Piscataway, NJ, USA.

He:2008:FED

[HW08] Zhoucan He and Qing Wang. A fast and effective dichotomy based hash algorithm for image matching. *Lecture Notes in CS*, 5358:328–337, 2008. CODEN LNCSD9. ISSN 0302-

9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-89639-5_32.

He:2018:MBF

[HWZP18] Jingsha He, Jianan Wu, Nafei Zhu, and Muhammad Salman Pathan. MinHash-based fuzzy keyword search of encrypted data across multiple cloud servers. *Future Internet*, 10(5):38, May 01, 2018. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/10/5/38.

Huang:2013:FDH

[HXLX13] Kun Huang, Gaogang Xie, Rui Li, and Shuai Xiong. Fast and deterministic hash table lookup using discriminative Bloom filters. *Journal of Network and Computer Applications*, 36(2): 657–666, March 2013. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804513000088.

Hohl:1994:SIH

[HXMW94] Walter Hohl, Lai Xuejia, Thomas Meier, and Christian Waldvogel. Security of iterated hash functions based on block ciphers. *Lecture Notes in CS*, 773:379–390, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hsu:1986:COE

[HY86] Meichun Hsu and Wei-Pang Yang. Concurrent operations in extendible hashing. In Chu et al. [CGO86], pages 241–247. ISBN 0-934613-18-4. LCCN QA 76.9 D3 I61 1986.

Ho:1989:COM

[HYH89] P. Ho, W. Yang, and M. Hsu. Concurrent operations in multi-dimensional extendible hashing. *Journal of Information and Engineering*, 5(??): 51–72, 1989.

Ho:1993:COM

[HYH93] Pao-Chung Ho, Wei-Pang Yang, and Meichun Hsu. Concurrent operations in multi-attribute linear hashing. *Information Sciences*, 74(1 / 2):29–??, October 15, 1993. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Hadjieleftheriou:2008:HSS

[HYKS08] Marios Hadjieleftheriou, Xiaohui Yu, Nick Koudas, and Divesh Srivastava. Hashed samples: selectivity estimators for set similarity selection queries. *Proceedings of the VLDB Endowment*, 1(1): 201–212, August 2008. CODEN ???? ISSN 2150-8097.

Hsieh:1999:OWH

[HYLT99] T.-M. Hsieh, Y.-S. Yeh, C.-H. Lin, and S.-H. Tuan. One-way hash functions with

changeable parameters. *Information Sciences*, 118(1): 223–239, September 1999. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Hill:1986:ESD

[HZ86] L. Owen Hill and David A. Zein. Extracting statistical data from free-form text. *IEEE Circuits and Devices Magazine*, 2(3):18–24, May 1986. CODEN ICDMEN. ISSN 8755-3996.

Aoe:1991:CAK

[iA91] Jun ichi Aoe. *Computer Algorithms: Key Search Strategies*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1991. ISBN 0-8186-2123-0 (paperback), 0-8186-2123-2 (hardcover), 0-8186-6123-2 (microfiche). xi + 139 pp. LCCN QA76.9.A43 C66 1991.

Aoe:1994:CAS

[iA94] Jun ichi Aoe. *Computer Algorithms: String Pattern Matching Strategies*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-8186-5461-9 (microfiche), 0-8186-5462-7 (hardcover), 0-8186-5460-0 (paperback). ix + 281 pp. LCCN QA76.9.A43 C67 1994. US$56.00.

Istvan:2015:HTL

[IABV15] Zsolt István, Gustavo Alonso, Michaela Blott, and Kees Vissers. A hash table for line-rate data processing. *ACM Transactions on Reconfigurable Technology and Systems*, 8(2):13:1–13:??, April 2015. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

IEEE:1986:ICD

[ICD86] *International Conference on Data Engineering (2nd), February 5–7, 1986, Bonaventure Hotel, Los Angeles, California, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1986. ISBN 0-8186-0655-X (paperback), 0-8186-8655-3 (hardcover), 0-8186-4655-1 (microfiche). LCCN QA 76.9 D3 I5582 1986.

IEEE:1987:DEP

[ICD87] *Data Engineering: Proceedings/Third International Conference on Data Engineering, February 3–5, 1987, Pacifica Hotel, Los Angeles, California, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. ISBN 0-8186-0762-9 (paperback) 0-8186-8762-2 (hard) 0-8186-4762-0 (microfiche). LCCN QA76.9.D3 I5582 1987.

IEEE:1988:PFI

[ICD88] *Proceedings, Fourth International Conference on Data Engineering: February 1–5, 1988, Los Angeles Airport Hilton and Towers, Los Angeles, California, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. ISBN 0-8186-0827-7 (paperback), 0-8186-8827-0 (hardcover), 0-8186-4827-9 (microfiche). LCCN QA76.9.D3 I5582 1988.

IEEE:1990:PSI

[ICD90] *Proceedings, Sixth International Conference on Data Engineering: February 5–9, 1990, Los Angeles Airport Hilton and Towers, Los Angeles, California, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. ISBN 0-8186-2025-0 (paperback), 0-8186-9025-9 (hardcover), 0-8186-6025-2 (microfiche). LCCN QA76.9.D3 I5582 1990.

IEEE:1991:PSI

[ICD91] *Proceedings/Seventh International Conference on Data Engineering, April 8–12, 1991, Kobe, Japan*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1991. ISBN 0-8186-2138-9 (paper), 0-8186-6138-0 (microfiche), 0-8186-9138-7 (hardcover). LCCN QA76.9.D3 I5582 1991.

IEEE:1993:ICD

[ICD93] *Proceedings/Ninth International Conference on Data Engineering, April 19–23, 1993, Vienna, Austria*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1993. ISBN 0-8186-3572-X (hardcover), 0-8186-3570-3 (paperback), 0-8186-3571-1 (microfiche). LCCN QA76.9.D3I57 1993.

IEEE:1974:ASS

[IEE74] IEEE, editor. *15th Annual Symposium on Switching and Automata Theory, October 14–16, 1974, the University of New Orleans*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1974.

IEEE:1976:ASF

[IEE76] *17th Annual Symposium on Foundations of Computer Science, October 25–27, 1976, Houston, Texas*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1976.

IEEE:1980:PCI

[IEE80a] *Proceedings 4, COMPSAC 80, the IEEE Computer Society's Fourth International Computer Software and Ap-*

plications Conference, October 27–31, 1980, the Palmer House, Chicago. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1980. LCCN QA 75.5 C586 1980.

IEEE:1980:ASF

[IEE80b] *21st Annual Symposium on Foundations of Computer Science: Oct. 13–15, 1980, Syracuse, NY*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1980.

IEEE:1982:SFC

[IEE82] *Symposium on Foundations of Computer Science (23rd: 1982: Chicago, IL) 23rd Annual Symposium on Foundations of Computer Science, November 3–5, 1982*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1982. LCCN QA76.6 .S95 1982.

IEEE:1984:ISL

[IEE84] *1984 International Symposium on Logic Programming, February 6–9, 1984, Bally's Park Place Casino, Atlantic City, New Jersey/sponsored by IEEE Computer Society, Technical Committee on Computer Languages*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1984. ISBN 0-8186-0522-7 (paperback), 0-8186-8522-0 (hardcover), 0-8186-4522-9 (microfiche). LCCN QA76.6 .I5735 1984.

IEEE:1985:FOC

[IEE85a] *26th annual Symposium on Foundations of Computer Science, October 21–23, 1985, Portland, OR*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1985. ISBN 0-8186-0644-4 (paperback), 0-8186-4644-6 (microfiche), 0-8186-8644-8 (hardcover). LCCN QA 76 S979 1985.

IEEE:1985:PFD

[IEE85b] *Proceedings: Foundations of Data Organization, Kyoto '85, Japan, International Conference on Foundations of Data Organization, May 21–24, 1985, Kyoto, Japan*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1985.

IEEE:1988:DPI

[IEE88a] *Digest of papers: intellectual leverage/COMPCON Spring 88, February 29-March 4, 1988, Thirty-Third IEEE Computer Society International Conference, Cathedral Hill Hotel, San Francisco, California*. IEEE Computer Society Press, 1109

Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. ISBN 0-8186-0828-5 (paperback), 0-8186-4828-7 (microfiche), 0-8186-8828-9 (hardcover). LCCN QA75.5 .C58 1988.

IEEE:1988:SIC

[IEE88b] *Second International Conference on Computer Vision: December 5–8, 1988, Innesbrook Resort, Tampa, Florida, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. ISBN 0-8186-8883-1, 0-8186-0883-8 (paperback). LCCN TA1632 .I5485 1988.

IEEE:1988:ASF

[IEE88c] *29th Annual Symposium on Foundations of Computer Science, October 24–26, 1988, White Plains, NY*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. ISBN 0-8186-0877-3 (paperback), 0-8186-4877-5 (microfiche), 0-8186-8877-7 (hardcover). LCCN QA 76 S979 1988.

IEEE:1988:ICP

[IEE88d] *9th International Conference on Pattern Recognition: 14–17 November 1988, Ergife Palace Hotel, Rome, Italy*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. ISBN 0-8186-0878-1 (paperback), 0-8186-4878-3 (microfiche), 0-8186-8878-5 (hardcover). LCCN TK7882.P3 I58 1988 v. 1-2 (1988).

IEEE:1989:ASF

[IEE89] *30th Annual Symposium on Foundations of Computer Science, October 30–November 1, 1989, Research Triangle Park, NC*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. CODEN ASFPDV. ISBN 0-8186-1982-1 (hardcover), 0-8186-5982-3 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1989.

IEEE:1990:PSN

[IEE90] IEEE, editor. *Proceedings, Supercomputing '90: November 12–16, 1990, New York Hilton at Rockefeller Center, New York, New York*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. ISBN 0-8186-2056-0 (paperback: IEEE Computer Society), 0-89791-412-0 (paperback: ACM). LCCN QA 76.88 S87 1990. ACM order number 415903. IEEE Computer Society Press order number 2056. IEEE catalog number 90CH2916-5.

IEEE:1991:PSA

[IEE91a] IEEE, editor. *Proceedings, Supercomputing '91: Albuquerque, New Mexico, November 18–22, 1991*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1991. ISBN 0-8186-9158-1 (IEEE case), 0-8186-2158-3 (IEEE paper), 0-8186-6158-5 (IEEE microfiche), 0-89791-459-7 (ACM). LCCN QA76.5 .S894 1991. ACM order number 415913. IEEE Computer Society Press order number 2158. IEEE catalog number 91CH3058-5.

IEEE:1991:PAS

[IEE91b] *Proceedings, 32nd Annual Symposium on Foundations of Computer Science: October 1–4, 1991, San Juan, Puerto Rico*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1991. ISBN 0-8186-2445-0 (paperback), 0-8186-2447-7 (hardcover). LCCN QA 76 S979 1991.

IEEE:1992:PII

[IEE92a] IEEE, editor. *Proceedings: IEEE Infocom '92, the conference on computer communications, one world through communications, eleventh annual joint conference of the IEEE Computer and Communications Societies, Florence, Italy*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. Three volumes. IEEE Computer Society order number 2860. IEEE catalog number 92CH3133-6.

IEEE:1992:PAS

[IEE92b] *Proceedings, 33rd Annual Symposium on Foundations of Computer Science: October 24–27, 1992, Pittsburgh, Pennsylvania*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. ISBN 0-8186-2900-2. LCCN QA 76 S979 1992.

IEEE:1993:PSP

[IEE93] IEEE, editor. *Proceedings, Supercomputing '93: Portland, Oregon, November 15–19, 1993*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1993. ISBN 0-8186-4340-4 (paperback), 0-8186-4341-2 (microfiche), 0-8186-4342-0 (hardback), 0-8186-4346-3 (CD-ROM). ISSN 1063-9535. LCCN QA76.5 .S96 1993.

IEEE:1994:DEI

[IEE94a] IEEE, editor. *Data engineering: 10th International conference — February 1994, Houston, TX*, INTERNATIONAL CONFERENCE ON DATA ENGINEERING 1994; 10th. IEEE Computer

Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-8186-5402-3, 0-8186-5400-7, 0-8186-5401-5. LCCN QA76.9.D3 I5582 1994.

IEEE:1994:NAE

[IEE94b] IEEE, editor. *National aerospace and electronics conference: – May 1994, Dayton, OH*, volume 1 of *PROCEEDINGS OF THE IEEE NATIONAL AEROSPACE AND ELECTRONICS CONFERENCE 1994*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-7803-1893-5, 0-7803-1894-3, 0-7803-1895-1. ISSN 0547-3578. LCCN TL 693 N37 1994. Two volumes.

IEEE:1994:PSH

[IEE94c] IEEE, editor. *Proceedings of the Scalable High-Performance Computing Conference, May 23–25, 1994, Knoxville, Tennessee*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-8186-5680-8, 0-8186-5681-6. LCCN QA76.58.S32 1994.

IEEE:1995:PNA

[IEE95] IEEE, editor. *Proceedings: the nineteenth annual International Computer Software and Applications Conference (COMPSAC '95): August 9–11, 1995, Dallas, Texas*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1995. ISBN 0-8186-7119-X. LCCN QA76.6 .I5 1995. IEEE Catalog No. 95CB35838.

IEEE:1999:ASF

[IEE99] IEEE, editor. *40th Annual Symposium on Foundations of Computer Science: October 17–19, 1999, New York City, New York*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1999. CODEN ASFPDV. ISBN 0-7695-0409-4 (softbound), 0-7803-5955-0 (casebound), 0-7695-0411-6 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 1999. IEEE Catalog Number 99CB37039.

IEEE:2001:PII

[IEE01] IEEE, editor. *Proceedings IEEE INFOCOM 2001: the conference on computer communications: proceedings: Twentieth annual joint conference of the IEEE Computer and Communications Societies: twenty years into the communications odyssey: 22–26 April 2001, Hilton Anchorage Hotel, Anchorage, Alaska USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD

20910, USA, 2001. ISBN 0-7803-7016-3 (softbound), 0-7803-7017-1 (microfiche), 0-7803-7018-X (CD-ROM). LCCN TK5105.5 .I48 2001. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=7321`.

IEEE:2002:STI

[IEE02] IEEE, editor. *SC2002: From Terabytes to Insight. Proceedings of the IEEE ACM SC 2002 Conference, November 16–22, 2002, Baltimore, MD, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2002. ISBN 0-7695-1524-X. LCCN ????

IEEE:2005:PIS

[IEE05] IEEE, editor. *Proceedings of the 17th IEEE Symposium on Computer Arithmetic, ARITH-17, June 27–29, 2005, Cape Cod, Massachusetts, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2005. ISBN ???? LCCN ????

IEEE:2006:AIS

[IEE06] IEEE, editor. *47th Annual IEEE Symposium on Foundations of Computer Science: FOCS 2006: 21–24 October, 2006, Berkeley, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2006. ISBN 0-7695-2720-5, 0-7695-2362-5. ISSN 0272-5428. LCCN QA76 .S974 2006. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=4031329`. IEEE Computer Society Order Number P2720.

IEEE:2007:PAI

[IEE07] IEEE, editor. *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science: [FOCS 2007]: October 20–23, 2007, Providence, Rhode Island*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2007. ISBN 0-7695-3010-9. ISSN 0272-5428. LCCN QA76 .S974 2007. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=4389466`. IEEE Computer Society order number P3010.

IEEE:2010:PIA

[IEE10] IEEE, editor. *Proceedings: 2010 IEEE 51st Annual Symposium on Foundations of Computer Science: 23–26 October 2010, Las Vegas, Nevada, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 1-4244-8525-8. LCCN ???? URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5669376`. IEEE

Computer Society Order Number P4244.

IEEE:2011:ICI

[IEE11a] IEEE, editor. *International Conference on Intelligent Computation Technology and Automation (ICICTA), 2011: 28–29 March 2011, Shenzhen, Guangdong, China; proceedings*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. ISBN 0-7695-4353-7, 1-61284-289-5. LCCN ???? URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5750113`.

IEEE:2011:PIA

[IEE11b] IEEE, editor. *Proceedings: 2011 IEEE 52nd Annual IEEE Symposium on Foundations of Computer Science: 22–25 October 2011, Palm Springs, California, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. ISBN 1-4577-1843-X. LCCN ????

IEEE:2013:PIA

[IEE13] IEEE, editor. *Proceedings of the 2012 IEEE 54th Annual Symposium on Foundations of Computer Science: 26–29 October 2013, Berkeley, CA, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2013. ISBN 0-7695-5135-1. ISSN 0272-5428. LCCN QA76 .S95 2012. URL `http://dimacs.rutgers.edu/FOCS13/`; `http://theory.stanford.edu/~tim/focs13/`. IEEE Computer Society order number P????.

Ida:1977:PPH

[IG77] Tetsuo Ida and Eiichi Goto. Performance of a parallel hash hardware with key deletion. In Gilchrist [Gil77], pages 643–647. ISBN 0-7204-0755-9. LCCN ????

Ihlenfeldt:1994:HCI

[IG94] Wolf Dietrich Ihlenfeldt and Johann Gasteiger. Hash codes for the identification and classification of molecular structure elements. *Journal of Computational Chemistry*, 15(8):793–813, August 1994. CODEN JCCHDD. ISSN 0192-8651 (print), 1096-987X (electronic).

Ioannidis:2005:ADS

[IGA05] Ioannis Ioannidis, Ananth Grama, and Mikhail Atallah. Adaptive data structures for IP lookups. *ACM Journal of Experimental Algorithmics*, 10:1.1:1–1.1:??, ???? 2005. CODEN ???? ISSN 1084-6654.

Ichikawa:1983:ARD

[IH83] T. Ichikawa and M. Hirakawa. ARES: a relational database, responsible

for data semantics. Technical Report TR.CSG 8, Hiroshima University, Hiroshima, Japan, August 1983. ?? pp.

Itoh:1995:ANS

[IH95] Toshiya Itoh and Kei Hayashi. Alternative necessary and sufficient conditions for collision intractable hashing. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, 78(1):19–??, January 1, 1995. CODEN IFESEX. ISSN 0916-8508 (print), 1745-1337 (electronic).

Ivanchykhin:2017:RAU

[IIL17] Dmytro Ivanchykhin, Sergey Ignatchenko, and Daniel Lemire. Regular and almost universal hashing: an efficient implementation. *Software—Practice and Experience*, 47(10):1299–1323, October 2017. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Ikeda:2013:CEM

[IJK13] S. Ikeda, M. Jibiki, and Y. Kuno. Coverage estimation in model checking with bitstate hashing. *IEEE Transactions on Software Engineering*, 39(4):477–486, April 2013. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6226428`.

ACM:1989:PIJ

[IJW89] *Proceedings of 4th International Joint Workshop on Computer Communications: at the University of Tokyo, Tokyo, Japan, July 13–15, 1989*. ACM Press, New York, NY 10036, USA, 1989. LCCN TK5105.5 .I574 1989.

Ichiyoshi:1992:ALB

[IK92] Nobuyuki Ichiyoshi and Kouichi Kimura. Asymptotic load balance of distributed hash tables. In Moto-oka [Mo92b], pages 869–876. ISBN 0-444-86440-7. LCCN QA76.5 .I545 1981.

Ishai:2005:SCC

[IKO05] Yuval Ishai, Eyal Kushilevitz, and Rafail Ostrovsky. Sufficient conditions for collision-resistant hashing. In Kilian [Kil05], pages 445–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171`.

Ishai:2008:CCC

[IKOS08] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with constant computational overhead. In ACM [ACM08b], pages 433–442. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Ivanov:1990:HSO

[IL90] M. B. Ivanov and V. A. Litvinov. Hash-sequential organization of data sets. *Programming and Computer Software; translation of Programmirovaniye, (Moscow, USSR) Plenum*, 15(2):70–75 (or 70–76??), January 1990. CODEN PCSODA. ISSN 0361-7688 (print), 1608-3261 (electronic).

Indyk:1997:LPH

[IMRV97] Piotr Indyk, Rajeev Motwani, Prabhakar Raghavan, and Santosh Vempala. Locality-preserving hashing in multidimensional spaces. In ACM [ACM97b], pages 618–625. ISBN 0-89791-888-6. LCCN QA76.5 .A849 1997. URL `http://www.acm.org/pubs/articles/proceedings/stoc/258533/p618-indyk/p618-indyk.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/258533/p618-indyk/`. ACM order no. 508970.

Impagliazzo:1989:ECS

[IN89] Russell Impagliazzo and Moni Naor. Efficient cryptographic schemes provably as secure as subset sum. *Annual Symposium on Foundations of Computer Science (Proceedings)*, pages 236–241, November 1989. CODEN ASFPDV. ISBN 0-8186-1982-1. ISSN 0272-5428. IEEE catalog number 89CH2808-4.

Ince:1981:IFS

[Inc81] D. C. Ince. The implementation of file structures in some high level languages. *SIGPLAN Notices*, 16(11):49–55, November 1981. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Indyk:2001:SAM

[Ind01] P. Indyk. A small approximately min-wise independent family of hash functions. *Journal of Algorithms*, 38(1):84–90, January 2001. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic).

Indyk:2013:SHH

[Ind13] Piotr Indyk. Sketching via hashing: from heavy hitters to compressed sensing to Sparse Fourier Transform. In Hull and Fan [HF13], pages 87–90. ISBN 1-4503-2066-X, 1-4503-2037-6. LCCN ????

URL http://dl.acm.org/citation.cfm?id=2463664; http://www.sigmod.org/2013/.

Indesteege:2008:CRH

[IP08] Sebastiaan Indesteege and Bart Preneel. Collisions for RC4-hash. *Lecture Notes in CS*, 5222:355–366, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-85886-7_25.

Indesteege:2011:PCE

[IP11] Sebastiaan Indesteege and Bart Preneel. Practical collisions for EnRUPT. *Journal of Cryptology*, 24(1):1–23, January 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=1&spage=1.

Irby:19xx:MRH

[Irbxx] Thomas C. Irby. Minimal retrieval hash codes. *Proceedings of the Texas Conference on Computing Systems*, ?? (??):8.1–8.5, ???? 19xx. CODEN PTCSDR. IEEE Comput Soc. Long Beach, Ca.

Imai:1993:ACA

[IRM93] Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors. *Advances in Cryptology, ASIACRYPT '91: International Conference on the Theory and Application of Cryptology, Fujiyoshida, Japan, November 11–14, 1991: Proceedings*, volume 739 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-57332-1 (New York), 3-540-57332-1 (Berlin). LCCN QA76.9.A25 I555 1991. DM96.00.

Inoue:1991:RRD

[ISH+91] Ushio Inoue, Tetsuji Satoh, Haruo Hayami, Hideaki Takeda, Toshio Nakamura, and Hideki Fukuoka. Rinda: a relational database processor with hardware specialized for searching and sorting. *IEEE Micro*, 11(6):61–70, November/December 1991. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Itano:1988:IPM

[ISHY88] Kozo Itano, Yutaka Sato, Hidemi Hirai, and Tomoyoshi Yamagata. An incremental pattern matching algorithm for the pipelined lexical scanner. *Information Processing Letters*, 27(5):253–258, April 28, 1988. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ishikawa:1993:MLI

[ISK+93] Hiroshi Ishikawa, Fumio Suzuki, Fumihiko Kozakura, Akifumi Makinouchi, Mika Miyagishima, Yoshio Izumida, Masaaki Aoshima, and Yasuo Yamane. The model, language, and implementation of an object-oriented multimedia knowledge base management system. *ACM Transactions on Database Systems*, 18(1): 1–50, March 1993. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1993-18-1/p1-ishikawa/p1-ishikawa.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1993-18-1/p1-ishikawa/`; `http://www.acm.org/pubs/toc/Abstracts/tods/151285.html`.

ISO:1997:ITS

[ISO97] ISO and IEC 10118. *Information technology — Security techniques — theory; distributed databases; hash filters; hash join Hash-functions, Part 1: General (IS, 1994); Part 2: Hash-functions using an n-bit block cipher algorithm, (IS, 1994); Part 3: Dedicated hash-functions (IS, 1997); Part 4: Hash-functions using modular arithmetic, (FCD, 1997).* International Organization for Standardization, Geneva, Switzerland, 1997. ?? pp.

ISO:2004:IIIb

[ISO04] ISO. *ISO/IEC 10118-3:2004: Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*. International Organization for Standardization, Geneva, Switzerland, February 2004. 94 pp. URL `http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39876`.

Itoh:1993:SCF

[IT93] Toshiya Itoh and Makoto Takeda. A simple construction for a family of collision intractable hash functions. *Electronics and communications in Japan. Part 3, Fundamental electronic science*, 76(12):77–84, December 1, 1993. CODEN ECJSER. ISSN 1042-0967 (print), 1520-6440 (electronic).

Ideguchi:2014:IDC

[ITP14] Kota Ideguchi, Elmar Tischhauser, and Bart Preneel. Internal differential collision attacks on the reduced-round Grøstl-0 hash function. *Designs, Codes, and Cryptography*, 70(3): 251–271, March 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (elec-

tronic). URL http://link.springer.com/article/10.1007/s10623-012-9674-6.

Jacobson:1992:ETH

[Jac92] David Jacobson. Engineer's toolbox: Hashing in Mathematica. *Mathematica Journal*, 2(4):??, Fall 1992. CODEN ???? ISSN 1047-5974 (print), 1097-1610 (electronic). URL http://www.mathematica-journal.com/issue/v2i4/tutorials/toolbox/index.html.

Jaeschke:1981:RHM

[Jae81] G. Jaeschke. Reciprocal hashing: a method for generating minimal perfect hashing functions. *Communications of the Association for Computing Machinery*, 24(12):829–833, December 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Hash functions, for a key x in a set S of positive integers, of the form $h(x) = (C/(Dx+E)) \bmod N$ are considered. Though the existence of h is guaranteed, the scheme suffers from many practical problems because of exhaustive nature of the search for h.

Jagannathan:1991:OPM

[Jag91] Raj Jagannathan. Optimal partial-match hashing design. *ORSA Journal on Computing*, 3(2):86–??, Spring 1991. CODEN OJCOE3. ISSN 0899-1499.

Jain:1989:CHS

[Jai89] Raj Jain. A comparison of hashing schemes for address lookup in computer networks. Technical Report DEC-TR-593, Digital Equipment Corporation, February 1989. ?? pp.

Jain:1992:CHSa

[Jai92a] R. Jain. A comparison of hashing schemes for address lookup in computer networks. Technical report, DEC, 1992. 17 pp. URL http://www.cis.ohio-state.edu/~jain/papers/hash_ps.htm.

Jain:1992:CHSb

[Jai92b] R. Jain. A comparison of hashing schemes for address lookup in computer networks. *IEEE Trans. Comm.*, 40(10):1570–1573, October 1, 1992. CODEN IECMBT. ISSN 0090-6778 (print), 1558-0857 (electronic). URL http://www.cis.ohio-state.edu/~jain/papers/hash_ieee_2col.htm.

Jain:19xx:CHS

[Jaixx] Raj Jain. A comparison of hashing schemes for address lookup in computer networks. Technical Report DEC-TR-566, Digital Equipment Corporation, 19xx. ??

pp. URL `jain%erlang.dec@decwrl.dec.com`.

Jaja:1990:SFM

[Jáj90] Joseph Jájá, editor. *The 3rd Symposium on the Frontiers of Massively Parallel Computation: Proceedings, Held at the University of Maryland, College Park, Maryland, October 8–10, 1990*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. ISBN 0-8186-9053-4. LCCN QA76.58 .S95 1990.

Jakobsson:1985:SRL

[Jak85] Matti Jakobsson. Sampling without replacement in linear time. *The Computer Journal*, 28(4):412–413, August 1985. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Janson:2005:IDL

[Jan05] Svante Janson. Individual displacements for linear probing hashing with different insertion policies. *ACM Transactions on Algorithms*, 1(2):177–213, October 2005. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

Janson:2008:IDH

[Jan08] Svante Janson. Individual displacements in hashing with coalesced chains. *Combinatorics, Probability and Computing*, 17(6):799–814, November 2008. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic).

Jarke:1994:ADT

[JBJ94] Matthias Jarke, Janis Bubenko, and Keith Jeffery, editors. *Advances in database technology — EDBT '94: 4th International Conference on Extending Database Technology, Cambridge, United Kingdom, March 28–31, 1994: proceedings*, volume 779 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. ISBN 0-387-57818-8 (New York), 3-540-57818-8 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.D3 I55844 1994. DM80.00.

Jiang:2011:GBM

[JBWK11] Xiaoyi Jiang, Klaus Broelemann, Steffen Wachenfeld, and Antonio Krüger. Graph-based markerless registration of city maps using geometric hashing. *Computer vision and image understanding: CVIU*, 115 (7):1032–1043, July 2011. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1077314211000828`.

Jan:1988:ALO

[JC88a] Jinn-Ke Jan and Chin-Chen

Chang. Addressing for letter-oriented keys. *Chung-kuo Kung Ch'eng Hsueh K'an/Journal of the Chinese Institute of Engineers*, 11(3): 279–284, May 1988. CODEN JCIEEZ, CKCKDZ. ISSN 0253-3839.

Jones:1988:FTV

[JC88b] Russell K. Jones and Tracy Crabtree. *FORTRAN tools for VAX/VMS and MS-DOS*. John Wiley, New York, NY, USA, 1988. ISBN 0-471-61976-0. xii + 447 pp. LCCN QA76.73.F25 J66 1988. US$29.95. Hash tables are used in the implementation of a FORTRAN preprocessor for macro statements.

Jiang:2000:CSM

[JCC00] J.-H. Jiang, C.-C. Chang, and T.-S. Chen. A compact sparse matrix representation using random hash functions. *Data and Knowledge Engineering*, 32(1):29–49, January 2000. CODEN DKENEW. ISSN 0169-023X (print), 1872-6933 (electronic).

Jun:2018:RBD

[JCK+18] Jaeyung Jun, Kyu Hyun Choi, Hokwon Kim, Sang Ho Yu, Seon Wook Kim, and Youngsun Han. Recovering from biased distribution of faulty cells in memory by reorganizing replacement regions through universal hashing. *ACM Transactions on Design Automation of Electronic Systems.*, 23(2):16:1–16:??, January 2018. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Chang:2012:TRR

[jCPB+12] Shu jen Chang, Ray Perlner, William E. Burr, Meltem Sönmez Turan, John M. Kelsey, Souradyuti Paul, and Lawrence E. Bassham. Third-round report of the SHA-3 Cryptographic Hash Algorithm Competition. Technical Report NISTIR 7896, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, November 2012. 84 pp. URL `http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf`.

Junczys-Dowmunt:2012:SEP

[JD12] Marcin Junczys-Dowmunt. A space-efficient phrase table implementation using minimal perfect hash functions. *Lecture Notes in CS*, 7499:320–327, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-32790-2_39`.

Jia:2019:ETS

[JDW+19] Ruoxi Jia, David Dao, Boxin Wang, Frances Ann Hubis,

Nezihe Merve Gurel, Bo Li, Ce Zhang, Costas Spanos, and Dawn Song. Efficient task-specific data valuation for nearest neighbor algorithms. *Proceedings of the VLDB Endowment*, 12(11): 1610–1623, July 2019. CODEN ???? ISSN 2150-8097.

Jenks:1976:SPA

[Jen76] Richard D. Jenks, editor. *Symsac '76: proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation, August 10–12, 1976, Yorktown Heights, New York*. ACM Press, New York, NY 10036, USA, 1976. LCCN QA155.7.E4 A15 1976. US$20.00.

Jenkins:1997:AAH

[Jen97] Bob Jenkins. Algorithm alley: Hash functions. *Dr. Dobbs Journal*, 22(9):107–109, 115–116, September 1997. CODEN DDJOEB. ISSN 1044-789X. Describes a new hash function which is much better at producing uniform key distributions than others commonly used, yet remains acceptably fast. See [Boy98] for comparison with a related algorithm.

Janzadeh:2009:SCB

[JFDF09] Hamed Janzadeh, Kaveh Fayazbakhsh, Mehdi Dehghan, and Mehran S. Fallah. A secure credit-based cooperation stimulating mechanism for MANETs using hash chains. *Future Generation Computer Systems*, 25(8): 926–934, September 2009. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Joux:1995:PAA

[JG95] A. Joux and L. Granboulan. A practical attack against knapsack based hash functions. In De Santis [De 95], pages 58–66. ISBN 3-540-60176-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E965 1995.

Jha:2015:IMM

[JHL+15] Saurabh Jha, Bingsheng He, Mian Lu, Xuntao Cheng, and Huynh Phung Huynh. Improving main memory hash joins on Intel Xeon Phi processors: an experimental approach. *Proceedings of the VLDB Endowment*, 8(6): 642–653, February 2015. CODEN ???? ISSN 2150-8097.

Jung:2011:SHB

[JK11] Hyunhee Jung and Hyun Sung Kim. Secure hash-based password authentication protocol using Smartcards. *Lecture Notes in CS*, 6786: 593–606, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-21934-4_48`.

Jeong:2014:ITP

[JL14] EunHee Jeong and ByungKwan Lee. An IP Traceback Protocol using a compressed hash table, a sinkhole router and data mining based on network forensics against network attacks. *Future Generation Computer Systems*, 33(??):42–52, April 2014. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X13002410`.

Jeong:2008:PBH

[JLH08] JongMin Jeong, GooYeon Lee, and Zygmunt J. Haas. Prevention of black-hole attack using one-way hash chain scheme in ad-hoc networks. *Lecture Notes in CS*, 5200:564–573, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-89524-4_56`.

Jin:2020:HAH

[JLL+20] H. Jin, Z. Li, H. Liu, X. Liao, and Y. Zhang. Hotspot-aware hybrid memory management for in-memory key–value stores. *IEEE Transactions on Parallel and Distributed Systems*, 31(4):779–792, April 2020. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Jovanov:2002:ANO

[JMH02] E. Jovanov, V. Milutinovic, and A. R. Hurson. Acceleration of nonnumeric operations using hardware support for the Ordered Table Hashing algorithms. *IEEE Transactions on Computers*, 51(9):1026–1040, September 2002. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1032623`.

Jean:2014:ICA

[JNPP14] Jérémy Jean, María Naya-Plasencia, and Thomas Peyrin. Improved cryptanalysis of `AES`-like permutations. *Journal of Cryptology*, 27(4):772–798, October 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9156-7`.

Jaeschke:1980:CMP

[JO80] G. Jaeschke and G. Osterburg. On Cichelli's minimal perfect hash functions method. *Communications of the Association for Computing Machinery*, 23(12):728–729, December 1980. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). This letter to the editor contains comments on [Cic80b], together with a re-

sponse from R. J. Cichelli [Cic80a].

Johnson:1961:ICM

[Joh61] L. R. Johnson. An indirect chaining method for addressing on secondary keys. *Communications of the Association for Computing Machinery*, 4(5):218–222, May 1961. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Johansson:1997:BHS

[Joh97] T. Johansson. Bucket hashing with a small key size. *Lecture Notes in CS*, 1233:149–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jouannaud:1985:FPL

[Jou85] Jean-Pierre Jouannaud, editor. *Functional Programming Languages and Computer Architecture. Proceedings of a Conference (Nancy, France, Sept. 1985)*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1985. ISBN 0-387-15975-4. LCCN QA76.7 .F861 1985.

Joux:2004:MIH

[Jou04] Antoine Joux. Multicollisions in iterated hash functions. application to cascaded constructions. In Franklin [Fra04], pages 306–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3152`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b99099`.

Joye:2003:TCC

[Joy03] Marc Joye, editor. *Topics in cryptology, CT-RSA 2003: the Cryptographers' Track at the RSA Conference 2003, San Francisco, CA, USA, April 13–17, 2003: Proceedings*, volume 2612 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612`.

Jutla:2007:PGC

[JP07] Charanjit S. Jutla and Anindya C. Patthak. Provably good codes for hash function design. *Lecture Notes in CS*, 4356: 376–393, 2007. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-74462-7_26.

Jensen:2008:OEM

[JP08] Morten Skaarup Jensen and Rasmus Pagh. Optimality in external memory hashing. *Algorithmica*, 52(3): 403–411, November 2008. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0178-4617&volume=52&issue=3&spage=403.

Jeon:2007:SAP

[JRPK07] Jin-Oh Jeon, Su-Bong Ryu, Sang-Jo Park, and Min-Sup Kang. Strong authentication protocol for RFID tag using SHA-1 hash algorithm. *Lecture Notes in CS*, 4705:634–643, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-74472-6_51.

Jin:2009:SMB

[JTOT09] Zhe Jin, Andrew Beng Jin Teoh, Thian Song Ong, and Connie Tee. Secure minutiae-based fingerprint templates using random triangle hashing. *Lecture Notes in CS*, 5857:521–531, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-05036-7_49.

Jung:1987:IRC

[Jun87] Achim Jung. Implementing the RSA cryptosystem. *Computers and Security*, 6(4): 342–350, August 1987. CODEN CPSEDU. ISSN 0167-4048.

Jacobs:1986:TRT

[Jv86] Christiaan T. M. Jacobs and Peter van Emde Boas. Two results on tables. *Information Processing Letters*, 22(1):43–48, January 1986. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Janson:2016:UAL

[JV16] Svante Janson and Alfredo Viola. A unified approach to linear probing hashing with buckets. *Algorithmica*, 75(4): 724–781, August 2016. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL http://link.springer.com/article/10.1007/s00453-015-0111-x.

Jia:2018:PPH

[JWM+18] C. J. Jia, Y. Wang, C. B. Mendl, B. Moritz, and T. P. Devereaux. Paradeisos: a perfect hashing algorithm for

many-body eigenvalue problems. *Computer Physics Communications*, 224(??): 81–89, March 2018. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0010465517303946`.

Jiang:2007:DHT

[JXY07] Yi Jiang, Guangtao Xue, and Jinyuan You. Distributed hash table based peer-to-peer version control system for collaboration. *Lecture Notes in CS*, 4402:489–498, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-72863-4_50`.

Joux:2014:SAC

[JY14] Antoine Joux and Amr Youssef, editors. *Selected areas in cryptography — SAC 2014: 21st International Conference, Montréal, QC, Canada, August 14–15, 2014: revised selected papers*, volume 8781 of *Lecture notes in computer science: LNCS sublibrary. SL 4, Security and cryptology*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2014. ISBN 3-319-13050-1 (print), 3-319-13051-X (e-book). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25.

Kabe:1987:RRT

[Kab87] D. G. Kabe. Reducing the retrieval time of hashing methods by using bucket size. *Industrial Mathematics*, 37(pt 1):93–102, 1987. CODEN IMTHAI. ISSN 0019-8528.

Kahrs:1992:UUL

[Kah92] S. Kahrs. Unlimp, uniqueness as a leitmotiv for implementation. In Bruynooghe and Wirsing [BW92], pages 115–129. ISBN 0-387-55844-6 (New York), 3-540-55844-6 (Berlin). LCCN QA76.7 .I5773 1992.

Kak:1983:EMP

[Kak83] Subhash C. Kak. Exponentiation modulo a polynomial for data security. *International Journal of Computer and Information Sciences*, 12(5):337–346, October 1983. CODEN IJCIAH. ISSN 0091-7036.

Kak:1993:NNA

[Kak93] Subhash Kak. Neural networks and artificial intelligence. *Information Sciences*, 70(1/2):1, 1993. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Kaliski:1993:SES

[Kal93] Burt Kaliski. A survey of encryption standards. *IEEE Micro*, 13(6):74–81, November/December 1993. CODEN IEMIDZ. ISSN 0272-

1732 (print), 1937-4143 (electronic).

Kaliski:2001:HFF

[Kal01] Burton S. Kaliski Jr. On hash function firewalls in signature schemes. *Lecture Notes in CS*, 2271:1–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2271/22710001.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2271/22710001.pdf`.

Kaman:1974:HC

[Kam74] Charles H. Kaman. Hash coding. *Polimery*, ??(??): 229–232, ???? 1974.

Kanada:1990:VTH

[Kan90] Yasusi Kanada. Vectorization technique of hashing and its application to several sorting algorithms. In *Proceedings — Parbase-90 International Conference on Databases, Parallel Architectures, and Their Applications (Mar 7–9 1990: Miami Beach, FL, USA)*, pages 147–151. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. IEEE catalog number 90CH2728-4.

Kanada:1991:MVP

[Kan91] Y. Kanada. A method of vector processing for shared symbolic data. In IEEE [IEE91a], pages 722–731. ISBN 0-8186-9158-1 (IEEE case), 0-8186-2158-3 (IEEE paper), 0-8186-6158-5 (IEEE microfiche), 0-89791-459-7 (ACM). LCCN QA76.5 .S894 1991. ACM order number 415913. IEEE Computer Society Press order number 2158. IEEE catalog number 91CH3058-5.

Kanada:1993:MVP

[Kan93] Y. Kanada. A method of vector processing for shared symbolic data. *Parallel Computing*, 19(10):1155–1175, October 1993. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Karlsson:1982:ACR

[Kar82] K. Karlsson. *Les Arbres Couvrants Reduits: Une Methode D'acces Compacte Pour Donnees Dynamiques*. PhD thesis, ????, Paris, France, 1982. ?? pp.

Karloff:1998:PNA

[Kar98] Howard Karloff, editor. *Proceedings of the ninth annual ACM-SIAM symposium on Discrete algorithms, San Francisco, California, January 25–27, 1998*, volume 95 of *Proceedings in Applied Mathematics Ser.* ACM

Press, New York, NY 10036, USA, 1998. ISBN 0-89871-410-9. LCCN QA76.6 .A278 1998. URL `http://dl.acm.org/citation.cfm?id=314613`.

Khanal:2022:UBI

[KAS+22] Yurika Pant Khanal, Abeer Alsadoon, Khurram Shahzad, Ahmad B. Al-Khalil, Penatiyana W. C. Prasad, Sabih Ur Rehman, and Rafiqul Islam. Utilizing blockchain for IoT privacy through enhanced ECIES with secure hash function. *Future Internet*, 14(3):77, February 28, 2022. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/14/3/77`.

Kawagoe:1985:MDH

[Kaw85] Kyoji Kawagoe. Modified dynamic hashing. In Navathe [Nav85], pages 201–213. ISBN 0-89791-160-1. LCCN QA 76.9 D3 I59 1985.

Kawamoto:2015:LSH

[Kaw15] Junpei Kawamoto. A locality sensitive hashing filter for encrypted vector databases. *Fundamenta Informaticae*, 137(2):291–304, April 2015. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Kanj:2018:SNN

[KBG18] Sawsan Kanj, Thomas Brüls, and Stéphane Gazut. Shared nearest neighbor clustering in a locality sensitive hashing framework. *Journal of Computational Biology*, 25(2): 236–250, February 2018. CODEN JCOBEM. ISSN 1066-5277 (print), 1557-8666 (electronic). URL `https://www.liebertpub.com/doi/abs/10.1089/cmb.2017.0113`; `https://www.liebertpub.com/doi/pdf/10.1089/cmb.2017.0113`.

Krause:1981:PHF

[KCB81] Max Krause, Nick Cercone, and John Boates. Perfect hash function search with application to natural language systems. Technical Report CMPT TR 81-6, Simon Fraser University, 1981. ?? pp. (email `library@cs.sfu.ca`).

Ku:2005:WYR

[KCC05] Wei-Chi Ku, Min-Hung Chiang, and Shen-Tien Chang. Weaknesses of Yoon–Ryu–Yoo's hash-based password authentication scheme. *Operating Systems Review*, 39 (1):85–89, January 2005. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Kirk:1984:CMI

[KCF84] M. Kirk, R. J. Chignell, and J. Finnie. Computer model to indentify incompatibilities between the FM sound broadcasting and aero-

nautical bands. *IERE Conference Proceedings*, 60, 1984. CODEN IERCB6. ISBN 0-903748-56-8. ISSN 0538-0006.

Ku:2003:WLL

[KCL03] Wei-Chi Ku, Chien-Ming Chen, and Hui-Lung Lee. Weaknesses of Lee–Li–Hwang's hash-based password authentication scheme. *Operating Systems Review*, 37(4):19–25, October 2003. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Kim:2011:SSE

[KCR11] Changhoon Kim, Matthew Caesar, and Jennifer Rexford. SEATTLE: a Scalable Ethernet Architecture for Large Enterprises. *ACM Transactions on Computer Systems*, 29(1):1:1–1:35, February 2011. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Koushik:1992:LDH

[KD92] Murlidhar Koushik and George Diehr. Linear-density hashing with dynamic overflow sharing. *Information system*, 17(5):359–380, September 1992. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Knott:1989:HTC

[KdlT89] Gary D. Knott and Pilar de la Torre. Hash table collision resolution with direct chaining. *Journal of Algorithms*, 10(1): 20–34, March 1989. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0196677489900217`.

Keller:1993:HRP

[Kel93] Joerg Keller. Hashing and rehashing in PRAM emulations. In *Proceedings of the 3rd Workshop on Parallel Algorithms (WOPA)*, page ?? ????, ????, May 1993.

Keller:1996:FRP

[Kel96] J. Keller. Fast rehashing in PRAM emulations. *Theoret. Comput. Sci.*, 155(2): 349–363, March 11, 1996. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Kennedy:1973:RSU

[Ken73] Ken Kennedy. Reduction in strength using hashed temporaries. Technical Report SETL Newsletter #102, Courant Inst. of Math. Sciences, New York University, New York, March 1973. ?? pp.

Kerr:1975:PIC

[Ker75] Douglas S. Kerr, editor. *Proceedings of the International*

Conference on Very Large Data Bases, Framingham, MA, USA, September 22–24, 1975. ACM Press, New York, NY 10036, USA, 1975. ISBN ???? ISSN 0278-2596. LCCN QA76.9.D3 I55 1975. US$15.00.

Kocberber:2015:AMA

[KFG15] Onur Kocberber, Babak Falsafi, and Boris Grot. Asynchronous memory access chaining. *Proceedings of the VLDB Endowment*, 9 (4):252–263, December 2015. CODEN ???? ISSN 2150-8097.

Kak:1995:ILM

[KG95] Avinash C. Kak and Lynne Grewe. Interactive learning of a multiple-attribute hash table classifier for fast object recognition. *Computer vision and image understanding: CVIU*, 61(3):387–??, May 1, 1995. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic).

Kaushik:2012:MGH

[KGJG12] Vandana Dixit Kaushik, Amit K. Gupta, Umarani Jayaraman, and Phalguni Gupta. Modified geometric hashing for face database indexing. *Lecture Notes in CS*, 6839:608–613, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-25944-9_79`.

Kralevska:2018:HEC

[KGJØ18] K. Kralevska, D. Gligoroski, R. E. Jensen, and H. Øverby. HashTag erasure codes: From theory to practice. *IEEE Transactions on Big Data*, 4(4):516–529, December 2018. ISSN 2332-7790.

Karplus:1984:FMP

[KH84] K. Karplus and G. Haggard. Finding minimal perfect hash functions. Technical Report 84-637, Cornell University, September 1984. ?? pp. (email `lmc@cs.cornell.edu`).

Khan:1995:PDH

[Kha95] Zahira S. Khan. *Performance of the distributed hash join algorithms in a distributed heterogeneous supercomputing environment*. Thesis (Ph.D.), Temple University, Philadelphia, PA, USA, 1995. xxii + 220 pp.

Kuo:1989:DSF

[KHH89] Y. S. Kuo, S.-Y. Hwang, and H. F. Hu. Data structure for fast region searches. *IEEE Design & Test of Computers*, 6(5):20–28, October 1989. CODEN IDTCEC. ISSN 0740-7475 (print), 1558-1918 (electronic).

Kortelainen:2010:MAG

[KHK10] Juha Kortelainen, Kimmo Halunen, and Tuomas Kortelainen. Multicollision attacks and generalized iterated hash functions. *Journal of Mathematical Cryptology*, 4(3):239–270, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Kanizo:2012:HTF

[KHK12] Yossi Kanizo, David Hay, and Isaac Keslassy. Hash tables with finite buckets are less resistant to deletions. *Computer Networks (Amsterdam, Netherlands: 1999)*, 56(4):1376–1389, March 16, 2012. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128611004476`.

Kanizo:2015:MTH

[KHK15] Yossi Kanizo, David Hay, and Isaac Keslassy. Maximizing the throughput of hash tables in network devices with combined SRAM/DRAM memory. *IEEE Transactions on Parallel and Distributed Systems*, 26(3): 796–809, March 2015. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL `http://www.computer.org/csdl/trans/td/2015/03/06781627-abs.html`.

Kitsuregawa:1989:JSK

[KHT89] M. Kitsuregawa, L. Harada, and M. Takagi. Join strategies on KD-tree indexed relations. In *Proceedings of the Fifth International Conference on Data Engineering*, pages 85–93. ????, Los Angeles, CA, USA, February 1989.

Kim:1991:ISSa

[KHW91a] Yul H. Kim, Mark D. Hill, and David A. Wood. Implementing stack simulation for highly-associative memories. Technical Report TR 997, Computer Sciences Department, University of Wisconsin–Madison, February 1991. ?? pp.

Kim:1991:ISSb

[KHW91b] Yul H. Kim, Mark D. Hill, and David A. Wood. Implementing stack simulation for highly-associative memories. *ACM SIGMETRICS Performance Evaluation Review*, 19 (1):212–213, May 1991. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Kak:1994:CVW

[KI94] A. C. Kak and K. Ikeuchi, editors. *2nd CAD-based vision workshop: – February 1994, Champion, PA*, PROCEEDINGS OF THE CAD BASED VISION WORKSHOP 1994; 2nd. IEEE Computer Society Press, 1109 Spring Street,

Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-8186-5310-8, 0-8186-5311-6. LCCN TA1632 .C33 1994.

Kiessling:1985:DFU

[Kie85] W. Kiessling. Dynamic filters: a uniform concept for query optimization in set-oriented database architectures. Technical report, Technical University ofMunchen, 1985. ?? pp.

Kiltz:2001:PPS

[Kil01] Eike Kiltz. A primitive for proving the security of every bit and about universal hash functions & hard core bits. *Lecture Notes in CS*, 2138:388–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2138/21380388.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2138/21380388.pdf`.

Kilian:2005:TCS

[Kil05] Joe Kilian, editor. *Theory of cryptography: Second theory of cryptography conference, TCC 2005, Cambridge, MA, USA, February 10–12, 2005, proceedings*, volume 3378 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T44 2005. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3378`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b106171`.

Kim:1980:QOR

[Kim80] W. Kim. *Query Optimization for Relational Database Systems*. PhD thesis, University of Illinois, Urbana, October 1980. ?? pp.

Kim:1999:NSP

[Kim99] Sun Kim. A new string-pattern matching algorithm using partitioning and hashing efficiently. *ACM Journal of Experimental Algorithmics*, 4:2:1–2:??, ???? 1999. ISSN 1084-6654.

Kim:2011:EHB

[KJC11] Nam-Uk Kim, Sung-Min Jung, and Tai-Myoung Chung. An efficient hash-based load balancing scheme to support parallel NIDS. *Lecture Notes in CS*, 6782: 537–549, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-21928-3_39`.

Kim:2017:MES

[KJS17] Minchul Kim, Younghoon Jung, and Junghwan Song. A modified exhaustive search on a password system using SHA-1. *International Journal of Information Security*, 16(3):263–269, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0332-2.

Kojima:1985:HFO

[KK85] Isao Kojima and Yahiko Kambayashi. Hash-based file organization utilizing large capacity main memory. In *Proceedings — Foundations of Data Organization.*, pages 41–50. Organizing Committee of the Int Conference on Foundations of Data Organization, Jpn, 1985. Kyoto Sangyo Univ. Computer Science Inst, Kyoto, Jpn.

Khan:1996:PCI

[KK96] Z. S. Khan and E. Kwatny. Performance comparison of interprocessor communication schemes for a hashing technique on the Connection Machine. *International Journal of Computer Systems Science and Engineering*, 11(4): 189–??, ???? 1996. CODEN CSSEEI. ISSN 0267-6192.

Kelsey:2006:HHF

[KK06] J. Kelsey and T. Kohno. Herding hash functions and the Nostradamus attack. In Vaudenay [Vau06], pages 183–200. ISBN 3-540-34547-7. LCCN ???? URL http://www.springerlink.com/content/978-3-540-34547-3.

Kakvi:2012:OSP

[KK12] Saqib A. Kakvi and Eike Kiltz. Optimal security proofs for full domain hash, revisited. *Lecture Notes in CS*, 7237:537–553, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_31; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_32/; http://link.springer.com/content/pdf/10.1007/978-3-642-29011-4_32.

Kakvi:2018:OSP

[KK18] Saqib A. Kakvi and Eike Kiltz. Optimal security proofs for full domain hash, revisited. *Journal of Cryptology*, 31(1):276–306, January 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9257-9.

Kim:2012:SSL

[KKC12] Saehoon Kim, Yoonseop Kang, and Seungjin Choi. Sequential spectral learning

to hash with multiple representations. *Lecture Notes in CS*, 7576:538–551, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-33715-4_39`.

Kim:2009:SVH

[KKL+09] Changkyu Kim, Tim Kaldewey, Victor W. Lee, Eric Sedlar, Anthony D. Nguyen, Nadathur Satish, Jatin Chhugani, Andrea Di Blas, and Pradeep Dubey. Sort vs. Hash revisited: fast join implementation on modern multicore CPUs. *Proceedings of the VLDB Endowment*, 2 (2):1378–1389, August 2009. CODEN ???? ISSN 2150-8097.

Lioma:2008:AHT

[KKMS10] Shahram Khazaei, Simon Knellwolf, Willi Meier, and Deian Stefan. Improved linear differential attacks on CubeHash. *Lecture Notes in CS*, 6055:407–418, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-12678-9_24`.

Kaski:2012:HHS

[KKN12] Petteri Kaski, Mikko Koivisto, and Jesper Nederlof. Homomorphic hashing for sparse coefficient extraction. *Lecture Notes in CS*, 7535: 147–158, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-33293-7_15/`.

Kim:1992:DSN

[KKP92] Won Kim, Y. Kambayashi, and In Sup Paik, editors. *Database systems for next-generation applications: principles and practice*, volume 1 of *Advanced Database Research and Development Series*. World Scientific Publishing Co. Pte. Ltd., P. O. Box 128, Farrer Road, Singapore 9128, 1992. ISBN 981-02-1315-8. LCCN QA76.9.D3 D3589 1992.

Kabiljo:2017:SHP

[KKP+17] Igor Kabiljo, Brian Karrer, Mayank Pundir, Sergey Pupyrev, and Alon Shalita. Social hash partitioner: a scalable distributed hypergraph partitioner. *Proceedings of the VLDB Endowment*, 10(11):1418–1429, August 2017. CODEN ???? ISSN 2150-8097.

Kim:2007:EIK

[KKRJ07] Mooseop Kim, Youngse Kim, Jaecheol Ryou, and Sungik Jun. Efficient implementation of the keyed-hash message authentication code based on SHA-1 algorithm

for mobile trusted computing. *Lecture Notes in CS*, 4610:410–419, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-73547-2_42`.

Kurosawa:1991:CFH

[KKT91] Kaoru Kurosawa, Hirofumi Kasai, and Shigeo Tsujii. Collision free hash function based on the r-th residue cryptosystem. *IEICE Transactions on Communications/Electronics/Information and Systems*, E74(8):2114–2117, 1991. CODEN IEITEF. ISSN 0917-1673.

Kemper:1999:GHT

[KKW99] Alfons Kemper, Donald Kossmann, and Christian Wiesner. Generalised hash teams for join and group-by. In Atkinson et al. [AOV+99], pages 30–41. ISBN 1-55860-615-7. LCCN QA76.9.D3 I559 1999. URL `http://www.vldb.org/dblp/db/conf/vldb/KemperKW99.html`. Also known as VLDB'99.

Kim:1987:ESJ

[KL87] Chang D. Kim and Yoon J. Lee. Execution strategies for join operation in multi-processor main memory based database system. In *Proceedings — TENCON 87: 1987 IEEE Region 10 Conference, 'Computers and Communications Technology Toward 2000'.*, pages 302–306. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. IEEE Service Cent. Piscataway, NJ, USA.

Knudsen:1995:NAA

[KL95] L. R. Knudsen and X. Lai. New attacks on all double block length hash functions of hash rate 1, including the parallel-DM. In De Santis [De 95], pages 410–418. ISBN 3-540-60176-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E965 1995.

Katajainen:1996:EUH

[KL96] Jyrki Katajainen and Michael Lykke. Experiments with universal hashing. DIKU Report 96/8, Department of Computer Science, University of Copenhagen, Copenhagen, Denmark, ???? 1996.

Kencl:2008:ALS

[KL08] Lukas Kencl and Jean-Yves Le Boudec. Adaptive load sharing for network processors. *IEEE/ACM Transactions on Networking*, 16(2): 293–306, April 2008. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Katz:2015:IMC

[KL15] Jonathan Katz and Yehuda Lindell. *Introduction to mod-*

ern cryptography. Chapman and hall/CRC cryptography and network security series. Taylor and Francis, London, UK and Boca Raton, FL, USA, second edition, 2015. ISBN 1-4665-7026-1 (hardcover). 583 pp. LCCN QA76.9.A25 K36 2014.

Karp:1993:EPS

[KLadH93] R. Karp, M. Luby, and F. Meyer auf der Heide. Efficient PRAM simulation on a distributed memory machine. Technical Report TR-93-040, International Computer Science Institute, Berkeley, CA, USA, August 1993. ?? pp.

Karger:1997:CHR

[KLL+97] David Karger, Eric Lehman, Tom Leighton, Rina Panigrahy, Matthew Levine, and Daniel Lewin. Consistent hashing and random trees: distributed caching protocols for relieving hot spots on the World Wide Web. In ACM [ACM97b], pages 654–663. ISBN 0-89791-888-6. LCCN QA76.5 .A849 1997. URL `http://www.acm.org/pubs/articles/proceedings/stoc/258533/p654-karger/p654-karger.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/258533/p654-karger/`. ACM order no. 508970.

Karp:1996:EPS

[KLM96] Richard M. Karp, Michael Luby, and Friedhelm Meyer auf der Heide. Efficient PRAM simulation on a distributed memory machine. *Algorithmica*, 16(4–5):517–542, 1996. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Knudsen:1998:AFD

[KLP98] Lars R. Knudsen, Xuejia Lai, and Bart Preneel. Attacks on fast double block length hash functions. *Journal of Cryptology*, 11(1):59–72, Winter 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/bibs/11n1p59.html`; `http://link.springer.de/link/service/journals/00145/bibs/11n1p59.pdf`; `http://link.springer.de/link/service/journals/00145/bibs/11n1p59.tex`; `http://link.springer.de/link/service/journals/00145/tocs/01101.html`.

Kompella:2012:RSF

[KLSV12] Ramana Rao Kompella, Kirill Levchenko, Alex C. Snoeren, and George Varghese. Router support for fine-grained latency measurements. *IEEE/ACM Transactions on Networking*, 20(3): 811–824, June 2012. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

King:2007:CRP

[KLSY07] Valerie King, Scott Lewis, Jared Saia, and Maxwell Young. Choosing a random peer in chord. *Algorithmica*, 49(2):147–169, October 2007. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0178-4617&volume=49&issue=2&spage=147`.

Koczkodaj:1992:IPF

[KLT92] Waldemar W. Koczkodaj, Peter E. Lauer, and Anestis A. Toptsis, editors. *ICCI '92: Proceedings, Fourth International Conference on Computing and Information, May 28–30, 1992, Toronto, Ontario*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. ISBN 0-8186-2812-X (hardcover), 0-8186-2811-1 (microfiche). LCCN QA75.5 .I587 1992.

Koerner:1986:IFB

[KM86] J. Koerner and K. Marton. Improved Fredman-Komlos bounds for perfect hashing via information theory. In *1986 IEEE International Symposium on Information Theory (ISIT)*., pages 118–?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1986. IEEE Service Cent. Piscataway, NJ, USA.

Korner:1988:NBP

[KM88a] J. Korner and K. Marton. New bounds for perfect hashing via information theory. *European Journal of Combinatorics*, 9(6):523–??, November 1, 1988. CODEN EJOCDI. ISSN 0195-6698.

Korner:1988:RAC

[KM88b] J. Korner and K. Marton. Random access communication and graph entropy. *IEEE Transactions on Information Theory*, 34(2):312–314, March 1988. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Kato:1992:PCI

[KM92] K. Kato and T. Masuda. Persistent caching: An implementation technique for complex objects with object identity. *IEEE Transactions on Software Engineering*, 18(7):631–645, July 1992. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=148481`.

Kirsch:2007:UQA

[KM07] A. Kirsch and M. Mitzenmacher. Using a queue to de-amortize cuckoo hashing in hardware. In ????, editor, *Proceedings of the 45th*

Annual Allerton Conference on Communication, Control, and Computing 2007: September 26-28, 2007, Monticello, Illinois, USA, pages 751–758. Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Urbana, IL, USA, 2007. ISBN 1-60560-086-5. LCCN QA76 A434 2007. URL ????.

Kirsch:2008:SSH

[KM08] Adam Kirsch and Michael Mitzenmacher. Simple summaries for hashing with choices. *IEEE/ACM Transactions on Networking*, 16 (1):218–231, February 2008. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Karroumi:2009:HBK

[KM09] Mohamed Karroumi and Ayoub Massoudi. Hash-based key management schemes for MPEG4–FGS. *Lecture Notes in CS*, 5451: 245–256, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-00843-6_22`.

Kirsch:2010:POM

[KM10] Adam Kirsch and Michael Mitzenmacher. The power of one move: hashing schemes for hardware. *IEEE/ACM Transactions on Networking*, 18(6):1752–1765, December 2010. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Kakarountas:2006:HSF

[KMM+06] Athanasios P. Kakarountas, Haralambos Michail, Athanasios Milidonis, Costas E. Goutis, and George Theodoridis. High-speed FPGA implementation of secure hash algorithm for IPSec and VPN applications. *The Journal of Supercomputing*, 37 (2):179–195, August 2006. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=37&issue=2&spage=179`.

Kirsch:2010:HBT

[KMV10] Adam Kirsch, Michael Mitzenmacher, and George Varghese. Hash-based techniques for high-speed packet processing. Part 2. In Cormode and Thottan [CT10], pages 181–218. ISBN 1-84882-764-4. LCCN TK5105.5 .A39523 2010. URL `http://www.springerlink.com/content/t607n8n626515k62/`.

Kirsch:2008:MRH

[KMW08] Adam Kirsch, Michael Mitzenmacher, and Udi Wieder.

More robust hashing: Cuckoo hashing with a stash. In Halperin and Mehlhorn [HM08], pages 611–622. CODEN LNCSD9. ISBN 3-540-87744-4, 3-540-87743-6 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A43 E83 2008. URL `http://link.springer.com/content/pdf/10.1007/978-3-540-87744-8_51`; `http://www.springerlink.com/content/24620h6712831010/`.

Kirsch:2010:MRH

[KMW10] Adam Kirsch, Michael Mitzenmacher, and Udi Wieder. More robust hashing: Cuckoo hashing with a stash. *SIAM Journal on Computing*, 39 (4):1543–1561, ???? 2010. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Knafl:1989:PSC

[Kna89] George J. Knafl, editor. *Proceedings 13: September 20–22, 1989: Compsac 89 / the Thirteenth Annual International Computer Software and Applications Conference, Hyatt Orlando Hotel, Orlando, Florida*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. ISBN 0-8186-1964-3. LCCN QA76.6 .C62951 1989.

Knott:1971:EOA

[Kno71] G. D. Knott. Expandable open addressing hash table storage and retrieval. In *ACM SIGFIDET, Codd(ed), 1971*, page ?? ????, ????, 1971.

Knott:1975:HF

[Kno75] Gary D. Knott. Hashing functions. *The Computer Journal*, 18(3):265–278, August 1975. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/18/3/265.full.pdf+html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/265.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/266.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/267.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/268.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/269.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/270.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/271.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/272.tif`;

http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/273.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/274.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/275.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/276.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/277.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_18/Issue_03/tiff/278.tif. Also published in/as: Stanford University Report, 1975. Section 3, "A history of hashing schemes", and the lengthy bibliography, are recommended and useful resources.

Knott:1984:DCC

[Kno84] Gary D. Knott. Direct-chaining with coalescing lists. *Journal of Algorithms*, 5(1): 7–21, March 1984. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic). URL http://www.sciencedirect.com/science/article/pii/0196677484900361.

Knott:1988:LOA

[Kno88] Gary D. Knott. Linear open addressing and Peterson's theorem rehashed. *BIT (Copenhagen)*, 28(2): 364–371, 1988. CODEN NBITAB.

Khovratovich:2010:RRA

[KNR10] Dmitry Khovratovich, Ivica Nikolić, and Christian Rechberger. Rotational rebound attacks on reduced Skein. Report, University of Luxembourg, Luxembourg, October 20, 2010. 20 pp. URL http://eprint.iacr.org/2010/538.

Kitsuregawa:1989:EBS

[KNT89] Masaru Kitsuregawa, Masaya Nakayama, and Mikio Takagi. The effect of bucket size tuning in the dynamic hybrid GRACE hash join method. In Apers and Wiederhold [AW89], pages 257–266. CODEN VLDBDP. ISBN 1-55860-101-5. LCCN QA 76.9 D3 I61 1989.

Knuth:1973:ACP

[Knu73] D. E. Knuth. *The Art of Computer Programming, Sorting and Searching*, volume 3. Addison-Wesley, Reading, MA, USA, 1973. ISBN 0-201-03803-X. xi + 723 pp. LCCN QA76.5 .K74.

Knuth:1974:CSR

[Knu74] Donald E. Knuth. Computer science and its relation to mathematics. *American Mathematical Monthly*, 81:323–343, April 1974. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic). A shorter form of this article appeared in *American Scientist* **61** (1973), 707–

713; reprinted in *Computers and People* **23**,9 (September 1974), 8–11; and in *Mathematics: People, Problems, Results*, ed. by Douglas M. Campbell and John C. Higgins, vol. 3 (Belmont, Calif.: Wadsworth, 1984), 37–47. Hungarian translation in *Matematikai Lapok* **24** (1973, published 1975), 345–363. Slovenian translation in *Obzornik za Matematiko in Fiziko* **22** (1975), 129–138, 161–167. Slovak translation (abridged) in *Pokroky Matematiky, Fiziky a Astronomie* **21** (1976), 88–96. Russian translation by Natal'ìà G. Gurevich in *Sovremennye Problemy Matematiki* **11**,12 (Moscow: Znanie, 1977), 4–32.

Knuth:1975:ACP

[Knu75] D. E. Knuth. *The Art of Computer Programming, Sorting and Searching*. Addison-Wesley, Reading, MA, USA, 2 edition, 1975. ISBN 0-201-03803-X. xi + 723 pp. LCCN QA76.5 .K74.

Knuth:1977:DPR

[Knu77] Donald E. Knuth. Deletions that preserve randomness. *IEEE Transactions on Software Engineering*, SE-3(5): 351–359, September 1977. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic).

Knudsen:1992:CL

[Knu92] Lars Ramkilde Knudsen. Cryptanalysis of LOKI. Technical Report DAIMI PB-403, Computer Science Department, Aarhus University, Århus, Denmark, July 1992. 17 pp.

Knuth:1998:LPG

[Knu98] Donald E. Knuth. Linear probing and graphs. *Algorithmica*, 22(4):561–568, December 1998. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL `http://link.springer.de/link/service/journals/00453/bibs/22n4p561.html`; `http://www.springerlink.com/openurl.asp?genre=article&issn=0178-4617&volume=22&issue=4&spage=561`. Average-case analysis of algorithms.

Knudsen:2019:LHA

[Knu19] Mathias Bæk Tejs Knudsen. Linear hashing is awesome. *SIAM Journal on Computing*, 48(2):736–741, ???? 2019. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Kitsuregawa:1990:BSP

[KO90] M. Kitsuregawa and Y. Ogawa. Bucket spreading parallel hash: a new, robust, parallel hash join method for skew in the super database computer

(SDC). In McLeod et al. [MSDS90], page 210. ISBN 1-55860-149-X. LCCN ???

Koehler:1972:SDB

[Koe72] Ch. Koehler. Ein System zur Darstellung und Bearbeitung Assoziativer Datenstrukturen. (German) [a system for displaying and editing associative data structures]. Technical report, ????, Bonn, Germany, 1972. ?? pp.

Kohonen:1980:CAM

[Koh80] Teuvo Kohonen. *Content-addressable memories*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1980. ISBN 0-387-09823-2 (New York), 3-540-09823-2 (Berlin). xi + 368 pp. LCCN TK7895.M4 K63. US$39.00. Hashing is covered in the discussion of software-based content-addressable memories in Chapter 2.

Konheim:2010:HCS

[Kon10] Alan G. Konheim. *Hashing in Computer Science: Fifty Years of Slicing and Dicing*. Wiley, New York, NY, USA, 2010. ISBN 0-470-34473-3, 0-470-63060-4. xvii + 386 pp. LCCN QA76.9.H36 K65 2010. URL `http://www.loc.gov/catdir/enhancements/fy1106/2009052123-b.html`; `http://www.loc.gov/catdir/enhancements/fy1106/2009052123-d.html`; `http://www.loc.gov/catdir/enhancements/fy1106/2009052123-t.html`.

Korf:2008:LTD

[Kor08] Richard E. Korf. Linear-time disk-based implicit graph search. *Journal of the Association for Computing Machinery*, 55(6):26:1–26:40, December 2008. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Koschke:2014:LSI

[Kos14] Rainer Koschke. Large-scale inter-system clone detection using suffix trees and hashing. *Journal of Software: Evolution and Process*, 26(8): 747–769, August 2014. CODEN ???? ISSN 2047-7473 (print), 2047-7481 (electronic).

Koushik:1993:DHD

[Kou93] Murlidhar Koushik. Dynamic hashing with distributed overflow space: a file organization with good insertion performance. *Information system*, 18(5):299–318, September 1993. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Kilov:1981:DMA

[KP81] Kh. I. Kilov and I. A. Popova. Data metabase architecture for relational DBMS. *Programming and*

Computer Software; translation of Programmirovaniye, (Moscow, USSR) Plenum, 7 (1):??, February 1981. CODEN PCSODA. ISSN 0361-7688 (print), 1608-3261 (electronic).

Kedem:1992:OPA

[KP92] Z. M. Kedem and K. V. Palem. Optimal parallel algorithms for forest and term matching. *Theoret. Comput. Sci.*, 93(2):245–264, February 17, 1992. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Krichevskii:1994:CSE

[KP94] R. E. Krichevskii and V. N. Potapov. Combinatorial source encoding and perfect hashing. *IEEE International Symposium on Information Theory*, pages 319–??, 1994. CODEN PISTFZ. ISSN 0271-4655.

Knudsen:1996:HFB

[KP96] L. Knudsen and B. Preneel. Hash functions based on block ciphers and quaternary codes. *Lecture Notes in CS*, 1163:77–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Knudsen:1997:FSH

[KP97] Lars Ramkilde Knudsen and Bart Preneel. Fast and secure hashing based on codes. *Lecture Notes in CS*, 1294:485–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940485.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1294/12940485.pdf`.

Katzenelson:1992:TMT

[KPS92] Jacob Katzenelson, Shlomit S. Pinter, and Eugen Schenfeld. Type matching, typegraphs, and the Schanuel conjecture. *ACM Transactions on Programming Languages and Systems*, 14 (4):574–588, October 1992. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0164-0925/133247.html`.

Kohonen:1979:VFA

[KR79] Teuvo Kohonen and Erkki Reuhkala. Very fast associative method for the recognition and correction of misspelt words, based on redundant hash addressing. *IEEE Technical Papers Presented at the Joint ASME/IEEE/AAR Railroad Conference (Association of American Railroads)*, ??(??): 807–809, ???? 1979.

Karp:1981:ERP

[KR81] R. M. Karp and M. O. Rabin. Efficient randomized pattern-matching algorithms. Technical Report TR-31-81, Harvard University, Cambridge, MA, USA, 1981. ?? pp. An incremental hash function is described for application to the string search problem.

Kelley:1986:IMK

[KR86a] K. L. Kelley and M. Rusinkiewicz. Implementation of multi-key extendible hashing as an access method for a relational DBMS. In ICDE'86 [ICD86], page ?? ISBN 0-8186-0655-X (paperback), 0-8186-8655-3 (hardcover), 0-8186-4655-1 (microfiche). LCCN QA 76.9 D3 I5582 1986.

Kelley:1986:IME

[KR86b] Keith L. Kelley and Marek Rusinkiewicz. Implementation of multi-key extendible hashing as an access method for a relational DBMS. In ICDE'86 [ICD86], pages 124–131. ISBN 0-8186-0655-X (paperback), 0-8186-8655-3 (hardcover), 0-8186-4655-1 (microfiche). LCCN QA 76.9 D3 I5582 1986. IEEE Service Cent. Piscataway, NJ, USA.

Kelley:1988:MEH

[KR88] Keith L. Kelley and Marek Rusinkiewicz. Multikey, extensible hashing for relational databases. *IEEE Software*, 5 (4):77–85, July 1988. CODEN IESOEG. ISSN 0740-7459 (print), 0740-7459 (electronic).

Keller:1991:APH

[KR91] A. Keller and S. Roy. Adaptive parallel hash join in main-memory databases. In PDIS'91 [PDI91], page ?? ISBN 0-8186-2295-4 (paperback), 0-8186-2296-2 (microfiche), 0-8186-2297-0 (hardcover). LCCN QA76.58 .I544 1991.

Krovetz:2001:FUH

[KR01] Ted Krovetz and Phillip Rogaway. Fast universal hashing with small keys and no preprocessing: The PolyR construction. *Lecture Notes in CS*, 2015:73–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2015/20150073.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2015/20150073.pdf`.

Krovetz:2006:VUH

[KR06] Ted Krovetz and Phillip Rogaway. Variationally universal hashing. *Information Processing Letters*, 100(1):36–39, October 16, 2006. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Kishore:2019:PCH

[KR19] Neha Kishore and Priya Raina. Parallel cryptographic hashing: Developments in the last 25 years. *Cryptologia*, 43(6): 504–535, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1609130`.

Krause:1982:PHF

[Kra82] M. Krause. Perfect hash function search. M.sc. thesis, Computing Science Department, Simon Fraser University, Burnaby, BC, Canada, 1982. 168 pp. Available from National Library of Canada, Canadian theses on microfiche, 62311 0227-3845.

Krawczyk:1994:LBH

[Kra94] H. Krawczyk. LFSR-based hashing and authentication. *Lecture Notes in CS*, 839: 129–139, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Krawczyk:1995:NHF

[Kra95] H. Krawczyk. New hash functions for message authentication. In Guillou and Quisquater [GQ95], pages 301–310. ISBN 3-540-59409-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C794 1995.

Krichevsky:1984:OH

[Kri84] R. E. Krichevsky. Optimal hashing. *Information and Control*, 62(1):64–92 (or 64–84??), July 1984. CODEN IFCNA4. ISSN 0019-9958 (print), 1878-2981 (electronic).

Krichevskii:1989:ADC

[Kri89] R. E. Krichevskii. Accelerated determination of codes and hash functions. *Soviet Physics—Doklady*, 34(4): 303–??, April 1, 1989. CODEN SPHDA9. ISSN 0038-5689.

Kohonen:1980:TWR

[KRJ+80] T. Kohonen, H. Riittinen, M. Jalanko, E. Reuhkala, and S. Haltsonen. Thousand-word recognition system based on the learning subspace method and redundant hash addressing. *NATO Conference Series, (Series) 4: Marine Sciences*, 1(??):158–165, ???? 1980.

Kawaguchi:2009:TBD

[KRJ09a] Ming Kawaguchi, Patrick Rondon, and Ranjit Jhala. Type-based data structure verification. *SIGPLAN Notices*, 44(6):304–315, June 2009. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Kim:2009:CIS

[KRJ09b] Mooseop Kim, Jaecheol Ryou, and Sungik Jun. Compact implementation of SHA-1 hash function for mobile trusted module. *Lecture Notes in CS*, 5379: 292–304, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-00306-6_22`.

Kwon:2009:FXD

[KRML09] Joonho Kwon, Praveen Rao, Bongki Moon, and Sukho Lee. Fast XML document filtering by sequencing twig patterns. *ACM Transactions on Internet Technology (TOIT)*, 9(4):13:1–13:??, September 2009. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Kohonen:1984:ORS

[KRRH84] T. Kohonen, H. Riittinen, E. Reuhkala, and S. Haltsonen. On-line recognition of spoken words from a large vocabulary. *Information Sciences*, 33(1/2):3–30, July–August 1984. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic). Application of hash tables to recognition of spoken words.

Knudsen:2007:GFH

[KRT07] L. Knudsen, C. Rechberger, and S. Thomsen. Grindahl — a family of hash functions. In Biryukov [Bir07], pages 39–47. ISBN 3-540-74617-X (softcover). LCCN QA76.9.A25 F77 2007. URL `http://www.springerlink.com/openurl.asp?genre=book\%26isbn=978-3-540-74617-1`.

Kruse:1984:DSP

[Kru84] Robert L. Kruse. *Data Structures and Program Design*. Prentice-Hall Software Series, Editor: Brian W. Kernighan. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1984. ISBN 0-13-196253-1. xxi + 486 pp. LCCN QA76.6 .K77 1984. US$28.95. A standard textbook treatment of well-known hashing algorithms appears on pp. 112–128.

Kriegel:1986:EMD

[KS86] H-P. Kriegel and Bernhard Seeger. Efficient multidimensional dynamic hashing for uniform and non-uniform record distributions. In Ausiello and Atzeni [AA86], page ?? ISBN 3-540-17187-8. LCCN QA76.9.D3 I55824 1986.

Kriegel:1987:MDH

[KS87a] H. P. Kriegel and B. Seeger. Multidimensional dynamic hashing is very efficient for nonuniform record distributions. In ICDE'87 [ICD87],

page 10. ISBN 0-8186-0762-9 (paperback) 0-8186-8762-2 (hard) 0-8186-4762-0 (microfiche). LCCN QA76.9.D3 I5582 1987.

Kriegel:1987:MDQ

[KS87b] Hans-Peter Kriegel and Bernhard Seeger. Multidimensional dynamic quantile hashing is very efficient for non-uniform record distributions. In ICDE'87 [ICD87], pages 10–17. ISBN 0-8186-0762-9 (paperback) 0-8186-8762-2 (hard) 0-8186-4762-0 (microfiche). LCCN QA76.9.D3 I5582 1987. IEEE Service Cent. Piscataway, NJ, USA.

Korner:1988:LDS

[KS88a] J. Korner and G. Simonyi. Locally different sequences. In *IEEE 1988 International Symposium on Information Theory — Abstracts of papers*, volume 25 n 13, pages 61–?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. Available from IEEE Service Cent (catalog number 88CH2621-1). Piscataway, NJ, USA.

Kriegel:1988:PHGa

[KS88b] H. P. Kriegel and B. Seeger. PLOP-hashing: a grid file without directory. In ICDE'88 [ICD88], page 369. ISBN 0-8186-0827-7 (paperback), 0-8186-8827-0 (hardcover), 0-8186-4827-9 (microfiche). LCCN QA76.9.D3 I5582 1988.

Kriegel:1988:PHGb

[KS88c] Hans-Peter Kriegel and Bernhard Seeger. *PLOP-Hashing: a Grid File without Directory*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. ISBN 0-8186-0827-7. 369–376 pp. LCCN QA 76.9 D3 I5582 1988. IEEE Service Cent. Piscataway, NJ, USA.

Kelly:1989:POM

[KS89a] Michael A. Kelly and Rudolph E. Seviora. Performance of OPS5 matching on CUPID. *Microprocessing and Microprogramming*, 27(1-5):397–404, August 1989. CODEN MMICDT. ISSN 0165-6074 (print), 1878-7061 (electronic).

Kriegel:1989:MQH

[KS89b] Hans-Peter Kriegel and Bernhard Seeger. Multidimensional quantile hashing is very efficient for nonuniform distributions. *Information Sciences*, 48(2):99–117, July 1, 1989. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Kniesburges:2012:BAH

[KS12] Sebastian Kniesburges and Christian Scheideler. Brief

announcement: Hashed predecessor Patricia trie- a data structure for efficient predecessor queries in peer-to-peer systems. *Lecture Notes in CS*, 7611:435–436, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-33651-5_45`.

Karger:1999:WCC

[KSB+99] David Karger, Alex Sherman, Andy Berkheimer, Bill Bogstad, Rizwan Dhanidina, Ken Iwamoto, Brian Kim, Luke Matkins, and Yoav Yerushalmi. Web caching with consistent hashing. *Computer Networks (Amsterdam, Netherlands: 1999)*, 31(11–16):1203–1213, May 17, 1999. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.elsevier.com/cas/tree/store/comnet/sub/1999/31/11-16/2181.pdf`.

Kwak:2011:DIB

[KSC11] Hukeun Kwak, Andrew Sohn, and Kyusik Chung. Dynamic information-based scalable hashing on a cluster of web cache servers. *Concurrency and Computation: Practice and Experience*, 24 (3):322–340, March 10, 2011. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Kwak:2012:DIB

[KSC12] Hukeun Kwak, Andrew Sohn, and Kyusik Chung. Dynamic information-based scalable hashing on a cluster of web cache servers. *Concurrency and Computation: Practice and Experience*, 24 (3):322–340, March 10, 2012. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Kalvin:1986:TDM

[KSSS86] Alan Kalvin, Edith Schonberg, Jacob T. Schwartz, and Micha Sharir. Two-dimensional, model-based, boundary matching using footprints. *International Journal of Robotics Research*, 5(4):38–55, Winter 1986. CODEN IJRREL. ISSN 0278-3649.

Kim:1999:LEO

[KST99] Jeong Han Kim, D. R. Simon, and P. Tetali. Limits on the efficiency of one-way permutation-based hash functions. In IEEE [IEE99], pages 535–542. CODEN ASFPDV. ISBN 0-7695-0409-4 (softbound), 0-7803-5955-0 (casebound), 0-7695-0411-6 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 1999. IEEE Catalog Number 99CB37039.

Kolbl:2020:TTC

[KTDB20] Stefan Kölbl, Elmar Tischhauser, Patrick Derbez, and Andrey Bogdanov. Troika: a ternary cryptographic hash function. *Designs, Codes, and Cryptography*, 88(1):91–117, January 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00673-2`.

Kitsuregawa:1983:AHD

[KTMo83a] M. Kitsuregawa, H. Tanaka, and T. Moto-oka. Application of hash to database machine and its architecture. *New Generation Computing*, 1(1):63–74, 1983. CODEN NGCOE5. ISSN 0288-3635 (print), 1882-7055 (electronic).

Kitsuregawa:1983:GRA

[KTMO83b] Masaru Kitsuregawa, Hidehiko Tanaka, and Tohru Moto-Oka. GRACE: Relational algebra machine based on hash and sort — its design concepts. *Journal of the Information Processing Society of Japan*, 6(3 (or 6??)): 148–155, ???? 1983. CODEN JIPRDE. ISSN 0387-6101.

Kitsuregawa:1983:RAM

[KTMo83c] Masaru Kitsuregawa, Hidehiko Tanaka, and Tohru Moto-oka. Relational algebra machine: GRACE. In Goto [Got83], pages 191–214. ISBN 0-387-11980-9 (New York), 3-540-11980-9 (Berlin). LCCN QA76.6 .R55 1983.

Kitsuregawa:1992:PGH

[KTN92] M. Kitsuregawa, S.-I. Tsudaka, and M. Nakano. Parallel GRACE hash join on shared-everything multiprocessor: Implementation and performance evaluation on symmetry S81. In Golshani [Gol92], pages 256–264. ISBN 0-8186-2545-7 (paper) 0-8186-2546-5 (microfiche) 0-8186-2547-3 (hardcover). LCCN QA76.9.D3 I5582 1992.

Karlin:1986:PHE

[KU86] A. R. Karlin and E. Upfal. Parallel hashing — an efficient implementation of shared memory. In ACM-TOC'86 [ACM86b], pages 160–168. ISBN 0-89791-193-8. LCCN QA76.6 .A14 198.

Karlin:1988:PHE

[KU88] Anna R. Karlin and Eli Upfal. Parallel hashing: An efficient implementation of shared memory. *Journal of the Association for Computing Machinery*, 35 (4):876–892, October 1988. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Ku:2004:HBS

[Ku04] Wei-Chi Ku. A hash-based strong-password authentication scheme without using Smart Cards. *Operating Systems Review*, 38(1):29–34, January 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Kuespert:1982:MLHa

[Kue82a] K. Kuespert. Modelle für die Leistungsanalyse von Hashtabellen mit 'separate Chaining'. Technical report, ????, Kaiserslautern, Germany, 1982. ?? pp.

Kuespert:1982:MLHb

[Kue82b] Klaus Kuespert. Modelle für die Leistungsanalyse von Hashtabellen mit 'Separate Chaining' [models for analyzing the performance of hash tables with separate chaining]. *Angew. Inf. Appl. Inf.*, V 24(N 9):456–462, September 1982.

Kuespert:1983:VZO

[Kue83] K. Kuespert. Vorschlaege zur Zeiteffizienten Onlinefehlererkennung in Speicherungsstrukturen von Datenbanksystemen. Technical report, ????, Kaiserslautern, Germany, 1983. ?? pp.

Kuespert:1984:USO

[Kue84a] K. Kuespert. Überlegungen zur Schnellen Online-fehlerbehandlung in Speicherstrukturen von Datenbanksystemen. Technical report, ????, Kaiserslautern, Germany, 1984. ?? pp.

Kuespert:1984:EED

[Kue84b] Klaus Kuespert. Efficient error detection techniques for hash tables in database systems. *Digest of Papers — FTCS (Fault-Tolerant Computing Symposium)*, pages 198–203, 1984. CODEN DPFTDL. ISBN 0-8186-0540-5. ISSN 0731-3071. IEEE Service Cent. Piscataway, NJ, USA.

Kuich:1992:ALP

[Kui92] Werner Kuich, editor. *Automata, Languages, and Programming: 19th International Colloquium, Wien, Austria, July 13–17, 1992: Proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992. ISBN 0-387-55719-9 (New York), 3-540-55719-9 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.623.

Kulkarni:1984:CHF

[Kul84] Vidyadhar G. Kulkarni. Compact hash function for paths in Pert networks. *Operations Research Letters*, 3(3): 137–140, August 1984. CODEN ORLED5. ISSN 0167-6377.

Kumar:1989:CCM

[Kum89a] Vijay Kumar. A concurrency control mechanism based on extendible hashing for main memory database systems. In Riehl [Rie89], pages 109–113. ISBN 0-89791-299-3. LCCN ???? US$36.00.

Kumar:1989:CCE

[Kum89b] Vijay Kumar. Concurrency control on extendible hashing. *Information Processing Letters*, 31(1):35–41, April 1989. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Kumar:1990:COE

[Kum90] Vijay Kumar. Concurrent operations on extensible hashing and its performance. *Communications of the Association for Computing Machinery*, 33(6):681–694, June 1990. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/78979.html`.

Kutzelnigg:2006:BRG

[Kut06] Reinhard Kutzelnigg. Bipartite random graphs and cuckoo hashing. *Discrete Mathematics & Theoretical Computer Science*, ??(??): 403–406, ???? 2006. ISSN 1365-8050 (print), 1462-7264 (electronic). URL `http://www.dmtcs.org/dmtcs-ojs/index.php/dmtcs/search; http://www.dmtcs.org/dmtcs-ojs/index.php/proceedings/article/download/dmAG0133/1710; http://www.dmtcs.org/dmtcs-ojs/index.php/proceedings/issue/view/84`.

Kutzelnigg:2010:IVC

[Kut10] Reinhard Kutzelnigg. An improved version of cuckoo hashing: Average case analysis of construction cost and search operations. *Mathematics in Computer Science*, 3(1):47–60, March 2010. CODEN ???? ISSN 1661-8270 (print), 1661-8289 (electronic). URL `http://www.springerlink.com/content/jxq4q02741625283/; http://www.springerlink.com/openurl.asp?genre=article&issn=1661-8270&volume=3&issue=1&spage=47`.

Kenyon:1991:MQS

[KV91] Claire M. Kenyon and Jeffrey Scott Vitter. Maximum queue size and hashing with lazy deletion. *Algorithmica*, 6(4):597–619, 1991. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Katz:2009:SPH

[KV09] Jonathan Katz and Vinod Vaikuntanathan. Smooth projective hashing and password-based authenticated key exchange from lattices. *Lec-*

ture Notes in CS, 5912: 636–652, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-10366-7_37.

Kortelainen:2012:GIH

[KVK12] Tuomas Kortelainen, Ari Vesanen, and Juha Kortelainen. Generalized iterated hash functions revisited: New complexity bounds for multicollision attacks. *Lecture Notes in CS*, 7668:172–190, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34931-7_11/.

Kroll:1994:DST

[KW94] Brigitte Kröll and Peter Widmayer. Distributing a search tree among a growing number of processors. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 23(2): 265–276, June 1994. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Klassen:2012:ITB

[KW12] Toryn Qwyllyn Klassen and Philipp Woelfel. Independence of tabulation-based hash classes. *Lecture Notes in CS*, 7256:506–517, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-29344-3_43.

Kaps:2005:ESU

[KYS05] J.-P. Kaps, K. Yuksel, and B. Sunar. Energy scalable universal hashing. *IEEE Transactions on Computers*, 54(12):1484–1495, December 2005. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1524931.

Kjellberg:1984:CH

[KZ84] Peter Kjellberg and Torben U. Zahle. Cascade hashing. In *VLDB*, pages 481–492. VLDB Endowment, Saratoga, CA, USA, August 1984.

Koslicki:2019:IMC

[KZ19] David Koslicki and Hooman Zabeti. Improving MinHash via the containment index with applications to metagenomic analysis. *Applied Mathematics and Computation*, 354(??):206–215, August 1, 2019. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S009630031930116X.

Louati:2018:LCT

[LACJ18] Thouraya Louati, Heithem Abbes, Christophe Cérin, and Mohamed Jemni. LXCloud-CR: Towards Linux containers distributed hash table based checkpoint-restart. *Journal of Parallel and Distributed Computing*, 111(??): 187–205, January 2018. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731517302411`.

Lai:1992:DSB

[Lai92] Xuejia Lai. *On the design and security of block ciphers*. Hartung-Gorre Verlag, Konstanz, Switzerland, 1992. ISBN 3-89191-573-X. xii + 108 pp. LCCN ??? This is the author's Ph.D. dissertation. "Secret-key block ciphers are the subject of this work. The design and security of block ciphers, together with their application in hashing techniques, are considered. In particular, iterated block ciphers that are based on iterating a weak round function several times are considered. Four basic constructions for the round function of an iterated cipher are studied.".

LakshmanYN:1996:IPI

[Lak96] Lakshman Y.N., editor. *ISSAC '96: Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation, July 24–26, 1996, Zurich, Switzerland*. ACM Press, New York, NY 10036, USA, 1996. ISBN 0-89791-796-0. LCCN QA 76.95 I59 1996.

Lee:2007:CFRa

[LAKW07] Younggyo Lee, Jeonghee Ahn, Seungjoo Kim, and Dongho Won. A countermeasure of fake root key installation using one-time hash chain. *Lecture Notes in CS*, 4496:1007–1016, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-72830-6_107`.

Lamport:1970:CBQ

[Lam70] Leslie Lamport. Comment on Bell's quadratic quotient method for hash code searching. *Communications of the Association for Computing Machinery*, 13(9):573–574, September 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Landau:2006:FMH

[Lan06] Susan Landau. Find me a hash. *Notices of the American Mathematical Society*, 53(3):330–332, March 2006. CODEN AMNOAN. ISSN 0002-9920 (print), 1088-9477 (electronic). URL `http:`

//www.ams.org/notices/200603/fea-landau.pdf.

Larson:1978:DH

[Lar78] Per-Åke Larson. Dynamic hashing. *BIT (Nordisk tidskrift for informationsbehandling)*, 18(2):184–201, 1978. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). See also [Reg85].

Larson:1980:ARH

[Lar80a] Per Ake Larson. Analysis of repeated hashing. *BIT (Copenhagen)*, 20(1):25–32, ???? 1980. CODEN NBITAB.

Larson:1980:LHP

[Lar80b] Per-Åke Larson. Linear hashing with partial expansions. In Lochovsky and Taylor [LT80], pages 224–232. ACM order no. 471800. IEEE catalog no. 80CH1534-7C. Long Beach order no. 322.

Larson:1980:PAL

[Lar80c] Per-Åke Larson. Performance analysis of linear hashing with partial expansions. Technical report, ????, Abo, Finland, 1980. ?? pp.

Larson:1981:EWC

[Lar81] Per-Åke Larson. Expected worst-case performance of hash files. Technical report, ????, Abo, Finland, 1981. ?? pp.

Larson:1982:EWC

[Lar82a] Per-Åke Larson. Expected worst-case performance of hash files. *The Computer Journal*, 25(3):347–352, August 1982. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Larson:1982:PAL

[Lar82b] Per-Åke Larson. Performance analysis of linear hashing with partial expansions. *ACM Transactions on Database Systems*, 7(4):566–587, December 1982. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Larson:1982:SFVa

[Lar82c] Per-Åke Larson. A single-file version of linear hashing with partial expansions. In VLDB'82 [VLD82], page 300. ISBN 0-934613-14-1. LCCN QA76.9.D3 I559 1982.

Larson:1982:SFVb

[Lar82d] Per-Åke Larson. Single-file version of linear hashing with partial expansions. *Very Large Data Bases, International Conference on Very Large Data Bases*, pages 300–309, 1982. CODEN VLDBDP.

Larson:1983:AUH

[Lar83] Per-Åke Larson. Analysis of uniform hashing. *Jour-*

nal of the Association for Computing Machinery, 30 (4):805–819, October 1983. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Larson:1984:AHC

[Lar84] Per-Åke Larson. Analysis of hashing with chaining in the prime area. *Journal of Algorithms*, 5(1):36–47, March 1984. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0196677484900385`.

Larson:1985:HFS

[Lar85a] Per-Åke Larson. *Hash Files: Some Recent Developments*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1985. ISBN 0-8186-0654-1. 671–679 pp. LCCN QA76.5 .I5481 1985. IEEE Service Cent. Piscataway, NJ, USA.

Larson:1985:LHO

[Lar85b] Per-Åke Larson. Linear hashing with overflow-handling by linear probing. *ACM Transactions on Database Systems*, 10(1):75–89, March 1985. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Larson:1985:PAS

[Lar85c] Per-Åke Larson. Performance analysis of a single-file version of linear hashing. *The Computer Journal*, 28 (3):319–329, July 1985. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Larson:1988:DHT

[Lar88a] Per-Åke Larson. Dynamic hash tables. *Communications of the Association for Computing Machinery*, 31 (4):446–457, April 1988. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Larson:1988:LHS

[Lar88b] Per-Åke Larson. Linear hashing with separators — a dynamic hashing scheme achieving one-access retrieval. *ACM Transactions on Database Systems*, 13(3): 366–388, September 1988. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Larson:19xx:LHP

[Larxx] Per Ake Larson. Linear hashing with partial expansions. *Very Large Data Bases, International Conference on Very Large Data Bases*, ??(??):224–232, ???? 19xx. CODEN VLDBDP. ACM (Order n 471800). Baltimore, Md.

Lassez:1987:PFI

[Las87] Jean-Louis Lassez, editor. *Proceedings of the Fourth International Conference on Logic Programming*, MIT Press Series in Logic Programming. MIT Press, Cambridge, MA, USA, 1987. ISBN 0-262-12125-5 (ensemble) 0-262-12129-8 (vol. 2). LCCN QA76.6 .L589 1987 v. 1-2.

Lopes:2007:IRQ

[LB07] Nuno Lopes and Carlos Baquero. Implementing range queries with a decentralized balanced tree over distributed hash tables. *Lecture Notes in CS*, 4658: 197–206, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-74573-0_21`.

Li:2002:RBA

[LBJ02] T. Li, R. Bhargava, and L. K. John. Rehashable BTB: An adaptive branch target buffer to improve the target predictability of Java code. *Lecture Notes in CS*, 2552:597–608, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lehman:1986:SIS

[LC86a] T. J. Lehman and M. J. Carey. A study of index structures for main memory database management systems. In Chu et al. [CGO86], page ?? ISBN 0-934613-18-4. LCCN QA76.9.D3 I559 1986.

Little:1986:PSS

[LC86b] Joyce Currie Little and Lillian N. Cassel, editors. *The Papers of the Seventeenth SIGCSE Technical Symposium on Computer Science Education*. ACM Press, New York, NY 10036, USA, 1986. ISBN 0-89791-178-4. LCCN QA76.27.A79 v.18 no.1. US$28.00.

Lewis:1988:HDS

[LC88] Ted G. Lewis and Curtis R. Cook. Hashing for dynamic and static internal tables. *Computer*, 21(10):45–57 (or 45–56??), October 1988. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). The authors survey the classical hashing function approach to information retrieval and show how general hashing techniques exchange speed for memory. It is a tutorial paper that covers, among other topics, dynamic and static hash tables, perfect hashing, and minimal perfect hashing.

Lomas:1995:RBH

[LC95] Mark Lomas and Bruce Christianson. Remote booting in a hostile world: to whom am I speaking? (computer security). *Computer*,

28(1):50–54, January 1995. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Liu:1996:HPS

[LC96] C. Liu and H. Chen. A hash partition strategy for distributed query processing. *Lecture Notes in CS*, 1057:373–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lai:2006:ACA

[LC06] Xuejia Lai and Kefei Chen, editors. *Advances in Cryptology — ASIACRYPT 2006: 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, December 3–7, 2006. Proceedings*, volume 4284 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. CODEN LNCSD9. ISBN 3-540-49475-8 (print), 3-540-49476-6 (e-book). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL `http://www.springerlink.com/content/978-3-540-49476-8`.

Liu:2012:PIH

[LC12] Fang Liu and Lee-Ming Cheng. Perceptual image hashing via wave atom transform. *Lecture Notes in CS*, 7128:468–478, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-32205-1_37`.

Liu:2013:RBP

[LC13] Jian Liu and Lusheng Chen. On the relationships between perfect nonlinear functions and universal hash families. *Theoret. Comput. Sci.*, 513(??):85–95, November 18, 2013. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S030439751300769X`.

Lessley:2020:DPH

[LC20] B. Lessley and H. Childs. Data-parallel hashing techniques for GPU architectures. *IEEE Transactions on Parallel and Distributed Systems*, 31(1):237–250, January 2020. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Liu:2014:SLE

[LCH+14] Yingfan Liu, Jiangtao Cui, Zi Huang, Hui Li, and Heng Tao Shen. SK–LSH: an efficient index structure for approximate nearest neighbor search. *Proceedings of the VLDB Endowment*, 7(9):

745–756, May 2014. CODEN ???? ISSN 2150-8097.

Lathrop:2011:SPI

[LCK11] Scott Lathrop, Jim Costa, and William Kramer, editors. *SC'11: Proceedings of 2011 International Conference for High Performance Computing, Networking, Storage and Analysis, Seattle, WA, November 12–18 2011*. ACM Press and IEEE Computer Society Press, New York, NY 10036, USA and 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. ISBN 1-4503-0771-X. LCCN ????

Liu:2020:FAD

[LCL+20] Xiulong Liu, Sheng Chen, Jia Liu, Wenyu Qu, Fengjun Xiao, Alex X. Liu, Jiannong Cao, and Jiangchuan Liu. Fast and accurate detection of unknown tags for RFID systems — hash collisions are desirable. *IEEE/ACM Transactions on Networking*, 28(1): 126–139, February 2020. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL `https://dl.acm.org/doi/abs/10.1109/TNET.2019.2957239`.

Li:2019:EEU

[LCLX19] Yongkun Li, Helen H. W. Chan, Patrick P. C. Lee, and Yinlong Xu. Enabling efficient updates in KV storage via hashing: Design and performance evaluation. *ACM Transactions on Storage*, 15 (3):20:1–20:??, August 2019. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3340287`.

Lu:2020:NMS

[LCM+20] Z. Lu, Q. Cao, F. Mei, H. Jiang, and J. Li. A novel multi-stage forest-based key–value store for holistic performance improvement. *IEEE Transactions on Parallel and Distributed Systems*, 31(4): 856–870, April 2020. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Liang:1994:OMK

[LCML94] J. Liang, C.-C. Chang, R. G. McFadyen, and R. C. T. Lee. Optimal multiple key hashing files for orthogonal range queries. *Information Sciences*, 79(1):145–??, 1994. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Lo:1993:OPA

[LCRY93] Ming-Ling Lo, Ming-Syan Chen, C. V. Ravishankar, and Philip S. Yu. On optimal processor allocation to support pipelined hash joins. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 22(2):69–78, June 1993. CODEN

SRECD8. ISBN 0-89791-592-5. ISSN 0163-5808 (print), 1943-5835 (electronic).

Lee:2012:OFL

[LDK12] Myungjin Lee, Nick Duffield, and Ramana Rao Kompella. Opportunistic flow-level latency estimation using consistent netflow. *IEEE/ACM Transactions on Networking*, 20(1):139–152, February 2012. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Lieuwen:1992:PBJ

[LDM92] Daniel F. Lieuwen, David J. DeWitt, and Manish Mehta. Pointer-based join techniques for object-oriented databases. Technical Report TR 1099, Computer Sciences Department, University of Wisconsin–Madison, July 1992. ?? pp.

Liu:2016:TRS

[LDY+16] Wenping Liu, Tianping Deng, Yang, Hongbo Jiang, Xiaofei Liao, Jiangchuan Liu, Bo Li, and Guoyin Jiang. Towards robust surface skeleton extraction and its applications in 3D wireless sensor networks. *IEEE/ACM Transactions on Networking*, 24(6):3300–3313, December 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Lebedev:1987:EEU

[Leb87] G. V. Lebedev. Estimating the efficiency of a uniform-grid two-dimensional hashing algorithm for hidden line and surface removal in computer graphics. *Automation and Remote Control (English translation of Avtomatika i Telemekhanika)*, 48(7 pt 2): 968–975, July 1987. CODEN AURCAT. ISSN 0005-1179.

Luo:2002:SHR

[LEHN02] Gang Luo, Curt J. Ellmann, Peter J. Haas, and Jeffrey F. Naughton. A scalable hash ripple join algorithm. In Franklin et al. [FMA02], pages 252–262. ISBN ???? LCCN ???? ACM order number 475020.

Leppanen:1998:BPS

[Lep98] V. Leppänen. Balanced PRAM simulations via moving threads and hashing. *J.UCS: Journal of Universal Computer Science*, 4(8):675–??, August 28, 1998. ISSN 0948-6968. URL `http://medoc.springer.de:8000/jucs/jucs_4_8/balanced_pram_simulations_via`.

Lesk:1988:GII

[Les88] Michael Lesk. GRAB—inverted indexes with low storage overhead. *Computing Systems*, 1(3):207–220, Summer 1988. CODEN CMSYE2. ISSN 0895-6340.

Levy:1989:LPT

[Lev89] G. Levy. A language for the P-any trees — applications to the dynamic virtual hashing methods. In Litwin and Schek [LS89], page ?? ISBN 0-387-51295-0. LCCN QA76.9.D3 F671 1989.

Levelt:1995:IPI

[Lev95] A. H. M. Levelt, editor. *ISSAC '95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation: July 10–12, 1995, Montréal, Canada*, ISSAC -PROCEEDINGS-1995. ACM Press, New York, NY 10036, USA, 1995. ISBN 0-89791-699-9. LCCN QA 76.95 I59 1995. ACM order number: 505950.

Lever:2000:LKH

[Lev00] Chuck Lever. Linux kernel hash table behavior: Analysis and improvements. In USENIX [USE00a], page ?? ISBN 1-880446-17-0. LCCN ???? URL `http://www.usenix.org/publications/library/proceedings/als2000/lever.html`.

Lewis:1982:SEA

[Lew82] T. G. Lewis. *Software Engineering: Analysis and Verification*. Reston Publishing Co. Inc., Reston, VA, USA, 1982. ISBN 0-8359-7023-X. x + 470 pp. LCCN QA76.6 .L477 1982. US$21.95. Hashing is covered in Chapters 4–7.

Laborde:2017:WFH

[LFD17] Pierre Laborde, Steven Feldman, and Damian Dechev. A wait-free hash map. *International Journal of Parallel Programming*, 45(3): 421–448, June 2017. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic).

ACM:1982:CRA

[LFP82] *Conference Record of the 1982 ACM Symposium on Lisp and Functional Programming: Papers Presented at the Symposium, Pittsburgh, Pennsylvania, August 15–18, 1982*. ACM Press, New York, NY 10036, USA, August 1982. ISBN 0-89791-082-6. LCCN QA76.73.L23 A26 1982. US$26.00. The papers were not formally refereed but were accepted on the bases of extended abstracts.

Louis-Gavet:1978:DAI

[LG78] Guy Louis-Gavet. Diverses applications issues d'une fonction f de compactage basée sur une étude mathématique du langage naturel (compactage de données, comparaison de textes, hash-coding). [various applications issued from a compression function f based on a mathematical study of the natural language (data compression,

comparison of texts, hashcoding)]. *RAIRO Informatique/Computer Science (Revue Française d'Automatique, d'Informatique et de Recherche Operationnelle)*, 12(1):47–71, ???? 1978. CODEN RSINDN.

Lamiroy:1996:ROI

[LG96] B. Lamiroy and P. Gros. Rapid object indexing and recognition using enhanced geometric hashing. *Lecture Notes in CS*, 1064:59–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Li:2013:NCD

[LG13] Zhijun Li and Guang Gong. On the node clone detection in wireless sensor networks. *IEEE/ACM Transactions on Networking*, 21(6): 1799–1811, December 2013. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Luo:2003:COA

[LH03a] Wenbin Luo and Gregory L. Heileman. Characterizing open addressing hash functions. In Debnath [Deb03], pages 21–24. ISBN 1-880843-46-3 (paperback). LCCN QA75.5 I76 2003; QA76.76.A65 I83 2003.

Luo:2003:CDO

[LH03b] Wenbin Luo and Gregory L. Heileman. Comparison of different open addressing hashing algorithms. In Debnath [Deb03], pages 1–4. ISBN 1-880843-46-3 (paperback). LCCN QA75.5 I76 2003; QA76.76.A65 I83 2003.

Luo:2004:IEH

[LH04] Wenbin Luo and Gregory L. Heileman. Improved exponential hashing. *IEICE Electronics Express*, 1(7):150–155, ???? 2004.

Lefebvre:2006:PSH

[LH06] Sylvain Lefebvre and Hugues Hoppe. Perfect spatial hashing. *ACM Transactions on Graphics*, 25(3): 579–588, July 2006. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Liu:2020:EIH

[LH20] Shiguang Liu and Ziqing Huang. Efficient image hashing with geometric invariant vector distance for copy detection. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 15(4):1–22, January 2020. ISSN 1551-6857 (print), 1551-6865 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3355394`.

Lin:2005:GPW

[LHC05] Iuon-Chang Lin, Min-Shiang Hwang, and Chin-Chen Chang. The general payword: a micro-payment

scheme based on n-dimension one-way hash chain. *Designs, Codes, and Cryptography*, 36(1):53–67, July 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=36&issue=1&spage=53`.

Lu:2020:DSH

[LHWL20] Baotong Lu, Xiangpeng Hao, Tianzheng Wang, and Eric Lo. Dash: scalable hashing on persistent memory. *Proceedings of the VLDB Endowment*, 13 (8):1147–1161, April 2020. CODEN ???? ISSN 2150-8097. URL `https://dl.acm.org/doi/abs/10.14778/3389133.3389134`.

Lu:2021:SDH

[LHWL21] Baotong Lu, Xiangpeng Hao, Tianzheng Wang, and Eric Lo. Scaling dynamic hash tables on real persistent memory. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 50 (1):87–94, June 2021. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic). URL `https://dl.acm.org/doi/10.1145/3471485.3471506`.

Litvinov:1980:GHF

[LI80] V. A. Litvinov and V. I. Ivanenko. Generalized hashing function and hashed file organization. *Programming and Computer Software (English Translation of Programmirovanie)*, 6(5): 247–249, September–October 1980. CODEN PCSODA.

Li:1995:CKH

[Li95] G. Li. Collisionful keyed hash functions with selectable collisions. *Information Processing Letters*, 55(3):167–170, August 11, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Li:2010:PAP

[Li10] Mengdong Li. Preimage awareness proofs of two compression functions. In Yang [Yan10], pages 660–664. ISBN 1-4244-6942-2. LCCN QA76.9.A25. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5680738`.

Li:2015:RDS

[Li15] Xuelong Li. Robust discrete spectral hashing for large-scale image semantic indexing. *IEEE Transactions on Big Data*, 1(4):162–171, December 2015. CODEN ???? ISSN 2332-7790.

Liang:1995:PHF

[Lia95] S. Liang. A perfect hashing function for exact diagonalization of many-body systems of identical particles. *Computer Physics*

Communications, 92(1):11–??, November 1, 1995. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic).

Lien:1981:AIC

[Lie81] Y. Edmund Lien, editor. *ACM-SIGMOD 1981 International Conference on Management of Data: April 29–May 1, the University of Michigan, Ann Arbor, Michigan*. ACM Press, New York, NY 10036, USA, 1981. ISBN 0-89791-040-0. LCCN QA76.9.D3 I59 1981.

Luhandjula:1992:FSI

[LII92] M. K. Luhandjula, H. Ichihashi, and M. Inuiguchi. Fuzzy and semite-infinite mathematical programming. *Information Sciences*, 61 (3):233, 1992. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Lin:1953:xxx

[Lin53] A. D. Lin. ??? The year is uncertain (???). Extends [Luh53] with an alternative overflow handling technique using "degenerative addresses" [Knu73, p. 541]., 1953.

Lin:1963:KAR

[Lin63] A. D. Lin. Key addressing of random access memories by radix transformation. In AFIPS SJCC '63 [AFI63], pages 355–366. LCCN TK7885.A1 J6 1963.

Lindner:1996:DSH

[Lin96] M. P. Lindner. Designing for safe hashing. implementing efficient dynamic search structures. *C++ Report*, 8(10):36–41, November–December 1996. CODEN CRPTE7. ISSN 1040-6042.

Lipmaa:2002:OHT

[Lip02] Helger Lipmaa. On optimal hash tree traversal for interval time-stamping. *Lecture Notes in CS*, 2433:357–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2433/24330357.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2433/24330357.pdf`.

Liskov:2007:CIH

[Lis07] Moses Liskov. Constructing an ideal hash function from weak ideal compression functions. *Lecture Notes in CS*, 4356:358–375, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-74462-7_25`.

Litwin:1977:ASD

[Lit77a] W. Litwin. Auto-structuration du fichier: Methodologie, organisation d'acces, extension du hash-codering. Technical report, ????, Paris, France, 1977. ?? pp.

Litwin:1977:MDP

[Lit77b] Witold Litwin. Méthodes d'acces par hash-coding virtuel (VHAM): Modelisation, application à la gestion de Mémoires. Technical report, University of Pierre et Marie Curie (Paris, France), Paris, France, November 1977. ?? pp.

Litwin:1978:VHD

[Lit78] W. Litwin. Virtual hashing: a dynamically changing hashing. In Yao [Yao78], pages 517–523.

Litwin:1979:HVN

[Lit79a] W. Litwin. *Hachage Virtuel: Une Nouvelle Technique d'Adressage de Mémoires*. PhD thesis, ????, Paris, France, 1979. ?? pp.

Litwin:1979:LVH

[Lit79b] W. Litwin. Linear virtual hashing: a new tool for files and tables implementation. Technical report, ????, Le Chesnay, France, 1979. ?? pp.

Litwin:1980:LHN

[Lit80] W. Litwin. Linear hashing: a new tool for file and table addressing. In Lochovsky and Taylor [LT80], pages 212–223 (or 260–276??). Reprinted in [Sto88, p. 570–581].

Litwin:1981:TH

[Lit81] W. Litwin. Trie hashing. In Lien [Lie81], pages 19–29. ISBN 0-89791-040-0. LCCN QA76.9.D3 I59 1981.

Litwin:1984:DAM

[Lit84] Witold Litwin. Data access methods and structures to enhance performance. *InfoTech State-of-the-Art Report, Database Performance*, ??(??):??, 1984.

Litwin:1985:THF

[Lit85] Witold Litwin. Trie hashing: Further properties and performance. In *Proceedings — Foundations of Data Organization.*, pages 51–60. Organizing Committee of the Int Conference on Foundations of Data Organization, Jpn, 1985. Koyto Sangyo Univ. Computer Science Inst, Kyoto, Jpn.

Litvinov:1989:HSO

[Lit89] V. A. Litvinov. Hash-sequential organization of data sets. *Programming and Computer Software; translation of Programmirovaniye, (Moscow, USSR) Plenum*, 15 (2):70–??, March 1, 1989. CODEN PCSODA. ISSN 0361-7688 (print), 1608-3261 (electronic).

Litsios:1991:NFH

[Lit91] James Litsios. Note on fast hashing of variable length text strings. *Communications of the Association for Computing Machinery*, 34(11):118–120, November 1991. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Suggests a simple extension of Pearson's hashing algorithm [Pea90] that supports non-character data. See also comments in [Dit91, Sav91, Pea91], and early work in [Dit76].

Litwin:19xx:LHN

[Litxxa] Witold Litwin. Linear hashing: a new tool for file and table addressing. *Very Large Data Bases, International Conference on Very Large Data Bases*, ??(??): 212–223, ???? 19xx. CODEN VLDBDP. ACM (Order number 471800). Baltimore, Md.

Litwin:19xx:VHD

[Litxxb] Witold Litwin. Virtual hashing: a dynamically changing hashing. *IEEE Cement Industry Technical Conference (Paper)*, ??(??):517–523, ???? 19xx. IEEE Comput Soc. Long Beach, Ca.

Li:2019:IID

[LJF19] Rongjia Li, Chenhui Jin, and Ruya Fan. Improved integral distinguishers on compression function of GOST R hash function. *The Computer Journal*, 62(4): 535–544, April 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/62/4/535/5224765`.

Lv:2017:IPL

[LJW+17] Qin Lv, William Josephson, Zhe Wang, Moses Charikar, and Kai Li. Intelligent probing for locality sensitive hashing: multi-probe LSH and beyond. *Proceedings of the VLDB Endowment*, 10(12):2021–2024, August 2017. CODEN ???? ISSN 2150-8097.

Larson:1984:FOI

[LK84] Per-Åke Larson and Aja Kajla. File organization: Implementation of a method guaranteeing retrieval in one access. *Communications of the Association for Computing Machinery*, 27(7): 670–677, July 1984. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Lucchesi:1993:AFA

[LK93] Claudio L. Lucchesi and Tomasz Kowaltowski. Applications of finite automata representing large vocabularies. *Software—Practice*

and Experience, 23(1):15–30, January 1993. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Lai:1994:ADB

[LK94] X. Lai and L. Knudsen. Attacks on double block length hash functions. In Anderson [And94], pages 157–165. ISBN 0-387-58108-1, 3-540-58108-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C36 1993.

Lagutin:2007:CIC

[LK07] Dmitrij Lagutin and Hannu H. Kari. Controlling incoming connections using certificates and distributed hash tables. *Lecture Notes in CS*, 4712:455–467, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-74833-5_38`.

Li:2011:TAB

[LK11] Ping Li and Arnd Christian König. Theory and applications of b-bit minwise hashing. *Communications of the Association for Computing Machinery*, 54(8):101–109, August 2011. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Lemire:2014:SUS

[LK14] Daniel Lemire and Owen Kaser. Strongly universal string hashing is fast. *The Computer Journal*, 57(11): 1624–1638, November 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/57/11/1624`.

Lemire:2016:FBU

[LK16] Daniel Lemire and Owen Kaser. Faster 64-bit universal hashing using carry-less multiplications. *Journal of Cryptographic Engineering*, 6(3): 171–185, September 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s13389-015-0110-5`; `http://link.springer.com/article/10.1007/s13389-015-0110-5`.

Lee:2010:PMH

[LKI10] David C. Lee, Qifa Ke, and Michael Isard. Partition min-hash for partial duplicate image discovery. *Lecture Notes in CS*, 6311:648–662, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-15549-9_47`.

Lee:2004:CUA

[LKY04] Sung-Woon Lee, Hyun-Sung Kim, and Kee-Young Yoo. Cryptanalysis of a user authentication scheme using hash functions. *Operating Systems Review*, 38(1):24–28, January 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Louchard:1983:PTC

[LL83] G. Louchard and G. Latouche. *Probability Theory and Computer Science*. Academic Press, New York, NY, USA, 1983. ISBN 0-12-455820-8. xiii + 209 pp. LCCN QA274 .P76 1983.

Lodi:1985:SSH

[LL85] E. Lodi and F. Luccio. Split sequence hash search. *Information Processing Letters*, 20 (3):131–136, April 1985. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Litwin:1986:BDA

[LL86] Witold Litwin and David B. Lomet. The bounded disorder access method. In *Proceedings of the International Conference on Data Engineering*, pages 38–48 (or 38–47??). IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, February 1986. ISBN 0-8186-0655-X. LCCN QA 76.9 D3 I5582 1986. IEEE Computer Society Order Number 655.

Litwin:1987:NMF

[LL87] Witold Litwin and David B. Lomet. New method for fast data searches with keys. *IEEE Software*, 4(2): 16–24, March 1987. CODEN IESOEG. ISSN 0740-7459 (print), 0740-7459 (electronic).

Leng:1992:OWA

[LL92] Chun-Wu Roger Leng and Dik Lun Lee. Optimal weight assignment for signature generation. *ACM Transactions on Database Systems*, 17(2): 346–373, June 1992. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1992-17-2/p346-leng/p346-leng.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1992-17-2/p346-leng/`; `http://www.acm.org/pubs/toc/Abstracts/tods/128907.html`.

Lenzerini:2008:PTS

[LL08] Maurizio Lenzerini and Domenico Lembo, editors. *Proceedings of the Twenty-Seventh ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems: PODS'08, Vancouver, BC, Canada, June 9–11, 2008*. ACM Press, New York,

NY 10036, USA, 2008. ISBN 1-59593-685-X. LCCN ????

Lee:2013:SQB

[LL13] Kisung Lee and Ling Liu. Scaling queries over big RDF graphs with semantic hash partitioning. *Proceedings of the VLDB Endowment*, 6(14):1894–1905, September 2013. CODEN ???? ISSN 2150-8097.

Lowden:2015:DPA

[LŁA15] Jason Lowden, Marcin Łukowiak, and Sonia Lopez Alarcon. Design and performance analysis of efficient Keccak tree hashing on GPU architectures. *Journal of Computer Security*, 23(5):541–562, ???? 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Leung:1989:LPA

[LLC89] K. S. Leung, K. H. Lee, and S. M. Cheang. Lists processing for artificial intelligence applications. *Microprocessing and Microprogramming*, 26(4):271–287, December 1989. CODEN MMICDT. ISSN 0165-6074 (print), 1878-7061 (electronic).

Li:2018:SBI

[LLDZ18] Yihong Li, Fangzheng Liu, Zhenyu Du, and Dubing Zhang. A Simhash-based integrative features extraction algorithm for malware detection. *Algorithms (Basel)*, 11 (8), August 2018. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL `https://www.mdpi.com/1999-4893/11/8/124`.

Luo:2012:IDE

[LLG12] Yiyuan Luo, Xuejia Lai, and Zheng Gong. Indifferentiability of domain extension modes for hash functions. *Lecture Notes in CS*, 7222:138–155, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32298-3_10/`.

Liu:2017:TQC

[LLG+17] Xiulong Liu, Keqiu Li, Song Guo, Alex X. Liu, Peng Li, Kun Wang, Jie Wu, Xiulong Liu, Keqiu Li, Song Guo, Alex X. Liu, Peng Li, Kun Wang, and Jie Wu. Top-k queries for categorized RFID systems. *IEEE/ACM Transactions on Networking*, 25 (5):2587–2600, October 2017. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Lee:2002:RUA

[LLH02] Cheng-Chi Lee, Li-Hua Li, and Min-Shiang Hwang. A remote user authentication scheme using hash functions. *Operating Systems Review*,

36(4):23–29, October 2002. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Luo:2015:ADL

[LLJ15] Yiyuan Luo, Xuejia Lai, and Tiejun Jia. Attacks on a double length blockcipher-based hash proposal. *Cryptography and Communications*, 7(3): 289–295, September 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0117-2`.

Lim:2009:SPE

[LLL09] Tong-Lee Lim, Tieyan Li, and Yingjiu Li. A security and performance evaluation of hash-based RFID protocols. *Lecture Notes in CS*, 5487:406–424, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-01440-6_30`.

Lin:2011:HAB

[LLL11] Po-Ching Lin, Ying-Dar Lin, and Yuan-Cheng Lai. A hybrid algorithm of backward hashing and automaton tracking for virus scanning. *IEEE Transactions on Computers*, 60(4):594–601, April 2011. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Li:2016:FSA

[LLL+16] Sheng Li, Hyeontaek Lim, Victor W. Lee, Jung Ho Ahn, Anuj Kalia, Michael Kaminsky, David G. Andersen, Seongil O., Sukhan Lee, and Pradeep Dubey. Full-stack architecting to achieve a billion-requests-per-second throughput on a single key–value store server platform. *ACM Transactions on Computer Systems*, 34(2): 5:1–5:??, May 2016. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Lin:2017:PHB

[LLLC17] Cheng-Hung Lin, Jin-Cheng Li, Chen-Hsiung Liu, and Shih-Chieh Chang. Perfect hashing based parallel algorithms for multiple string matching on graphic processing units. *IEEE Transactions on Parallel and Distributed Systems*, 28(9):2639–2650, September 2017. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL `https://www.computer.org/csdl/trans/td/2017/09/07864442-abs.html`.

Lloyd:1981:ICI

[Llo81] J. W. Lloyd. Implementing clause indexing in deductive database systems. Technical

Report 81/4, Dept. of Computer Science, University of Melbourne, Australia, 1981. ?? pp.

Liu:2021:DHB

[LLT21] Zhuotong Liu, Chen Li, and Lihua Tian. Deep hashing based on triplet labels and quantitative regularization term with exponential convergence. *Concurrency and Computation: Practice and Experience*, 34(1):e5583:1–e5583:??, August 10, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Liu:2010:MPI

[LLW10] Xiaowen Liu, Jinyan Li, and Lusheng Wang. Modeling protein interacting groups by quasi-bicliques: Complexity, algorithm, and application. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 7 (2):354–364, April 2010. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Liang:2010:LVB

[LLZ10] Yingyu Liang, Jianmin Li, and Bo Zhang. Learning vocabulary-based hashing with AdaBoost. *Lecture Notes in CS*, 5916: 545–555, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-11301-7_54`.

Lueker:1988:MAD

[LM88] G. S. Lueker and M. Molodowitch. More analysis of double hashing. In ACM-TOC'88 [ACM88b], pages 354–359. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988.

Lai:1993:HFBa

[LM93a] X. Lai and J. L. Massey. Hash functions based on block ciphers. In Rueppel [Rue93], pages 53–66. ISBN 0-387-56413-6 (New York), 3-540-56413-6 (Berlin). LCCN QA76.9.A25 E964 1992.

Lai:1993:HFBb

[LM93b] X. Lai and J. L. Massey. Hash functions based on block ciphers. *Lecture Notes in CS*, 658:55–70, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lueker:1993:MAD

[LM93c] G. S. Lueker and Mariko Molodowitch. More analysis of double hashing. *Combinatorica*, 13(1):83–96, 1993. CODEN COMBDI. ISSN 0209-9683 (print), 1439-6912 (electronic).

Leighton:1995:LPF

[LM95] F. T. Leighton and S. Micali. Large provably fast

and secure digital signature schemes from secure hash functions. US Patent 5,432,852., 1995.

Lee:2007:FDF

[LMC07] Sungju Lee, Daesung Moon, and Yongwha Chung. Feature distribution of the fingerprint template generated by the geometric hashing-based fuzzy vault. *Lecture Notes in CS*, 4693: 816–823, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-74827-4_103`.

Li:2012:SPS

[LMD+12] Boduo Li, Edward Mazur, Yanlei Diao, Andrew McGregor, and Prashant Shenoy. SCALLA: a platform for scalable one-pass analytics using MapReduce. *ACM Transactions on Database Systems*, 37(4):27:1–27:??, December 2012. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Lee:2007:PSK

[LMJC07] Sungju Lee, Daesung Moon, Seunghwan Jung, and Yongwha Chung. Protecting secret keys with fuzzy fingerprint vault based on a 3D geometric hash table. *Lecture Notes in CS*, 4432:432–439, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-71629-7_49`.

Liu:2014:MIK

[LMLC14] Xianglong Liu, Yadong Mu, Bo Lang, and Shih-Fu Chang. Mixed image-keyword query adaptive hashing over multilabel images. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 10(2):22:1–22:??, February 2014. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Lu:2008:CBN

[LMP+08] Yi Lu, Andrea Montanari, Balaji Prabhakar, Sarang Dharmapurikar, and Abdul Kabbani. Counter braids: a novel counter architecture for per-flow measurement. *ACM SIGMETRICS Performance Evaluation Review*, 36(1): 121–132, June 2008. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Luykx:2015:TPB

[LMPW15] Atul Luykx, Bart Mennink, Bart Preneel, and Laura Winnen. Two-permutation-based hashing with binary mixing. *Journal of Mathematical Cryptology*, 9(3): 139–150, 2015. CODEN

???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Lynch:2002:ADA

[LMR02] Nancy Lynch, Dahlia Malkhi, and David Ratajczak. Atomic data access in distributed hash tables. *Lecture Notes in CS*, 2429:295–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2429/24290295.htm`; `http://link.springer.de/link/service/series/0558/papers/2429/24290295.pdf`.

Lin:1989:PIB

[LMSF89] Chih-Chen Lin, Leo Mark, Timos Sellis, and Christos Faloutsos. Performance issues in the binary relationship model. *Data and Knowledge Engineering*, 4(3):195–221, September 1989. CODEN DKENEW. ISSN 0169-023X (print), 1872-6933 (electronic).

Legtchenko:2009:CRR

[LMSM09] Sergey Legtchenko, Sébastien Monnet, Pierre Sens, and Gilles Muller. Churn-resilient replication strategy for peer-to-peer distributed hash-tables. *Lecture Notes in CS*, 5873:485–499, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-05118-0_34`.

Legtchenko:2012:RCR

[LMSM12] Sergey Legtchenko, Sébastien Monnet, Pierre Sens, and Gilles Muller. RelaxDHT: a churn-resilient replication strategy for peer-to-peer distributed hash-tables. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 7(2):28:1–28:??, July 2012. CODEN ???? ISSN 1556-4665 (print), 1556-4703 (electronic).

Lipton:1993:CAH

[LN93] Richard J. Lipton and Jeffrey F. Naughton. Clocked adversaries for hashing. *Algorithmica*, 9(3):239–252, March 1993. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Liu:2008:GBK

[LND08] Donggang Liu, Peng Ning, and Wenliang Du. Group-based key predistribution for wireless sensor networks. *ACM Transactions on Sensor Networks*, 4(2):11:1–11:??, March 2008. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Litwin:1993:LLH

[LNS93] Witold Litwin, Marie-Anne A. Neimat, and Donovan A. Schneider. LH* — linear hashing for distributed files.

SIGMOD Record (ACM Special Interest Group on Management of Data), 22(2):327–336, June 1993. CODEN SRECD8. ISBN 0-89791-592-5. ISSN 0163-5808 (print), 1943-5835 (electronic).

Litwin:1996:LSD

[LNS96] Witold Litwin, Marie-Anna Neimat, and Donovan A. Schneider. LH* — a scalable, distributed data structure. *ACM Transactions on Database Systems*, 21(4):480–525, December 1996. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1996-21-4/p480-litwin/p480-litwin.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1996-21-4/p480-litwin/`.

Lee:2011:SJS

[LNS11] Hongrae Lee, Raymond T. Ng, and Kyuseok Shim. Similarity join size estimation using locality sensitive hashing. *Proceedings of the VLDB Endowment*, 4(6):338–349, March 2011. CODEN ???? ISSN 2150-8097.

Lohman:1989:IQO

[Loh89] Guy Lohman. Is query optimization a 'solved' problem? In ODBF '89 [ODB89], page ?? ISBN ?? LCCN ?? Technical Report CS/E 89-005.

Lomet:1983:BIE

[Lom83] David B. Lomet. Bounded index exponential hashing. *ACM Transactions on Database Systems*, 8(1): 136–165, March 1983. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Lomet:1988:SBD

[Lom88] David B. Lomet. A simple bounded disorder file organization with good performance. *ACM Transactions on Database Systems*, 13(4): ??, December 1988. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Lomet:1993:FDO

[Lom93] David B. Lomet, editor. *Foundations of Data Organization and Algorithms: 4th International Conference, FODO '93, Chicago, Illinois, USA, October 13–15, 1993: Proceedings*, volume 730 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-57301-1 (New York), 3-540-57301-1 (Berlin). LCCN QA76.9.D3 I5535 1993.

Lin:2001:EHM

[LÖON01] Shu Lin, M. Tamer Özsu,

Vincent Oria, and Raymond T. Ng. An extendible hash for multi-precision similarity querying of image databases. In Apers et al. [AAC+01], pages 221–230. ISBN 1-55860-804-4. LCCN QA76.9.D3 I559 2001. URL http://www.vldb.org/conf/2001/P221.pdf.

Liang:2000:OMD

[LOY00] Weifa Liang, Maria E. Orlowska, and Jeffrey X. Yu. Optimizing multiple dimensional queries simultaneously in multidimensional databases. *VLDB Journal: Very Large Data Bases*, 8(3–4):319–338, February 2000. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic). URL http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/l/Liang:Weifa.html; http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/o/Orlowska:Maria_E=.html; http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/y/Yu:Jeffrey_X=.html; http://link.springer.de/link/service/journals/00778/bibs/0008003/00080319.htm; http://link.springer.de/link/service/journals/00778/papers/0008003/00080319.pdf. Electronic edition.

Li:2012:OPH

[LOZ12] Ping Li, Art B. Owen, and Cun-Hui Zhang. One permutation hashing. In F. Pereira, C. J. C. Burges, L. Bottou, and K. Q. Weinberger, editors, *25th Annual Conference on Neural Information Processing Systems 2011. December 12–15, 2011, Granada, Spain*, pages 3122–3130. Curran Associates, Inc., Red Hook, NY, USA, 2012. ISBN 1-61839-599-8. LCCN QP363.3 A244 v. 24. URL https://papers.nips.cc/paper/4778-one-permutation-hashing.

Leung:2004:LPD

[LP04] Hing Leung and Viktor Podolskiy. The limitedness problem on distance automata: Hashiguchi's method revisited. *Theoret. Comput. Sci.*, 310(1–3):147–158, January 1, 2004. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Lin:2015:CRN

[LP15] Huijia Lin and Rafael Pass. Constant-round nonmalleable commitments from any one-way function. *Journal of the Association for Computing Machinery*, 62(1):5:1–5:??, February 2015. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Landelle:2016:CFR

[LP16] Franck Landelle and Thomas Peyrin. Cryptanalysis of full RIPEMD-128. *Journal of Cryptology*, 29(4):927–951, October 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s00145-015-9213-5`; `http://link.springer.com/article/10.1007/s00145-015-9213-5`.

Luccio:1991:APU

[LPP91] Fabrizio Luccio, Andrea Pietracaprina, and Geppino Pucci. Analysis of parallel uniform hashing. *Information Processing Letters*, 37 (2):67–69, January 31, 1991. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Luccio:1992:AIP

[LPP92] F. Luccio, A. Pietracaprina, and G. Pucci. Analysis and implementation of parallel uniform hashing. *International Journal of Foundations of Computer Science*, 3 (1):55–64, March 1992. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Leifer:2003:GAS

[LPSW03] James J. Leifer, Gilles Peskine, Peter Sewell, and Keith Wansbrough. Global abstraction-safe marshalling with hash types. *SIGPLAN Notices*, 38(9):87–98, September 2003. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Li:2012:WHT

[LPT12] Yinan Li, Jignesh M. Patel, and Allison Terrell. WHAM: a high-throughput sequence alignment method. *ACM Transactions on Database Systems*, 37(4):28:1–28:??, December 2012. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Long:2006:GCA

[LPWW06] Shoulun Long, Josef Pieprzyk, Huaxiong Wang, and Duncan S. Wong. Generalised cumulative arrays in secret sharing. *Designs, Codes, and Cryptography*, 40 (2):191–209, August 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=40&issue=2&spage=191`.

Li:2018:LLP

[LQH18] Kai Li, Guo-Jun Qi, and Kien A. Hua. Learning label preserving binary codes for multimedia retrieval: a general approach. *ACM*

Transactions on Multimedia Computing, Communications, and Applications, 14 (1):2:1–2:??, January 2018. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Lei:2014:FND

[LQZH14] Yanqiang Lei, Guoping Qiu, Ligang Zheng, and Jiwu Huang. Fast near-duplicate image detection using uniform randomized trees. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 10 (4):35:1–35:??, June 2014. ISSN 1551-6857 (print), 1551-6865 (electronic).

Larson:1985:EPH

[LR85] Per-Åke Larson and M. V. Ramakrishna. External perfect hashing. In Navathe [Nav85], pages 190–200. ISBN 0-89791-160-1. LCCN QA 76.9 D3 I59 1985.

Lee:1996:DRW

[LR96a] Dik Lun Lee and Liming Ren. Document ranking on weight-partitioned signature files. *ACM Transactions on Information Systems*, 14(2):109–137, April 1996. CODEN ATISET. ISSN 1046-8188. URL `http://www.acm.org:80/tois/abstracts/lee.html`.

Lo:1996:SHJ

[LR96b] Ming-Ling Lo and Chinya V. Ravishankar. Spatial hash-joins. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 25 (2):247–258, June 1996. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Li:1999:FJU

[LR99] Zhe Li and Kenneth A. Ross. Fast joins using join indices. *VLDB Journal: Very Large Data Bases*, 8(1):1–24, April 1999. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic). URL `http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/l/Li:Zhe.html`; `http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/r/Ross:Kenneth_A=.html`; `http://link.springer.de/link/service/journals/00778/bibs/9008001/90080001.htm`; `http://link.springer.de/link/service/journals/00778/papers/9008001/90080001.pdf`. Electronic edition.

Litwin:1991:THC

[LRLH91] W. A. Litwin, N. Roussopoulos, G. Levy, and W. Hong. Trie hashing with controlled load. *IEEE Transactions on Software Engineering*, 17(7):678–691, July 1991. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520

(electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=83904`.

Litwin:1989:THC

[LRLW89] W. Litwin, N. Roussopoulos, G. Levy, and H. Wang. Trie hashing with controlled load. Technical Report UMIACS-TR-89-11, CS-TR-2189, SRC-TR-89-13, INRIA; Institute for Advanced Computer Studies and Systems Research Center, Department of Computer Science, 78150 Le Chesnay France; University of Maryland, College Park, MD 20742, February 1989. 1–29 pp.

Leskovec:2014:MMD

[LRU14] Jurij Leskovec, Anand Rajaraman, and Jeffrey D. Ullman. *Mining of massive datasets*. Cambridge University Press, Cambridge, UK, second edition, 2014. ISBN 1-107-07723-0 (hardcover), 1-316-14731-2 (e-book), 1-139-92480-X (e-book). xii + 467 pp. LCCN QA76.9.D343 R35 2014eb.

Lipton:1978:EHS

[LRY78] R. J. Lipton, A. Rosenberg, and A. C. Yao. External hashing schemes for collections of data structures. Technical Report Dep. Report STA, Stanford University, December 1978. ?? pp.

Lipton:1980:EHS

[LRY80] Richard J. Lipton, Arnold L. Rosenberg, and Andrew C. Yao. External hashing schemes for collections of data structures. *Journal of the Association for Computing Machinery*, 27(1):81–95, January 1980. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Liu:2015:MDT

[LRY+15] Chang Liu, R. Ranjan, Chi Yang, Xuyun Zhang, Lizhe Wang, and Jinjun Chen. MuR-DPA: Top-down levelled multi-replica Merkle hash tree based secure public auditing for dynamic big data storage on cloud. *IEEE Transactions on Computers*, 64(9):2609–2622, ???? 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Lange:1985:DS

[LS85] O. Lange and G. Stegemann. *Datenstrukturen und Speichertechniken*. Friedrich Vieweg und Sohn, Braunschweig, Germany, 1985. ISBN 3-528-04314-8. ?? pp.

Litwin:1989:FDO

[LS89] W. Litwin and H.-J. Schek, editors. *Foundations of Data Organization and Algorithms: 3rd International Conference, FODO 1989,*

Paris, France, June 21–23, 1989: Proceedings, volume 367 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1989. ISBN 0-387-51295-0. LCCN QA76.9.D3 F671 1989.

Linial:1996:NEH

[LS96] Nathan Linial and Ori Sasson. Non-expansive hashing. In ACM [ACM96], pages 509–518. ISBN 0-89791-785-5. LCCN QA 76.6 A13 1996. URL `http://www.acm.org/pubs/articles/proceedings/stoc/237814/p509-linial/p509-linial.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/237814/p509-linial/`. ACM order no. 508960. Also known as Federated Computing Research Conference (FCRS '96).

Liu:2006:ECS

[LS06] Lihua Liu and Hao Shen. Explicit constructions of separating hash families from algebraic curves over finite fields. *Designs, Codes, and Cryptography*, 41(2): 221–233, November 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=2&spage=221`.

Laccetti:2007:BFA

[LS07a] G. Laccetti and G. Schmid. Brute force attacks on hash functions. *Journal of Discrete Mathematical Sciences and Cryptography*, 10(3):439–460, June 2007. CODEN ???? ISSN 0972-0529. URL `http://www.connectjournals.com/achivestoc.php?bookmark=CJ-003072&volume=10&issue_id=03`.

Lu:2007:MPC

[LS07b] Haibin Lu and Sartaj Sahni. $O(\log W)$ multidimensional packet classification. *IEEE/ACM Transactions on Networking*, 15(2):462–472, April 2007. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Lee:2015:MFA

[LS15] Jooyoung Lee and Martijn Stam. MJH: a faster alternative to MDC-2. *Designs, Codes, and Cryptography*, 76(2):179–205, August 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-014-9936-6`.

Lohman:1991:VLD

[LSC91] Guy M. Lohman, Amáilcar Sernadas, and Rafael Camps, editors. *Very Large Data Bases Proceedings: Proceedings of the Seventeenth Inter-*

national Conference on Very Large Data Bases, September 3–6, 1991, Barcelona (Catalonia, Spain). Morgan Kaufmann Publishers, San Francisco, CA, 1991. ISBN 1-55860-150-3. LCCN QA 76.9 D3 I61 1991.

Litwin:1989:CTH

[LSV89] W. Litwin, Y. Sagiv, and K. Vidyasankar. Concurrency and trie hashing. *Acta Informatica*, 26 (7):597–614, 1989. CODEN AINFA2. ISSN 0001-5903 (print), 1432-0525 (electronic).

Luo:2021:NMH

[LSZ+21] Ye Luo, Zehai Su, Wei Zheng, Zhaobin Chen, Fuqin Wang, Zhemin Zhang, and Jinjun Chen. A novel memory-hard password hashing scheme for blockchain-based cyber-physical systems. *ACM Transactions on Internet Technology (TOIT)*, 21(2): 42:1–42:21, June 2021. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL `https://dl.acm.org/doi/10.1145/3408310`.

Lochovsky:1980:SIC

[LT80] Frederick H. Lochovsky and ?. Taylor, editors. *Sixth International Conference on Very Large Data Bases: reprinted from Very large data bases*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1980. ACM order no. 471800. IEEE catalog no. 80CH1534-7C. Long Beach order no. 322.

Lipski:1985:PFD

[LT85] W. Lipski and K. Tanaka, editors. *Proceedings: Foundations of Data Organization: May 21–24, 1985, Kyoto, Japan*. FODO'85, Computer Science Institute, Kyoto Sangyo University, Kyoto, Japan, 1985.

Lehmann:2009:MDH

[LT09] Anja Lehmann and Stefano Tessaro. A modular design for hash functions: Towards making the mix-compress-mix approach practical. *Lecture Notes in CS*, 5912:364–381, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-10366-7_22`.

Larangeira:2012:RCN

[LT12] Mario Larangeira and Keisuke Tanaka. Reduction-centric non-programmable security proof for the full domain hash in the random oracle model. *Lecture Notes in CS*, 7690:124–143, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.`

1007/978-3-642-35416-8_10/.

Lu:1990:HBJ

[LTS90] H. Lu, K. L. Tan, and M. C. Shan. Hash-based join algorithms for multiprocessors with shared memory. In McLeod et al. [MSDS90], page 198. ISBN 1-55860-149-X. LCCN ???

Luccio:1972:WIL

[Luc72] Fabrizio Luccio. Weighted increment linear search for scatter tables. *Communications of the Association for Computing Machinery*, 15(12):1045–1047, December 1972. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Luhn:1953:xxx

[Luh53] Hans Peter Luhn. ??? Internal IBM memo that first suggested the idea of hashing, and one of the first applications of linked linear lists. Luhn is also the inventor of KWIC indexing, in 1960 [Knu73, p. 437]. See also [Lin53]., January 1953.

Luhn:1958:BIS

[Luh58] Hans Peter Luhn. A business intelligence system. *IBM Journal of Research and Development*, 2 (4):314–319, ???? 1958. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5392644.

Lum:1973:GPA

[Lum73] Vincent Y. Lum. General performance analysis of key-to-address transformation methods using an abstract file concept. *Communications of the Association for Computing Machinery*, 16 (10):603–612, October 1973. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Lutterbach:1988:NSD

[Lut88] Herbert Lutterbach, editor. *Non-standard Datenbanken fuer Anwendungen der Graphischen Datenverarbeitung: GI-Fachgesprach, Dortmund, 21./22. Marz 1988: proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. ISBN 0-387-19175-5. LCCN T385 .N66 1988.

Li:2011:EDH

[LVD+11] Tonglin Li, Raman Verma, Xi Duan, Hui Jin, and Ioan Raicu. Exploring distributed hash tables in HighEnd computing. *ACM SIGMETRICS Performance Evaluation Review*, 39(3):128–130, December 2011. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Lamdan:1988:GHG

[LW88] Yehezkel Lamdan and Haim J. Wolfson. Geometric hashing: a general and efficient model-based recognition scheme. In IEEE-CV'88 [IEE88b], pages 238–249. ISBN 0-8186-8883-1, 0-8186-0883-8 (paperback). LCCN TA1632 .I5485 1988. Available from IEEE Service Cent (catalog number 88CH2664-1). Piscataway, NJ, USA.

Lee:2004:IAK

[LW04] Narn-Yih Lee and Chien-Nan Wu. Improved authentication key exchange protocol without using one-way hash function. *Operating Systems Review*, 38(2):85–92, April 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Lenstra:2017:TPR

[LW17] Arjen K. Lenstra and Benjamin Wesolowski. Trustworthy public randomness with sloth, unicorn, and trx. *International Journal of Applied Cryptography. IJACT*, 3(4):330–343, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL `https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.089354`.

Lin:2011:EVO

[LWG11] Dai-Rui Lin, Chih-I Wang, and D. J. Guan. Efficient vehicle ownership identification scheme based on triple-trapdoor chameleon hash function. *Journal of Network and Computer Applications*, 34(1):12–19, January 2011. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804510001232`.

Wu:1991:PIC

[lWSS91] Chuan lin Wu (v.1), Herbert D. Schwetman (v.2), and Kimming So (v.3), editors. *Proceedings of the 1991 International Conference on Parallel Processing, August 12–16, 1991*. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 1991. ISBN 0-8493-0190-4 (set), 0-8493-0191-2 (v. 1), 0-8493-0192-0 (v. 2), 0-8493-0193-9 (v. 3). LCCN QA76.58 .I55 1991. ????

Lu:2020:VAN

[LWWK20] Kejing Lu, Hongya Wang, Wei Wang, and Mineichi Kudo. VHP: approximate nearest neighbor search via virtual hypersphere partitioning. *Proceedings of the VLDB Endowment*, 13 (9):1443–1455, May 2020. CODEN ???? ISSN 2150-8097. URL `https:/`

/dl.acm.org/doi/abs/10.14778/3397230.3397240.

Lin:2008:AZH

[LWWQ08] Pin Lin, Wenling Wu, Chuankun Wu, and Tian Qiu. Analysis of Zipper as a hash function. *Lecture Notes in CS*, 4991: 392–403, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-79104-1_28.

Lu:2018:WLS

[LWXS18] Kejing Lu, Hongya Wang, Yingyuan Xiao, and Hui Song. Why locality sensitive hashing works: A practical perspective. *Information Processing Letters*, 136(??):49–58, August 2018. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019018300796.

Liu:2018:MCM

[LWZ+18] R. Liu, S. Wei, Y. Zhao, Z. Zhu, and J. Wang. Multiview cross-media hashing with semantic consistency. *IEEE MultiMedia*, 25(2):71–86, April/June 2018. CODEN IEMUE4. ISSN 1070-986x (print), 1941-0166 (electronic).

Liu:2019:EPB

[LXL+19] Jia Liu, Bin Xiao, Xuan Liu, Kai Bu, Lijun Chen, and Changhai Nie. Efficient polling-based information collection in RFID systems. *IEEE/ACM Transactions on Networking*, 27(3): 948–961, June 2019. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Lum:1972:ARK

[LY72] Vincent Y. Lum and P. S. T. Yuen. Additional results on key-to-address transform techniques: a fundamental performance study on large existing formatted files. *Communications of the Association for Computing Machinery*, 15(11):996–997, November 1972. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Lum:1971:KAT

[LYD71] V. Y. Lum, P. S. T. Yuen, and M. Dodd. Key-to-address transform techniques: a fundamental performance study on large existing formatted files. *Communications of the Association for Computing Machinery*, 14(4):228–239, April 1971. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Survey of several hash functions, with performance results.

Lin:2019:TTS

[LYDA19] Qiongzheng Lin, Lei Yang, Chunhui Duan, and Zhenlin An. Tash: Toward selective reading as hash primitives for Gen2 RFIDs. *IEEE/ACM Transactions on Networking*, 27(2):819–834, April 2019. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Liu:2013:IRQ

[LYJ+13] Dong Liu, Shuicheng Yan, Rong-Rong Ji, Xian-Sheng Hua, and Hong-Jiang Zhang. Image retrieval with query-adaptive hashing. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 9 (1):2:1–2:??, February 2013. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Lyon:1978:HLP

[Lyo78a] Gordon Lyon. Hashing with linear probing and frequency ordering. *Journal of Research of the National Bureau of Standards (United States)*, 83(5):445–447, September–October 1978. CODEN JRNBAG.

Lyon:1978:PST

[Lyo78b] Gordon Lyon. Packed scatter tables. *Communications of the Association for Computing Machinery*, 21(10):857–865, October 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Lyon:1979:BSS

[Lyo79] Gordon Lyon. Batch scheduling from short lists. *Information Processing Letters*, 8 (2):57–59, February 15, 1979. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lyon:1983:PCC

[Lyo83] Gordon Lyon. Performance and cost characterization of A-tree (real-time) hashing. In *Proceedings of the 17th Annual Conference on Information Sciences and Systems.*, pages 477–?? Johns Hopkins Univ, Baltimore, Md, USA, 1983.

Lyon:1985:AHT

[Lyo85] Gordon Lyon. Achieving hash table searches in one or two bucket probes. *The Computer Journal*, 28(3): 313–318, July 1985. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Lu:2018:LCC

[LYW+18] Jianyuan Lu, Tong Yang, Yi Wang, Huichen Dai, Xi Chen, Linxiao Jin, Haoyu Song, and Bin Liu. Low computational cost Bloom filters. *IEEE/ACM Transactions on Networking*, 26 (5):2254–2267, October 2018. CODEN IEANEP. ISSN

1063-6692 (print), 1558-2566 (electronic).

Lai:2019:NIB

[LYX+19] Qiqi Lai, Bo Yang, Zhe Xia, Yannan Li, Yuan Chen, and Zhenlong Li. Novel identity-based hash proof system with compact master public key from lattices in the standard model. *International Journal of Foundations of Computer Science*, 30(4):589–606, June 2019. ISSN 0129-0541. URL `https://www.worldscientific.com/doi/10.1142/S0129054119400148`.

Lai:2018:NSH

[LYY+18] Qiqi Lai, Bo Yang, Yong Yu, Yuan Chen, and Jian Bai. Novel smooth hash proof systems based on lattices. *The Computer Journal*, 61 (4):561–574, April 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/61/4/561/4725104`.

Li:2006:FSS

[LZ06] Kang Li and Zhenyu Zhong. Fast statistical spam filter by approximate classifications. *ACM SIGMETRICS Performance Evaluation Review*, 34 (1):347–358, June 2006. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Liu:2016:MHN

[LZ16] Wei Liu and Tongtao Zhang. Multimedia hashing and networking. *IEEE MultiMedia*, 23(3):75–79, July/September 2016. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL `https://www.computer.org/csdl/mags/mu/2016/03/mmu2016030075-abs.html`.

Litwin:1988:MTH

[LZL88] W. Litwin, D. Zegour, and G. Levy. Multilevel trie hashing. *Lecture Notes in CS*, 303:309–??, April 1988. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). Also published in/as: Institut National de la Recherche en Informatique et Automatique, TR-723, Aug. 1987.

Monnerat:2015:ESH

[MA15] Luiz Monnerat and Claudio L. Amorim. An effective single-hop distributed hash table with high lookup performance and low traffic overhead. *Concurrency and Computation: Practice and Experience*, 27(7):1767–1788, May 2015. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Macii:1995:ECP

[Mac95] Enrico Macii. The effect of clustering on the per-

formance of hashing algorithms. *Conference proceedings / IEEE Pacific Rim Conference on Communications, Computers and Signal Processing; sponsored by IEEE Victoria Section ... [et al.]*, pages 149–152, May 1995. ISSN 0893-4266.

Maddison:1980:FLH

[Mad80] J. A. T. Maddison. Fast lookup in hash tables with direct rehashing. *The Computer Journal*, 23(2):188–189, May 1980. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Mairson:1983:PCS

[Mai83] Harry G. Mairson. Program complexity of searching a table. *Annual Symposium on Foundations of Computer Science (Proceedings)*, pages 40–47, 1983. CODEN ASFPDV. ISBN 0-8186-0508-1. ISSN 0272-5428. IEEE Service Cent. Piscataway, NJ, USA.

Mairson:1992:ETE

[Mai92] Harry G. Mairson. The effect of table expansion on the program complexity of perfect hash functions. *BIT (Nordisk tidskrift for informationsbehandling)*, 32(3): 430–440, 1992. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Michail:2012:EHT

[MAK+12] Harris E. Michail, George S. Athanasiou, Vasilis Kelefouras, George Theodoridis, and Costas E. Goutis. On the exploitation of a high-throughput SHA-256 FPGA design for HMAC. *ACM Transactions on Reconfigurable Technology and Systems*, 5(1):2:1–2:??, March 2012. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Mallach:1977:SST

[Mal77] E. G. Mallach. Scatter storage techniques: a uniform viewpoint and a method for reducing retrieval times. *The Computer Journal*, 20 (2):137–140, May 1977. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Mandelbrod:2012:LHA

[Man12] Matan Mandelbrod. Layered hashing algorithm for real-time systems. *Theory of Computing Systems*, 50(2):279–295, ???? 2012. CODEN TCSYFI. ISSN 1432-4350 (print), 1433-0490 (electronic). URL `http://www.springerlink.com/content/g271t221n70h4p87/`.

Martin:1964:HCF

[Mar64] William A. Martin. Hash-coding functions of a complex variable. Report A. I. MEMO

70 and MAC-M-165, Massachusetts Institute of Technology, A. I. Lab., Cambridge, Massachusetts, June 1964. ?? pp.

Martin:1971:DEA

[Mar71] William A. Martin. Determining the equivalence of algebraic expressions by hash coding. *Journal of the Association for Computing Machinery*, 18(4):549–558, October 1971. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Martin:1975:CDB

[Mar75] James Martin. *Computer Data-base Organization*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1975. ISBN 0-13-165506-X. xviii + 558 pp. LCCN QA76 .M324.

Martin:1977:CDB

[Mar77] James Martin. *Computer Data-base Organization*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 2 edition, 1977. ISBN 0-13-165423-3. xviii + 713 pp. LCCN QA76.9.D3 M36 1977.

Matias:1993:HPR

[Mat93] Yossi Matias. Highly parallel randomized algorithmics. In *Proceedings of the 3rd Workshop on Parallel Algorithms (WOPA)*, page ?? ????, ????, May 1993.

Mathieu:2009:PTA

[Mat09] Claire Mathieu, editor. *Proceedings of the Twentieth Annual ACM–SIAM Symposium on Discrete Algorithms, New York, NY, January 4–6, 2009*, Proceedings of the annual ACM-SIAM Symposium on Discrete Algorithms, 1071-9040. ACM Press, New York, NY 10036, USA, 2009. ISBN 0-89871-680-2. LCCN QA76.6 A849 2009. URL `http://www.siam.org/proceedings/soda/2009/soda09.php`.

Maurer:1968:PTI

[Mau68] Ward Douglas Maurer. Programming technique: An improved hash code for scatter storage. *Communications of the Association for Computing Machinery*, 11(1):35–38, January 1968. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Maurer:1983:IHC

[Mau83] W. D. Maurer. An improved hash code for scatter storage. *Communications of the Association for Computing Machinery*, 26(1):36–38, January 1983. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Martini:2003:DHM

[MB03] Paul M. Martini and Walter A. Burkhard. Double

hashing with multiple passbits. *International Journal of Foundations of Computer Science*, 14(6):1165–??, December 2003. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Marton:2012:OCC

[MBBS12] Zoltan-Csaba Marton, Ferenc Balint-Benczedi, and Florian Seidel. Object categorization in clutter using additive features and hashing of part-graph descriptors. *Lecture Notes in CS*, 7463:17–33, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32732-2_2/`.

Manegold:2000:ODA

[MBK00] Stefan Manegold, Peter A. Boncz, and Martin L. Kersten. Optimizing database architecture for the new bottleneck: memory access. *VLDB Journal: Very Large Data Bases*, 9(3):231–246, December 2000. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Mazeika:2007:ESA

[MBKS07] Arturas Mazeika, Michael H. Böhlen, Nick Koudas, and Divesh Srivastava. Estimating the selectivity of approximate string queries. *ACM Transactions on Database Systems*, 32(2):12:1–12:??, June 2007. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Munro:1986:TCR

[MC86] J. Ian Munro and Pedro Celis. *Techniques for Collision Resolution in Hash Tables with Open Addressing*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1986. ISBN 0-8186-0743-2. 601–610 pp. LCCN QA75.5 .F35 1986. IEEE Service Cent. Piscataway, NJ, USA.

McMillan:1989:RRU

[MC89] Thomas McMillan and William Collins. Recurrence relation in uniform hashing. In *Computing Trends in the 1990's. Proceedings 1989 ACM Seventeenth Annual Computer Science Conference (Feb 21–23 1989: Louisville, KY, USA)*, pages 410–?? ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-299-3. LCCN ????

McCarney:1979:LLH

[McC79] Gary McCarney. Learn the lingo and hash your way into faster data base management. *Electronic Design*, 27 (11):146–149, May 1979. CODEN ELODAW. ISSN 0013-4872.

McDonell:1977:III

[McD77] K. J. McDonell. An inverted index implementation. *The Computer Journal*, 20(2):116–123, May 1977. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_20/Issue_02/tiff/116.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_20/Issue_02/tiff/117.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_20/Issue_02/tiff/118.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_20/Issue_02/tiff/119.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_20/Issue_02/tiff/120.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_20/Issue_02/tiff/121.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_20/Issue_02/tiff/122.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_20/Issue_02/tiff/123.tif`.

McGrew:2017:IDH

[MCF17] Danile McGrew, M. Curcio, and Scott Fluhrer. Internet-draft: Hash-based signatures. Internet Engineering Task Force document., 2017. URL `http://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs`.

McIlroy:1963:VMF

[McI63] M. D. McIlroy. A variant method of file searching. *Communications of the Association for Computing Machinery*, 6(3):101, 1963. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

McIlroy:1982:DSL

[McI82] M. Douglas McIlroy. Development of a spelling list. *IEEE Trans. Comm.*, COM-30(1 pt 1):91–99, January 1982. CODEN IECMBT. ISSN 0096-1965.

McKenney:1989:HSEa

[McK89a] P. McKenney. High-speed event counting and classification using a dictionary hash technique. In McAuliffe and Kogge [MK89], pages 71–75. ISBN 0-271-00686-2. LCCN QA76.6 .I548 1989. Three volumes.

McKenney:1989:HSEb

[McK89b] Paul E. McKenney. High-speed event counting and classification using a dictionary hash technique. *Proceedings of the International Conference on Parallel Processing*, 3:71–75, 1989. CODEN PCPADL. ISSN 0190-3918. IEEE catalog number 89CH2701-1.

McNichol:2003:HTM

[McN03] Tom McNichol. How two math geeks with a lava

lamp and a webcam are about to unleash chaos on the Internet. *Wired*, 11 (8):??, August 2003. CODEN WREDEM. ISSN 1059-1028 (print), 1078-3148 (electronic). URL `http://www.lavarnd.org`; `http://www.wired.com/wired/archive/11.08/random.html`.

Markowsky:1978:AUC

[MCW78] G. Markowsky, J. L. Carter, and M. N. Wegman. Analysis of a universal class of hash functions. In Winkowski [Win78], pages 345–354. ISBN 0-387-08917-9. LCCN QC770 .I55 1978.

Mahapatra:1997:SGL

[MD97] Nihar R. Mahapatra and Shantanu Dutt. Scalable global and local hashing strategies for duplicate pruning in parallel $A*$ graph search. *IEEE Transactions on Parallel and Distributed Systems*, 8(7):738–756, July 1997. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL `http://dlib.computer.org/td/books/td1997/pdf/l0738.pdf`; `http://www.computer.org/tpds/td1997/l0738abs.htm`.

Macchetti:2005:QPH

[MD05] Marco Macchetti and Luigi Dadda. Quasi-pipelined hash circuits. In Montuschi and Schwarz [MS05], page ?? ISBN 0-7695-2366-8. LCCN QA76.9.C62 .S95 2005. URL `http://arith17.polito.it/final/paper-149.pdf`.

Mehlhorn:1977:EA

[Meh77] K. Mehlhorn. *Effiziente Algorithmen*. B. G. Teubner, Stuttgart, Germany, 1977. ISBN 3-519-02343-1. 240 pp. LCCN QA76.6 .M43.

Mehlhorn:1982:PSP

[Meh82] Kurt Mehlhorn. On the program size of perfect and universal hash functions. In IEEE-FOCS'82 [IEE82], pages 170–175. CODEN ASFPDV. ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE Serv Cent. Piscataway, NJ, USA.

Mehlhorn:1984:SS

[Meh84] Kurt Mehlhorn. *Sorting and Searching*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1984. ISBN 0-387-13302-X. xiv + 336 pp. LCCN QA76.9 .D35 M43.

Mehlhorn:1986:DEA

[Meh86] K. Mehlhorn. *Datenstrukturen und Effiziente Algorithmen Band 1: Suchen und Sortieren*. B. G. Teubner, Stuttgart, Germany, 1986. ISBN 3-519-02255-9. ?? pp.

Meijer:1995:HFB

[Mei95] A. R. Meijer. Hash functions based on modular squaring. *Transactions — The South African Institute of Electrical Engineers. Handelinge — Die Suid-Afrikaanse Instituut van Elektriese Ingenieurs*, 86(2):91–??, 1995. CODEN TSAEA9. ISSN 0038-2221.

Mekouar:1983:EPD

[Mek83] Faical Mekouar. Etude des performances du hachage digital. Technical report, Institut National de Recherche en Informatique et Automatique, June 1983. ?? pp.

Miranda:2014:RSE

[MEK+14] Alberto Miranda, Sascha Effert, Yangwook Kang, Ethan L. Miller, Ivan Popov, Andre Brinkmann, Tom Friedetzky, and Toni Cortes. Random slicing: Efficient and scalable data placement for large-scale storage systems. *ACM Transactions on Storage*, 10(3):9:1–9:??, July 2014. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic).

Mendelson:1982:AEH

[Men82] Haim Mendelson. Analysis of extendible hashing. *IEEE Transactions on Software Engineering*, SE-8(6): 611–619, November 1982. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic).

Mennink:2012:OCS

[Men12] Bart Mennink. Optimal collision security in double block length hashing with single length key. *Lecture Notes in CS*, 7658:526–543, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-34961-4_32`.

Mennink:2017:OCS

[Men17] Bart Mennink. Optimal collision security in double block length hashing with single length key. *Designs, Codes, and Cryptography*, 83 (2):357–406, May 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-016-0227-2`; `http://link.springer.com/article/10.1007/s10623-016-0227-2`.

Mergenthaler:1972:HCT

[Mer72] Erhard Mergenthaler. Hashcode-techniken, uebersicht. Technical report, ????, Stuttgart, Germany, 1972. ?? pp.

Merkle:1990:FSO

[Mer90a] Ralph C. Merkle. A fast software one-way hash function. *Journal of Cryptology*, 3(1):43–58, ???? 1990. CO-

DEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Merkle:1990:OWH

[Mer90b] Ralph C. Merkle. One way hash functions and DES. In Brassard [Bra90], pages 428–446 (or 428–466??). CODEN LNCSD9. ISBN 0-387-97317-6, 3-540-97317-6. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1989. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0435.htm`; `http://www.springerlink.com/content/978-0-387-97317-3`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=435`. Based on unpublished paper from 1979 and his Ph.D thesis, Stanford, 1979.

MeyerAufDerHeide:1993:HSS

[Mey93] Friedhelm Meyer Auf Der Heide. Hashing strategies for simulating shared memory on distributed memory machines. *Lecture Notes in CS*, 678:20–29, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Mor:1982:HCM

[MF82] M. Mor and A. S. Fraenkel. A hash code method for detecting and correcting spelling errors. *Communications of the Association for Computing Machinery*, 25(12): 935–940 (or 935–938??), December 1982. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Manolopoulos:1992:AHF

[MF92] Y. Manolopoulos and N. Fistas. Algorithms for a hashed file with variable-length records. *Information Sciences*, 63(3):229, 1992. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Munoz:2004:CRS

[MFES04] Jose L. Muñoz, Jordi Forne, Oscar Esparza, and Miguel Soriano. Certificate revocation system implementation based on the Merkle hash tree. *International Journal of Information Security*, 2 (2):110–124, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-003-0026-4`.

Mueller:2006:SMG

[MFK+06] Maik Mueller, Michael Freidrich, Klaus Kiefer, Ralf Miko, and Juergen Schneider. System and method for generating pseudo-random numbers. United States Patent 7,894,602., March 31, 2006. URL `http:`

www.google.com/patents/US7894602.

Mochizuki:2000:ERA

[MH00] H. Mochizuki and Y. Hayashi. An efficient retrieval algorithm of compound words using extendible hashing. *International Journal of Computer Processing of Oriental Languages (IJCPOL)*, 13(1): 15–??, 2000. CODEN ???? ISSN 0219-4279.

McKenzie:1990:SHA

[MHB90] Bruce J. McKenzie, R. Harries, and Timothy C. Bell. Selecting a hashing algorithm. *Software—Practice and Experience*, 20(2):209–224, February 1, 1990. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Mou:2013:CBC

[MHT+13] Luntian Mou, Tiejun Huang, Yonghong Tian, Menglin Jiang, and Wen Gao. Content-based copy detection through multimodal feature representation and temporal pyramid matching. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 10(1):5:1–5:??, December 2013. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Machii:1984:HMF

[MI84] M. Machii and Y. Igarashi. A hashing method of finding the maxima of a set of vectors. Technical Report CS-84-2, Department of Computer Science, Gunma University, Gunma, Japan, 1984. ?? pp.

Micciancio:2002:ICH

[Mic02] Daniele Micciancio. Improved cryptographic hash functions with worst-case/average-case connection. In ACM [ACM02], pages 609–618. ISBN 1-58113-495-9. LCCN QA75.5 .A22 2002. ACM order number 508020.

Maabreh:2018:MHT

[MIGA18] Majdi Maabreh, Hafez Irshid, Ajay Gupta, and Izzat Alasmadi. A multithreading and hashing technique for indexing Target–Decoy peptides databases. *Concurrency and Computation: Practice and Experience*, 30(9), May 10, 2018. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic). URL https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.4371.

Miller:1985:PHF

[Mil85] L. L. Miller. Performance of hash files in a microcomputer based parallel file system. In ACM-CONF'85' [ACM85a], pages 29–34. ISBN 0-89791-170-9. LCCN QA 76 R36 1985.

Miller:1987:STS

[Mil87] Webb Miller. *A Software Tools Sampler*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1987. ISBN 0-13-822305-X. viii + 344 pp. LCCN QA76.754 M55 1987. US$24.95.

Miller:1995:RAC

[Mil95] J. W. Miller. Random access from compressed datasets with perfect value hashing. *IEEE International Symposium on Information Theory*, pages 454–??, 1995. CODEN PISTFZ. ISSN 0271-4655.

Miltersen:1998:ECC

[Mil98] Peter Bro Miltersen. Error correcting codes, perfect hashing circuits, and deterministic dynamic dictionaries. In Karloff [Kar98], pages 556–563. ISBN 0-89871-410-9. LCCN QA76.6 .A278 1998. URL http://dl.acm.org/citation.cfm?id=314613.

Miltersen:1999:CPC

[Mil99] P. B. Miltersen. Cell probe complexity — a survey. In Raman et al. [RRR99], page ?? CODEN LNCSD9. ISBN 3-540-66836-5 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1738. URL http://link.springer-ny.com/link/service/series/0558/tocs/t1738.htm; http://www.springerlink.com/content/978-3-540-66836-7; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1738.

Miyaguchi:1989:NHF

[MIO89] S. Miyaguchi, M. Iwata, and K. Ohta. New 128-bit hash function. In IJWCC'89 [IJW89], pages 279–288. LCCN TK5105.5 .I574 1989.

Mironov:2001:HFM

[Mir01] Ilya Mironov. Hash functions: From Merkle-Damgård to Shoup. *Lecture Notes in CS*, 2045:166–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2045/20450166.htm; http://link.springer-ny.com/link/service/series/0558/papers/2045/20450166.pdf.

Mirrokni:2017:OOM

[Mir17] Vahab Mirrokni. Online optimization for markets and the cloud: Theory and practice. *ACM SIGMETRICS Performance Evaluation Review*, 45(1):47–48, June 2017. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Mitra:1973:SHP

[Mit73] Debasis Mitra. Solution to the hashing problem for

code length 3. *Information and Control*, 23(3):205–220, October 1973. CODEN IFCNA4. ISSN 0019-9958 (print), 1878-2981 (electronic).

Mitzenmacher:2002:GHT

[Mit02] Michael Mitzenmacher. Good hash tables and multiple hash functions. *Dr. Dobbs Journal*, 27(5):28, 30–32, May 2002. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/ftp/2002/2002_05/hash.txt`.

Mitzenmacher:2009:SOQ

[Mit09] Michael Mitzenmacher. Some open questions related to cuckoo hashing. In Fiat and Sanders [FS09], pages 1–10. CODEN LNCSD9. ISBN 3-642-04127-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A43 E83 2009. URL `http://www.springerlink.com/content/xmk215105743x3p9/`.

Mittelbach:2012:HCS

[Mit12] Arno Mittelbach. Hash combiners for second pre-image resistance, target collision resistance and pre-image resistance have Long output. *Lecture Notes in CS*, 7485:522–539, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-32928-9_29`.

Mitzenmacher:2017:BBH

[Mit17] Michael Mitzenmacher. Building a better hash function: technical perspective. *Communications of the Association for Computing Machinery*, 60(7):93, July 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2017/7/218877/fulltext`.

Mathew:2008:JBH

[MJ08] S. Mathew and K. P. Jacob. JERIM-320: a 320-bit hash function with dual applications — a statistical analysis. *Journal of Discrete Mathematical Sciences and Cryptography*, 11 (4):471–482, August 2008. CODEN ???? ISSN 0972-0529. URL `http://www.connectjournals.com/achivestoc.php?bookmark=CJ-003072&volume=11&issue_id=04`.

Muthusamy:2014:IFC

[MJ14] Vinod Muthusamy and Hans-Arno Jacobsen. Infrastructure-free content-based publish/subscribe. *IEEE/ACM Transactions on Networking*, 22(5):1516–1530, October 2014. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Michelogiannakis:2011:PCE

[MJBD11] George Michelogiannakis, Nan Jiang, Daniel U. Becker, and William J. Dally. Packet chaining: Efficient single-cycle allocation for on-chip networks. *IEEE Computer Architecture Letters*, 10(2): 33–36, July/December 2011. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Mukherjee:2002:ECV

[MJT+02] R. Mukherjee, J. Jain, K. Takayama, J. A. Abraham, D. S. Fussell, and M. Fujita. Efficient combinational verification using overlapping local BDDs and a hash table. *Formal Methods in System Design*, 21(1): 95–101, July 2002. CODEN FMSDE6. ISSN 0925-9856.

McAuliffe:1989:PIC

[MK89] Kevin P. McAuliffe and Peter M. Kogge, editors. *Proceedings of the 1989 International Conference on Parallel Processing, August 8–12, 1989*, volume 1. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. ISBN 0-271-00686-2. LCCN QA76.6 .I548 1989. Three volumes.

Miller:1993:RFS

[MK93] Ethan L. Miller and Randy H. Katz. RAMA: a file system for massively-parallel computers. In Coleman [Col93], pages 163–168. ISBN 0-8186-3462-6. LCCN TK7895.M4 I5 1993.

Manoharan:2011:PAM

[MK11] Arun Manoharan and Ammasi Krishnan. Power analysis of multiple hashing Bloom filter architecture for network applications. *International Journal of Computer Applications*, 33(4):316–322, 2011. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.2316/Journal.202.2011.4.202-3052`.

Miliaraki:2012:FDS

[MK12] Iris Miliaraki and Manolis Koubarakis. FoXtrot: Distributed structural and value XML filtering. *ACM Transactions on the Web (TWEB)*, 6(3):12:1–12:??, September 2012. CODEN ???? ISSN 1559-1131 (print), 1559-114X (electronic).

Mozaffari-Kermani:2017:FDA

[MKAA17] Mehran Mozaffari-Kermani, Reza Azarderakhsh, and Anita Aghaie. Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC. *ACM Transactions on Embedded Computing Systems*, 16(2):59:1–59:??, April 2017. CODEN ???? ISSN

1539-9087 (print), 1558-3465 (electronic).

Mozaffari-Kermani:2018:ERE

[MKASJ18] Mehran Mozaffari-Kermani, Reza Azarderakhsh, Ausmita Sarker, and Amir Jalali. Efficient and reliable error detection architectures of hash-counter-hash tweakable enciphering schemes. *ACM Transactions on Embedded Computing Systems*, 17(2): 54:1–54:??, April 2018. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

McGrew:2016:SMH

[MKF+16] Daniel McGrew, Panos Kampanakis, Scott Fluhrer, Stefan-Lukas Gazdag, Denis Butin, and Johannes Buchmann. State management for hash-based signatures. *Lecture Notes in CS*, 10074:244–260, 2016. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `https://link.springer.com/chapter/10.1007/978-3-319-49100-4_11`.

Varalakshmi:2021:HPI

[MKL21] Varalakshmi M, Amit P. Kesarkar, and Daphne Lopez. High-performance implementation of a two-bit geohash coding technique for nearest neighbor search. *Concurrency and Computation: Practice and Experience*, 33 (5):e6029:1–e6029:??, March 10, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Mochizuki:1998:SSA

[MKSiA98] H. Mochizuki, M. Koyama, M. Shishibori, and J. i. Aoe. A substring search algorithm in extendible hashing. *Information Sciences*, 108(1): 13–30, July 1998. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Maurer:1975:HTM

[ML75] W. D. Maurer and T. G. Lewis. Hash table methods. *ACM Computing Surveys*, 7 (1):5–19, March 1975. CODEN CMSVAN. ISSN 0010-4892.

Mackert:1986:ROV

[ML86] L. F. Mackert and G. M. Lohman. R* optimizer validation and performance evaluation for distributed queries. In Chu et al. [CGO86], pages 149–159. ISBN 0-934613-18-4. LCCN QA76.9.D3 I559 1986.

Manolopoulos:1994:PLH

[ML94] Y. Manolopoulos and N. Lorentzos. Performance of linear hashing schemes for primary key retrieval. *Information system*, 19(5):433–??, 1994. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Myllymaki:1995:DTJ

[ML95] Jussi Myllymaki and Miron Livny. Disk-tape joins: synchronizing disk and tape access. *ACM SIGMETRICS Performance Evaluation Review*, 23(1):279–290, May 1995. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Martin:19xx:ETJ

[MLxx] T. P. Martin and P. A. Larson. An evaluation of three join algorithms for a shared-memory multiprocessor environment. *???*, ??(??):????, 19xx.

Ma:2015:TDH

[ML15] Chao Ma and Chuancai Liu. Two dimensional hashing for visual tracking. *Computer vision and image understanding: CVIU*, 135(??): 83–94, June 2015. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic). URL `http://www.sciencedirect.com/science/article/pii/S107731421500017X`.

Martin:1994:PHB

[MLD94] T. P. Martin, P.-A. Larson, and V. Deshpande. Parallel hash-based join algorithms for a shared-everything environment. *IEEE Transactions on Knowledge and Data Engineering*, 6(5):750–??, October 1, 1994. CODEN ITKEEH. ISSN 1041-4347.

Ma:2017:NDC

[MLHK17] Dekui Ma, Jian Liang, Ran He, and Xiangwei Kong. Nonlinear discrete cross-modal hashing for visual-textual data. *IEEE MultiMedia*, 24(2):56–65, April/June 2017. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL `https://www.computer.org/csdl/mags/mu/2017/02/mmu2017020056-abs.html`.

Martinez:2007:OXH

[MLP07] Christopher J. Martinez, Wei-Ming Lin, and Parimal Patel. Optimal XOR hashing for non-uniformly distributed address lookup in computer networks. *Journal of Network and Computer Applications*, 30(4): 1397–1427, November 2007. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804506000786`.

Madria:2001:FCC

[MMC01] S. Kumar Madria, S. N. Maheshwari, and B. Chandra. Formalization and correctness of a concurrent linear hash structure algorithm using nested transactions and I/O automata. *Data and Knowledge Engineering*, 37 (2):139–176, May 2001. CODEN DKENEW. ISSN

0169-023X (print), 1872-6933 (electronic).

Mehrotra:2010:RII

[MMG10] Hunny Mehrotra, Banshidhar Majhi, and Phalguni Gupta. Robust iris indexing scheme using geometric hashing of SIFT keypoints. *Journal of Network and Computer Applications*, 33(3):300–313, May 2010. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804509001416`.

McEvoy:2009:IWH

[MMMT09] Robert P. McEvoy, Colin C. Murphy, William P. Marnane, and Michael Tunstall. Isolated WDDL: a hiding countermeasure for differential power analysis on FPGAs. *ACM Transactions on Reconfigurable Technology and Systems*, 2(1):3:1–3:??, March 2009. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Mourad:1994:LPH

[MMSY94] A. N. Mourad, R. J. T. Morris, A. Swami, and H. C. Young. Limits of parallelism in hash join algorithms. *Performance evaluation*, 20(1 / 3):301–??, May 1, 1994. CODEN PEEVD9. ISSN 0166-5316 (print), 1872-745X (electronic).

Mehlhorn:1990:BOD

[MN90] Kurt Mehlhorn and Stefan Naeher. Bounded ordered dictionaries in $O(\log \log n)$ time and $O(n)$ space. *Information Processing Letters*, 35(4):183–189, August 1990. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Mehlhorn:1999:LPC

[MN99] Kurt Mehlhorn and Stefan Näher. *LEDA: a platform for combinatorial and geometric computing*. Cambridge University Press, Cambridge, UK, 1999. ISBN 0-521-56329-1 (hardcover). xvi + 1018 pp. LCCN QA76.73.C153 M44 1999. URL `http://www.loc.gov/catdir/description/cam0210/99024952.html`; `http://www.loc.gov/catdir/toc/cam027/99024952.html`.

Motwani:2008:LBL

[MNP08] Rajeev Motwani, Assaf Naor, and Rina Panigrahy. Lower bounds on locality sensitive hashing. *SIAM Journal on Discrete Mathematics*, 21(4): 930–935, ???? 2008. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Moran:2007:DHI

[MNS07] Tal Moran, Moni Naor, and Gil Segev. Deterministic history-independent strate-

gies for storing information on write-once memories. In Arge et al. [ACJT07], pages 303–315. ISBN 3-540-73419-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267 .I55 2007. URL `http://www.springerlink.com/content/b28632551tt5657q/`; `http://www.wisdom.weizmann.ac.il/~naor/PAPERS/writeonce.pdf`.

Mendel:2012:CAR

[MNS12] Florian Mendel, Tomislav Nad, and Martin Schläffer. Collision attacks on the reduced dual-stream hash function RIPEMD-128. *Lecture Notes in CS*, 7549: 226–243, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-34047-5_14/`.

Mansour:1990:CCU

[MNT90] Yishay Mansour, Noam Nisan, and Prasoon Tiwari. The computational complexity of universal hashing. In ACM-TOC'90 [ACM90], pages 235–243. ISBN 0-89791-361-2. LCCN ????

Mansour:1993:CCU

[MNT93] Y. Mansour, N. Nisan, and P. Tiwari. The computational complexity of universal hashing. *Theoret. Comput. Sci.*, 107(1):121–133, January 4, 1993. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Matsumoto:1981:NCM

[MNY81] K. Matsumoto, M. Naka, and H. Yamamoto. New clustering method for Landsat images using local maximums of a multi-dimensional histogram. In *7th International Symposium — Machine Processing of Remotely Sensed Data with Special Emphasis on Range, Forest, and Wetlands Assessment.*, pages 321–326. Purdue Res Found, West Lafayette, Indiana, USA, 1981. IEEE. Piscataway, NJ, USA.

Monien:1992:DSE

[MO92a] B. Monien and Th. Ottmann, editors. *Data Structures and Efficient Algorithms: Final Report on the DFG Special Joint Initiative*, volume 594 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992. ISBN 0-387-55488-2 (New York), 3-540-55488-2 (Berlin). viii + 389 pp. LCCN QA76.9.D35D36 1992. Papers presented at a symposium held at the Freie Universität Berlin, Sept. 23–26, 1991.

Moto-oka:1992:FGC

[Mo92b] Toru Moto-oka, editor. *Fifth generation computer systems: proceedings of the International Conference on Fifth Generation Computer Systems, Tokyo, Japan, October 19–22, 1981*. ACM Press, New York, NY 10036, USA, 1992. ISBN 0-444-86440-7. LCCN QA76.5 .I545 1981.

Mohan:1990:ACC

[Moh90] C. Mohan. ARIES/LHS: a concurrency control and recovery method using write-ahead logging for linear hashing with separators. Technical report, IBM Corporation, San Jose, CA, USA, March 1990. ?? pp.

Mohan:1993:ACC

[Moh93] C. Mohan. ARIES/LHS: a concurrency control and recovery method using write-ahead logging for linear hashing with separators. In ICDE'93 [ICD93], page 243. ISBN 0-8186-3572-X (hardcover), 0-8186-3570-3 (paperback), 0-8186-3571-1 (microfiche). LCCN QA76.9.D3I57 1993.

Mohassel:2011:OTS

[Moh11] Payman Mohassel. One-time signatures and Chameleon hash functions. *Lecture Notes in CS*, 6544:302–319, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-19574-7_21`.

Miyaguchi:1990:CSH

[MOI90] S. Miyaguchi, K. Ohta, and M. Iwata. Confirmation that some hash functions are not collision free. In Damgård [Dam90a], pages 293–308. ISBN 0-387-53587-X (New York), 3-540-53587-X (Berlin). LCCN QA76.9.A25 E964 1990. DM69.00.

Miyaguchi:1991:CSH

[MOI91] Shoji Miyaguchi, Kazuo Ohta, and Masahiko Iwata. Confirmation that some hash functions are not collision free. *Lecture Notes in CS*, 473:326–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730326.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0473/04730326.pdf`.

Molodowitch:1990:ADAa

[Mol90a] Mariko Molodowitch. *Analysis and design of algorithms: double hashing and parallel graph searching*. PhD thesis, Dept. of Information and Computer Science, University of California, Irvine,

Irvine, CA, USA, 1990. xiii + 164 pp.

Molodowitch:1990:ADAb

[Mol90b] Mariko Molodowitch. Analysis and design of algorithms: double hashing and parallel graph searching. Technical Report TR 90-43, Dept. of Information and Computer Science, University of California, Irvine, 1990. xii + 112 pp. Originally presented as the author's Ph.D. thesis.

Monico:2019:CHF

[Mon19] Chris Monico. Cryptanalysis of a hash function, and the modular subset sum problem. *Groups. Complexity. Cryptology*, 11(1):17–??, May 2019. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL `https://www.degruyter.com/view/j/gcc.2019.11.issue-1/gcc-2019-2001/gcc-2019-2001.xml`.

Morris:1968:SST

[Mor68] Robert Morris. Scatter storage techniques. *Communications of the Association for Computing Machinery*, 11(1):38–44, January 1968. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Influential survey of the subject of hashing, and first introduction of random probing with secondary clustering. Appears to be the first publication where the word 'hashing' appeared, although it was in common use at the time. Knuth [Knu73, p. 542] found only one earlier printed use of the word, in a 1961 unpublished memorandum by W. W. Peterson.

Moran:1983:CDO

[Mor83a] Shlamo Moran. On the complexity of designing optimal partial match retrieval systems. *ACM Transactions on Database Systems*, 8(4):543–551, December 1983. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Morris:1983:SST

[Mor83b] Morris. Scatter storage techniques. *Communications of the Association for Computing Machinery*, 26(??): ??, ???? 1983. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Motoyoshi:1984:HAC

[Mot84] Fumio Motoyoshi. Hash addressing chip. *Denshi Gijutsu Sogo Kenkyusho Iho/Bulletin of the Electrotechnical Laboratory*, 48(8):736–738, ???? 1984. CODEN DGSKAR. ISSN 0366-9092.

Midkiff:1990:ICO

[MP90] Samuel P. Midkiff and David A. Padua. Issues in the compile-time optimization of parallel programs. Techni-

cal Report CSRD 993, University of Illinois at Urbana-Champaign, Center for Supercomputing Research and Development, Urbana, IL 61801, USA, May 1990. 26 pp.

Mennink:2012:HFB

[MP12] Bart Mennink and Bart Preneel. Hash functions based on three permutations: a generic security analysis. *Lecture Notes in CS*, 7417:330–347, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32009-5_20/`.

Mennink:2016:EPH

[MP16] Bart Mennink and Bart Preneel. Efficient parallelizable hashing using small non-compressing primitives. *International Journal of Information Security*, 15(3): 285–300, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-015-0288-7`.

Martinez:2009:DFN

[MPL09] Christopher J. Martinez, Devang K. Pandya, and Wei-Ming Lin. On designing fast nonuniformly distributed IP address lookup hashing algorithms. *IEEE/ACM Transactions on Networking*, 17(6):1916–1925, December 2009. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Malensek:2014:EGG

[MPP14] Matthew Malensek, Sangmi Pallickara, and Shrideep Pallickara. Evaluating geospatial geometry and proximity queries using distributed hash tables. *Computing in Science and Engineering*, 16 (4):53–61, July/August 2014. CODEN CSENFA. ISSN 1521-9615.

Moody:2016:ISF

[MPST16] Dustin Moody, Souradyuti Paul, and Daniel Smith-Tone. Indifferentiability security of the fast wide pipe hash: breaking the birthday barrier. *Journal of Mathematical Cryptology*, 10(2): 101–133, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Mendel:2007:CTH

[MR07] Florian Mendel and Vincent Rijmen. Cryptanalysis of the Tiger hash function. *Lecture Notes in CS*, 4833:536–550, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-76900-2_33`.

MedeirosDuarte:2019:CPC

[MRL+19] Rodrigo Medeiros Duarte, André Rauber Du Bois, Maurício Lima Pilla, Gerson Geraldo H. Cavalheiro, and Renata Hax Sander Reiser. Comparing the performance of concurrent hash tables implemented in Haskell. *Science of Computer Programming*, 173(??): 56–70, March 15, 2019. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167642318302491`.

Mendel:2010:RAR

[MRST10] Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen. Rebound attacks on the reduced Grøstl hash function. *Lecture Notes in CS*, 5985:350–365, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-11925-5_24`.

Mitchell:1989:RHF

[MRW89] Chris Mitchell, Dave Rush, and Michael Walker. A remark on hash functions for message authentication. *Computers and Security*, 8 (1):55–58, February 1, 1989. CODEN CPSEDU. ISSN 0167-4048.

Mikkilineni:1988:ERJ

[MS88a] Krishna P. Mikkilineni and Stanley Y. W. Su. An evaluation of relational join algorithms in a pipelined query processing environment. *IEEE Transactions on Software Engineering*, 14(6):838–848, June 1988. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6162`.

Murthy:1988:SSC

[MS88b] D. Murthy and Pradip K. Srimani. Split sequence coalesced hashing. *Information system*, 13(2):211–218, May 1988. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Malard:2002:DDH

[MS02] J. M. Malard and R. D. Stewart. Distributed dynamic hash tables using IBM LAPI. In IEEE [IEE02], page ?? ISBN 0-7695-1524-X. LCCN ???? URL `http://www.sc-2002.org/paperpdfs/pap.pap247.pdf`.

Montuschi:2005:PIS

[MS05] Paolo Montuschi and Eric (Eric Mark) Schwarz, editors. *Proceedings of the 17th IEEE Symposium on Computer Arithmetic, ARITH-17 2005, June 27–29, 2005,*

Cape Cod, Massachusetts, USA. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2005. ISBN 0-7695-2366-8. LCCN QA76.9.C62 .S95 2005.

Mashatan:2009:ITC

[MS09] Atefeh Mashatan and Douglas R. Stinson. Interactive two-channel message authentication based on Interactive–Collision Resistant hash functions. *International Journal of Information Security*, 8(1):49–60, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-008-0063-0`.

Makrushin:2012:IRB

[MS12] Andrey Makrushin and Tobias Scheidat. Improving reliability of biometric hash generation through the selection of dynamic handwriting features. *Lecture Notes in CS*, 7228:19–41, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31971-6_2/`.

Morawiecki:2013:SBP

[MS13] Pawel Morawiecki and Marian Srebrny. A SAT-based preimage analysis of reduced Keccak hash functions. *Information Processing Letters*, 113(10–11): 392–397, May/June 2013. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019013000811`.

Maier:2016:CHT

[MSD16] Tobias Maier, Peter Sanders, and Roman Dementiev. Concurrent hash tables: fast and general?(!). *SIGPLAN Notices*, 51(8):34:1–34:??, August 2016. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Maier:2019:CHT

[MSD19] Tobias Maier, Peter Sanders, and Roman Dementiev. Concurrent hash tables: Fast and general(?)! *ACM Transactions on Parallel Computing (TOPC)*, 5(4):16:1–16:??, March 2019. CODEN ???? ISSN 2329-4949 (print), 2329-4957 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3309206`.

McCleod:1990:VLD

[MSDS90] Dennis McLeod, Ron Sacks-Davis, and Hans Schek, editors. *Very Large Data Bases: 16th International Conference on Very Large Data Bases, August 13–16, 1990,*

Brisbane, Australia. Morgan Kaufmann Publishers, San Francisco, CA, 1990. ISBN 1-55860-149-X. LCCN ???

Malhotra:1996:SED

[MSK96] Vishv M. Malhotra, Bala Srinivasan, and Santosh Kulkarni. Storage-efficient data structure for large lookup dictionaries. *Information Processing Letters*, 58 (4):201–206, May 27, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Mouha:2012:CIR

[MSP12] Nicky Mouha, Gautham Sekar, and Bart Preneel. Challenging the increased resistance of regular hash functions against birthday attacks. *Journal of Mathematical Cryptology*, 6(3–4):229–248, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/view/j/jmc.2012.6.issue-3-4/jmc-2011-0010/jmc-2011-0010.xml`.

MeyeraufderHeide:1996:ESR

[MSS96] F. Meyer auf der Heide, C. Scheideler, and V. Stemann. Exploiting storage redundancy to speed up randomized shared memory simulations. *Theoret. Comput. Sci.*, 162(2):245–281, August 20, 1996. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Meichun:1990:COL

[MSSWP90] Hs Meichun, Tung Shang-Sheng, and Yang Wei-Pang. Concurrent operations in linear hashing. *Information Sciences*, 51(2):193–212, 1990. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Maitin-Shepard:2017:ECM

[MSTA17] Jeremy Maitin-Shepard, Mehdi Tibouchi, and Diego F. Aranha. Elliptic curve multiset hash. *The Computer Journal*, 60(4):476–490, March 23, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `https://academic.oup.com/comjnl/article/60/4/476/2608055`.

Morrison:1987:QAH

[MSV87] John A. Morrison, Larry A. Shepp, and Christopher J. Van Wyk. A queueing analysis of hashing with lazy deletion. *SIAM Journal on Computing*, 16(6):1155–1164, December 1987. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Maier:2019:DSE

[MSW19] Tobias Maier, Peter Sanders, and Stefan Walzer. Dynamic space efficient hashing. *Algorithmica*, 81(8):

3162–3185, August 2019. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Ma:2020:TDE

[MSZ+20] Zhulin Ma, Edwin H.-M. Sha, Qingfeng Zhuge, Weiwen Jiang, Runyu Zhang, and Shouzhen Gu. Towards the design of efficient hash-based indexing scheme for growing databases on non-volatile memory. *Future Generation Computer Systems*, 105(??):1–12, April 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X18331005`.

March:2011:ROD

[MT11] Verdi March and Yong Meng Teo. A read-only distributed hash table. *Journal of Grid Computing*, 9(4):501–529, December 2011. CODEN ???? ISSN 1570-7873 (print), 1572-9184 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=1570-7873&volume=9&issue=4&spage=501`.

Mullan:2016:HHF

[MT16] Ciaran Mullan and Boaz Tsaban. SL_2 homomorphic hash functions: worst case to average case reduction and short collision search. *Designs, Codes, and Cryptography*, 81(1):83–107, October 2016. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-015-0129-8`; `http://link.springer.com/article/10.1007/s10623-015-0129-8`.

Madria:2000:MLT

[MTB00] S. K. Madria, M. A. Tubaishat, and B. Bhargava. Multi-level transaction model for semantic concurrency control in linear hash structures. *Information and Software Technology*, 42(7):445–464, May 1, 2000. CODEN ISOTE7. ISSN 0950-5849 (print), 1873-6025 (electronic).

Muehlbacher:2004:FHT

[Mue04] Joerg R. Muehlbacher. Full hash table search using primitive roots of the prime residue group Z/p. *J.UCS: Journal of Universal Computer Science*, 10(9):1239–1249, September 28, 2004. CODEN ???? ISSN 0948-6968. URL `http://www.jucs.org/jucs_10_9/full_hash_table_search`.

Mullin:1972:IIS

[Mul72] James K. Mullin. An improved indexed-sequential access method using hashed overflow. *Communications of the Association for Computing Machinery*, 15(5):

301–307, May 1972. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Mullin:1981:TCL

[Mul81] James K. Mullin. Tightly controlled linear hashing without separate overflow storage. *BIT (Nordisk tidskrift for informationsbehandling)*, 21(4):390–400, 1981. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Mullen:1984:UDH

[Mul84a] J. Mullen. Unified dynamic hashing. In Dayal et al. [DSS84], pages 473–480.

Mullin:1984:UDH

[Mul84b] James K. Mullin. Unified dynamic hashing. In *Proceedings — Very Large Data Bases, Tenth International Conference.*, pages 473–480. VLDB Endowment, Saratoga, CA, USA, 1984.

Mullin:1985:SSE

[Mul85] James K. Mullin. Spiral storage: Efficient dynamic hashing with constant performance. *The Computer Journal*, 28(3): 330–334, July 1985. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Mullin:1991:CUC

[Mul91] James K. Mullin. A caution on universal classes of hash functions. *Information Processing Letters*, 37(5):247–256, March 14, 1991. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Mullin:1992:HFH

[Mul92] J. K. Mullin. Hash functions for hash-based join methods. *The Computer Journal*, 35(6):A499–A503, December 1992. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Mathieu:1988:MQS

[MV88] Claire M. Mathieu and Jeffrey Scott Vitter. Maximum queue size and hashing with lazy deletion. In Wegman et al. [WGM88], pages 743–748. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a208838.pdf`.

Matias:1990:PHI

[MV90] Y. Matias and U. Vishkin. On parallel hashing and integer sorting. In Paterson [Pat90], page ?? ISBN 0-387-52826-1 (New York), 3-540-52826-1 (Berlin). LCCN QA267.A1 L43 no.443.

Matias:1991:CHP

[MV91a] Yossi Matias and Uzi Vishkin. Converting high probability

into nearly-constant time, with applications to parallel hashing. In ACM-TOC'91 [ACM91e], pages 307–316. ISBN 0-89791-397-3. LCCN QA 76.6 A13 1991.

Matias:1991:PHI

[MV91b] Yossi Matias and Uzi Vishkin. On parallel hashing and integer sorting. *Journal of Algorithms*, 12(4):573–606, December 1, 1991. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic).

Menezes:1991:ACC

[MV91c] Alfred J. Menezes and Scott A. Vanstone, editors. *Advances in Cryptology–CRYPTO '90: Proceedings*, volume 537 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1991. ISBN 0-387-54508-5 (New York), 3-540-54508-5 (Berlin). LCCN QA76.9.A25 C79 1990. Conference held Aug. 11–15, 1990, at the University of California, Santa Barbara.

Mihcak:2001:PAH

[MV01] M. Kıvanç Mıhçak and Ramarathnam Venkatesan. A perceptual audio hashing algorithm: a tool for robust audio identification and information hiding. *Lecture Notes in CS*, 2137:51–65, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370051.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2137/21370051.pdf`.

Mihcak:2002:NIG

[MV02] M. Kivanç Mihçak and Ramarathnam Venkatesan. New iterative geometric methods for robust perceptual image hashing. *Lecture Notes in CS*, 2320:13–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2320/23200013.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2320/23200013.pdf`.

Mitzenmacher:2008:WSH

[MV08] M. Mitzenmacher and S. Vadhan. Why simple hash functions work: Exploiting the entropy in a data stream. In ACM [ACM08a], pages 746–755. ISBN 0-89871-647-0. LCCN QA76.9.A43 A34 2008.

Mendelson:2021:ASC

[MVB+21] Gal Mendelson, Shay Vargaftik, Katherine Barabash, Dean H. Lorenz, Isaac Keslassy, and Ariel Orda.

AnchorHash: a scalable consistent hash. *IEEE/ACM Transactions on Networking*, 29(2):517–528, April 2021. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL `https://dl.acm.org/doi/10.1109/TNET.2020.3039547`.

Martirosyan:2008:ECP

[MvT08] Sosina Martirosyan and Tran van Trung. Explicit constructions for perfect hash families. *Designs, Codes, and Cryptography*, 46(1):97–112, January 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=1&spage=97`.

Mittermeir:1995:AVS

[MW95] R. T. Mittermeir and L. Wuerfl. Abstract visualization of software. A basis for a complex hash-key? *Lecture Notes in CS*, 945:545–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Matsushita:2009:PCH

[MW09] Yusuke Matsushita and Toshikazu Wada. Principal component hashing: an accelerated approximate nearest neighbor search. *Lecture Notes in CS*, 5414:374–385, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-92957-4_33`.

Mu:2012:ALS

[MWC12] Yadong Mu, John Wright, and Shih-Fu Chang. Accelerated large scale optimization by concomitant hashing. *Lecture Notes in CS*, 7572:414–427, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-33718-5_30`.

Majewski:1992:FGM

[MWCH92] Bohdan S. Majewski, Nicholas C. Wormald, Zbigniew J. Czech, and George Havas. A family of generators of minimal perfect hash functions. Technical Report 92-16, Center for Discrete Mathematics and Theoretical Computer Science (DIMACS) at Rutgers University, New Jersey, 1992. ?? pp.

Majewski:1996:FPH

[MWHC96] Bohdan S. Majewski, Nicholas C. Wormald, George Havas, and Zbigniew J. Czech. A family of perfect hashing methods. *The Computer Journal*, 39(6):547–554, ???? 1996. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067

(electronic). URL http://www.oup.co.uk/jnls/list/comjnl/hdb/Volume_39/Issue_06/390547.sgm.abs.html; http://www3.oup.co.uk/computer_journal/Volume_39/Issue_06/Vol39_06.body.html#AbstractMajewski. This paper claims the discovery of order-preserving perfect hashing methods that run in linear time.

Ma:2012:HPO

[MXL+12] Yuan Ma, Luning Xia, Jingqiang Lin, Jiwu Jing, Zongbin Liu, and Xingjie Yu. Hardware performance optimization and evaluation of SM3 hash algorithm on FPGA. *Lecture Notes in CS*, 7618:105–118, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34129-8_10/.

Mendelson:1979:PMO

[MY79] H. Mendelson and U. Yechiali. Performance measures for ordered lists in random-access files. *Journal of the Association for Computing Machinery*, 26(4):654–677, October 1979. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Mendelson:1980:NAA

[MY80] Haim Mendelson and Uri Yechiali. A new approach to the analysis of linear probing schemes. *Journal of the Association for Computing Machinery*, 27(3):474–483, July 1980. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Mimaroglu:2012:ADC

[MYS12] Selim Mimaroglu, Murat Yagci, and Dan A. Simovici. Approximative distance computation by random hashing. *The Journal of Supercomputing*, 61(3):572–589, September 2012. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=61&issue=3&spage=572.

Ma:2018:GEG

[MZD+18] Jiacheng Ma, Xiao Zheng, Yaozu Dong, Wentai Li, Zhengwei Qi, Bingsheng He, and Haibing Guan. gMig: Efficient GPU live migration optimized by software dirty page for full virtualization. *SIGPLAN Notices*, 53(3):31–44, March 2018. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Mihaljevic:1998:CAB

[MZI98] Miodrag Mihaljevic, Yuliang Zheng, and Hideki Imai. A cellular automaton based

fast one-way hash function suitable for hardware implementation. *Lecture Notes in CS*, 1431:217–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1431/14310217.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1431/14310217.pdf`.

Metreveli:2012:CCP

[MZK12] Zviad Metreveli, Nickolai Zeldovich, and M. Frans Kaashoek. CPHASH: a cache-partitioned hash table. *SIGPLAN Notices*, 47 (8):319–320, August 2012. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). PPOPP '12 conference proceedings.

Ma:2019:BSB

[MZL+19] W. Ma, Y. Zhu, C. Li, M. Guo, and Y. Bao. BiloKey : a scalable bi-index locality-aware in-memory key–value store. *IEEE Transactions on Parallel and Distributed Systems*, 30(7):1528–1540, July 2019. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Namanya:2020:SHB

[NADY20] Anitta Patience Namanya, Irfan U. Awan, Jules Pagna Disso, and Muhammad Younas. Similarity hash based scoring of portable executable files for efficient malware detection in IoT. *Future Generation Computer Systems*, 110(??): 824–832, September 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X18325913`.

Naeslund:1995:UHF

[Nae95] M. Naeslund. Universal hash functions and hard core bits. In Guillou and Quisquater [GQ95], pages 356–366. ISBN 3-540-59409-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C794 1995. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0921/09210356.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0921/09210356.pdf`.

Nuida:2015:MPS

[NAK+15] Koji Nuida, Takuro Abe, Shizuo Kaji, Toshiaki Maeno, and Yasuhide Numata. A mathematical problem for security analysis of hash functions and pseudorandom generators. *International Journal of Foundations of Computer Science*, 26(2):169–??, February 2015. CODEN IFCSEN. ISSN 0129-0541.

Nakatani:2021:SAB

[Nak21] Y. Nakatani. Structured allocation-based consistent hashing with improved balancing for cloud infrastructure. *IEEE Transactions on Parallel and Distributed Systems*, 32(9):2248–2261, September 2021. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Namba:1986:SIU

[Nam86] K. Namba. Some improvements on Utah standard LISP. *SIGSAM Bulletin (ACM Special Interest Group on Symbolic and Algebraic Manipulation)*, 20(1/2):29–36, February/May 1986. CODEN SIGSBZ. ISSN 0163-5824 (print), 1557-9492 (electronic).

NIST:1992:PYA

[Nat92] National Institute of Standards and Technology (NIST). *Publication YY: Announcement and Specifications for a Secure Hash Standard (SHS)*, January 22 1992. ?? pp.

NIST:1995:FPSb

[Nat95] National Institute of Standards and Technology. *FIPS PUB 180-1: Secure Hash Standard*. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, April 17, 1995. URL `http://www.itl.nist.gov/fipspubs/fip180-1.htm`. Supersedes FIPS PUB 180 1993 May 11.

Navathe:1985:PAI

[Nav85] Sham Navathe, editor. *Proceedings of ACM-SIGMOD 1985 International Conference on Management of Data, May 28–31, 1985, LaMansion Hotel, Austin, Texas*. ACM Press, New York, NY 10036, USA, 1985. ISBN 0-89791-160-1. LCCN QA 76.9 D3 I59 1985.

Nakano:2011:AMI

[NCFK11] Yuto Nakano, Carlos Cid, Kazuhide Fukushima, and Shinsaku Kiyomoto. Analysis of message injection in stream cipher-based hash functions. *Lecture Notes in CS*, 6715:498–513, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-21554-4_29`.

Narayanan:2008:DAQ

[NDMR08] Dushyanth Narayanan, Austin Donnelly, Richard Mortier, and Antony Rowstron. Delay aware querying with Seaweed. *VLDB Journal: Very Large Data Bases*, 17(2):315–331, March 2008. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Neeb:1979:ISO

[Nee79] V. Neeb. Implementierungstechniken fuer satzuebergreifende operationen in relationalen datenbanken. Master's thesis, Technischen Universität Carolo-Wilhelmina zu Braunschweig, Braunschweig, Germany, 1979. ?? pp.

Ng:1979:ESS

[Ng79] Edward W. Ng, editor. *Symbolic and Algebraic Computation: EUROSAM '79, an International Symposium on Symbolic and Algebraic Manipulation, Marseille, France, June 1979*, volume 72 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1979. ISBN 0-387-09519-5. LCCN QA155.7.E4 I57 1979.

Nguyen:2006:MDH

[Ngu06] Quan Son Nguyen. Multidimensional hash chains and application to micropayment schemes. In Ytrehus [Ytr06], pages 218–228. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Nishihara:1974:FTQ

[NH74] S. Nishihara and H. Hagiwara. A full table quadratic search method eliminating secondary clustering. *International Journal of Computer and Information Sciences*, 3(2):123–128, June 1974. CODEN IJCIAH. ISSN 0091-7036.

Nievergelt:1984:GFA

[NHS84] J. Nievergelt, H. Hinterberger, and K. C. Sevcik. The grid file: An adaptable symmetric multikey file structure. *ACM Transactions on Database Systems*, 9(1): 38–71, March 1984. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Nishihara:1983:RRT

[NI83] Seiichi Nishihara and Katsuo Ikeda. Reducing the retrieval time of hashing method by using predictors. *Communications of the Association for Computing Machinery*, 26(12):1082–1088, December 1983. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Nichols:2017:NDH

[Nic17] Shaun Nichols. NiceHash diced up by hackers, thousands of Bitcoin pilfered. Mining outfit says its entire wallet gone, estimated $62m. *The Register*, ??(??):??, December 6, 2017. URL `http://www.bbc.com/news/technology-42275523`; `http://www.bleepingcomputer.com/news/security/largest-cryptocurrency-mining-market-nicehash-`

hacked/; http://www.theregister.co.uk/2017/12/06/nicehash_diced_up_by_hackers_thousands_of_bitcoin_pilfered/; http://www.wsj.com/articles/millions-may-be-missing-in-bitcoin-heist-1512625176.

Niemeyer:1975:DV

[Nie75] Gerhard Niemeyer. *Dateiorganisation und -verarbeitung*. Franz Vahlen, München, Germany, 1975. ISBN 3-8006-0528-7. 258 pp. LCCN QA76 .N52. DM24.80.

Nilli:1994:PHP

[Nil94] A. Nilli. Perfect hashing and probability. *Combinatorics, Probability and Computing*, 3(3):407–409, 1994. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic).

NIST:1993:FPS

[NIS93] NIST. *FIPS PUB 180: Secure Hash Standard (SHS)*. National Institute of Standards and Technology, Gaithersburg, MD, USA, May 11, 1993. ?? pp.

NIST:2015:SSP

[NIS15] NIST. SHA-3 standard: Permutation-based hash and extendable-output functions. FIPS PUB 202, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 2015. viii + 29 pp.

Nielsen:2016:SLF

[NK16] Jesper Puge Nielsen and Sven Karlsson. A scalable lock-free hash table with open addressing. *SIGPLAN Notices*, 51(8):33:1–33:??, August 2016. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Nakayama:1988:HPJ

[NKT88] M. Nakayama, M. Kitsuregawa, and M. Takagi. Hash-partitioned join method using dynamic destaging strategy. In Bancilhon and DeWitt [BD88], page 468. ISBN 0-934613-75-3. LCCN QA76.9.D3 I559 1988.

Nakajima:2002:PAP

[NM02a] Junko Nakajima and Mitsuru Matsui. Performance analysis and parallel implementation of dedicated hash functions. *Lecture Notes in CS*, 2332:165–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320165.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320165.pdf.

Newhall:2002:CPC

[NM02b] Tia Newhall and Lisa Meeden. A comprehensive

project for CS2: combining key data structures and algorithms into an integrated Web browser and search engine. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 34(1):386–390, March 2002. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic). Inroads: paving the way towards excellence in computing education.

Nakaike:2010:LER

[NM10] Takuya Nakaike and Maged M. Michael. Lock elision for read-only critical sections in Java. *SIGPLAN Notices*, 45(6):269–278, June 2010. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Nazir:2022:DIE

[NMQ22] Azra Nazir, Roohie Naaz Mir, and Shaima Qureshi. Deflate-inflate: Exploiting hashing trick for bringing inference to the edge with scalable convolutional neural networks. *Concurrency and Computation: Practice and Experience*, 34(3):e6593:1–e6593:??, February 1, 2022. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Nanevski:2008:YDT

[NMS+08] Aleksandar Nanevski, Greg Morrisett, Avraham Shinnar, Paul Govereau, and Lars Birkedal. Ynot: dependent types for imperative programs. *SIGPLAN Notices*, 43(9):229–240, September 2008. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Ntantogian:2019:EPH

[NMX19] Christoforos Ntantogian, Stefanos Malliaros, and Christos Xenakis. Evaluation of password hashing schemes in open source web platforms. *Computers and Security*, 84 (??):206–224, July 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404818308332`.

Naor:1990:SPS

[NN90] Joseph Naor and Moni Naor. Small-bias probability spaces. efficient constructions and applications. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (May 14–16 1990: Baltimore, MD, USA)*, pages 213–223. ACM Press, New York, NY 10036, USA, 1990. ISBN 0-89791-361-2. LCCN ????

Narita:2012:LJH

[NNA12] Kazuyo Narita, Shinji Nakadai, and Takuya Araki. Landmark-Join: Hash-join based string

similarity joins with edit distance constraints. *Lecture Notes in CS*, 7448: 180–191, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32584-7_15/`.

Noltemeier:1982:I

[Nol82a] Hartmut Noltemeier. *Informatik*. Carl Hanser, München, Germany, 1982. ISBN 3-446-13570-7. ?? pp.

Noltemeier:1982:IIE

[Nol82b] Hartmut Noltemeier. *Informatik III: Einfuehrung in Datenstrukturen*. Carl Hanser, München, Germany, 1982. ISBN 3-446-13570-7. ?? pp.

Negri:1991:DJN

[NP91] M. Negri and G. Pelagatti. Distributive join: a new algorithm for joining relations. *ACM Transactions on Database Systems*, 16 (4):655–669, December 1991. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Nevelsteen:1999:SPU

[NP99] W. Nevelsteen and B. Preneel. Software performance of universal hash functions. *Lecture Notes in CS*, 1592:24–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nguyen:2012:SOU

[NR12] Long Hoang Nguyen and A. W. Roscoe. Short-output universal hash functions and their use in fast and secure data authentication. *Lecture Notes in CS*, 7549:326–345, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-34047-5_19/`.

Newman:1990:PHG

[NRW90] Ilan Newman, Prabhakar Ragde, and Avi Wigderson. Perfect hashing, graph entropy, and circuit complexity. In CTCP '90 [CTC90], pages 91–99. ISBN 0-8186-2072-2 (paper), 0-8186-6072-4 (microfiche), 0-8186-9072-0 (case). LCCN QA267.7 .S75 1990.

Nielsen:1982:ALP

[NS82] Mogens Nielsen and Erik Meineche Schmidt, editors. *Automata, Languages, and Programming: Ninth Colloquium, Aarhus, Denmark, July 12–16, 1982*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1982. ISBN 0-387-11576-5. LCCN QA267.A1 L43 no.140.

Neelima:2016:PHF

[NS16a] Arambam Neelima and Kh Manglem Singh. Perceptual hash function based on scale-invariant feature transform and singular value decomposition. *The Computer Journal*, 59(9):1275–1281, September 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/9/1275.

Nyang:2016:RCC

[NS16b] DaeHun Nyang and DongOh Shin. Recyclable counter with confinement for real-time per-flow measurement. *IEEE/ACM Transactions on Networking*, 24(5):3191–3203, October 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Naito:2006:ICS

[NSS+06] Yusuke Naito, Yu Sasaki, Takeshi Shimoyama, Jun Yajima, Noboru Kunihiro, and Kazuo Ohta. Improved collision search for SHA-0. *Lecture Notes in CS*, 4284:21–36, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11935230_2.pdf.

Naor:2008:HIC

[NSW08] Moni Naor, Gil Segev, and Udi Wieder. History-independent cuckoo hashing. In Aceto et al. [ADG+08], pages 631–642. CODEN LNCSD9. ISBN 3-540-70574-0 (softcover). LCCN ???? URL http://link.springer.com/content/pdf/10.1007/978-3-540-70583-3_51; http://www.wisdom.weizmann.ac.il/~naor/PAPERS/cuckoo_hi_abs.html.

Neven:2009:HFR

[NSW09] Gregory Neven, Nigel P. Smart, and Bogdan Warinschi. Hash function requirements for Schnorr signatures. *Journal of Mathematical Cryptology*, 3(1):69–87, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Naor:2001:APH

[NT01] Moni Naor and Vanessa Teague. Anti-persistence: history independent data structures. In ACM [ACM01], pages 492–501. ISBN 1-58113-349-9. LCCN QA76.6 .A13 2001. URL http://www.wisdom.weizmann.ac.il/%7Enaor/PAPERS/history.ps.gz. ACM order number 508010.

Ntarmos:2009:DHS

[NTW09] N. Ntarmos, P. Triantafillou, and G. Weikum. Distributed

hash sketches: Scalable, efficient, and accurate cardinality estimation for distributed multisets. *ACM Transactions on Computer Systems*, 27(1): 2:1–2:??, February 2009. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Nguyen:2012:LRS

[NTY12] Manh Ha Nguyen, Keisuke Tanaka, and Kenji Yasunaga. Leakage-resilience of stateless/stateful public-key encryption from hash proofs. *Lecture Notes in CS*, 7372: 208–222, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31448-3_16/`.

Naor:2007:NAP

[NW07] Moni Naor and Udi Wieder. Novel architectures for P2P applications: The continuous-discrete approach. *ACM Transactions on Algorithms*, 3(3):34:1–34:??, August 2007. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

Nie:2013:CHB

[NXB13] Xuyun Nie, Zhaohu Xu, and Johannes Buchmann. Cryptanalysis of hash-based tamed transformation and minus signature scheme. *Lecture Notes in CS*, 7932: 155–164, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_10/`.

Norton:1985:PMO

[NY85] R. M. Norton and D. P. Yeager. A probability model for overflow sufficiency in small hash tables. *Communications of the Association for Computing Machinery*, 28(10): 1068–1075, October 1985. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Naor:1989:UOW

[NY89a] M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In ACM-TOC'89 [ACM89c], pages 33–43. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989.

Naor:1989:UOH

[NY89b] Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing. (May 15–17 1989: Seattle, WA, USA)*, pages 33–43. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989.

Nyberg:1996:FAH

[Nyb96] K. Nyberg. Fast accumulated hashing. *Lecture Notes in CS*, 1039:83–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ouksel:1989:CML

[OA89] M. Ouksel and J. AbdulGhaffar. Concurrency in multidimensional linear hashing. In Litwin and Schek [LS89], page ?? ISBN 0-387-51295-0. LCCN QA76.9.D3 F671 1989.

Oaks:1998:BSH

[Oak98] Scott Oaks. The burden of synchronization: Hashtable vs. hashmap. *Java Report: The Source for Java Development*, 3(??):??, August 1998. CODEN JREPFI. ISSN 1086-4660.

Oligeri:2011:REA

[OCDG11] Gabriele Oligeri, Stefano Chessa, Roberto Di Pietro, and Gaetano Giunta. Robust and efficient authentication of video stream broadcasting. *ACM Transactions on Information and System Security*, 14(1):5:1–5:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Anonymous:1989:DQO

[ODB89] *Database Query Optimization: Proceedings of the ODBF Workshop, Beaverton, OR*. Oregon Graduate Center, Portland, OR, USA, 1989. ISBN ?? LCCN ?? Technical Report CS/E 89-005.

Olagunju:1994:DPH

[OG94a] Amos Olagunju and Rashaunda Gourdine. A dynamic perfect hashing algorithm using prime numbers. *Journal of the Elisha Mitchell Scientific Society*, 110(2):68–??, Summer 1994. CODEN JEMSA5. ISSN 0013-6220.

Olagunju:1994:ILS

[OG94b] Amos Olagunju and Rashaunda Gourdine. Innovative least squares algorithms for perfect hashing. *Journal of the Elisha Mitchell Scientific Society*, 110(2):76–??, Summer 1994. CODEN JEMSA5. ISSN 0013-6220.

Ordonez:2014:BVS

[OGAB14] Carlos Ordonez, Carlos Garcia-Alvarado, and Veerabhadaran Baladandayuthapani. Bayesian variable selection in linear regression in one pass for large datasets. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 9(1): 3:1–3:??, August 2014. CODEN ???? ISSN 1556-4681 (print), 1556-472X (electronic).

Oberschelp:1980:IID

[OK80] W. Oberschelp and H. Klocke. Informatik III (datenstrukturen). Technical report, ????, Aachen, Germany, 1980. ?? pp.

Okamoto:1988:DMS

[Oka88] Tatsuaki Okamoto. Digital multisignature scheme using bijective public-key cryptosystems. *ACM Transactions on Computer Systems*, 6(4):432–441, November 1988. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Omiecinski:1989:HBI

[OL89] Edward R. Omiecinski and Eileen Tien Lin. Hash-based and index-based join algorithms for cube and ring connected multicomputers. *IEEE Transactions on Knowledge and Data Engineering*, 1(3):329–343, September 1, 1989. CODEN ITKEEH. ISSN 1041-4347. See also September 1991 TKDE.

Omicinski:1991:AHJ

[OL91] E. Omicinski and E. T. Lin. The adaptive-hash join algorithm for a hypercube multicomputer. Technical report, School of Information and Computer Science, Georgia Institute of Technology, 1991. 30 pp.

Omiecinski:1992:AHJ

[OL92] E. Omiecinski and E. T. Lin. The adaptive-hash join algorithm for a hypercube multicomputer. *IEEE Transactions on Parallel and Distributed Systems*, 3(3):334–349, May 1, 1992. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Ollmert:1989:DD

[Oll89] Hans Joachim Ollmert. *Datenstrukturen und Datenorganisationen*. R. Oldenbourg Verlag, Munich, Germany and Vienna, Austria, 1989. ISBN 3-486-20667-2. ?? pp.

Olsen:1969:RRF

[Ols69] Charles A. Olsen. Random access file organization for indirectly accessed records. In ?? [??69], pages 539–549. LCCN ?? Discusses practical considerations in the design of external scatter tables.

Omiecinski:1988:CSS

[Omi88] Edward Omiecinski. Concurrent storage structure conversion: From B^+ tree to linear hash file. In ICDE'88 [ICD88], pages 589–596. ISBN 0-8186-0827-7 (paperback), 0-8186-8827-0 (hardcover), 0-8186-4827-9 (microfiche). LCCN QA76.9.D3 I5582 1988. IEEE Service Cent. Piscataway, NJ, USA.

Omiecinski:1989:CFC

[Omi89a] Edward Omiecinski. Concurrent file conversion between B^+-tree and linear hash files. *Information system*, 14(5):371–383, 1989. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Omiecinski:1989:HJP

[Omi89b] Edward R. Omiecinski. Heuristics for join processing using nonclustered indexes. *IEEE Transactions on Software Engineering*, 15(1):18–25, January 1989. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=21722`.

Omiecinski:1991:PAL

[Omi91] E. Omiecinski. Performance analysis of a load balancing hash-jpoin algorithm for a shared memory multiprocessor. In Lohman et al. [LSC91], pages 375–385. ISBN 1-55860-150-3. LCCN QA 76.9 D3 I61 1991.

Omar:2012:HEC

[OOB12] Sami Omar, Raouf Ouni, and Saber Bouanani. Hashing with elliptic curve *L*-functions. *Lecture Notes in CS*, 7369:196–207, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31662-3_14/`.

Omar:2017:DHS

[OOB17] Yasser M. K. Omar, Hoda Osama, and Amr Badr. Double hashing sort algorithm. *Computing in Science and Engineering*, 19(2):63–69, March/April 2017. CODEN CSENFA. ISSN 1521-9615 (print), 1558-366X (electronic). URL `https://www.computer.org/csdl/mags/cs/2017/02/mcs2017020063-abs.html`.

Odaira:2010:ERT

[OOK+10] Rei Odaira, Kazunori Ogata, Kiyokuni Kawachiya, Tamiya Onodera, and Toshio Nakatani. Efficient runtime tracking of allocation sites in Java. *SIGPLAN Notices*, 45(7):109–120, July 2010. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Ostlin:2003:UHC

[OP03] Anna Ostlin and Rasmus Pagh. Uniform hashing in constant time and linear space. In ACM [ACM03a], pages 622–628. ISBN ???? LCCN QA75.5 .A22 2003. ACM order number 508030.

Orenstein:1983:DHF

[Ore83] Jack A. Orenstein. A dynamic hash file for random and sequential accessing. In Schkolnick and

Thanos [ST83a], pages 132–141. CODEN VLDBDP.

Olken:1990:RSH

[ORX90] Frank Olken, Doron Rotem, and Ping Xu. Random sampling from hash files. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 19(2): 375–386, June 1990. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Ouksel:1983:SMM

[OS83a] Mohamed Ouksel and Peter Scheuermann. Storage mappings for multidimensional linear dynamic hashing. In Ouksel & Scheuermann [ACM83b], pages 90–105. ISBN 0-89791-097-4. LCCN QA76.9.D3 A15 1983. US$25.00.

Ouskel:1983:SMM

[OS83b] M. Ouskel and P. Scheuermann. Storage mappings for multidimensional linear dynamic hashing. In ACM-PODS'83 [ACM83b], page 90. ISBN 0-89791-097-4. LCCN QA76.9.D3 A15 1983. US$25.00.

Ouksel:1988:IDS

[OS88] Mohamed Ouksel and Peter Scheuermann. Implicit data structures for linear hashing schemes. *Information Processing Letters*, 29(4):183–189, November 1988. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ostafe:2010:PNH

[OS10] Alina Ostafe and Igor E. Shparlinski. Pseudorandom numbers and hash functions from iterations of multivariate polynomials. *Cryptography and Communications*, 2 (1):49–67, April 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-009-0016-0`.

Omar:2014:FHF

[OS14] Sami Omar and Houssem Sabri. Fast hash functions and convolution product. *Journal of Mathematical Cryptology*, 8(2):169–187, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Ou:2010:DIH

[OSR10] Yang Ou, Chul Sur, and Kyung Hyune Rhee. Discriminative image hashing based on region of interest. *Lecture Notes in CS*, 5916:701–706, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-11301-7_72`.

Omiecinski:1989:HBJ

[OT89] Edward Omiecinski and Eileen Tien. A hash-based join algorithm for a cube-connected parallel computer. *Information Processing Letters*, 30(5):269–275, March 13, 1989. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ou:1991:HSU

[OT91] Seng Fat Ou and Alan L. Tharp. High storage utilisation for single-probe retrieval linear hashing. *The Computer Journal*, 34(5):455–468, October 1, 1991. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Otken:1991:HF

[Otk91] John Otken. Hashing functions. *Programmer's Journal*, 9(3):69–??, May 1, 1991. ISSN 0747-5861.

Ogawara:2011:DFP

[OTKH11] Koichi Ogawara, Yasufumi Tanabe, Ryo Kurazume, and Tsutomu Hasegawa. Detecting frequent patterns in video using partly locality sensitive hashing. *Lecture Notes in CS*, 6468:287–296, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-22822-3_29`.

Otoo:1984:MFD

[Oto84] Ekow J. Otoo. A mapping function for the directory of a multidimensional extendible hashing. In Dayal et al. [DSS84], pages 493–506.

Otoo:1985:MDH

[Oto85a] Ekow J. Otoo. A multidimensional digital hashing scheme for files with composite keys. In Navathe [Nav85], pages 214–229. ISBN 0-89791-160-1. LCCN QA 76.9 D3 I59 1985.

Otoo:1985:SDI

[Oto85b] Ekow J. Otoo. Symmetric dynamic index maintenance scheme. In *Proceedings — Foundations of Data Organization.*, pages 283–296. Organizing Committee of the Int Conference on Foundations of Data Organization, Jpn, 1985. Kyoto Sangyo Univ. Computer Science Inst, Kyoto, Jpn.

Otoo:1986:BME

[Oto86] E. J. Otoo. Balanced multidimensional extendible hash tree. In ACM-PODS'86 [ACM86a], pages 100–113. ISBN 0-89791-179-2. LCCN QA76.9.D3 A296 1986. US$24.00.

Otoo:1988:LDG

[Oto88a] Ekow J. Otoo. Linearizing the directory growth in order preserving extendible hashing. In ICDE'88 [ICD88],

pages 580–588. ISBN 0-8186-0827-7. LCCN ???? IEEE Service Cent. Piscataway, NJ, USA.

Otoo:1988:LBC

[Oto88b] Ekow J. Otoo. Locally balanced compact trie hashing. In Beeri et al. [BDS88], page ?? ISBN 0-934613-95-8. LCCN QA76.9.D3 I5541 1988.

Ouksel:1983:OPD

[Ouk83] M. Ouksel. *Order-preserving Dynamic Hashing Schemes for Associative Searching in Database Systems*. PhD thesis, Northwestern University, Evanston, IL, USA, 1983. 212 pp.

Ostrovsky:1994:IHSa

[OVY94a] R. Ostrovsky, R. Venkatesan, and M. Yung. Interactive hashing simplifies zero-knowledge protocol design. *Lecture Notes in CS*, 765:267–273, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ostrovsky:1994:IHSb

[OVY94b] R. Ostrovsky, R. Venkatesan, and M. Yung. Interactive hashing simplifies zero-knowledge protocol design. In Helleseth [Hel94], page ?? ISBN 0-387-57600-2 (New York), 3-540-57600-2 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1993.

ODonnell:2014:OLB

[OWZ14] Ryan O'Donnell, Yi Wu, and Yuan Zhou. Optimal lower bounds for locality-sensitive hashing (except when q is tiny). *ACM Transactions on Computation Theory*, 6(1): 5:1–5:??, March 2014. CODEN ???? ISSN 1942-3454 (print), 1942-3462 (electronic).

Oxborrow:1986:PFB

[Oxb86] E. A. Oxborrow, editor. *Proceedings of the Fifth British National Conference on Databases (BNCOD 5): University of Kent at Canterbury, 14–16 July, 1986*. Cambridge University Press, Cambridge, UK, 1986. ISBN 0-521-33260-5. LCCN QA76.9.D3 B75 1986.

Pouchol:2009:HHS

[PACT09] Mickael Pouchol, Alexandre Ahmad, Benoit Crespin, and Olivier Terraz. A hierarchical hashing scheme for nearest neighbor search and broad-phase collision detection. *Journal of Graphics, GPU, and Game Tools*, 14(2):45–59, ???? 2009. CODEN ???? ISSN 2151-237X. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=2151-237X&volume=14&issue=2&spage=45`.

Pramanik:1993:MDH

[PADHY93] Sakti Pramanik, Anastasia Analyti, Henry Davies, and Chou Hsiao-Yu. Multidirectory hashing. *Information system*, 18(1):63–74, January 1993. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Pagli:1985:SAH

[Pag85] Linda Pagli. Self-adjusting hash tables. *Information Processing Letters*, 21(1): 23–25, July 1985. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Pagh:1999:HDE

[Pag99] R. Pagh. Hash and displace: Efficient evaluation of minimal perfect hash functions. *Lecture Notes in CS*, 1663:49–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pagh:2001:CPC

[Pag01] Rasmus Pagh. On the cell probe complexity of membership and perfect hashing. In ACM [ACM01], pages 425–432. ISBN 1-58113-349-9. LCCN QA76.6 .A13 2001. ACM order number 508010.

Pagh:2006:CHU

[Pag06] Rasmus Pagh. Cuckoo hashing for undergraduates. Report, IT University of Copenhagen, Copenhagen, Denmark, March 27, 2006. URL `http://www.itc.dk/people/pagh/papers/cuckoo-undergrad.pdf`.

Pagh:2018:CLS

[Pag18] Rasmus Pagh. CoveringLSH: Locality-sensitive hashing without false negatives. *ACM Transactions on Algorithms*, 14(3):29:1–29:??, July 2018. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3155300`.

Palem:1993:HEA

[PAKR93] Krishna V. Palem, Yonathan Aumann, Zvi Kedem, and Michael Rabin. Highly efficient asynchronous execution of large-grained parallel programs. In *Proceedings of the 3rd Workshop on Parallel Algorithms (WOPA)*, page ?? ????, ????, May 1993.

Pal:1992:SPD

[Pal92] Srimanta Pal. Search performance of double-linked coalesced hashing can not exceed "bucketing". *Information Sciences*, 65(1 / 2):123–142, November 1, 1992. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

Panigrahy:2005:EHL

[Pan05] Rina Panigrahy. Efficient hashing with lookups in

two memory accesses. In ACM [ACM05], pages 830–839. ISBN 0-89871-585-7. LCCN QA76.6 A184p 2005. URL http://dl.acm.org/citation.cfm?id=1070432.

Papadopoulos:1994:NHA

[Pap94] Constantinos V. Papadopoulos. A new hashing algorithm for parallel processors. *Parallel Algorithms and Applications*, 4(3–4):223–237, November 1994. CODEN PAAPEC. ISSN 1063-7192. URL http://www.informaworld.com/smpp/content~content=a777314733. This is a *plagiarized* article. See http://www.sics.se/europar95/plagiarism.html for details. The original work from which the material in this paper was stolen is due to Thomas J. Sheffler and Randal E. Bryant, CMU report MCU-CS-92-172.

Palma:2008:EPC

[PAPV08] Wenceslao Palma, Reza Akbarinia, Esther Pacitti, and Patrick Valduriez. Efficient processing of continuous join queries using distributed hash tables. *Lecture Notes in CS*, 5168:632–641, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-85451-7_67.

Park:2018:OTP

[Par18] Chang-Seop Park. One-time password based on hash chain without shared secret and re-registration. *Computers and Security*, 75(??): 138–146, June 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818301391.

Paterson:1990:ALP

[Pat90] Michael S. Paterson, editor. *Automata, Languages, and Programming: 17th International Colloquium, Warwick University, England, July 16–20, 1990: Proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. ISBN 0-387-52826-1 (New York), 3-540-52826-1 (Berlin). LCCN QA267.A1 L43 no.443.

Patarin:1994:HFA

[Pat94] J. Patarin. How to find and avoid collisions for the knapsack hash function. In Helleseth [Hel94], pages 305–317. ISBN 0-387-57600-2 (New York), 3-540-57600-2 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1993.

Patarin:1995:CID

[Pat95] J. Patarin. Collisions and inversions for Damgaard's

whole hash function. In Pieprzyk and Safavi-Naini [PSN95], pages 307–321. ISBN 3-540-59339-X. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I555 1994.

Papadimitriou:1980:PBH

[PB80] Christos H. Papadimitriou and Philip A. Bernstein. On the performance of balanced hashing functions when the keys are not equiprobable. *ACM Transactions on Programming Languages and Systems*, 2(1):77–89, January 1980. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic).

Purdom:1985:AA

[PB85] Paul Walton Purdom, Jr. and Cynthia A. Brown. *The Analysis of Algorithms*. Holt, Rinehart, and Winston, New York, NY, USA, 1985. ISBN 0-03-072044-3. xv + 540 pp. LCCN QA76.6 .P86 1985. US$33.95. Chapter 4 discusses random hashing.

Prokopec:2012:CTE

[PBBO12] Aleksandar Prokopec, Nathan Grasso Bronson, Phil Bagwell, and Martin Odersky. Concurrent tries with efficient non-blocking snapshots. *SIGPLAN Notices*, 47(8):151–160, August 2012. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). PPOPP '12 conference proceedings.

Preneel:1997:CHF

[PBD97] Bart Preneel, Antoon Bosselaers, and Hans Dobbertin. The cryptographic hash function RIPEMD-160. *CryptoBytes*, 3(2):9–14, Autumn 1997. URL `ftp://ftp.rsa.com/pub/cryptobytes/crypto3n2.pdf`.

Pepper:1995:RSH

[PBDD95] P. Pepper, R. Betschko, S. Dick, and K. Didrich. Realizing sets by hash tables. *Lecture Notes in CS*, 1009:58–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Preneel:1989:CHB

[PBGV89] Bart Preneel, Antoon Bosselaers, Rene Govaerts, and Joos Vandewalle. Collision-free hashfunctions based on blockcipher algorithms. In *Proceedings 1989 International Carnahan Conference on Security Technology (Oct 3–5 1989: Zurich, Switzerland)*, pages 203–210. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. IEEE catalog number 89CH2774-8.

Park:1995:UPR

[PCK95] U. K. Park, H. K. Choi, and T. G. Kim. Uniform parti-

tioning of relations using histogram equalization framework: An efficient parallel hash-based join. *Information Processing Letters*, 55(5): 283–??, September 15, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Pang:1993:PPHa

[PCL93a] H. Pang, M. Carey, and M. Livny. Partially preemptible hash joins. Technical Report CS TR 1144, University of Wisconsin–Madison, Madison, WI, USA, 1993. ?? pp. PPHJ long version.

Pang:1993:PPHb

[PCL93b] HweeHwa H. Pang, Michael J. Carey, and Miron Livny. Partially preemptible hash joins. In *SIGMOD Record (ACM Special Interest Group on Management of Data)* [BJ93], pages 59–68. CODEN SRECD8. ISBN 0-89791-592-5. ISSN 0163-5808 (print), 1943-5835 (electronic). URL `http://www.acm.org/pubs/articles/proceedings/mod/170035/p59-pang/p59-pang.pdf`; `http://www.acm.org/pubs/citations/proceedings/mod/170035/p59-pang/`.

Park:2015:NSH

[PCM15] Yongjoo Park, Michael Cafarella, and Barzan Mozafari. Neighbor-sensitive hashing. *Proceedings of the VLDB Endowment*, 9(3):144–155, November 2015. CODEN ???? ISSN 2150-8097.

Patel:1994:AMH

[PCV94] Jignesh M. Patel, Michael J. Carey, and Mary K. Vernon. Accurate modeling of the hybrid hash join algorithm. *ACM SIGMETRICS Performance Evaluation Review*, 22(1):56–66, May 1994. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Park:1995:EHB

[PCY95] Jong Soo Park, Ming-Syan Chen, and Philip S. Yu. An effective hash-based algorithm for mining association rules. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 24 (2):175–186, May 1, 1995. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

ACM:1991:PFI

[PDI91] *Proceedings of the First International Conference on Parallel and Distributed Information Systems: December 4–6, 1991, Fontainebleu Hilton Resort, Miami Beach, Florida*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1991. ISBN 0-8186-2295-4 (paperback), 0-8186-2296-2 (microfiche), 0-8186-2297-0

(hardcover). LCCN QA76.58 .I544 1991.

Pearson:1990:FHV

[Pea90] Peter K. Pearson. Fast hashing of variable-length text strings. *Communications of the Association for Computing Machinery*, 33(6):677–680, June 1990. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/78978.html`. See [Dit76, Dit91, Lit91, Pea91, Sav91].

Pearson:1991:NFH

[Pea91] Peter Pearson. Note on fast hashing of variable length text strings. *Communications of the Association for Computing Machinery*, 34 (11):120, November 1991. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Responds to several comments [Dit91, Lit91, Sav91] on the author's earlier paper [Pea90], and early work [Dit76].

Peiler:1982:ZRV

[Pei82] M. Peiler. Zugriffsoperationen auf Rdbm-verwaltungsdaten — 1. Teil. Master's thesis, Technischen Universität Carolo-Wilhelmina zu Braunschweig, Braunschweig, Germany, 1982. ?? pp.

Perry:1973:IME

[Per73] O. R. Perry. Indexing method employing hashing. *IBM Technical Disclosure Bulletin*, 16(3):694–697, August 1973. CODEN IBMTAA. ISSN 0018-8689.

Pescio:1996:AAM

[Pes96] Carlo Pescio. Algorithm alley: Minimal perfect hashing. *Dr. Dobbs Journal*, 21(7): 101–102, 104, 116–117, July 1996. CODEN DDJOEB. ISSN 1044-789X.

Pujol:2012:LEC

[PES+12] Josep M. Pujol, Vijay Erramilli, Georgos Siganos, Xiaoyuan Yang, Nikolaos Laoutaris, Parminder Chhabra, and Pablo Rodriguez. The little engine(s) that could: scaling online social networks. *IEEE/ACM Transactions on Networking*, 20 (4):1162–1175, August 2012. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Peterson:1957:ARA

[Pet57] W. W. Peterson. Addressing for random-access storage. *IBM Journal of Research and Development*, 1(2):130–146, April 1957. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5392733`. First

major paper dealing with the problem of searching in large files. Defined open addressing in general, analyzed the performance of uniform hashing, and the behavior of linear open addressing with various bucket sizes.

Petersen:1983:AVV

[Pet83] D. Petersen. Auswahl eines verfahrens zur verwaltung des sekundaerspeichers der relationalen datenbankmaschine (rdbm). Studienarbeit, 1983.

Petersson:2013:MDL

[Pet13] Niclas Petersson. The maximum displacement for linear probing hashing. *Combinatorics, Probability and Computing*, 22(3):455–476, ???? 2013. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic).

Peyrin:2015:CAG

[Pey15] Thomas Peyrin. Collision attack on `Grindahl`. *Journal of Cryptology*, 28(4):879–898, October 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-014-9186-9`.

Pramanik:1985:DH

[PF85] S. Pramanik and F. Fotouhi. Distributed hashing, March 1985.

Pramanik:1988:OCR

[PF88] Sakti Pramanik and Farshad Fotouhi. Optimizing the cost of relational queries using partial-relation schemes. *Information system*, 13(1):71–79, 1988. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Papadakis:2009:HBO

[PFM+09] Harris Papadakis, Paraskevi Fragopoulou, Evangelos P. Markatos, Marios D. Dikaiakos, and Alexandros Labrinidis. Hash-based overlay partitioning in unstructured peer-to-peer systems. *Parallel Processing Letters*, 19(1): 57–71, March 2009. CODEN PPLTEE. ISSN 0129-6264 (print), 1793-642X (electronic).

Perrizo:1995:DDV

[PG95] W. Perrizo and V. N. R. Goli. Dynamic domain vector perfect hash: a join method for dynamic memory allocations. *Microcomputer Applications*, 14(3):93–??, 1995. CODEN MIAPEZ. ISSN 0820-0750.

Patil:2017:HHA

[PG17] Adarsh Patil and Ramaswamy Govindarajan. HAShCache: Heterogeneity-aware shared DRAMCache for integrated heterogeneous systems. *ACM Transactions on Architecture and Code Optimization*, 14(4):51:1–51:??, December

2017. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic).

Preneel:1990:ATH

[PGV90a] B. Preneel, R. Govaerts, and J. Vandewalle. An attack on two hash functions by Zheng–Matsumoto–Imai. In Seberry and Pieprzyk [SP90], page ?? ISBN 0-387-53000-2 (New York), 3-540-53000-2 (Berlin). LCCN QA76.9.A25 A87 1990.

Preneel:1990:PMD

[PGV90b] B. Preneel, R. Govaerts, and J. Vandewalle. On the power of memory in the design of collision resistant hash functions. In Seberry and Pieprzyk [SP90], page ?? ISBN 0-387-53000-2 (New York), 3-540-53000-2 (Berlin). LCCN QA76.9.A25 A87 1990.

Preneel:1991:CRH

[PGV91] B. Preneel, R. Govaerts, and J. Vandewalle. Collision resistant hash functions based on blockciphers. In Feigenbaum [Fei91], page ?? ISBN 0-387-55188-3 (New York), 3-540-55188-3 (Berlin). LCCN QA76.9.A25 C79 1991.

Preneel:1992:CSH

[PGV92] B. Preneel, R. Govaerts, and J. Vandewalle. Cryptographically secure hash functions: an overview. In *????*, page ?? ????, ????, 1992. Reference in [PS93, p. 186].

Prencel:1993:ATH

[PGV93a] B. Prencel, R. Govaerts, and J. Vandewalle. An attack on two hash functions by Zheng-Matsumoto-Imai. In Seberry and Zheng [SZ93], pages 535–538. ISBN 0-387-57220-1 (New York), 3-540-57220-1 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 A87 1992.

Preneel:1993:ATH

[PGV93b] B. Preneel, R. Govaerts, and J. Vandewalle. An attack on two hash functions by Zheng-Matsumoto-Imai. *Lecture Notes in CS*, 718:535–538, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Preneel:1993:CSI

[PGV93c] B. Preneel, R. Govaerts, and J. Vandewalle, editors. *Computer security and industrial cryptography: state of the art and evolution: ESAT course — May 1991, Leuven, Belgium*, number 741 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-57341-0, 3-540-57341-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C6373 1993.

Preneel:1993:CHF

[PGV93d] B. Preneel, R. Govaerts, and J. Vandewalle. Cryptographic hash functions. In Wolfowicz [Wol93a], pages 161–171.

Preneel:1993:HFB

[PGV93e] B. Preneel, R. Govaerts, and J. Vandewalle. Hash functions based on block ciphers: a synthetic approach. In Stinson [Sti93], pages 368–378. ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). LCCN QA76.9.A25 C79 1993.

Preneel:1993:IAH

[PGV93f] B. Preneel, R. Govaerts, and J. Vandewalle. Information authentication: Hash functions and digital signatures. In *Computer security and industrial cryptography: state of the art and evolution: ESAT course — May 1991, Leuven, Belgium* [PGV93c], pages 87–131. ISBN 0-387-57341-0, 3-540-57341-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C6373 1993.

Preneel:1993:PMD

[PGV93g] B. Preneel, R. Govaerts, and J. Vandewalle. On the power of memory in the design of collision resistant hash functions. In Seberry and Zheng [SZ93], pages 105–121. ISBN 0-387-57220-1 (New York), 3-540-57220-1 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 A87 1992.

Preneel:1994:HFB

[PGV94] Bart Preneel, Rene Govaerts, and Joos Vandewalle. Hash functions based on block ciphers: a synthetic approach. *Lecture Notes in CS*, 773:368–378, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pawson:1973:CHT

[PH73] A. J. D. Pawson and F. R. A. Hopgood. Correspondence: Hashing techniques for table searching. *The Computer Journal*, 16(3):285, August 1973. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_16/Issue_03/tiff/285.tif`. See [HD72].

Paul:2012:NPB

[PHG12] Souradyuti Paul, Ekawat Homsirikamol, and Kris Gaj. A novel permutation-based hash mode of operation FP and the hash function SAMOSA. *Lecture Notes in CS*, 7668:509–527, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.`

springer.com/content/pdf/10.1007/978-3-642-34931-7_29.

Park:2001:VNH

[PHL01] Nan Kyoung Park, Joon Ho Hwang, and Pil Joong Lee. HAS-V: a new hash function with variable output length. *Lecture Notes in CS*, 2012:202–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2012/20120202.htm; http://link.springer-ny.com/link/service/series/0558/papers/2012/20120202.pdf.

Pippenger:1979:ACT

[Pip79] Nicholas Pippenger. On the application of coding theory to hashing. *IBM Journal of Research and Development*, 23(2):225–226, March 1979. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Pippolini:1994:JIH

[Pip94] F. Pippolini. Join indexes and hash algorithms: Two methods for join processing. In Anonymous [Ano94], pages 9–18.

Pittel:1987:PAC

[Pit87] B. Pittel. On probabilistic analysis of a coalesced hashing algorithm. *Annals of Probability*, 15(3): 1180–1202, July 1987. CODEN APBYAE. ISSN 0091-1798 (print), 2168-894X (electronic). URL http://projecteuclid.org/euclid.aop/1176992090.

Piwowarski:1985:CBS

[Piw85] Marek Piwowarski. Comments on batched searching of sequential and tree-structured files. *ACM Transactions on Database Systems*, 10(2):285–287, June 1985. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL http://www.acm.org/pubs/articles/journals/tods/1985-10-2/p285-piwowarski/p285-piwowarski.pdf; http://www.acm.org/pubs/citations/journals/tods/1985-10-2/p285-piwowarski/; http://www.acm.org/pubs/toc/Abstracts/tods/214294.html. See [SG76b, BG82].

Panneerselvam:1990:RSA

[PJBM90] G. Panneerselvam, G. A. Jullien, S. Bandyopadhyay, and W. C. Miller. Reconfigurable systolic architectures for hashing. In *Proceedings — Parbase-90 International Conference on Databases, Parallel Architectures, and Their Applications (Mar 7–9 1990: Miami Beach, FL, USA)*, pages 543–

?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. IEEE catalog number 90CH2728-4.

Panneerselvam:1988:NAS

[PJM88] G. Panneerselvam, G. A. Jullien, and W. C. Miller. New architectures for systolic hashing. In *PROCEEDINGS — INTERNATIONAL CONFERENCE ON SYSTOLIC ARRAYS (May 25–27 1988: San Diego, CA, USA)*, pages 73–82. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. ISBN 0-8186-8860-2. LCCN QA76.5 .I546 1988 Sci-Eng. Available from IEEE Service Cent (catalog number 88CH2603-9). Piscataway, NJ, USA.

Pflug:1987:LPN

[PK87] Georg Ch. Pflug and Hans W. Kessler. Linear probing with a nonuniform address distribution. *Journal of the Association for Computing Machinery*, 34(2):397–410, April 1987. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Plachy:1989:PIC

[PK89] Emily C. Plachy and Peter M. Kogge, editors. *Proceedings of the 1989 International Conference on Parallel Processing, August 8–12, 1989*, volume 2. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. ISBN 0-271-00686-2. LCCN QA76.6 .I548 1989. Three volumes.

Popic:2018:FMB

[PKSB18] Victoria Popic, Volodymyr Kuleshov, Michael Snyder, and Serafim Batzoglou. Fast metagenomic binning via hashing and Bayesian clustering. *Journal of Computational Biology*, 25(7): 677–688, July 2018. CODEN JCOBEM. ISSN 1066-5277 (print), 1557-8666 (electronic). URL `https://www.liebertpub.com/doi/abs/10.1089/cmb.2017.0250`; `https://www.liebertpub.com/doi/pdf/10.1089/cmb.2017.0250`.

Pineda:2009:UOD

[PKW09] Gibran Fuentes Pineda, Hisashi Koga, and Toshinori Watanabe. Unsupervised object discovery from images by mining local features using hashing. *Lecture Notes in CS*, 5856:978–985, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-10268-4_114`.

Periasamy:2021:EHF

[PL21] J. K. Periasamy and B. Latha.

Efficient hash function-based duplication detection algorithm for data deduplication deduction and reduction. *Concurrency and Computation: Practice and Experience*, 33(3):e5213:1–e5213:??, February 10, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Plauger:1998:SCCk

[Pla98] P. J. Plauger. Standard C/C++: Hash tables. *C/C++ Users Journal*, 16 (11):10–??, November 1998. CODEN CCUJEX. ISSN 1075-2838.

Park:2007:SDN

[PLKS07] Kwangkyu Park, JongHyup Lee, Taekyoung Kwon, and Jooseok Song. Secure dynamic network reprogramming using supplementary hash in wireless sensor networks. *Lecture Notes in CS*, 4611:653–662, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-73549-6_64`.

Poblete:1989:LCF

[PM89] Patricio V. Poblete and J. Ian Munro. Last-come-first-served hashing. *Journal of Algorithms*, 10(2):228–248, June 1, 1989. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic).

Petrucci:2020:ISS

[PNPC20] Enrico Petrucci, Laurent Noé, Cinzia Pizzi, and Matteo Comin. Iterative spaced seed hashing: Closing the gap between spaced seed hashing and k-mer hashing. *Journal of Computational Biology*, 27(2):223–233, February 2020. CODEN JCOBEM. ISSN 1066-5277 (print), 1557-8666 (electronic). URL `https://www.liebertpub.com/doi/abs/10.1089/cmb.2019.0298`; `https://www.liebertpub.com/doi/pdf/10.1089/cmb.2019.0298`.

Poblete:1986:AFT

[Pob86] Patricio V. Poblete. Approximating functions by their Poisson transform. *Information Processing Letters*, 23 (3):127–130, October 1986. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ponder:1987:AHA

[Pon87] Carl D. Ponder. Applications of hashing in algebraic manipulation (an annotated bibliography). *SIGSAM Bulletin (ACM Special Interest Group on Symbolic and Algebraic Manipulation)*, 21(4): 10–13, November 1987. CODEN SIGSBZ. ISSN 0163-5824 (print), 1557-9492 (electronic).

Pagh:2008:UHC

[PP08] Anna Pagh and Rasmus Pagh. Uniform hashing in constant time and optimal space. *SIAM Journal on Computing*, 38(1): 85–96, ???? 2008. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Pereira:2016:SHB

[PPB16] Geovandro C. C. F. Pereira, Cassius Puodzius, and Paulo S. L. M. Barreto. Shorter hash-based signatures. *The Journal of Systems and Software*, 116(??):95–100, June 2016. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121215001466`.

Pagh:2007:LPC

[PPR07] Anna Pagh, Rasmus Pagh, and Milan Ruzic. Linear probing with constant independence. In ACM [ACM07], pages 318–327. ISBN 1-59593-631-9. LCCN ????

Pagh:2009:LPC

[PPR09] Anna Pagh, Rasmus Pagh, and Milan Ružić. Linear probing with constant independence. *SIAM Journal on Computing*, 39(3):1107–1120, ???? 2009. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Panwar:2021:FES

[PPS21] Kirtee Panwar, Ravindra Kumar Purwar, and Garima Srivastava. A fast encryption scheme suitable for video surveillance applications using SHA-256 hash function and 1D sine–sine chaotic map. *International Journal of Image and Graphics (IJIG)*, 21(02): ??, April 2021. ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S0219467821500224`.

Pieprzyk:1998:RSF

[PQ98] Josef Pieprzyk and Cheng Xin Qu. Rotation-symmetric functions and fast hashing. *Lecture Notes in CS*, 1438:169–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1438/14380169.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1438/14380169.pdf`.

Pieprzyk:1999:RSF

[PQ99] J. Pieprzyk and Ch. Xin Qu. Rotation-symmetric functions and fast hashing. *J.UCS: Journal of Universal Computer Science*, 5(1):20–31, January 28, 1999. CODEN ???? ISSN 0948-6968. URL `http://www.jucs.`

org/jucs_5_1/rotation_symmetric_functions_and.

Pagh:2001:CH

[PR01] Rasmus Pagh and Flemming Friche Rodler. Cuckoo hashing. *Lecture Notes in CS*, 2161:121–133, 2001. CODEN LNCSD9. ISBN 3-540-42493-8. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2161/21610121.htm; http://link.springer-ny.com/link/service/series/0558/papers/2161/21610121.pdf.

Pagh:2004:CH

[PR04] Rasmus Pagh and Flemming Friche Rodler. Cuckoo hashing. *Journal of Algorithms*, 51(2):122–144, May 2004. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0196677403001925.

Preneel:1993:ADC

[Pre93] B. Preneel. *Analysis and Design of Cryptographic Hash Functions*. Thesis (Ph.D.), Katholieke Universiteit Leuven, Leuven, Belgium, January 1993. 355 pp. URL http://wwwlib.umi.com/dissertations/fullcit/f64276.

Preneel:1994:DPD

[Pre94a] B. Preneel. Design principles for dedicated hash functions. In Anderson [And94], pages 71–82. ISBN 0-387-58108-1, 3-540-58108-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C36 1993.

Preneel:1994:CHF

[Pre94b] Bart Preneel. Cryptographic hash functions. *Eur. Trans. Telecommun. Relat. Technol.*, 5(4):431–448, 1994. CODEN ETTTET. ISSN 1120-3862.

Prenel:1994:CHF

[Pre94c] B. Prenel. Cryptographic hash functions. *Eur. Trans. Telecommun. Relat. Technol.*, 5(4):431–??, July 1, 1994. CODEN ETTTET. ISSN 1120-3862.

Preneel:1997:HFM

[Pre97a] B. Preneel. Hash functions and MAC algorithms based on block ciphers. *Lecture Notes in CS*, 1355:270–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Preneel:1997:MHF

[Pre97b] B. Preneel. MACs and hash functions: State of the art. *Information Security Technical Report*, 2(2):33–43, 1997. CODEN ???? ISSN 1363-4127.

Preneel:1999:SCH

[Pre99] B. Preneel. The state of cryptographic hash functions. *Lecture Notes in CS*, 1561:158–182, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Price:1971:TLT

[Pri71] C. E. Price. Table lookup techniques. *ACM Computing Surveys*, 3(2):49–64, June 1971. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Pritchard:1995:SSQ

[Pri95] Paul Pritchard. A simple sub-quadratic algorithm for computing the subset partial order. *Information Processing Letters*, 56(6):337–341, December 22, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0020019095001654`.

Peyravian:1998:PHV

[PRK98] M. Peyravian, A. Roginsky, and A. Kshemkalyani. On probabilities of hash value matches. *Computers and Security*, 17(2):171–176, March 1998. CODEN CPSEDU. ISSN 0167-4048.

Pontarelli:2016:PDP

[PRM16] S. Pontarelli, P. Reviriego, and J. A. Maestro. Parallel d-pipeline: A cuckoo hashing implementation for increased throughput. *IEEE Transactions on Computers*, 65(1): 326–331, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Provenzano:1989:HTM

[Pro89] Tom Provenzano. A hash table manager in C++. *C Users Journal*, 7(11):83–??, November 1989. ISSN 0898-9788.

Prodinger:1994:ACP

[Pro94] Helmut Prodinger. An asymptotic comment on a paper by A. Analyti and S. Pramanik: "Performance analysis of a main memory multidirectory hashing technique" [Inform. Process. Lett. **45** (1993), no. 4, 191–197; MR 93k:68026]. *Information Processing Letters*, 49(6):327–328, March 22, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Prokopec:2018:CTC

[Pro18] Aleksandar Prokopec. Cachetries: concurrent lock-free hash tries with constant-time operations. *SIGPLAN Notices*, 53(1):137–151, January 2018. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Paiva:2015:ASS

[PRRR15] João Paiva, Pedro Ruivo, Paolo Romano, and Luís Rodrigues. AutoPlacer: Scalable self-tuning data placement in distributed key-value stores. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 9(4):19:1–19:??, January 2015. CODEN ???? ISSN 1556-4665 (print), 1556-4703 (electronic).

Peyravian:1999:HBE

[PRZ99] M. Peyravian, A. Roginsky, and N. Zunic. Hash-based encryption system. *Computers and Security*, 18(4):345–350, 1999. CODEN CPSEDU. ISSN 0167-4048.

Pieprzyk:1993:DHA

[PS93] Josef Pieprzyk and Babak Sadeghiyan. *Design of Hashing Algorithms*, volume 756 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. CODEN LNCSD9. ISBN 3-540-57500-6 (Berlin), 0-387-57500-6 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). xiii + 194 pp. LCCN QA76.9.H36 P53 1993. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0756.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=756`.

Pavlou:2008:FAD

[PS08] Kyriacos E. Pavlou and Richard T. Snodgrass. Forensic analysis of database tampering. *ACM Transactions on Database Systems*, 33(4):30:1–30:??, November 2008. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Porat:2012:CHV

[PS12] E. Porat and B. Shalem. A cuckoo hashing variant with improved memory utilization and insertion time. In Storer and Marcellin [SM12], pages 347–356. ISBN 1-4673-0715-7 (paperback). ISSN 1068-0314. LCCN ???? URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6189266`. IEEE Computer Society order number P4656.

Pieprzyk:1995:ACA

[PSN95] J. Pieprzyk and R. Safavi-Naini, editors. *Advances in cryptology: ASIACRYPT '94: 4th International conference on theory and applications of cryptology — November 1994, Wollongong, Australia*, number 917 in Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. ISBN 3-540-59339-X. ISSN 0302-

9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 I555 1994.

Pramanik:1990:HSK

[PSR90] S. Pramanik, C. Severance, and T. Rosenau. A high speed KDL-RAM file system for parallel computers. In Rishe et al. [RNT90], pages 195–203. ISBN 0-8186-2035-8 (paper), 0-8186-6035-X (microfiche). LCCN QA76.9.D3 P3473 1990. IEEE catalog number 90CH2728-4.

Putze:2009:CHS

[PSS09] Felix Putze, Peter Sanders, and Johannes Singler. Cache-, hash-, and space-efficient Bloom filters. *ACM Journal of Experimental Algorithmics*, 14(1):4:1–4:??, December 2009. CODEN ???? ISSN 1084-6654.

Pahins:2017:HSL

[PSSC17] Cícero A. L. Pahins, Sean A. Stephens, Carlos Scheidegger, and João L. D. Comba. Hashedcubes: Simple, low memory, real-time visual exploration of big data. *IEEE Transactions on Visualization and Computer Graphics*, 23(1):671–680, ???? 2017. CODEN ITVGEA. ISSN 1077-2626 (print), 1941-0506 (electronic), 2160-9306.

Pinkas:2018:SPS

[PSZ18] Benny Pinkas, Thomas Schneider, and Michael Zohner. Scalable private set intersection based on OT extension. *ACM Transactions on Privacy and Security (TOPS)*, 21(2):7:1–7:??, February 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3154794`.

Patrascu:2010:IRL

[PT10a] Mihai Pătraşcu and Mikkel Thorup. On the k-independence required by linear probing and minwise independence. In Abramsky et al. [AGK+10], pages 715–726. CODEN LNCSD9. ISBN 3-642-14164-1 (vol. 1: paperback), 3-642-14161-7 (vol. 2: paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267 .I55 2010. URL `http://www.springerlink.com/content/978-3-642-14164-5/`.

Pong:2010:SSS

[PT10b] Fong Pong and Nian-Feng Tzeng. SUSE: superior storage-efficiency for routing tables through prefix transformation and aggregation. *IEEE/ACM Transactions on Networking*, 18(1): 81–94, February 2010. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Patrascu:2011:PST

[PT11a] Mihai Pătraşcu and Mikkel Thorup. The power of sim-

ple tabulation hashing. In ACM [ACM11], pages 1–10. ISBN ???? LCCN ???? URL `http://www.gbv.de/dms/tib-ub-hannover/63314455x`..

Pong:2011:HRP

[PT11b] Fong Pong and Nian-Feng Tzeng. HaRP: Rapid packet classification via hashing round-down prefixes. *IEEE Transactions on Parallel and Distributed Systems*, 22(7): 1105–1119, July 2011. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Patrascu:2012:PST

[PT12a] Mihai Pătraşcu and Mikkel Thorup. The power of simple tabulation hashing. *Journal of the Association for Computing Machinery*, 59 (3):14:1–14:50, June 2012. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Pong:2012:CLT

[PT12b] Fong Pong and Nian-Feng Tzeng. Concise lookup tables for IPv4 and IPv6 longest prefix matching in scalable routers. *IEEE/ACM Transactions on Networking*, 20 (3):729–741, June 2012. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Patrascu:2013:TTH

[PT13] Mihai Pătraşcu and Mikkel Thorup. Twisted tabulation hashing. In Sanjeev Khanna, editor, *SODA '13: Proceedings of the twenty-fourth annual ACM-SIAM symposium on Discrete Algorithms*, pages 209–228. ACM Press, New York, NY 10036, USA, 2013. ISBN 1-61197-251-5, 1-61197-310-4 (e-book).

Patrascu:2016:IRL

[PT16] Mihai Pătraşcu and Mikkel Thorup. On the k-independence required by linear probing and minwise independence. *ACM Transactions on Algorithms*, 12 (1):8:1–8:??, February 2016. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

Papamanthou:2016:AHT

[PTT16] Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Authenticated hash tables based on cryptographic accumulators. *Algorithmica*, 74(2): 664–712, February 2016. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL `http://link.springer.com/article/10.1007/s00453-014-9968-3`.

Pirotte:1985:VLD

[PV85] A. Pirotte and Y. Vassiliou, editors. *Very Large Data*

Bases: Stockholm, 1985/ 11th International Conference on Very Large Data Bases, Stockholm, August 21–23, 1985. Morgan Kaufmann Publishers, San Francisco, CA, 1985. ISBN 0-934613-17-6. LCCN QA 76.9 D3 I61 1985.

Panti:1992:MOH

[PV92] Maurizio Panti and Salvatore Valenti. A modulus oriented hash function for the construction of minimal perfect tables. *SIGPLAN Notices*, 27(11):33–38, November 1992. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Preneel:1995:MBF

[PV95] B. Preneel and P. C. Van Oorschot. MDx-MAC and building fast MACs from hash functions. In Coppersmith [Cop95a], pages 1–14. ISBN 3-540-60221-6. LCCN QA76.9.A25 C79 1995.

Pasini:2007:HSW

[PV07] Sylvain Pasini and Serge Vaudenay. Hash-and-sign with weak hashing made secure. *Lecture Notes in CS*, 4586:338–354, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-73458-1_25`.

Poblete:2019:ARH

[PV19] P. V. Poblete and A. Viola. Analysis of Robin Hood and other hashing algorithms under the random probing model, with and without deletions. *Combinatorics, Probability and Computing*, 28(4):600–617, July 2019. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic). URL `https://www.cambridge.org/core/journals/combinatorics-probability-and-computing/article/analysis-of-robin-hood-and-other-hashing-algorithms-under-the-random-probing-model-with-and-without-deletions/933D4F203E3C70EF1505328741`

Petit:2008:EPR

[PVCQ08] C. Petit, N. Veyrat-Charvillon, and J.-J. Quisquater. Efficiency and pseudo-randomness of a variant of Zémor–Tillich hash function. In *15th IEEE International Conference on Electronics, Circuits and Systems, 2008 (ICECS 2008)*, pages 906–909. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, August 2008.

Poblete:1994:AHS

[PVM94] P. V. Poblete, A. Viola, and J. I. Munro. The analysis of a hashing scheme by the diagonal Poisson transform. *Lecture Notes in CS*, 855:94–??, 1994. CO-

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Poblete:1997:ALL

[PVM97] Patricio V. Poblete, Alfredo Viola, and J. Ian Munro. Analyzing the LCFS linear probing hashing algorithm with the help of Maple. *Maple Technical Newsletter*, 4(1):8–13, Winter 1997. ISSN 1061-5733.

Preneel:1995:MMB

[PvO95] B. Preneel and P. C. van Oorschot. MD-x MAC and building fast MACs from hash functions. In Coppersmith [Cop95b], pages 1–14. CODEN LNCSD9. ISBN 3-540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1995. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0963.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=963`. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy.

Piper:1993:DSH

[PW93] F. Piper and P. Wild. Digital signatures and hash functions. In Anonymous [Ano93a], pages 124–130. ISBN 1-85617-211-2. LCCN ????

Prasanna:1994:SDP

[PW94] V. K. Prasanna and C.-L. Wang. Scalable data parallel object recognition using geometric hashing on the CM-5. In IEEE [IEE94c], pages 817–824. ISBN 0-8186-5680-8, 0-8186-5681-6. LCCN QA76.58.S32 1994.

Phan:2006:SCI

[PW06] Raphael C.-W. Phan and David Wagner. Security considerations for incremental hash functions based on pair block chaining. *Computers and Security*, 25(2): 131–136, March 2006. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404805002063`.

Peikert:2008:LTF

[PW08] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In ACM [ACM08b], pages 187–196. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Pan:2013:CHF

[PWY+13] Ping Pan, Licheng Wang, Yixian Yang, Yuanju Gan, Lihua Wang, and Chengqian Xu. Chameleon hash functions and one-time signature schemes from inner au-

tomorphism groups. *Fundamenta Informaticae*, 126(1): 103–119, January 2013. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Pagh:2010:COH

[PWYZ10] Rasmus Pagh, Zhewei Wei, Ke Yi, and Qin Zhang. Cache-oblivious hashing. In Van Gucht [Van10], pages 297–304. ISBN 1-4503-0033-2. LCCN ????

Pagh:2014:COH

[PWYZ14] Rasmus Pagh, Zhewei Wei, Ke Yi, and Qin Zhang. Cache-oblivious hashing. *Algorithmica*, 69(4):864–883, August 2014. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL `http://link.springer.com/article/10.1007/s00453-013-9763-6`.

Pittel:1988:STE

[PY88] Boris Pittel and Jenn-Hwa Yu. On search times for early-insertion coalesced hashing. *SIAM Journal on Computing*, 17(3):492–503, June 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Quittner:1981:CSH

[QCH+81] P. Quittner, S. Csoka, S. Halasz, D. Kotsis, and K. Varnai. Comparison of synonym handling and bucket organization methods. *Communications of the Association for Computing Machinery*, 24(9):579–582, September 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Quinlan:2002:VNA

[QD02] Sean Quinlan and Sean Dorward. Venti: a new approach to archival storage. Technical report, Computing Sciences Research Center, Bell Laboratories, Murray Hill, NJ, USA, May 2, 2002. 13 pp. URL `http://plan9.bell-labs.com/sys/doc/venti/venti.pdf`.

Quisquater:1989:BHF

[QG89] J. J. Quisquater and M. Girault. $2n$-bit hash-functions using n-bit symmetric block cipher algorithms. In Quisquater and Vandewalle [QV89], page ?? ISBN 0-387-53433-4 (New York), 3-540-53433-4 (Berlin). LCCN QA76.9.A25 E964 1989. DM98.00.

Quisquater:1990:BHF

[QG90] Jean-Jacques Quisquater and Marc Girault. $2n$-bit hash-functions using n-bit symmetric block cipher algorithms. *Lecture Notes in CS*, 434:102–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.`

com/link/service/series/0558/bibs/0434/04340102.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340102.pdf.

Quisquater:1995:ACE

[QG95] J.-J. Quisquater and Louis C. Guillou, editors. *Advances in cryptology, EUROCRYPT '95: International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21–25, 1995: proceedings*, volume 921 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. CODEN LNCSD9. ISBN 3-540-59409-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C794 1995.

Quisquater:1997:ASS

[QJ97] Jean-Jacques Quisquater and Marc Joye. Authentication of sequences with the SL_2 hash function: application to video sequences. *Journal of Computer Security*, 5(3):213–223, ???? 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Qi:1998:DAH

[QM98] Hongbin Qi and Charles U. Martel. Design and analysis of hashing algorithms with cache effects. Report, Department of Computer Science, University of California, Davis, Davis, CA, USA, 1998. URL http://theory.cs.ucdavis.edu/.

Qu:2016:CHT

[QP16] Yun R. Qu and Viktor K. Prasanna. Compact hash tables for decision-trees. *Parallel Computing*, 54(??):121–127, May 2016. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic). URL http://www.sciencedirect.com/science/article/pii/S016781911500157X.

Quittner:1983:ECI

[Qui83] Páe Quittner. Efficient combination of index tables and hashing. *Software—Practice and Experience*, 13(6):471–478, June 1983. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Quisquater:1989:ACE

[QV89] Jean-Jacques Quisquater and Joos Vandewalle, editors. *Advances in Cryptology–EUROCRYPT '89: Workshop on the Theory and Application of Cryptographic Techniques, Houthalen, Belgium, April 10–13, 1989: Proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1989. ISBN 0-387-53433-4 (New York), 3-

540-53433-4 (Berlin). LCCN QA76.9.A25 E964 1989. DM98.00.

Quisquater:1990:ACE

[QV90] Jean-Jacques Quisquater and Joos Vandewalle, editors. *Advances in cryptology — EUROCRYPT '89: Workshop on the Theory and Application of Cryptographic Techniques, Houthalen, Belgium, April 10–13, 1989: proceedings*, volume 434 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. CODEN LNCSD9. ISBN 0-387-53433-4 (New York), 3-540-53433-4 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1989; QA267.A1 L43 no.434. DM98.00. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0434.htm`; `http://www.springerlink.com/content/978-0-387-53433-6`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=434`.

Qiu:2020:FKF

[QXL+20] Y. Qiu, J. Xie, H. Lv, W. Yin, W. Luk, L. Wang, B. Yu, H. Chen, X. Ge, Z. Liao, and X. Shi. FULL–KV: Flexible and ultra-low-latency in-memory key–value store system design on CPU-FPGA. *IEEE Transactions on Parallel and Distributed Systems*, 31(8): 1828–1444, 2020. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Qi:2018:TSL

[QZD+18] Lianyong Qi, Xuyun Zhang, Wanchun Dou, Chunhua Hu, Chi Yang, and Jinjun Chen. A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment. *Future Generation Computer Systems*, 88(??): 636–643, November 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X18301420`.

Radke:1970:UQR

[Rad70] C. E. Radke. The use of quadratic residue research. *Communications of the Association for Computing Machinery*, 13(2):103–150, February 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Radue:1983:DIS

[Rad83] Jon Radue. On the design of an interactive spelling dictionary for personal computers. *SIGPC Notes (ACM Special Interest Group on Per-*

sonal Computing), 6(2):197–199, 1983. CODEN SPCNDH. ISBN 0-89791-123-7. ACM (Order n 609830). Baltimore, MD, USA.

Radhakrishnan:1992:IBC

[Rad92] Jaikumar Radhakrishnan. Improved bounds for covering complete uniform hypergraphs. *Information Processing Letters*, 41(4):203–207, March 18, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Richter:2015:SDA

[RAD15] Stefan Richter, Victor Alvarez, and Jens Dittrich. A seven-dimensional analysis of hashing methods and its implications on query processing. *Proceedings of the VLDB Endowment*, 9(3):96–107, November 2015. CODEN ???? ISSN 2150-8097.

Ragde:1993:PSC

[Rag93] P. Ragde. The parallel simplicity of compaction and chaining. *Journal of Algorithms*, 14(3):371–380, May 1993. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0196677483710199`.

Roman:2007:SCP

[RAL07] Rodrigo Roman, Cristina Alcaraz, and Javier Lopez. A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes. *Mobile Networks and Applications*, 12(4):231–244, August 2007. CODEN ???? ISSN 1383-469X.

Ramakrishna:1987:CPH

[Ram87] M. V. Ramakrishna. Computing the probability of hash table/urn overflow. *Communications in Statistics: Theory and Methods*, 16(11):3343–3353, 1987. CODEN CSTMDC. ISSN 0361-0926 (print), 1532-415X (electronic).

Ramakrishna:1988:EPM

[Ram88a] M. V. Ramakrishna. An exact probability model for finite hash tables. In ICDE'88 [ICD88], pages 362–368. ISBN 0-8186-0827-7. LCCN ???? IEEE Service Cent. Piscataway, NJ, USA.

Ramakrishna:1988:HPA

[Ram88b] M. V. Ramakrishna. Hashing in practice: Analysis of hashing and universal hashing. In Boral and Larson [BL88], pages 191–199. ISBN 0-89791-268-3. LCCN QA 76.9 D3 S53 v.17 no.3 1988. US$33.00.

Ramakrishna:1989:ARP

[Ram89a] M. V. Ramakrishna. Analysis of random probing hashing. *Information Pro-*

cessing Letters, 31(2):83–90, April 26, 1989. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ramakrishna:1989:PPB

[Ram89b] M. V. Ramakrishna. Practical performance of Bloom filters and parallel free-text searching. *Communications of the Association for Computing Machinery*, 32(10): 1237–1239, October 1989. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). *Computing Reviews*: "This short communication deals with a special kind of hash function called 'Bloom filters.' These filters are used, for example, to search a differential file containing updates to a main file.".

Ramakrishna:1992:SPH

[Ram92] M. V. Ramakrishna. A simple perfect hashing method for static sets. In Koczkodaj et al. [KLT92], pages 401–404. ISBN 0-8186-2812-X (hardcover), 0-8186-2811-1 (microfiche). LCCN QA75.5 .I587 1992.

Raman:1997:KFM

[Ram97] Anand V. Raman. The Katapayadi formula and the modern hashing technique. *IEEE Annals of the History of Computing*, 19(4):49–52, 1997. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic).

Ramakrishna:1991:DPH

[RB91] M. V. Ramakrishna and Y. Bannai. Direct perfect hashing functions for external files. *J. Database Adm.*, 2(1):19–29, 1991. CODEN JDADEX. ISSN 1047-9430.

Rijmen:2001:WHF

[RB01] Vincent Rijmen and Paulo S. L. M. Barreto. The WHIRLPOOL hash function. World-Wide Web document, 2001. URL `http://paginas.terra.com.br/informatica/paulobarreto/WhirlpoolPage.html`; `http://planeta.terra.com.br/informatica/paulobarreto/whirlpool.zip`.

Rigoutsos:1994:SPS

[RC94] Isidore Rigoutsos and Andrea Califano. Searching in parallel for similar strings. *IEEE Computational Science & Engineering*, 1(2):60–75, Summer 1994. CODEN ISCEE4. ISSN 1070-9924 (print), 1558-190X (electronic).

Rao:2011:STE

[RCF11] Weixiong Rao, Lei Chen, and Ada Wai-Chee Fu. STAIRS: Towards efficient full-text filtering and dissemination in DHT environments. *VLDB Journal: Very Large Data Bases*, 20(6):793–817, December 2011. CODEN

VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Regnier:1981:AHT

[Reg81] Mireille Regnier. On the average height of trees in digital search and dynamic hashing. *Information Processing Letters*, 13(2):64–66, November 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Regnier:1982:LHG

[Reg82] Mireille Regnier. Linear hashing with groups of reorganization: an algorithm for files without history. In Scheuermann [Sch82a], pages 257–272. ISBN 0-12-624080-9. LCCN QA76.9.D3 .I558 1982. US$34.00.

Regnier:1985:AGF

[Reg85] Mireille Regnier. Analysis of grid file algorithms. *BIT (Nordisk tidskrift for informationsbehandling)*, 25 (2):335–357, 1985. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Regnier:1988:THA

[Reg88] Mireille Regnier. Trie hashing analysis. In ICDE'88 [ICD88], pages 377–381. ISBN 0-8186-0827-7 (paperback), 0-8186-8827-0 (hardcover), 0-8186-4827-9 (microfiche). LCCN QA76.9.D3 I5582 1988. IEEE Service Cent. Piscataway, NJ, USA.

Reif:1988:AWC

[Rei88] John H. Reif, editor. *Aegean Workshop on Computing (3rd: 1988: Kerkyra, Corfu Island, Greece) VLSI algorithms and architectures: 3rd Aegean Workshop on Computing, AWOC 88, Corfu, Greece, June 28-July 1, 1988: proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. ISBN 0-387-96818-0. LCCN TK7874 .A338 1988. Lecture notes in computer science # 319.

Reid:2003:SSE

[Rei03] Jason Reid. *Secure Shell in the Enterprise*. Sun blueprints. Sun Microsystems Press, Palo Alto, CA, USA, 2003. ISBN 0-13-142900-0 (paperback). xxiii + 198 pp. LCCN QA76.76.O63 R448 2003. US$39.00.

Remy:1992:ERE

[Rém92] Didier Rémy. Efficient represent of extensible records. In Anonymous ??? [Ano92], pages 12–16.

Reyes:2014:FKM

[Rey14] Kristofer Reyes. Fast kinetic Monte Carlo simulations using hash table based caching with applications to nanowire growth and sintering. *Multiscale Modeling & Simulation*,

12(1):200–224, ???? 2014. CODEN MMSUBT. ISSN 1540-3459 (print), 1540-3467 (electronic).

Ramakrishna:1997:EHH

[RFB97] M. V. Ramakrishna, E. Fu, and E. Bahcekapili. Efficient hardware hashing functions for high performance computers. *IEEE Transactions on Computers*, 46(12): 1378–1381, December 1997. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=641938`.

Richter:1989:HJA

[RG89] Karol Richter and Dan Grigoras. Hash-join algorithms for SIMD-MIMD computer architecture. *Computers and Artificial Intelligence = Vychislitel'nye mashiny i iskusstvennyi intellekt*, 8(4): 369–384, 1989. CODEN CARIDY. ISSN 0232-0274.

Ramirez-Gutierrez:2012:IRT

[RGNMPM12] Kelsey A. Ramirez-Gutierrez, Mariko Nakano-Miyatake, and Hector M. Perez-Meana. Improvement of Radon transform-based perceptual hashing using image normalization. *International Journal of Computer Applications*, 34(4): 249–259, 2012. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.2316/Journal.202.2012.4.202-3530`.

Raghavan:1990:RIM

[RH90] R. Raghavan and J. P. Hayes. On randomly interleaved memories. In IEEE [IEE90], pages 49–58. ISBN 0-8186-2056-0 (paperback: IEEE Computer Society), 0-89791-412-0 (paperback: ACM). LCCN QA 76.88 S87 1990. ACM order number 415903. IEEE Computer Society Press order number 2056. IEEE catalog number 90CH2916-5.

Rigoutsos:1992:MPM

[RH92] Isidore Rigoutsos and Robert Hummel. Massively parallel model matching: Geometric hashing on the Connection Machine. *Computer*, 25(2): 33–42, February 1992. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Rigoutsos:1995:BAM

[RH95] Isidore Rigoutsos and Robert Hummel. A Bayesian approach to model matching with geometric hashing. *Computer vision and image understanding: CVIU*, 62(1): 11–26, July 1995. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic).

Risson:2009:TDR

[RHM09] John Risson, Aaron Harwood, and Tim Moors.

Topology dissemination for reliable one-hop distributed hash tables. *IEEE Transactions on Parallel and Distributed Systems*, 20(5):680–694, May 2009. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Riehl:1989:CTS

[Rie89] Arthur M. Riehl, editor. *Computing Trends in the 1990's: Seventeenth annual ACM Computer Science Conference, February 21–23, 1989, Commonwealth Convention Center, Louisville, KY*. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-299-3. LCCN QA75.5 .A1371 1989. US$36.00.

Rivest:1974:HCA

[Riv74a] R. L. Rivest. On hash-coding algorithms for partial-match retrieval. In IEEE [IEE74], pages 95–103.

Rivest:1974:AAR

[Riv74b] Ronald L. Rivest. Analysis of associative retrieval algorithms. Technical Report TR.54, Institut de la Recherche en Informatique et Automatique, now Institut National de Recherche en Informatique et Automatique (INRIA), Domaine de Voluceau — Rocquencourt — B.P. 105, 78153 Le Chesnay Cedex, France, February 1974. ?? pp. Also published in/as: Stanford CSD report 74-415. Also published in/as: SIAM Journal for Computing, Springer-Verlag (Heidelberg, FRG and New York NY, USA)-Verlag, 1976, with mod. title.

Rivest:1976:OAK

[Riv76] Ronald L. Rivest. Optimal arrangement of keys in a hash table. Technical Report MIT/LCS/TM-73, Massachusetts Institute of Technology, Computer Science Lab., Cambridge, Massachusetts, July 1976. ?? pp.

Rivest:1978:OAK

[Riv78] Ronald L. Rivest. Optimal arrangement of keys in a hash table. *Journal of the Association for Computing Machinery*, 25(2):200–209, April 1978. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). See [Yao85a].

Rjasko:2012:BBP

[Rja12] Michal Rjaško. Black-box property of cryptographic hash functions. *Lecture Notes in CS*, 6888: 181–193, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-27901-0_14/`.

Reuhkala:1979:RHA

[RJK79] Erkki Reuhkala, Matti Jalanko, and Teuvo Kohonen. Redundant hash addressing method adapted for the postprocessing and error-correction of computer-recognized speech. *Record — IEEE International Conference on Acoustics, Speech & Signal Processing*, ??(??):591–594, ???? 1979. CODEN RIIPDR.

Ris:1989:PIC

[RK89] Fred Ris and Peter M. Kogge, editors. *Proceedings of the 1989 International Conference on Parallel Processing, August 8–12, 1989*, volume 3. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. ISBN 0-271-00686-2. LCCN QA76.6 .I548 1989 v.1-3. Three volumes.

Roy:1991:LBH

[RK91] S. Roy and A. Keller. Load balancing in hash-based parallel join computation in presence of data skew. Technical report, ????, 1991. ?? pp. Submitted to DE91.

Rottenstreich:2015:BPW

[RK15] Ori Rottenstreich and Isaac Keslassy. The Bloom paradox: when not to use a Bloom filter. *IEEE/ACM Transactions on Networking*, 23(3):703–716, June 2015. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Rottenstreich:2014:VIC

[RKK14] Ori Rottenstreich, Yossi Kanizo, and Isaac Keslassy. The variable-increment counting Bloom filter. *IEEE/ACM Transactions on Networking*, 22(4):1092–1105, August 2014. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Ragan-Kelley:2011:DSG

[RKLC+11] Jonathan Ragan-Kelley, Jaakko Lehtinen, Jiawen Chen, Michael Doggett, and Frédo Durand. Decoupled sampling for graphics pipelines. *ACM Transactions on Graphics*, 30(3):17:1–17:??, May 2011. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Rothnie:1974:ABF

[RL74] James B. Rothnie, Jr. and Tomas Lozano. Attribute based file organization in a paged memory environment. *Communications of the Association for Computing Machinery*, 17(2):63–69, February 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See remarks [Cha84a].

Ramamohanarao:1982:DHS

[RL82] K. Ramamohanarao and John W. Lloyd. Dynamic hashing schemes. *The Computer Journal*, 25(4):479–485, November 1982. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Ramakrishna:1989:FOU

[RL89] M. V. Ramakrishna and Per-Åke Larson. File organization using composite perfect hashing. *ACM Transactions on Database Systems*, 14(2): 231–263, June 1, 1989. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Rathi:1990:PCE

[RLH90] A. Rathi, H. Lu, and G. E. Hedrick. Performance comparison of extendible hashing and linear hashing techniques. In Hal Berghel, E. A. (Elizabeth A.) Unger, and Richard Rankin, editors, *Proceedings of the ACM SIGSMALL/PC Symposium on Small Systems, Arlington, VA, March 28–30, 1990*, pages 178–185. ACM Press, 1990. ISBN 0-89791-347-7. LCCN QA76.5 .A155 1990. URL `http://portal.acm.org/toc.cfm?id=99412`.

Rathi:1991:PCE

[RLH91] Ashok Rathi, Huizu Lu, and G. E. Hedrick. Performance comparison of extendible hashing an linear hashing techniques. *SIGSMALLslash PC Notes*, 17(2): 19–??, Summer 1991. CODEN SGBLEC. ISSN 0893-2875.

Richardson:1987:DEP

[RLM87] James P. Richardson, Hongjun Lu, and Krishna Mikkilineni. Design and evaluation of parallel pipelined join algorithms. In Dayal and Traiger [DT87], pages 399–409. ISBN 0-89791-236-5. LCCN QA 76.9 D3 P76 1987. URL `http://www.acm.org/pubs/articles/proceedings/mod/38713/p399-richardson/p399-richardson.pdf`; `http://www.acm.org/pubs/citations/proceedings/mod/38713/p399-richardson/`. ACM order number 472870.

Ramamohanarao:1983:PMR

[RLT83] K. Ramamohanarao, John W. Lloyd, and James A. Thom. Partial-match retrieval using hashing and descriptors. *ACM Transactions on Database Systems*, 8(4):552–576, December 1983. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1983-8-4/p552-ramamohanarao/p552-ramamohanarao.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1983-8-4/p552-ramamohanarao/`.

Ramakrishna:1988:ABD

[RM88] M. V. Ramakrishna and P. Mukhopadhyay. Analysis of bounded disorder file organization. In ACM [ACM88a], pages 117–125. ISBN 0-89791-263-2. LCCN QA76.9.D3 A15 1988. URL `http://www.acm.org/pubs/articles/proceedings/pods/308386/p117-ramakrishna/p117-ramakrishna.pdf`; `http://www.acm.org/pubs/citations/proceedings/pods/308386/p117-ramakrishna/`.

Rosas:2011:CBC

[RMB11] Erika Rosas, Olivier Marin, and Xavier Bonnaire. Corps: Building a community of reputable peers in distributed hash tables. *The Computer Journal*, 54(10):1721–1735, October 2011. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/54/10/1721.full.pdf+html`.

Robey:2013:HBA

[RNR13] Rachel N. Robey, David Nicholaeff, and Robert W. Robey. Hash-based algorithms for discretized data. *SIAM Journal on Scientific Computing*, 35(4):C346–C368, ???? 2013. CODEN SJOCE3. ISSN 1064-8275 (print), 1095-7197 (electronic).

Rishe:1990:PIC

[RNT90] Naphtali Rishe, Sham Navathe, and Doron Tal, editors. *PARBASE-90, International Conference on Databases, Parallel Architectures, and Their Applications: March 7–9, 1990, Miami Beach, Florida*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. ISBN 0-8186-2035-8 (paper), 0-8186-6035-X (microfiche). LCCN QA76.9.D3 P3473 1990.

Robinson:1986:OPL

[Rob86] T. J. Robinson. Order preserving linear hashing using dynamic key statistics. In ACM-PODS'86 [ACM86a], pages 91–99. ISBN 0-89791-179-2. LCCN QA76.9.D3 A296 1986. US$24.00.

Roe:1994:PSC

[Roe94] M. Roe. Performance of symmetric ciphers and one-way hash functions. In Anderson [And94], pages 83–89. ISBN 0-387-58108-1, 3-540-58108-1. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C36 1993.

Roe:1995:PBC

[Roe95] M. Roe. Performance of block ciphers and hash functions — one year later. *Lecture Notes in CS*, 1008: 359–??, 1995. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rogaway:1995:BHA

[Rog95] P. Rogaway. Bucket hashing and its application to fast message authentication. *Lecture Notes in CS*, 963:29–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rogaway:1999:BHA

[Rog99] Phillip Rogaway. Bucket hashing and its application to fast message authentication. *Journal of Cryptology*, 12(2):91–115, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/bibs/12n2p91.html`; `http://link.springer.de/link/service/journals/00145/papers/12n2p91.pdf`; `http://link.springer.de/link/service/journals/00145/papers/12n2p91.tex`.

Rogers:2019:AFH

[Rog19a] J. Andrew Rogers. AquaHash: Fast hashing with AES intrinsics. Web site., March 6, 2019. URL `https://www.jandrewrogers.com/2019/03/06/aquahash/`.

Rogers:2019:FPH

[Rog19b] J. Andrew Rogers. Fast perfect hashing of integral types. Web site., March 6, 2019. URL `https://www.jandrewrogers.com/2019/02/12/fast-perfect-hashing/`.

Ronnblom:2007:HEA

[Rön07] Johan Rönnblom. High-error approximate dictionary search using estimate hash comparisons. *Software—Practice and Experience*, 37(10):1047–1059, August 2007. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Rosenfeld:1974:IPP

[Ros74] Jack L. Rosenfeld, editor. *Information processing, 1974; Proceedings of IFIP Congress 74, Stockholm, Sweden, August 5–10, 1974*. North-Holland, Amsterdam, The Netherlands, 1974. ISBN 0-444-10689-8. LCCN QA 76 I615.

Rosenberg:1977:SRA

[Ros77] A. L. Rosenberg. On storing ragged arrays by hashing. *Mathematical Systems Theory*, 10(??):??, 1977. CODEN MASTBA. ISSN 0025-5661.

Ross:2006:EHP

[Ros06] Kenneth A. Ross. Efficient hash probes on modern processors. Research Report

RC24100 (W0611-039), IBM Corporation, Almaden, CA, USA, November 8, 2006. 12 pp.

Ross:2007:EHP

[Ros07] Kenneth A. Ross. Efficient hash probes on modern processors. In IEEE, editor, *Proceedings of the 2007 IEEE 23rd International Conference on Data Engineering, Istanbul, Turkey, 11–15 April 2007*, pages 1297–1301. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2007. ISBN 1-4244-0802-4. LCCN QA76.9.D3 I5564 2007. URL `http://doi.ieeecomputersociety.org/10.1109/ICDE.2007.368997`. IEEE catalog number 07EX1614.

Rosenfeld:2012:OCC

[Ros12] Meni Rosenfeld. Overview of colored coins. Web document., 2012. URL `https://bitcoil.co.il/BitcoinX.pdf`; `https://web.archive.org/web/20170922052930/https://bitcoil.co.il/BitcoinX.pdf`.

Ross:2021:TPS

[Ros21] Kenneth A. Ross. Technical perspective: Scaling dynamic hash tables on real persistent memory. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 50(1):86, June 2021. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic). URL `https://dl.acm.org/doi/10.1145/3471485.3471505`.

Rotem:1989:CMH

[Rot89] Doron Rotem. Clustered multiattribute hash files. In ACM-PODS'89 [ACM89b], pages 225–234. ISBN 0-89791-308-6. LCCN QA 76.9 D3 A26 1989.

Roussev:2009:HDF

[Rou09] Vassil Roussev. Hashing and data fingerprinting in digital forensics. *IEEE Security & Privacy*, 7(2):49–55, March/April 2009. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Rovan:1990:MFC

[Rov90] B. Rovan, editor. *Mathematical Foundations of Computer Science, 1990: Banska Bystrica, Czechoslovakia, August 27–31, 1990: Proceedings*, volume 452 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. ISBN 0-387-52953-5 (New York), 3-540-52953-5 (Berlin). LCCN QA76.9.M35 M386 1990.

Ramakrishna:1991:PHF

[RP91] M. V. Ramakrishna and G. A. Portice. Perfect hashing functions for hardware

applications. In ICDE'91 [ICD91], page 464. ISBN 0-8186-2138-9 (paper), 0-8186-6138-0 (microfiche), 0-8186-9138-7 (hardcover). LCCN QA76.9.D3 I5582 1991.

Rijmen:1995:ICD

[RP95] V. Rijmen and B. Preneel. Improved characteristics for differential cryptanalysis of hash functions based on block ciphers. *Lecture Notes in CS*, 1008:242–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ramakrishna:1992:ODS

[RR92] M. V. Ramakrishna and E. A. Ramos. Optimal distribution of signatures in signature hashing. *IEEE Transactions on Knowledge and Data Engineering*, 4(1):83–88, February 1, 1992. CODEN ITKEEH. ISSN 1041-4347.

Rechberger:2008:NRN

[RR08] C. Rechberger and V. Rijmen. New results on NMAC/HMAC when instantiated with popular hash functions. *J.UCS: Journal of Universal Computer Science*, 14(3):347–376, ???? 2008. CODEN ???? ISSN 0948-6968. URL `http://www.jucs.org/jucs_14_3/new_results_on_nmac`.

Raman:1999:FST

[RRR99] V. Raman, C. Pandu Rangan, and R. Ramanujam, editors. *Foundations of Software Technology and Theoretical Computer Science: 19th Conference, Chennai, India, December 13–15, 1999: Proceedings*, volume 1738 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. CODEN LNCSD9. ISBN 3-540-66836-5 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1738. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1738.htm`; `http://www.springerlink.com/content/978-3-540-66836-7`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1738`.

Rechberger:2006:NCW

[RRS06] Christian Rechberger, Vincent Rijmen, and Nicolas Sklavos. The NIST Cryptographic Workshop on Hash Functions. *IEEE Security & Privacy*, 4(1):54–56, January/February 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `http://ieeexplore.ieee.org/iel5/8013/33481/01588827.pdf`; `http://ieeexplore.`

ieee.org/xpls/abs_all.jsp?isnumber=33481&arnumber=1588827; http://www.csrc.nist.gov/pki/HashWorkshop/.

Raman:2007:SID

[RRS07] Rajeev Raman, Venkatesh Raman, and Srinivasa Rao Satti. Succinct indexable dictionaries with applications to encoding k-ary trees, prefix sums and multisets. *ACM Transactions on Algorithms*, 3(4):43:1–43:??, November 2007. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

Renda:2012:LBH

[RRS12] M. Elena Renda, Giovanni Resta, and Paolo Santi. Load balancing hashing in geographic hash tables. *IEEE Transactions on Parallel and Distributed Systems*, 23(8): 1508–1519, August 2012. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Rosenberg:1975:HSE

[RS75] A. L. Rosenberg and L. J. Stockmeyer. Hashing schemes for extendible arrays. In ACM-TOC'75 [ACM75c], pages 159–166.

Rosenberg:1977:HSE

[RS77] Arnold L. Rosenberg and Larry J. Stockmeyer. Hashing schemes for extendible arrays. *Journal of the Association for Computing Machinery*, 24(2):199–221, April 1977. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Raschid:1992:PPS

[RS92] Louiqa Raschid and Stanley Y. W. Su. A parallel pipelined strategy for evaluating linear recursive predicates in a multiprocessor environment. *Journal of Parallel and Distributed Computing*, 14(2): 146–162, February 1992. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic).

Rogaway:2008:CCH

[RS08] Phillip Rogaway and John Steinberger. Constructing cryptographic hash functions from fixed-key blockciphers. *Lecture Notes in CS*, 5157:433–450, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-85174-5_24.

Reyhanitabar:2012:CHD

[RS12] Mohammad Reza Reyhanitabar and Willy Susilo. On capabilities of hash domain extenders to preserve enhanced security properties. *Lecture Notes in CS*, 7496:288–299, 2012. CO-

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33272-2_19/.

Rivest:2014:SSR

[RS14] Ronald L. Rivest and Jacob C. N. Schuldt. Spritz —- a spongy RC4-like stream cipher and hash function. Report, MIT CSAIL and Research Institute for Secure Systems, Cambridge, MA 02139, USA and AIST, Japan, October 27, 2014. 30 pp. URL http://people.csail.mit.edu/rivest/pubs/RS14.pdf.

Ramamohanarao:1984:RLH

[RSD84] K. Ramamohanarao and R. Sacks-Davis. Recursive linear hashing. *ACM Transactions on Database Systems*, 9(3):369–391, September 1984. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Ramamohanarao:1985:PMR

[RSD85] K. Ramamohanarao and R. Sacks-Davis. Partial match retrieval using recursive linear hashing. *BIT (Nordisk tidskrift for informationsbehandling)*, 25(3):477–484, 1985. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Riazi:2017:CSC

[RSK17] M. Sadegh Riazi, Mohammad Samragh, and Farinaz Koushanfar. CAMsure: Secure content-addressable memory for approximate search. *ACM Transactions on Embedded Computing Systems*, 16(5s):136:1–136:??, October 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Ramamohanarao:1989:PMRa

[RSSD89a] K. Ramamohanarao, J. Shepherd, and R. Sacks-Davis. Partial-match retrieval for dynamic files using linear hashing with partial expansions. In Litwin and Schek [LS89], page ?? ISBN 0-387-51295-0. LCCN QA76.9.D3 F671 1989.

Ramamohanarao:1989:PMRb

[RSSD89b] K. Ramamohanarao, J. Shepherd, and R. Sacks-Davis. Partial-match retrieval using multiple-key hashing with multiple file copies. In *Proc. of the 1st Intern. Symposium on Database Systems for Advanced Applications, Seoul, Korea*, page ?? ????, ????, April 1989.

Ramamohanarao:1990:MAH

[RSSD90] Kotagiri Ramamohanarao, John Shepherd, and Ron Sacks-Davis. Multi-attribute hashing with multiple file copies for high performance partial-match retrieval. *BIT*

(Nordisk tidskrift for informationsbehandling), 30(3): 404–423, 1990. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Ramamohanarao:1992:PRU

[RSSD92] K. Ramamohanarao, J. Shepherd, and R. Sacks-Davis. Partial-match retrieval using multiple-key hashing with multiple file copies. In Kim et al. [KKP92], pages 250–275. ISBN 981-02-1315-8. LCCN QA76.9.D3 D3589 1992.

Raghavan:1981:ELS

[RT81] R. Raghavan and W. B. Thompson. Efficient local searching in sparse images. *Proceedings — IEEE Computer Society Conference on Pattern Recognition and Image Processing*, pages 548–553, 1981. CODEN PIRPDG.

Raite:1987:PTC

[RT87a] T. Raita and J. Teuhola. Predictive test compression by hashing. In Yu and Rijsbergen [YR87], pages 223–233. ISBN 0-89791-232-2. LCCN Z 699 A1 I58 1987. US$19.

Ruchte:1987:LHP

[RT87b] Willard D. Ruchte and Alan L. Tharp. Linear hashing with priority splitting: a method for improving the retrieval performance of linear hashing. In ICDE'87 [ICD87], pages 2–9. ISBN 0-8186-0762-9. LCCN QA76.9.D3I5582 1987. IEEE Service Cent. Piscataway, NJ, USA.

Ramakrishna:1989:DEH

[RT89] M. V. Ramakrishna and W. R. Tout. Dynamic external hashing with guaranteed single access retrieval. In Litwin and Schek [LS89], page ?? ISBN 0-387-51295-0. LCCN QA76.9.D3 F671 1989.

Rattanaritnont:2012:CTS

[RTK12] Geerajit Rattanaritnont, Masashi Toyoda, and Masaru Kitsuregawa. Characterizing topic-specific hashtag cascade in Twitter based on distributions of user influence. *Lecture Notes in CS*, 7235:735–742, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-29253-8_71`.

Ruckert:2015:MSS

[Ruc15] Martin Ruckert. *The MMIX supplement: supplement to* The Art of Computer Programming, volumes 1, 2, 3 *by Donald E. Knuth*. Addison-Wesley, Reading, MA, USA, 2015. ISBN 0-13-399231-4 (paperback), 0-13-399289-6. xxi + 193 pp. LCCN QA76.6 .K64 2005 Suppl. 1. URL `http://mmix.cs.hm.edu/`.

Rueppel:1993:ACE

[Rue93] Rainer A. Rueppel, editor. *Advances in Cryptology–EUROCRYPT '92: Workshop on the Theory and Application of Cryptographic Techniques, Balatonfured, Hungary, May 24–28, 1992: Proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-56413-6 (New York), 3-540-56413-6 (Berlin). LCCN QA76.9.A25 E964 1992.

Ruland:1993:RDS

[Rul93] Christoph Ruland. Realizing digital signatures with one-way hash functions. *Cryptologia*, 17(3): 285–300, July 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639237~db=all~order=page`. digital signatures; one-way hash functions; asymmetric cryptographic systems; smart cards; one-time signatures; optimally implemented hash functions; asymmetric algorithms; one-bit signatures; N-bit signatures; infinite signature trees; performance.

Russell:1992:NSC

[Rus92] Alexander Russell. Necessary and sufficient conditions for collision-free hashing. In Brickell [Bri92], pages 433–441. ISBN 0-387-57340-2 (New York), 3-540-57340-2 (Berlin). LCCN QA76.9.A25 C79 1992. DM104.00.

Russell:1993:NSC

[Rus93] A. Y. Russell. Necessary and sufficient conditions for collision-free hashing. *Lecture Notes in CS*, 740:433–441, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Russell:1995:NSC

[Rus95] Alexander Russell. Necessary and sufficient conditions for collision-free hashing. *Journal of Cryptology*, 8 (2):87–99, Spring 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Ruzic:2008:UDD

[Ruž08] Milan Ružić. Uniform deterministic dictionaries. *ACM Transactions on Algorithms*, 4(1):1:1–1:??, March 2008. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

Rijmen:2002:PCP

[RVPV02] V. Rijmen, B. Van Rompay, B. Preneel, and J. Vandewalle. Producing collisions for PANAMA. *Lecture Notes in CS*, 2355:37–51, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL ????.

Rickman:1973:SIL

[RW73] J. Rickman and W. E. Walden. Structures for an interactive on-line thesaurus. *International Journal of Computer and Information Sciences*, 2(2):115–127, June 1973. CODEN IJCIAH. ISSN 0091-7036.

Rigoutsos:1997:GEI

[RW97] Isidore Rigoutsos and Haim J. Wolfson. Guest Editors' introduction: Geometric hashing. *IEEE Computational Science & Engineering*, 4(4): 9, October/December 1997. CODEN ISCEE4. ISSN 1070-9924 (print), 1558-190X (electronic). URL `http://dlib.computer.org/cs/books/cs1997/pdf/c4009.pdf`.

Ramaswamy:2007:HSP

[RW07] Ramaswamy Ramaswamy and Tilman Wolf. High-speed prefix-preserving IP address anonymization for passive measurement systems. *IEEE/ACM Transactions on Networking*, 15(1): 26–39, February 2007. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Reyhanitabar:2007:NIM

[RWSN07] Mohammad Reza Reyhanitabar, Shuhong Wang, and Reihaneh Safavi-Naini. Non-interactive manual channel message authentication based on eTCR hash functions. *Lecture Notes in CS*, 4586:385–399, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-73458-1_28`.

Rabitti:1990:DST

[RZ90] F. Rabitti and P. Zezula. A dynamic signature technique for multimedia databases. In Vidick [Vid90], page 193. ISBN 0-89791-408-2. LCCN QA76.9.D3I5588 1990, Z 699 A1 I582 1990.

Ramakrishna:1997:PPS

[RZ97] M. V. Ramakrishna and Justin Zobel. Performance in practice of string hashing functions. In Rodney W. Topor and Katsumi Tanaka, editors, *Database Systems for Advanced Applications '97, Proceedings of the Fifth International Conference on Database Systems for Advanced Applications (DASFAA), Melbourne, Australia, April 1–4, 1997*, volume 6 of *Advanced Database Research and Development Series*, pages 215–224. World Scientific Publishing Co. Pte. Ltd., P. O. Box 128, Farrer Road, Singapore 9128, 1997. ISBN 981-02-3107-5, 981-02-3118-0 (paperback). LCCN QA76.9.D3 I5565 1997. URL `http://www.worldscientific.com/doi/`

abs/10.1142/9789812819536_0023.

Surendro:1997:NRO

[SA97] K. Surendro and Y. Anzai. Non-rigid object recognition using principal component analysis and geometric hashing. *Lecture Notes in CS*, 1296:50–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sohrabi:2017:PSS

[SA17] Mohammad Karim Sohrabi and Hosseion Azgomi. Parallel set similarity join on big data based on Locality-Sensitive Hashing. *Science of Computer Programming*, 145 (??):1–12, October 1, 2017. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167642317300813.

Saarinen:2012:CAG

[Saa12] Markku-Juhani Olavi Saarinen. Cycling attacks on GCM, GHASH and other polynomial MACs and hashes. *Lecture Notes in CS*, 7549:216–225, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34047-5_13/.

Sabourin:1994:CCP

[Sab94] Conrad F. Sabourin. *Computational character processing: character coding, input, output, synthesis, ordering, conversion, text compression, encryption, display hashing, literate programming: bibliography*. Infolingua, Montréal, PQ, Canada, 1994. ISBN 2-921173-18-2. vii + 579 pp. LCCN ????

Sacco:1986:FTE

[Sac86] G. M. Sacco. Fragmentation: a technique for efficient query processing. *ACM Transactions on Database Systems*, 11(2):113–133, June 1986. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). Also published in/as: University of Torino, TR., Aug. 1983.

Sager:1984:NMG

[Sag84] Thomas J. Sager. A new method for generating minimal perfect hashing functions. Technical Report TR CSc-84-15, University of Missouri–Rolla, Rolla, MO, USA, November 1984. ?? pp.

Sager:1985:PTG

[Sag85a] Thomas J. Sager. A polynomial time generator for minimal perfect hash functions. *Communications of the Association for Computing Machinery*, 28(5): 523–532, May 1985. CO-

DEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Sager:1985:TCS

[Sag85b] Thomas J. Sager. A technique for creating small fast compiler frontends. *SIGPLAN Notices*, 20(10):87–94, October 1985. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Salzberg:1988:FS

[Sal88] Betty Salzberg. *File Structures*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1988. ISBN 0-13-314691-X. x + 342 pp. LCCN QA76.9.F5 S25 1988. US$36.95.

Samson:1976:TOA

[Sam76] W. B. Samson. Testing overflow algorithms for a table of variable size. *The Computer Journal*, 19(1): 92, February 1976. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/19/1/92.full.pdf+html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_19/Issue_01/tiff/92.tif`.

Samson:1981:HTC

[Sam81] W. B. Samson. Hash table collision handling on storage devices with latency. *The Computer Journal*, 24 (2):130–131, May 1981. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Santoro:1976:FTS

[San76] Nicola Santoro. Full table search by polynomial functions. *Information Processing Letters*, 5(3):72–74, August ??, 1976. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Sarwate:1980:NUC

[Sar80] Dilip V. Sarwate. A note on: "Universal classes of hash functions" [J. Comput. System Sci. **18** (1979), no. 2, 143–154; MR 80f:68110a] by J. L. Carter and M. N. Wegman. *Information Processing Letters*, 10(1):41–45, February 1980. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Sarkar:2010:SGC

[Sar10] Palash Sarkar. A simple and generic construction of authenticated encryption with associated data. *ACM Transactions on Information and System Security*, 13(4):33:1–33:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Sarkar:2011:TBC

[Sar11] Palash Sarkar. A trade-off between collision probability and key size in universal hashing using polynomials. *Designs, Codes, and Cryptography*, 58(3):271–278, March 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=58&issue=3&spage=271`.

Sarkar:2013:NML

[Sar13] Palash Sarkar. A new multilinear universal hash family. *Designs, Codes, and Cryptography*, 69(3):351–367, December 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9672-8`.

Sarkar:2015:FNR

[Sar15] Santanu Sarkar. Further non-randomness in RC4, RC4A and VMPC. *Cryptography and Communications*, 7(3): 317–330, September 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0119-0`.

Sasaki:2011:MMP

[Sas11] Yu Sasaki. Meet-in-the-middle preimage attacks on AES hashing modes and an application to Whirlpool. *Lecture Notes in CS*, 6733: 378–396, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-21702-9_22`.

Savoy:1990:SBF

[Sav90] Jacques Savoy. Statistical behavior of fast hashing of variable length test strings. *SIGIR forum*, 24(3):62–??, Fall 1990. CODEN FASRDV. ISSN 0163-5840.

Savoy:1991:NFH

[Sav91] Jacques Savoy. Note on fast hashing of variable length text strings. *Communications of the Association for Computing Machinery*, 34(11):118–119, November 1991. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Suggests an improvement to Pearson's hashing algorithm [Pea90] that avoids secondary clustering. Exhibits a key set for which Pearson's algorithm produces alarming clustering. See also comments in [Dit91, Lit91, Pea91], and early work in [Dit76].

Sheffler:1993:AHP

[SB93] Thomas J. Sheffler and Randal E. Bryant. An analysis of

hashing on parallel and vector computers. In Hariri and Berra [HB93], pages III.29–III.36. ISBN 0-8493-8983-6 (set), 0-8493-8984-4 (vol. 1), 0-8493-8985-2 (vol. 2), 0-8493-8986-0 (vol. 3). LCCN QA76.58 .I55 1993.

Sabharwal:1995:PHT

[SB95] C. L. Sabharwal and S. K. Bhatia. Perfect hash table algorithm for image databases using negative associated values. *Pattern Recognition*, 28(7):1091–??, 1995. CODEN PTNRA8. ISSN 0031-3203 (print), 1873-5142 (electronic).

Sabharwal:1997:IDN

[SB97] C. L. Sabharwal and S. K. Bhatia. Image databases and near-perfect hash table. *Pattern Recognition*, 30(11): 1867–1876, November 1997. CODEN PTNRA8. ISSN 0031-3203 (print), 1873-5142 (electronic).

Shankar:2007:DAI

[SB07] Ajeet Shankar and Rastislav Bodík. DITTO: automatic incrementalization of data structure invariant checks (in Java). *SIGPLAN Notices*, 42(6):310–319, June 2007. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Saikia:2014:PHF

[SB14] Navajit Saikia and Prabin K. Bora. Perceptual hash function for scalable video. *International Journal of Information Security*, 13(1):81–93, February 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-013-0211-z`.

Stevens:2017:AFS

[SBK+17] Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, Yarik Markov, Alex Petit Bianco, and Clement Baisse. Announcing the first SHA1 collision. Web report, February 23, 2017. URL `https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html`.

Scolari:2016:SCP

[SBS16] Alberto Scolari, Davide Basilio Bartolini, and Marco Domenico Santambrogio. A software cache partitioning system for hash-based caches. *ACM Transactions on Architecture and Code Optimization*, 13(4):57:1–57:??, December 2016. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic).

Sprague:1977:PTH

[SC77] Ralph H. Sprague and R. Chattergy, editors. *Proceedings of the Tenth Hawaii*

International Conference on System Sciences, Supplement: Selected Papers in Management Information Systems. Western Periodicals Co.,, North Hollywood, CA, 1977. LCCN ??

Shekita:1990:PEPb

[SC90a] E. J. Shekita and M. J. Carey. A performance evaluation of pointer-based joins. In Garcia-Molina and Jagadish [GMJ90], page ?? ISBN 0-89791-365-5. LCCN QA 76.9 D3 S53 v.19 no.2 1990.

Shekita:1990:PEPa

[SC90b] Eugene J. Shekita and Michael J. Carey. A performance evaluation of pointer-based joins. Technical Report TR 916, Computer Sciences Department, University of Wisconsin–Madison, March 1990. ?? pp.

Shekita:1990:PEPc

[SC90c] Eugene J. Shekita and Michael J. Carey. A performance evaluation of pointer-based joins. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 19 (2):300–311, June 1990. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic). URL `http://www.acm.org/pubs/articles/proceedings/mod/93597/p300-shekita/p300-shekita.pdf`; `http://www.acm.org/pubs/citations/proceedings/mod/93597/p300-shekita/`.

Schauer:1976:PA

[Sch76] Helmut Schauer. *Pascal für Anfänger*. R. Oldenbourg Verlag, Munich, Germany and Vienna, Austria, 1976. ISBN 3-7029-0091-8. 175 pp.

Scheuermann:1979:OHH

[Sch79a] Peter Scheuermann. Overflow handling in hashing tables: a hybrid approach. *Information system*, 4(3):183–194, ???? 1979. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Scholl:1979:PAN

[Sch79b] M. Scholl. Performance analysis of new file organizations based on dynamic hashcoding. Technical report, ????, Le Chesnay, France, March 1979. ?? pp.

Scholl:1981:NFO

[Sch81] Michel Scholl. New file organizations based on dynamic hashing. *ACM Transactions on Database Systems*, 6(1): 194–211, March 1981. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Scheuermann:1982:PSI

[Sch82a] P. Scheuermann, editor. *International Conference on Databases: Improving Usability and Responsiveness*

(2nd: 1982: Hebrew University of Jerusalem), Jerusalem, Israel, June 22–24, 1982. Academic Press, New York, NY, USA, 1982. ISBN 0-12-624080-9. LCCN QA76.9.D3 .I558 1982. US$34.00.

Schmitt:1982:CPF

[Sch82b] Alfred Schmitt. On the computational power of the floor function. *Information Processing Letters*, 14(1):1–3, March 27, 1982. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Schmidt:1990:GPH

[Sch90a] Douglas C. Schmidt. GPERF: a perfect hash function generator. In USENIX-C++'90 [USE90], pages 87–101.

Schneider:1990:CQP

[Sch90b] Donovan A. Schneider. Complex query processing in multiprocessor database machines. Technical Report TR 965, University of Wisconsin, September 1990. ?? pp.

Schneier:1991:OWH

[Sch91a] Bruce Schneier. One-way hash functions: Probabilistic algorithms can be used for general-purpose pattern matching. *Dr. Dobbs Journal*, 16(9):148–151, September 1, 1991. CODEN DDJOEB. ISSN 1044-789X.

Schnorr:1991:FHE

[Sch91b] C. P. Schnorr. FFT-hashing, an efficient cryptographic hash function. In Feigenbaum [Fei91], page ?? ISBN 0-387-55188-3 (New York), 3-540-55188-3 (Berlin). LCCN QA76.9.A25 C79 1991.

Schnorr:1993:FHIa

[Sch93a] C. P. Schnorr. FFT-hash II, efficient cryptographic hashing. In Rueppel [Rue93], pages 41–51. ISBN 0-387-56413-6 (New York), 3-540-56413-6 (Berlin). LCCN QA76.9.A25 E964 1992.

Schnorr:1993:FHIb

[Sch93b] C. P. Schnorr. FFT-hash II, efficient cryptographic hashing. *Lecture Notes in CS*, 658:45–54, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schnorr:1993:FIE

[Sch93c] C. P. Schnorr. FFT-hash II, efficient cryptographic hashing. *Lecture Notes in CS*, 658:45–54, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Scharinger:2001:CDD

[Sch01a] J. Scharinger. Construction of data dependent chaotic permutation hashes to ensure communications integrity. *Lecture Notes*

in CS, 2094:196–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2094/20940196.htm; http://link.springer-ny.com/link/service/series/0558/papers/2094/20940196.pdf.

Scharinger:2001:ASK

[Sch01b] Josef Scharinger. Application of signed Kolmogorov hashes to provide integrity and authenticity in Web-based software distribution. *Lecture Notes in CS*, 2178:257–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2178/21780257.htm; http://link.springer-ny.com/link/service/series/0558/papers/2178/21780257.pdf.

Schlaffer:2011:SDR

[Sch11] Martin Schläffer. Subspace distinguisher for 5/8 rounds of the ECHO-256 hash function. *Lecture Notes in CS*, 6544:369–387, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-19574-7_25.

Severance:1976:PGA

[SD76] D. G. Severance and R. A. Duhne. A practitioner's guide to addressing algorithms. *Communications of the Association for Computing Machinery*, 19(6): 314–326, June 1976. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Samson:1978:STU

[SD78] W. B. Samson and R. H. Davis. Search times using hash tables for records with non-unique keys. *The Computer Journal*, 21(3): 210–214, August 1978. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Sacks-Davis:1985:PMK

[SD85] Ron Sacks-Davis. Performance of a multi-key access method based on descriptors and superimposed coding techniques. *Information system*, 10(4):391–403, 1985. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic). Hashing algorithm used to create descriptors for file indexing; this extends the author's earlier work [SDR83b].

Schneider:1989:PEFc

[SD89a] D. Schneider and D. DeWitt. A performance evaluation of four parallel join algorithms

in a shared-nothing multiprocessor environment. In Clifford et al. [CLM89], page 110. ISBN 0-89791-317-5. LCCN QA 76.9 D3 S53 v.18 no.2 1989.

Schneider:1989:DTA

[SD89b] Donovan Schneider and David J. DeWitt. Design tradeoffs of alternative query tree representations for multiprocessor database machines. Technical Report TR 869, Computer Sciences Department, University of Wisconsin–Madison, August 1989. ?? pp.

Schneider:1989:PEFa

[SD89c] Donovan A. Schneider and David J. DeWitt. A performance evaluation of four parallel join algorithms in a shared-nothing multiprocessor environment. Technical Report TR 836, University of Wisconsin, April 1989. ?? pp.

Schneider:1989:PEFb

[SD89d] Donovan A. Schneider and David J. DeWitt. A performance evaluation of four parallel join algorithms in a shared-nothing multiprocessor environment. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 18(2): 110–121, June 1989. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic). URL `http://www.acm.org/pubs/articles/proceedings/mod/67544/p110-schneider/p110-schneider.pdf`; `http://www.acm.org/pubs/citations/proceedings/mod/67544/p110-schneider/`. Also published in [CLM89].

Schneider:1990:TPCb

[SD90a] D. Schneider and D. DeWitt. Tradeoffs in processing complex join queries via hashing in multiprocessor database machines. In McLeod et al. [MSDS90], page 469. ISBN 1-55860-149-X. LCCN ???

Schneider:1990:TPCa

[SD90b] Donovan Schneider and David J. DeWitt. Tradeoffs in processing complex join queries via hashing in multiprocessor database machines. Technical Report TR 930, University of Wisconsin, April 1990. ?? pp.

Stern:1995:IPV

[SD95] U. Stern and D. L. Dill. Improved probabilistic verification by hash compaction. In Camurati and Eveking [CE95], pages 206–224. ISBN 3-540-60385-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7874.75 .A39 1995.

ACM:1990:PFA

[SDA90] *Proceedings of the First Annual ACM-SIAM Symposium on Discrete Algorithms*. Society for Industrial

and Applied Mathematics, Philadelphia, PA, USA, 1990. ISBN 0-89871-251-3. LCCN QA76.6 .A278 1990.

ACM:1991:PSA

[SDA91] *Proceedings of the Second Annual ACM-SIAM Symposium on Discrete Algorithms*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1991. LCCN QA76.9.A43 A34 199. Symposium held Jan. 28–30, 1991, San Francisco, CA, USA.

Shih:1991:CDC

[SDK91] C.-S. Shih, A. Dan, and W. H. Kohler. Comparison of distributed concurrency control protocols on a distributed database testbed. Technical Report COINS TR 91-13, University of Massachusetts, 1991. ?? pp.

Sacks-Davis:1987:MAM

[SDKR87] R. Sacks-Davis, A. Kent, and K. Ramamohanarao. Multikey access methods based on superimposed coding techniques. *ACM Transactions on Database Systems*, 12 (4):655–696, December 1987. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Sajadieh:2012:RDL

[SDMS12] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Pouyan Sepehrdad. Recursive diffusion layers for block ciphers and hash functions. *Lecture Notes in CS*, 7549:385–401, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-34047-5_22`.

Sajadieh:2015:ERD

[SDMS15] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Pouyan Sepehrdad. Efficient recursive diffusion layers for block ciphers and hash functions. *Journal of Cryptology*, 28(2):240–256, April 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9163-8`.

Sacks-Davis:1983:ILH

[SDR83a] R. Sacks-Davis and K. Ramamohanarao. Implementation of linear hashing schemes. In Barter [Bar83], pages 27:1–27:10. Published as Australian Computer Science Communications; vol 6, no. 1.

Sacks-Davis:1983:TLS

[SDR83b] R. Sacks-Davis and K. Ramamohanarao. A two level superimposed coding scheme for partial match retrieval. *Information system*, 8(4): 273–280, 1983. CODEN INSYD6. ISSN 0306-4379

(print), 1873-6076 (electronic). See [SD85].

Sorenson:1975:DDH

[SDT75] P. G. Sorenson, R. F. Deutscher, and J. P. Tremblay. Distribution-dependent hashing functions and their characteristics. In *19 ACM SIGMOD Conf. on the Management of Data, King(ed)*, page ?? ACM Press, New York, NY 10036, USA, May 1975.

Schellhorn:2014:SCP

[SDW14] Gerhard Schellhorn, John Derrick, and Heike Wehrheim. A sound and complete proof technique for linearizability of concurrent data structures. *ACM Transactions on Computational Logic*, 15 (4):31:1–31:??, September 2014. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic).

Spirovska:2021:OCC

[SDZ21] K. Spirovska, D. Didona, and W. Zwaenepoel. Optimistic causal consistency for geo-replicated key–value stores. *IEEE Transactions on Parallel and Distributed Systems*, 32(3):527–542, March 2021. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Smith:1989:ITD

[SE89] F. J. Smith and L. C. Emerson. Indexing technical data in a materials database. In *Second International Conference on Data and Knowledge Systems for Manufacturing and Engineering (Oct 16–18 1989: Gaithersburg, MD, USA)*, pages 12–18. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. IEEE catalog number 89CH2806-8.

Shafieinejad:2021:SPQ

[SE21] Masoumeh Shafieinejad and Navid Nasr Esfahani. A scalable post-quantum hash-based group signature. *Designs, Codes, and Cryptography*, 89(5):1061–1090, May 2021. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-021-00857-9`.

Sedgewick:1983:MAC

[Sed83a] R. Sedgewick. Part III. mathematical analysis of combinatorial algorithms. In *Probability Theory and Computer Science* [LL83], page Part III. Mathematical analysis of combinatorial algorithm. ISBN 0-12-455820-8. LCCN QA274 .P76 1983. Analysis of hashing with linear probing.

Sedgewick:1983:A

[Sed83b] Robert Sedgewick. *Algorithms*. Addison-Wesley,

Reading, MA, USA, 1983. ISBN 0-201-06672-6. viii + 551 pp. LCCN QA76.6 .S435 1983.

Sedgewick:1988:A

[Sed88] Robert Sedgewick. *Algorithms*. Addison-Wesley, Reading, MA, USA, second edition, 1988. ISBN 0-201-06673-4. xii + 657 pp. LCCN QA76.6 .S435 1988. US$34.95.

Sedgewick:1990:AC

[Sed90] Robert Sedgewick. *Algorithms in C*. Addison-Wesley, Reading, MA, USA, 1990. ISBN 0-201-51425-7. xii + 657 pp. LCCN QA76.73.C15 S43 1990.

Sedgewick:1992:AC

[Sed92] Robert Sedgewick. *Algorithms in C++*. Addison-Wesley, Reading, MA, USA, 1992. ISBN 0-201-36118-3, 0-201-51059-6. xiv + 656 pp. LCCN QA76.73.C153 S38 1992.

Sedgewick:1993:AM

[Sed93] Robert Sedgewick. *Algorithms in Modula-3*. Addison-Wesley, Reading, MA, USA, 1993. ISBN 0-201-53351-0. xiv + 656 pp. LCCN QA76.73.M63 S43 1993.

Severance:1974:ISM

[Sev74] Dennis G. Severance. Identifier search mechanisms: a survey and generalized model. *ACM Computing Surveys*, 6(3):175–194, September 1974. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Scott:1988:SMT

[SF88] Michael L. Scott and Raphael A. Finkel. A simple mechanism for type security across compilation units. *IEEE Transactions on Software Engineering*, 14(8): 1238–1239, August 1988. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7631`.

Sherkat:2019:NSE

[SFA+19] Reza Sherkat, Colin Florendo, Mihnea Andrei, Rolando Blanco, Adrian Dragusanu, Amit Pathak, Pushkar Khadilkar, Neeraj Kulkarni, Christian Lemke, Sebastian Seifert, Sarika Iyer, Sasikanth Gottapu, Robert Schulze, Chaitanya Gottipati, Nirvik Basak, Yanhong Wang, Vivek Kandiyanallur, Santosh Pendap, Dheren Gala, Rajesh Almeida, and Prasanta Ghosh. Native store extension for SAP HANA. *Proceedings of the VLDB Endowment*, 12(12):2047–2058, August 2019. CODEN ???? ISSN 2150-8097.

Simon:1972:APN

[SG72] J. C. Simon and G. Guiho. On algorithms preserving neighborhood, to file and retrieve information in a memory. *International Journal of Computer and Information Sciences*, 1(1):3–15, March 1972. CODEN IJCIAH. ISSN 0091-7036.

Sassa:1976:HMF

[SG76a] M. Sassa and E. Goto. A hashing method for fast set operations. *Information Processing Letters*, 5 (2):31–34, 1976. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Shneiderman:1976:BSS

[SG76b] Ben Shneiderman and Victor Goodman. Batched searching of sequential and tree structured files. *ACM Transactions on Database Systems*, 1(3):268–275, September 1976. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1976-1-3/p268-shneiderman/p268-shneiderman.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1976-1-3/p268-shneiderman/`. See comments in [Piw85]. Also published in/as: Indiana Un., CSD Tech. Ref. 0132.

Shasha:1988:CSS

[SG88] Dennis Shasha and Nathan Goodman. Concurrent search structure algorithms. *ACM Transactions on Database Systems*, 13(1):53–90, March 1988. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1988-13-1/p53-shasha/p53-shasha.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1988-13-1/p53-shasha/`; `http://www.acm.org/pubs/toc/Abstracts/tods/42204.html`.

Shangguan:2016:SHF

[SG16] Chong Shangguan and Gennian Ge. Separating hash families: a Johnson-type bound and new constructions. *SIAM Journal on Discrete Mathematics*, 30(4): 2243–2264, ???? 2016. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Steinwandt:2000:WHS

[SGGB00] Rainer Steinwandt, Markus Grassl, Willi Geiselmann, and Thomas Beth. Weaknesses in the $\mathrm{SL}_2(\mathbf{F}_{2^n})$ hashing scheme. In Bellare [Bel00], pages 287–299. ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2000 Bar. URL `http://link.springer-ny.`

com/link/service/series/0558/bibs/1880/18800287.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800287.pdf.

Sharma:2009:DAC

[SGK09] Arun Sharma, P. S. Grover, and Rajesh Kumar. Dependency analysis for component-based software systems. *ACM SIGSOFT Software Engineering Notes*, 34(4): 1–6, July 2009. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

Shaolan:2011:EDE

[SGY11] Zhang Shaolan, Xing Guobo, and Yang Yixian. An efficient domain extension to construct a cryptographic hash function. In IEEE [IEE11a], pages 424–427. ISBN 0-7695-4353-7, 1-61284-289-5. LCCN ???? URL http://ieeexplore.ieee.org/servlet/opac?punumber=5750113.

Seiden:1992:FSO

[SH92] Steven S. Seiden and Daniel S. Hirschberg. Finding succinct ordered minimal perfect hashing functions. Technical Report TR 92-23, Information and Computer Science, University of California, Irvine, 1992. 10 pp.

Seiden:1994:FSO

[SH94] Steven S. Seiden and Daniel S. Hirschberg. Finding succinct ordered minimal perfect hash functions. *Information Processing Letters*, 51(6):283–288, September 26, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Shapiro:1986:JPD

[Sha86] L. D. Shapiro. Join processing in database systems with large main memories. *ACM Transactions on Database Systems*, 11(3): 239–264, September 1986. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Smith:1997:EHF

[SHA97] Bradley J. Smith, Gregory L. Heileman, and Chaouki Abdallah. The exponential hash function. *ACM Journal of Experimental Algorithmics*, 2:3:1–3:??, ???? 1997. ISSN 1084-6654.

Sheil:1978:MST

[She78] B. A. Sheil. Median split trees: a fast lookup technique for frequently occurring keys. *Communications of the Association for Computing Machinery*, 21(11): 947–958, November 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Early work on

minimal perfect hash functions.

Shekita:1991:HPF

[She91] Eugene Shekita. High-performance implementation techniques for next-generation database systems. Technical Report TR 1026, Computer Sciences Department, University of Wisconsin–Madison, May 1991. ?? pp.

Sher:2006:MDS

[She06] David B. Sher. Motivating data structures with caching Internet stock data. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 38(3): 344, September 2006. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Shemanske:2017:MCE

[She17] Thomas R. Shemanske. *Modern Cryptography and Elliptic Curves: a Beginner's Guide*, volume 83 of *Student mathematical library*. American Mathematical Society, Providence, RI, USA, 2017. ISBN 1-4704-3582-9, 1-4704-4123-3 (e-book). xii + 250 pp. LCCN QA567.2.E44 S534 2017. URL `http://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=4940250`.

Sun:2017:CMC

[SHF+17] Yuanyuan Sun, Yu Hua, Dan Feng, Ling Yang, Pengfei Zuo, Shunde Cao, and Yuncheng Guo. A collision-mitigation cuckoo hashing scheme for large-scale storage systems. *IEEE Transactions on Parallel and Distributed Systems*, 28(3):619–632, March 2017. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL `https://www.computer.org/csdl/trans/td/2017/03/07523403-abs.html`.

Shim:2017:PME

[Shi17] Hyotaek Shim. PHash: a memory-efficient, high-performance key-value store for large-scale data-intensive applications. *The Journal of Systems and Software*, 123 (??):33–44, January 2017. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121216301959`.

Shmoys:2000:PAA

[Shm00] David Editor Shmoys, editor. *Proceedings of the 11th Annual ACM–SIAM Symposium on Discrete Algorithms, San Francisco, California, January 9–11, 2000*, volume 101 of *Proceedings in Applied Mathematics Ser.* Society for Industrial and Applied Mathemat-

ics, Philadelphia, PA, USA, 2000. ISBN 0-89871-453-2. LCCN QA76.6 .A278 2000. URL http://encompass.library.cornell.edu/cgi-bin/checkIP.cgi?access=gateway_standard\%26url=http://dl.acm.org/citation.cfm?id=338219.

Shoup:1996:FPS

[Sho96] V. Shoup. On fast and provably secure message authentication based on universal hashing. *Lecture Notes in CS*, 1109:313–??, ???? 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shoup:2000:CTU

[Sho00a] Victor Shoup. A composition theorem for universal one-way hash functions. *Lecture Notes in CS*, 1807:445–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070445.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070445.pdf.

Shoup:2000:UHF

[Sho00b] Victor Shoup. Using hash functions as a hedge against chosen ciphertext attack. *Lecture Notes in CS*, 1807:275–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070275.htm; http://link.springer-ny.com/link/service/series/0558/papers/1807/18070275.pdf.

Shoup:2005:ACC

[Sho05] Victor Shoup, editor. *Advances in cryptology: CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14–18, 2005: proceedings*, volume 3621 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621.

Starzetz:2009:HBC

[SHRD09] Paul Starzetz, Martin Heusse, Franck Rousseau, and Andrzej Duda. Hashing backoff: a collision-free wireless access method. *Lecture Notes in CS*, 5550:429–441, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-

tronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-01399-7_34.

Shen:2020:VRS

[SHZ+20] Ling Shen, Richang Hong, Haoran Zhang, Xinmei Tian, and Meng Wang. Video retrieval with similarity-preserving deep temporal hashing. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 15(4):1–16, January 2020. ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3356316.

Sockut:2009:ORD

[SI09] Gary H. Sockut and Balakrishna R. Iyer. Online reorganization of databases. *ACM Computing Surveys*, 41(3): 14:1–14:136, July 2009. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Siegel:1989:UCF

[Sie89] Alan Siegel. On universal classes of fast high performance hash functions, their time-space tradeoff, and their applications. In IEEE-FOCS'89 [IEE89], pages 20–25. CODEN ASFPDV. ISBN 0-8186-1982-1 (hardcover), 0-8186-5982-3 (microfiche). ISSN 0272-5428. LCCN ???? IEEE catalog number 89CH2808-4.

Siegel:2004:UCE

[Sie04] Alan Siegel. On universal classes of extremely random constant-time hash functions. *SIAM Journal on Computing*, 33(3): 505–543, June 2004. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/38621.

Silverstein:2002:JIS

[Sil02a] Alan Silverstein. *Judy IV Shop Manual*. Hewlett–Packard Corporation, ????, August 5, 2002. URL http://judy.sourceforge.net/; http://judy.sourceforge.net/doc/shop_interm.pdf.

Silverstein:2002:PPH

[Sil02b] Craig Silverstein. A practical perfect hashing algorithm. In Goldwasser et al. [GJM02], pages xi + 256. ISBN 0-8218-2892-4 (hardcover). LCCN QA76.9.D35 D385 2002.

Simon:1998:FCO

[Sim98] Daniel R. Simon. Finding collisions on a one-way street: Can secure hash functions be based on general assumptions? *Lecture Notes in CS*, 1403:334–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/

0558/bibs/1403/14030334.htm; http://link.springer-ny.com/link/service/series/0558/papers/1403/14030334.pdf.

Sakti:1988:GPP

[SK88] Pramanik Sakti and Myoung Ho Kim. Generalized parallel processing models for database systems. *Proceedings of the International Conference on Parallel Processing*, 3:76–83, 1988. CODEN PCPADL. ISSN 0190-3918. Available from IEEE Service Cent (catalog number 88CH2625-2). Piscataway, NJ, USA.

Shintani:1998:MAS

[SK98] T. Shintani and M. Kitsuregawa. Mining algorithms for sequential patterns in parallel: Hash based approach. *Lecture Notes in CS*, 1394:283–294, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schneier:1999:SAL

[SK99] Bruce Schneier and John Kelsey. Secure audit logs to support computer forensics. *ACM Transactions on Information and System Security*, 2(2):159–176, May 1999. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic). URL http://www.acm.org/pubs/citations/journals/tissec/1999-2-2/p159-schneier/.

Sklavos:2005:ISH

[SK05] N. Sklavos and O. Koufopavlou. Implementation of the SHA-2 hash family standard using FPGAs. *The Journal of Supercomputing*, 31 (3):227–248, March 2005. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=31&issue=3&spage=227.

S:2020:SPE

[SK20] Ajish S. and K. S. Anil Kumar. Security and performance enhancement of fingerprint biometric template using symmetric hashing. *Computers and Security*, 90(??):Article 101714, March 2020. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL http://www.sciencedirect.com/science/article/pii/S016740482030002X.

Sohn:2007:DDI

[SKC07] Andrew Sohn, Hukeun Kwak, and Kyusik Chung. DISH — Dynamic Information-Based Scalable Hashing on a cluster of Web cache servers. *Lecture Notes in CS*, 4782:785–796, 2007. CODEN LNCSD9. ISSN 0302-

9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-75444-2_73`.

Schuhknecht:2015:SDS

[SKD15] Felix Martin Schuhknecht, Pankaj Khanchandani, and Jens Dittrich. On the surprising difficulty of simple things: the case of radix partitioning. *Proceedings of the VLDB Endowment*, 8(9):934–937, May 2015. CODEN ???? ISSN 2150-8097.

Suzuki:2001:ESB

[SKM01] Koutarou Suzuki, Kunio Kobayashi, and Hikaru Morita. Efficient sealed-bid auction using hash chain. *Lecture Notes in CS*, 2015:183–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2015/20150183.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2015/20150183.pdf`.

Stevens:2015:FCF

[SKP15] Marc Stevens, Pierre Karpman, and Thomas Peyrin. Freestart collision on full SHA-1. Cryptology ePrint Archive, Report 2015/967., 2015. URL `https://eprint.iacr.org/2015/967`.

Shang:1988:DCP

[SL88] C. C. Shang and C. H. Lin. On the difficulty of constructing perfect hashing functions. In *IEEE 1988 International Symposium on Information Theory — Abstracts of papers*, volume 25 n 13, pages 241–?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. Available from IEEE Service Cent (catalog number 88CH2621-1). Piscataway, NJ, USA.

Shahzad:2016:AEP

[SL16] Muhammad Shahzad and Alex X. Liu. Accurate and efficient per-flow latency measurement without probing and time stamping. *IEEE/ACM Transactions on Networking*, 24(6): 3477–3492, December 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Schweller:2007:RSE

[SLC+07] Robert Schweller, Zhichun Li, Yan Chen, Yan Gao, Ashish Gupta, Yin Zhang, Peter A. Dinda, Ming-Yang Kao, and Gokhan Memik. Reversible sketches: enabling monitoring and analysis over high-speed data streams. *IEEE/ACM Transactions on Networking*, 15 (5):1059–1072, October 2007. CODEN IEANEP. ISSN

1063-6692 (print), 1558-2566 (electronic).

Shultz:1987:TSM

[SM87] R. Shultz and I. Miller. Tree structured multiple processor join methods. In *Proceedings of the International Conference on Data Engineering*, pages 190–199. IEEE Computer Society, IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, February 1987.

Shin:1994:NJA

[SM94] Dong Keun Shin and Arnold Charles Meltzer. A new join algorithm. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 23 (4):13–18, December 1994. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Sit:2002:SCP

[SM02] Emil Sit and Robert Morris. Security considerations for peer-to-peer distributed hash tables. *Lecture Notes in CS*, 2429:261–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2429/24290261.htm`; `http://link.springer.de/link/service/series/0558/papers/2429/24290261.pdf`.

Storer:2008:DDC

[SM08] James A. (James Andrew) Storer and Michael W. Marcellin, editors. *DCC 2008: 2008 Data Compression Conference: March 25–27, 2008, Snowbird, Utah: proceedings*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. ISBN 0-7695-3121-0. ISSN 1068-0314. LCCN QA76.9.D33 D372 2008; QA76.9.D33 INTERNET. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4483271`.

Storer:2012:DDC

[SM12] James A. Storer and Michael W. Marcellin, editors. *DCC 2012: 2012 Data Compression Conference: proceedings, 10–12 April 2012, Snowbird, Utah*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2012. ISBN 1-4673-0715-7 (paperback). ISSN 1068-0314. LCCN ???? URL `http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6189093`. IEEE Computer Society order number P4656.

Sriram:1991:VPC

[SMS91] Kotikalapudi Sriram, R. Scott McKinney, and Mostafa Hashem Sherif. Voice packetization and compression in broad-

band ATM networks. *IEEE Journal on Selected Areas in Communications*, 9(3): 294–304, April 1991. CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). IEEE Log Number 9042034.

Scionti:2018:EMM

[SMZ18] Alberto Scionti, Somnath Mazumdar, and Stephane Zuckerman. Enabling massive multi-threading with fast hashing. *IEEE Computer Architecture Letters*, 17(1):1–4, January/June 2018. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Sarkar:2019:CKN

[SN19] Pinaki Sarkar and Sukumar Nandi. A class of key-node indexed hash chains based key predistribution (KPS): Signed weighted graphs. *Computer Networks (Amsterdam, Netherlands: 1999)*, 164(??):Article 106881, December 9, 2019. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128618303669`.

Snader:1987:LIF

[Sna87] Jon C. Snader. Look it up faster with hashing. *Byte Magazine*, 12(1):128–144, January 1987. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Safavi-Naini:1998:MH

[SNBC98] Rei Safavi-Naini, Shahram Bakhtiari, and Chris Charnes. MRD hashing. *Lecture Notes in CS*, 1372:134–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1372/13720134.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1372/13720134.pdf`.

Safavi-naini:2005:MH

[SnC05] R. Safavi-naini and C. Charnes. MRD hashing. *Designs, Codes, and Cryptography*, 37 (2):229–242, November 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=37&issue=2&spage=229`.

Snellen:1992:ITS

[Sne92] David Snellen. Ingres table structures. *DBMS*, 5(8): 60–63, July 1992. CODEN DBMSEO. ISSN 1041-5173.

Safavi-Naini:2006:SSS

[SNW06] Rei Safavi-Naini and Huaxiong Wang. Secret sharing schemes with partial broadcast channels. *Designs, Codes, and Cryptography*, 41(1):5–22, October 2006.

CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=41&issue=1&spage=5.

Soloviev:1993:THA

[Sol93] V. Soloviev. A truncating hash algorithm for processing band-join queries. In Soloviev [ICD93], pages 419–427. ISBN 0-8186-3572-X (hardcover), 0-8186-3570-3 (paperback), 0-8186-3571-1 (microfiche). LCCN QA76.9.D3I57 1993.

Somervuo:1999:RHA

[Som99] P. Somervuo. Redundant hash addressing of feature sequences using the self-organizing map. *Neural Processing Letters*, 10(1):25–34, August 1999. CODEN ???? ISSN 1370-4621.

Soukup:1992:SCL

[Sou92] J. Soukup. Selecting a C++ library. *C++ Report*, 4(1):1, 4–6, January 1992. CODEN CRPTE7. ISSN 1040-6042.

Spetka:1989:THJ

[SP89] Scott Edward Spetka and Gerald Popek. Three-way hash join query processing in distributed relational database systems. Technical report, UCLA Computer Science Dept., Los Angeles, CA, USA, 1989. 17 pp.

Seberry:1990:ACA

[SP90] Jennifer Seberry and Josef Pieprzyk, editors. *Advances in Cryptology–AUSCRYPT '90: International Conference on Cryptology, Sydney, Australia, January 8–11, 1990: proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. ISBN 0-387-53000-2 (New York), 3-540-53000-2 (Berlin). LCCN QA76.9.A25 A87 1990.

Sadeghiyan:1991:COW

[SP91] B. Sadeghiyan and J. Pieprzyk. A construction for one way hash functions and pseudorandom bit generators. In Davies [Dav91], pages 431–445. ISBN 0-387-54620-0 (New York), 3-540-54620-0 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1991.

Satuluri:2012:BLS

[SP12] Venu Satuluri and Srinivasan Parthasarathy. Bayesian locality sensitive hashing for fast similarity search. *Proceedings of the VLDB Endowment*, 5(5):430–441, January 2012. CODEN ???? ISSN 2150-8097.

Shaikh:2021:STB

[SP21] Ayesha S. Shaikh and Vibha D. Patel. Significance of the transition to biometric template protection:

Explore the future. *International Journal of Image and Graphics (IJIG)*, 21(02): ??, April 2021. ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S021946782150025X`.

Spector:1988:CFD

[SPB88] A. Z. Spector, R. F. Pausch, and G. Bruell. CAMELOT: a flexible, distributed transaction processing system. In IEEE-COMPCON'88 [IEE88a], page ?? ISBN 0-8186-0828-5 (paperback), 0-8186-4828-7 (microfiche), 0-8186-8828-9 (hardcover). LCCN QA75.5 .C58 1988.

Spetka:1992:DAD

[Spe92] S. Spetka. A decomposition algorithm for distributed hash join query processing. In Yu [Yu92], pages 53–60. ISBN 0-8186-2660-7, 0-8186-2661-5, 0-8186-2662-3. LCCN QA76.9.D3 I593 1992.

Safkhani:2014:CCA

[SPLHCB14] Masoumeh Safkhani, Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, and Nasour Bagheri. Cryptanalysis of the Cho et al. protocol: a hash-based RFID tag mutual authentication protocol. *Journal of Computational and Applied Mathematics*, 259 (part B)(??): 571–577, March 15, 2014. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042713005281`. See [CJP12].

Sprugnoli:1977:PHF

[Spr77] Renzo Sprugnoli. Perfect hashing functions: a single probe retrieving method for static sets. *Communications of the Association for Computing Machinery*, 20(11): 841–850, November 1977. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). This is the first discussion on perfect hashing; describes heuristics for constructing perfect hash functions. See comments in [AA79a].

Sourlas:2016:EHR

[SPSP16] Vasilis Sourlas, Ioannis Psaras, Lorenzo Saino, and George Pavlou. Efficient hash-routing and domain clustering techniques for information-centric networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 103(??):67–83, July 5, 2016. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128616300998`.

Severance:1990:DLH

[SPW90] C. Severance, S. Pramanik, and P. Wolberg. Distributed linear hashing and parallel projection in main memory

databases. In McLeod et al. [MSDS90], page 674. ISBN 1-55860-149-X. LCCN ???

Schay:1963:MKA

[SR63] G. Schay and N. Raver. A method for key-to-address transformation. *IBM Journal of Research and Development*, 7(2):121–126, April 1963. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Sethi:1989:FSR

[SR89] Ishwar K. Sethi and Nagarajan Ramesh. A flexible shape recognition approach through hashing. In *Proc. ROBEX '89 (sponsored by Robotics and Expert Systems Division, Instrument Society of America)*, pages 185–188. ????, ????, 1989.

Song:2001:HMO

[SR01] Zhexuan Song and Nick Roussopoulos. Hashing moving objects. *Lecture Notes in CS*, 1987:161–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1987/19870161.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1987/19870161.pdf`.

Shin:1998:NHF

[SRRL98] Sang Uk Shin, Kyung Hyune Rhee, Dae Hyun Ryu, and Sang Jin Lee. A new hash function based on MDx-family and its application to MAC. *Lecture Notes in CS*, 1431:234–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1431/14310234.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1431/14310234.pdf`.

Shin:1999:HFM

[SRY99] Sang Uk Shin, Kyung Hyune Rhee, and Jae Woo Yoon. Hash functions and the MAC using all-or-nothing property. *Lecture Notes in CS*, 1560:263–275, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schay:1962:AFA

[SS62] G. Schay, Jr. and W. G. Spruth. Analysis of a file addressing method. *Communications of the Association for Computing Machinery*, 5(8): 459–462, August 1962. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Early analysis of linear probing.

Schmidt:1980:IPC

[SS80] Jeanette P. Schmidt and Eli Shamir. An improved program for constructing open

hash tables. In de Bakker and van Leeuwen [dBvL80], pages 569–581. ISBN 0-387-10003-2. LCCN QA267.A1 L43 no.85.

Shen:1983:OSU

[SS83] John Paul Shen and Michael A. Schuette. On-line self-monitoring using signatured instruction streams. *Digest of Papers — International Test Conference*, pages 275–282, 1983. CODEN DITCDP. ISBN 0-8186-0502-2. IEEE Service Cent. Piscataway, NJ, USA.

Schmidt:1988:SCO

[SS88a] Jeanette P. Schmidt and Alan Siegel. The spatial complexity of oblivious k—probe hash functions. Ultracomputer Note 142, ????, June 1988. ?? pp.

Shasha:1988:ECE

[SS88b] Dennis Shasha and Marc Snir. Efficient and correct execution of parallel programs that share memory. *ACM Transactions on Programming Languages and Systems*, 10(2):282–312, April 1988. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0164-0925/42277.html`.

Schmidt:1989:AUP

[SS89a] Jeanette P. Schmidt and Alan Siegel. On aspects of universality and performance for closed hashing. In ACM-TOC'89 [ACM89c], pages 355–366. ISBN 0-89791-307-8. LCCN ????

Sequin:1989:PRT

[SS89b] Carlo H. Séquin and Eliot K. Smyrl. Parameterized ray tracing. *Computer Graphics*, 23(3):307–314, July 1989. CODEN CGRADI, CPGPBZ. ISSN 0097-8930 (print), 1558-4569 (electronic). URL `http://www.acm.org:80/pubs/citations/proceedings/graph/74333/p307-sequin/`.

Schmidt:1990:ACH

[SS90a] Jeanette P. Schmidt and Alan Siegel. The analysis of closed hashing under limited randomness. In ACM-TOC'90 [ACM90], pages 224–234. ISBN 0-89791-361-2. LCCN ????

Schmidt:1990:SCO

[SS90b] Jeanette P. Schmidt and Alan Siegel. The spatial complexity of oblivious k-probe hash functions. *SIAM Journal on Computing*, 19(5): 775–786, October 1990. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Schmidt:1992:GPH

[SS92] Douglas C. Schmidt and Tatsuya Suda. GPERF: a perfect hash function generator.

Technical Report TR 92-47, Information and Computer Science, University of California, Irvine, Irvine, CA, USA, 1992. 19 pp.

Sarkar:2001:PAE

[SS01] P. Sarkar and P. J. Schellenberg. A parallel algorithm for extending cryptographic hash functions. *Lecture Notes in CS*, 2247:40–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470040.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2247/22470040.pdf`.

Shalev:2006:SOL

[SS06] Ori Shalev and Nir Shavit. Split-ordered lists: Lock-free extensible hash tables. *Journal of the Association for Computing Machinery*, 53(3):379–405, May 2006. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Smith:2015:BPF

[SS15] Jason Smith and Scott Schaefer. Bijective parameterization with free boundaries. *ACM Transactions on Graphics*, 34(4):70:1–70:??, August 2015. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Shpilrain:2016:CLF

[SS16] Vladimir Shpilrain and Bianca Sosnovski. Compositions of linear functions and applications to hashing. *Groups. Complexity. Cryptology*, 8 (2):155–161, November 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Sara:2001:SCT

[ŠSaS01] Radim Šára, Daniel Smutek, and Petr Sucharda andtŠtépán Svačina. Systematic construction of texture features for Hashimoto's lymphocytic thyroiditis recognition from sonographic images. *Lecture Notes in CS*, 2101:339–348, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2101/21010339.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2101/21010339.pdf`.

Shen:2018:MDH

[SSL+18] Xiaobo Shen, Fumin Shen, Li Liu, Yun-Hao Yuan, Weiwei Liu, and Quan-Sen Sun. Multiview discrete hashing for scalable multimedia search. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 9(5):

53:1–53:??, July 2018. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic).

Soomro:2005:DDH

[SSS05] H. K. Soomro, S. A. A. Shah, and A. A. G. Shaikh. Development of dynamic hashing key generation method for Java based Sindhi programming environment. *Mehran University Research Journal of Engineering and Technology*, 24(2):125–130, 2005. CODEN ???? ISSN 0254-7821.

Stipic:2013:PGT

[SSU+13] Srdan Stipić, Vesna Smiljković, Osman Unsal, Adrián Cristal, and Mateo Valero. Profile-guided transaction coalescing-lowering transactional overheads by merging transactions. *ACM Transactions on Architecture and Code Optimization*, 10(4):50:1–50:??, December 2013. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic).

Sagonas:1994:XED

[SSW94] Konstantinos Sagonas, Terrance Swift, and David S. Warren. XSB as an efficient deductive database engine. In Snodgrass and Winslett [SW94b], pages 442–453. ISBN 0-89791-639-5. ISSN 0163-5808 (print), 1943-5835 (electronic). LCCN QA 76.9 D3 S53 v.23 no.2 1994. URL `http://www.acm.org/pubs/articles/proceedings/mod/191839/p442-sagonas/p442-sagonas.pdf`; `http://www.acm.org/pubs/citations/proceedings/mod/191839/p442-sagonas/`.

Schkolnick:1983:ICV

[ST83a] Mario Schkolnick and C. Thanos, editors. *9th International Conference on Very Large Data Bases: Florence, Italy, October 31–November 2, 1983*. Very Large Data Bases Endowment, Saratoga, CA, USA, 1983.

Schkolnick:1983:NIC

[ST83b] Mario Schkolnick and Costantino Thanos, editors. *Ninth International Conference on Very Large Data Bases, Florence, Italy, October 31-November 2, 1983*. Very Large Data Bases Endowment, Saratoga, CA, USA, 1983. ISBN 0-934613-15-X. LCCN QA 76.9 D3 I61 1983.

Sebesta:1985:MPH

[ST85] Robert W. Sebesta and Mark A. Taylor. Minimal perfect hash functions for reserved word lists. *SIGPLAN Notices*, 20(12):47–53, December 1985. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Sebesta:1986:FIA

[ST86] Robert W. Sebesta and Mark A. Taylor. Fast identification of Ada and Modula-2 reserved words. *Journal of Pascal, Ada and Modula-2*, 5 (2):36–39, March/April 1986. CODEN JPAME8, JOPAD5. ISSN 0747-1351, 0735-1232.

Schweitz:1993:AHS

[ST93] Eric A. Schweitz and Alan L. Tharp. Adaptive hashing with signatures. *Information system*, 18(8):597–??, 1993. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Stahl:1973:HGH

[Sta73] Hans Michael Stahl. Hashcodingverfahren. (German). [Hash coding techniques]. *Angewandte Informatik/Applied Informatics*, 15(10):435–440, October 1973. CODEN AWIFA7.

Stallings:1994:SSH

[Sta94] William Stallings. SHA: The Secure Hash Algorithm. *Dr. Dobbs Journal*, 19(4):32, 34, April 1, 1994. CODEN DDJOEB. ISSN 1044-789X.

Stallings:1999:HAK

[Sta99] William Stallings. The HMAC algorithm: Key hashing for message authentication. *Dr. Dobbs Journal*, 24(4):46, 48–49, April 1999. CODEN DDJOEB. ISSN 1044-789X. URL `http://www.ddj.com/ftp/1999/1999_04/hmac.txt`.

Stallings:2006:WSH

[Sta06a] William Stallings. The Whirlpool secure hash function. *Cryptologia*, 30(1): 55–67, January 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741992009~db=all~order=page`.

Stamp:2006:ISP

[Sta06b] Mark Stamp. *Information security: principles and practice*. Wiley-Interscience, New York, NY, USA, 2006. ISBN 0-471-73848-4 (cloth). xxi + 390 pp. LCCN QA76.9.A25 S69 2006. URL `http://www.loc.gov/catdir/enhancements/fy0645/2005005152-b.html`; `http://www.loc.gov/catdir/enhancements/fy0645/2005005152-d.html`; `http://www.loc.gov/catdir/toc/ecip058/2005005152.html`.

Stewart:1982:DSV

[Ste82] Neil Stewart. Data structures for virtual-circuit implementation. *Computer Communications*, 5(4):196–201, August 1982. CODEN COCOD7. ISSN 0140-3664 (print), 1873-703X (electronic).

Stevens:2018:HPL

[Ste18] Hallam Stevens. Hans Peter Luhn and the birth of the hashing algorithm. *IEEE Spectrum*, 55(2):44–49, February 2018. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Stinson:1991:UHA

[Sti91] D. R. Stinson. Universal hashing and authentication codes. *Lecture Notes in CS*, 576:74–85, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stinson:1993:ACC

[Sti93] Douglas R. Stinson, editor. *Advances in Cryptology, CRYPTO '93: 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22–26, 1993: Proceedings*, volume 773 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). LCCN QA76.9.A25 C79 1993.

Stinson:1994:CTU

[Sti94a] D. R. Stinson. Combinatorial techniques for universal hashing. *Journal of Computer and System Sciences*, 48(2): 337–346, April 1, 1994. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic).

Stinson:1994:UHA

[Sti94b] D. R. Stinson. Universal hashing and authentication codes. *Designs, Codes, and Cryptography*, 4(4):369–380, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

Stinson:1994:ACC

[Sti94c] Douglas R. Stinson, editor. *Advances in Cryptology, CRYPTO '93: 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22–26, 1993: Proceedings*, volume 773 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. CODEN LNCSD9. ISBN 0-387-57766-1 (New York), 3-540-57766-1 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1993. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0773.htm`; `http://www.springerlink.com/content/978-0-387-57766-1`; `http://www.springerlink.com/openurl.`

asp?genre=issue&issn=0302-9743&volume=773.

Stinson:2006:SOT

[Sti06] D. R. Stinson. Some observations on the theory of cryptographic hash functions. *Designs, Codes, and Cryptography*, 38(2):259–277, February 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=38&issue=2&spage=259.

Stonebraker:1988:RDS

[Sto88] Michael Stonebraker, editor. *Readings in Database Systems*. Morgan Kaufmann Publishers, San Francisco, CA, 1988. ISBN 0-934613-65-6. xii + 644 pp. LCCN QA76.9.D3 R4 1988. US$29.95. Contains reprint of [Lit80].

Stonebraker:1992:PAS

[Sto92] Michael Stonebraker, editor. *Proceedings of the 1992 ACM SIGMOD International Conference on Management of Data, San Diego, California, June 2–5, 1992*, volume 21(2) of *SIGMOD Record (ACM Special Interest Group on Management of Data)*. ACM Press, New York, NY 10036, USA, 1992. ISBN 0-89791-521-6. ISSN 0163-5808 (print), 1943-5835 (electronic). LCCN ????

Sundaram:2013:SSS

[STS+13] Narayanan Sundaram, Aizana Turmukhametova, Nadathur Satish, Todd Mostak, Piotr Indyk, Samuel Madden, and Pradeep Dubey. Streaming similarity search over one billion tweets using parallel locality-sensitive hashing. *Proceedings of the VLDB Endowment*, 6(14):1930–1941, September 2013. CODEN ???? ISSN 2150-8097.

Stumm:1982:UMZ

[Stu82] Gisela Stumm. Untersuchung zu mehrfachattribut-zugriffsverfahren fuer datenbanken. Master's thesis, Technischen Universität Carolo-Wilhelmina zu Braunschweig, Braunschweig, Germany, 1982. ?? pp.

Sturc:1985:MHU

[Stu85] Jan Sturc. Multidimensional hashing used for conjunctive queries evaluation. *Computers and Artificial Intelligence = Vychislitel'nye mashiny i iskusstvennyi intellekt*, 4(2): 143–151, 1985. CODEN CARIDY. ISSN 0232-0274.

Samples:1986:SSB

[SUH86] A. D. Samples, D. Ungar, and P. Hilfinger. SOAR: Smalltalk without bytecodes. *SIGPLAN Notices*, 21(11): 107, November 1986. CODEN SINODQ. ISSN 0362-1340 (print), 1523-

2867 (print), 1558-1160 (electronic).

Sundar:1991:LBD

[Sun91] R. Sundar. A lower bound for the dictionary problem under a hashing model. In IEEE-FOCS'91 [IEE91b], pages 612–621. ISBN 0-8186-2445-0 (paperback), 0-8186-2447-7 (hardcover). LCCN QA 76 S979 1991.

Sundar:1993:LBC

[Sun93] R. Sundar. A lower bound on the cell probe complexity of the dictionary problem. Cited in [ANS09], but perhaps never published., 1993.

Sun:2002:BJP

[Sun02] Sun Microsystems. *BigDecimal (Java 2 Platform SE v1.4.0)*. Sun Microsystems, Mountain View, CA, USA, 2002. 17 pp. URL `http://java.sun/com/products`.

Sun:2015:CCH

[Sun15] Zhenan Sun. Code consistent hashing based on information-theoretic criterion. *IEEE Transactions on Big Data*, 1(3):84–94, September 2015. CODEN ???? ISSN 2332-7790.

Schnorr:1994:PFH

[SV94a] C. Schnorr and S. Vaudenay. Parallel FFT-Hashing. *Lecture Notes in CS*, 809: 149–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schnorr:1994:BBC

[SV94b] C. P. Schnorr and S. Vaudenay. Black box cryptanalysis of hash networks based on multipermutations. Technical Report TR-94-017, International Computer Science Institute, Berkeley, CA, USA, April 1994. ?? pp.

Schnorr:1995:BBC

[SV95] C. P. Schnorr and S. Vaudenay. Black box cryptanalysis of hash networks based on multipermutations. In De Santis [De 95], pages 47–57. ISBN 3-540-60176-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E965 1995.

Suganya:2006:LRK

[SV06] A. Suganya and N. Vijayarangan. Landau–Ramanujan keyed hash functions for message authentication. *Journal of Discrete Mathematical Sciences and Cryptography*, 9 (1):1–8, 2006. CODEN ???? ISSN 0972-0529.

Steindorfer:2015:CSM

[SV15a] Michael J. Steindorfer and Jurgen J. Vinju. Code specialization for memory efficient hash tries (short paper). *SIGPLAN Notices*, 50(3):11–14, March 2015. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Steindorfer:2015:OHA

[SV15b] Michael J. Steindorfer and Jurgen J. Vinju. Optimizing hash-array mapped tries for fast and lean immutable JVM collections. *SIGPLAN Notices*, 50(10):783–800, October 2015. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Steindorfer:2018:MOA

[SV18] Michael J. Steindorfer and Jurgen J. Vinju. To-many or to-one? All-in-one! Efficient purely functional multi-maps with type-heterogeneous hash-tries. *SIGPLAN Notices*, 53(4):283–295, April 2018. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Stanca:2001:HAC

[SVCC01] Marian Stanca, Stamatis Vassiliadis, Sorin Cotofana, and Henk Corporaal. Hashed addressed caches for embedded pointer based codes (research note). *Lecture Notes in CS*, 1900:965–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1900/19000965.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1900/19000965.pdf`.

Slot:1984:TVC

[SvEB84] C. Slot and P. van Emde Boas. On tape versus core: An application of space efficient perfect hash functions to the invariance of space. In ACM-TOC'84 [ACM84b], pages 391–400.

Sincovec:1986:DSU

[SW86] R. F. Sincovec and R. S. Wiener. *Data Structures Using Modula-2*. John Wiley, New York, NY, USA, 1986. ISBN 0-471-81489-X. xxiii + 500 pp. LCCN QA76.73.M63 S56 1986.

Stubbs:1987:DSA

[SW87] Daniel F. Stubbs and Neil W. Webre. *Data Structures with Abstract Data Types and Modula-2*. Brooks/Cole, Pacific Grove, CA, USA, 1987. ISBN 0-534-07302-6. xx + 556 pp. LCCN QA76.9.D35 S76 1987. US$43.25. Textbook treatment of hashing.

Shasha:1991:OEQ

[SW91] Dennis Shasha and Tsong-Li Wang. Optimizing equijoin queries in distributed databases where relations are hash-partitioned. *ACM Transactions on Database Systems*, 16(2):279–??, June 1, 1991. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Snodgrass:1994:SIC

[SW94a] R. T. Snodgrass and M. Winslett, editors. *SIGMOD '94: International conference on management of data — May 1994, Minneapolis, MN*, volume 23 (2) of *SIGMOD RECORD 1994*. ACM Press, New York, NY 10036, USA, 1994. ISBN 0-89791-639-5. ISSN 0163-5808 (print), 1943-5835 (electronic). LCCN QA 76.9 D3 S53 v.23 no.2 1994.

Snodgrass:1994:PAS

[SW94b] Richard T. Snodgrass and Marianne Winslett, editors. *Proceedings of the 1994 ACM SIGMOD International Conference on Management of Data / SIGMOD '94, Minneapolis, Minnesota, May 24–27, 1994*, volume 23(2) of *SIGMOD Record (ACM Special Interest Group on Management of Data)*. ACM Press, New York, NY 10036, USA, 1994. ISBN 0-89791-639-5. ISSN 0163-5808 (print), 1943-5835 (electronic). LCCN QA 76.9 D3 S53 v.23 no.2 1994.

Sun:2014:SSA

[SWQ+14] Yifang Sun, Wei Wang, Jianbin Qin, Ying Zhang, and Xuemin Lin. SRS: solving c-approximate nearest neighbor queries in high dimensional Euclidean space with a tiny index. *Proceedings of the VLDB Endowment*, 8(1): 1–12, September 2014. CODEN ???? ISSN 2150-8097.

Sun:2018:MSM

[SWTX18] P. Sun, Y. Wen, D. N. B. Ta, and H. Xie. MetaFlow: A scalable metadata lookup service for distributed file systems in data centers. *IEEE Transactions on Big Data*, 4(2):203–216, June 2018. ISSN 2332-7790.

Shen:2008:HBP

[SX08] Haiying Shen and Cheng-Zhong Xu. Hash-based proximity clustering for efficient load balancing in heterogeneous DHT networks. *Journal of Parallel and Distributed Computing*, 68(5): 686–702, May 2008. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic).

Su:2016:PSN

[SXL16] Shenghui Su, Tao Xie, and Shuwang Lü. A provably secure non-iterative hash function resisting birthday attack. *Theoret. Comput. Sci.*, 654(??):128–142, November 22, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397516001547`.

Sung:2008:LSI

[SXLL08] Minho Sung, Jun Xu, Jun Li, and Li Li. Large-

scale IP traceback in high-speed Internet: practical techniques and information-theoretic foundation. *IEEE/ACM Transactions on Networking*, 16(6):1253–1266, December 2008. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Seltzer:1991:NHP

[SY91] Margo Seltzer and Ozan Yigit. A new hashing package for UNIX. In USENIX-WINTER'91 [USE91], pages 173–184.

Shibata:2008:LFD

[SY08] Tomoyuki Shibata and Osamu Yamaguchi. Local Fisher discriminant component hashing for fast nearest neighbor classification. *Lecture Notes in CS*, 5342: 339–349, 2008. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-89689-0_38`.

Sasaki:2011:KKD

[SY11] Yu Sasaki and Kan Yasuda. Known-key distinguishers on 11-round Feistel and collision attacks on its hashing modes. *Lecture Notes in CS*, 6733:397–415, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-21702-9_23`.

Shao:2020:HCS

[SYW+20] T. Shao, Y. Yang, Y. Weng, Q. Hou, and K. Zhou. H-CNN: Spatial hashing based CNN for 3D shape analysis. *IEEE Transactions on Visualization and Computer Graphics*, 26(7):2403–2416, 2020. CODEN ITVGEA. ISSN 1077-2626.

Seberry:1993:ACA

[SZ93] Jennifer Seberry and Yuliang Zheng, editors. *Advances in Cryptology–AUSCRYPT '92: Workshop on the Theory and Application of Cryptographic Techniques, Gold Coast, Queensland, Australia, December 13–16, 1992: Proceedings*, volume 718 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-57220-1 (New York), 3-540-57220-1 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 A87 1992.

Sun:2020:RRL

[SZO+20] Guolin Sun, Tong Zhan, Boateng Gordon Owusu, Ayepah-Mensah Daniel, Guisong Liu, and Wei Jiang. Revised reinforcement learning based on anchor graph hashing for autonomous cell activation in

cloud-RANs. *Future Generation Computer Systems*, 104(??):60–73, March 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X18318788`.

Szymanski:1982:HTR

[Szy82] Thomas G. Szymanski. Hash table reorganization. In *Proceedings of the 1982 Conference on Information Sciences and Systems.*, pages 480–484. Princeton University Press, Princeton, NJ, USA, 1982.

Szymanski:1985:HTR

[Szy85] T. G. Szymanski. Hash table reorganization. *Journal of Algorithms*, 6(3):322–325, September 1985. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic).

Tenenbaum:1981:DSU

[TA81] Aaron M. Tenenbaum and Moshe J. Augenstein. *Data Structures Using Pascal*. Prentice-Hall Software Series, Editor: Brian W. Kernighan. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1981. ISBN 0-13-196501-8. xiv + 545 pp. LCCN QA76.9.D35 T46.

Tenenbaum:1986:DSU

[TA86] Aaron M. Tenenbaum and Moshe J. Augenstein. *Data Structures Using Pascal*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, second edition, 1986. ISBN 0-13-196668-5. x + 774 pp. LCCN QA76.9.D35 T46 1986. US$36.95. New section on dynamic hashing added for this edition.

Tai:1979:IPT

[Tai79] Kuo-Chung Tai. On the implementation of parsing tables. *SIGPLAN Notices*, 14 (1):100–101, January 1979. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Tamminen:1981:OPE

[Tam81] Markku Tamminen. Order preserving extendible hashing and bucket tries. *BIT (Nordisk tidskrift for informationsbehandling)*, 21(4): 419–435, 1981. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Tamminen:1982:EHO

[Tam82] Markku Tamminen. Extendible hashing with overflow. *Information Processing Letters*, 15(5):227–232, December 1982. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Tamminen:1985:SAC

[Tam85] Markku Tamminen. On search by address compu-

tation. *BIT (Nordisk tidskrift for informationsbehandling)*, 25(1):135–147, 1985. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). Discusses hashing applications to file searching.

Tanaka:1983:DSD

[Tan83] Y. Tanaka. A data-stream database machine with large capacity. In *Advanced Database Machine Architecture* [Hsi83], pages 168–202. ISBN 0-13-011262-3. LCCN QA76.9.D3 A343 1983.

Taylor:1989:SIA

[Tay89] Jeff Taylor. String-indexed arrays in C++. *Computer Language Magazine*, 6(12): 43–??, December 1, 1989. CODEN COMLEF. ISSN 0749-2839.

Tharp:1991:TBD

[TB91] Alan L. Tharp and William Boswell. B^+ trees, bounded disorder and adaptive hashing. *Information system*, 16(1):65–72, 1991. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Tang:2005:LTO

[TBC+05] Chunqiang Tang, Melissa J. Buco, Rong N. Chang, Sandhya Dwarkadas, Laura Z. Luan, Edward So, and Christopher Ward. Low traffic overlay networks with large routing tables. *ACM SIGMETRICS Performance Evaluation Review*, 33(1):14–25, June 2005. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Tsichritzis:1983:MF

[TC83] D. Tsichritzis and S. Christodoulakis. Message files. *ACM Transactions on Office Information Systems*, 1(1):88–98, January 1983. CODEN ATOSDO. ISSN 0734-2047. URL `http://www.acm.org:80`. Discusses application of hashing to signatures for text searching.

Tang:1993:URH

[TC93] S. M. Tang and L. R. Chow. Using rank hashing function to develop a data allocating scheme for a two-disk system. *The Journal of Systems and Software*, 22(2): 107–116, August 1, 1993. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Tang:2004:AHR

[TC04] Xueyan Tang and Samuel T. Chanson. Adaptive hash routing for a cluster of client-side Web proxies. *Journal of Parallel and Distributed Computing*, 64(10): 1168–1184, October 2004. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic).

Trinder:2017:SRI

[TCP+17] Phil Trinder, Natalia Chechina, Nikolaos Papaspyrou, Konstantinos Sagonas, Simon Thompson, Stephen Adams, Stavros Aronis, Robert Baker, Eva Bihari, Olivier Boudeville, Francesco Cesarini, Maurizio Di Stefano, Sverker Eriksson, Viktória Fördős, Amir Ghaffari, Aggelos Giantsios, Rickard Green, Csaba Hoch, David Klaftenegger, Huiqing Li, Kenneth Lundin, Kenneth Mackenzie, Katerina Roukounaki, Yiannis Tsiouris, and Kjell Winblad. Scaling reliably: Improving the scalability of the Erlang distributed actor platform. *ACM Transactions on Programming Languages and Systems*, 39(4):17:1–17:??, September 2017. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic).

Tang:2013:TOH

[TCW+13] Jinhui Tang, Qiang Chen, Meng Wang, Shuicheng Yan, Tat-Seng Chua, and Ramesh Jain. Towards optimizing human labeling for interactive image tagging. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 9 (4):29:1–29:??, August 2013. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Tang:2020:VHD

[TCY+20] Zhenjun Tang, Lv Chen, Heng Yao, Xianquan Zhang, and Chunqiang Yu. Video hashing with DCT and NMF. *The Computer Journal*, 63 (7):1017–1030, July 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/63/7/1017/5540176`.

Turau:1993:ETC

[TD93] V. Turau and H. Duchene. Equality testing for complex objects based on hashing. *Data and Knowledge Engineering*, 10(1):101–112, February 1993. CODEN DKENEW. ISSN 0169-023X (print), 1872-6933 (electronic).

Terashima:1987:EPL

[Ter87] Motoaki Terashima. Extended property list — its concept and applications. *Journal of the Information Processing Society of Japan*, 10(3):154–160, 1987. CODEN JIPRDE. ISSN 0387-6101.

Tenenhaus:2010:GAN

[TGGF10] Arthur Tenenhaus, Vincent Guillemot, Xavier Gidrol, and Vincent Frouin. Gene association networks from microarray data using a regularized estimation of partial correlation based on PLS regression. *IEEE/ACM Transac-*

tions on Computational Biology and Bioinformatics, 7 (2):251–262, April 2010. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Tomasic:1997:DSE

[TGL+97] Anthony Tomasic, Luis Gravano, Calvin Lue, Peter Schwarz, and Laura Haas. Data structures for efficient broker implementation. *ACM Transactions on Information Systems*, 15(3):223–253, July 1997. CODEN ATISET. ISSN 1046-8188. URL `http://www.acm.org:80/tois/abstracts/tomasic.html`.

Tharp:1988:FOP

[Tha88] Alan L. Tharp. *File Organization and Processing*. John Wiley, New York, NY, USA, 1988. ISBN 0-471-60521-2. xv + 398 pp. LCCN QA76.9.F5 T48 1988. US$28.00. Textbook treatment of hashing in Chapter 7.

Thorup:2000:ESU

[Tho00] Mikkel Thorup. Even strongly universal hashing is pretty fast. In Shmoys [Shm00], pages 496–497. ISBN 0-89871-453-2. LCCN QA76.6 .A278 2000. URL `http://encompass.library.cornell.edu/cgi-bin/checkIP.cgi?access=gateway\_standard\%26url=http://dl.acm.org/citation.cfm?id=338219`.

Thorup:2013:STF

[Tho13] M. Thorup. Simple tabulation, fast expanders, double tabulation, and high independence. In IEEE [IEE13], pages 90–99. ISBN 0-7695-5135-1. ISSN 0272-5428. LCCN QA76 .S95 2012. URL `http://dimacs.rutgers.edu/FOCS13/`; `http://theory.stanford.edu/~tim/focs13/`. IEEE Computer Society order number P????.

Thorup:2017:FPH

[Tho17] Mikkel Thorup. Fast and powerful hashing using tabulation. *Communications of the Association for Computing Machinery*, 60(7): 94–101, July 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2017/7/218878/fulltext`.

Taylor:1997:AHN

[THS97] Stephen Taylor, Nabil Hachem, and Stanley Selkow. The average height of a node in the BANG abstract directory tree. *Information Processing Letters*, 61(1):55–61, January 14, 1997. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Tang:2018:PIH

[THY+18] Zhenjun Tang, Ziqing Huang, Heng Yao, Xianquan Zhang, Lv Chen, and Chunqiang Yu. Perceptual image hashing with weighted DWT features for reduced-reference image quality assessment. *The Computer Journal*, 61 (11):1695–1709, November 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/61/11/1695/4993055`.

Tao:2012:HCG

[TI12] Liang Tao and Horace H. S. Ip. Hashing with Cauchy graph. *Lecture Notes in CS*, 7674:21–32, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-34778-8_3/`.

Thakkar:1985:VAT

[TK85] Shreekant S. Thakkar and Alan E. Knowles. *Virtual Address Translation Using Parallel Hashing Hardware*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1985. ISBN 0-8186-0654-1. 697–705 pp. LCCN ???? IEEE Service Cent. Piscataway, NJ, USA.

Tanaka:1988:HSS

[TK88] Eiichi Tanaka and Atsuko Kogawara. High speed string edit methods using hierarchical files and hashing technique. In IEEE-ICPR'88 [IEE88d], pages 334–336. CODEN PICREG. ISBN 0-8186-0878-1. LCCN ???? Available from IEEE Service Cent (catalog number 88CH2614-6). Piscataway, NJ, USA.

Tran:2007:FBC

[TK07] Thinh Ngoc Tran and Surin Kittitornkun. FPGA-based cuckoo hashing for pattern matching in NIDS/NIPS. *Lecture Notes in CS*, 4773:334–343, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-75476-3_34`.

Tibouchi:2017:IEC

[TK17] Mehdi Tibouchi and Taechan Kim. Improved elliptic curve hashing and point representation. *Designs, Codes, and Cryptography*, 82(1–2):161–177, January 2017. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s10623-016-0288-2`; `http://link.springer.com/article/10.1007/s10623-016-0288-2`.

Takemasa:2020:DPF

[TKH20] Junji Takemasa, Yuki Koizumi, and Toru Hasegawa. Data prefetch for fast NDN software routers based on hash table-based forwarding tables. *Computer Networks (Amsterdam, Netherlands: 1999)*, 173(??):Article 107188, May 22, 2020. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S138912861931196X`.

Torres:1999:SIS

[TKI99] Marco A. Torres, Susumu Kuroyanagi, and Akira Iwata. The Self-Indexed Search Algorithm: a bit-level approach to minimal perfect hashing. *Information Processing Letters*, 69(5):253–258, March 12, 1999. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Takata:1989:MMM

[TKT+89] H. Takata, S. Komori, T. Tamura, F. Asai, T. Tokuda, K. Shima, H. Nishikawa, and H. Terada. 100 mega-access matching memory for a data-driven microprocessor. In *Symposium on VLSI Circuits Digest of Technical Papers (May 25–27 1989: Kyoto, Japan)*, pages 123–124. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. IEEE catalog number 89TH0262-6.

Tan:1993:RSM

[TL93] Kian-Lee Tan and Hongium Lu. On resource scheduling of multi-join queries in parallel database systems. *Information Processing Letters*, 48(4):189–195, November 29, 1993. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Tang:1995:SLO

[TL95] S. M. Tang and R. Chow Louis. The study of letter-oriented hashing schemes. *The Journal of Systems and Software*, 28(2):157–167, February 1, 1995. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Tseng:2007:DHS

[TLLL07] Kuo-Kun Tseng, Ying-Dar Lin, Tsern-Huei Lee, and Yuan-Cheng Lai. Deterministic high-speed root-hashing automaton matching coprocessor for embedded network processor. *ACM SIGARCH Computer Architecture News*, 35(3):36–43, June 2007. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Tseng:2009:FSA

[TLLL09] Kuo-Kun Tseng, Yuan-Cheng Lai, Ying-Dar Lin,

and Tsern-Huei Lee. A fast scalable automaton-matching accelerator for embedded content processors. *ACM Transactions on Embedded Computing Systems*, 8(3):19:1–19:??, April 2009. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Thai:2018:TLB

[TLLL18] Minh-Tuan Thai, Ying-Dar Lin, Po-Ching Lin, and Yuan-Cheng Lai. Towards load-balanced service chaining by Hash-based Traffic Steering on Softswitches. *Journal of Network and Computer Applications*, 109 (??):1–10, May 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804518300699`.

Tang:2016:RIH

[TLZL16] Zhenjun Tang, Huan Lao, Xianquan Zhang, and Kai Liu. Robust image hashing via DCT and LLE. *Computers and Security*, 62(??): 133–148, September 2016. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404816300852`.

Tubaishat:2002:PEL

[TMB02] Malik Ayed Tubaishat, Sanjay Kumar Madria, and Bharat Bhargava. Performance evaluation of linear hash structure model in a nested transaction environment. *The Journal of Systems and Software*, 63(3): 219–239, September 15, 2002. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Triplett:2010:SCH

[TMW10] Josh Triplett, Paul E. McKenney, and Jonathan Walpole. Scalable concurrent hash tables via relativistic programming. *Operating Systems Review*, 44(3): 102–109, July 2010. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Tsudaka:1992:PHJ

[TNKT92] S.-I. Tsudaka, M. Nakano, M. Kitsuregawa, and M. Takagi. Parallel hash join on shared-everything multiprocessor: Implementation and performance evaluation. In Golshani [Gol92], page ?? ISBN 0-8186-2545-7 (paper) 0-8186-2546-5 (microfiche) 0-8186-2547-3 (hardcover). LCCN QA76.9.D3 I5582 1992.

Tomkins:2020:NZT

[TNS20] Hayley Tomkins, Monica Nevins, and Hadi Salmasian. New Zémor–Tillich type hash functions over $\mathrm{GL}_2(\mathbf{F}_{p^n})$. *Journal of Mathematical*

Cryptology, 14(1):236–253, August 1, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL `https://www.degruyter.com/document/doi/10.1515/jmc-2019-0033/html`.

Toptsis:1992:LBP

[Top92] Anestis A. Toptsis. Load balancing in parallel hash join with data skew. In Finin et al. [FNY92], page ?? ISBN 0-387-57419-0 (New York), 3-540-57419-0 (Berlin). LCCN QA76.9.D3 I5586 1992.

Torn:1984:HOI

[Tor84] Aimo A. Torn. Hashing with overflow indexing. *BIT (Nordisk tidskrift for informationsbehandling)*, 24(3): 317–332, 1984. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Toyama:1986:DOQ

[Toy86] M. Toyama. Data organizations and query processing in database systems. In Chu et al. [CGO86], pages 25–32. ISBN 0-934613-18-4. LCCN QA76.9.D3 I559 1986.

Toyama:1993:JAM

[Toy93] Motomichi Toyama. Join algorithm for multidimensional linear hash databases. *Advances in software science and technology*, 4(??):43–62, 1993. ISSN 1044-7997.

Tout:1995:DLB

[TP95] W. R. Tout and S. Pramanik. Distributed load balancing for parallel main memory hash join. *IEEE Transactions on Parallel and Distributed Systems*, 6(8):841–??, August 1, 1995. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Tong:2015:HTS

[TP15] Da Tong and Viktor Prasanna. High throughput sketch based online heavy hitter detection on FPGA. *ACM SIGARCH Computer Architecture News*, 43(4):70–75, September 2015. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Taniar:2002:PSH

[TR02] David Taniar and J. Wenny Rahayu. Parallel sort-hash object-oriented collection join algorithms for shared-memory machines. *Parallel Algorithms and Applications*, 17(2):85–126, ???? 2002. CODEN PAAPEC. ISSN 1063-7192. URL `http://www.informaworld.com/smpp/content~content=a777924083`.

Trainiter:1963:ARA

[Tra63] M. Trainiter. Addressing for random-access storage with multiple bucket capabilities. *Journal of the Association*

for Computing Machinery, ??(3):307–315, July 1963. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Thom:1986:SAD

[TRN86] J. A. Thom, K. Ramamohanarao, and L. Naish. A superjoin algorithm for deductive databases. In Chu et al. [CGO86], pages 189–196. ISBN 0-934613-18-4. LCCN QA76.9.D3 I559 1986.

Trono:1992:UPC

[Tro92] John A. Trono. An undergraduate project to compute minimal perfect hashing functions. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 24(3):??, 1992. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Trono:1995:CTS

[Tro95] John A. Trono. A comparison of three strategies for computing letter oriented, minimal perfect hashing functions. *SIGPLAN Notices*, 30(4):29–35, April 1, 1995. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). This paper introduces a simple modification that produces dramatic speedups to the algorithms of Cichelli [Cic80b] and Cook and Oldehoeft [CO82b].

Trono:2006:OTL

[Tro06] John A. Trono. Optimal table lookup for reserved words in Ada. *ACM SIGADA Ada Letters*, 26(1): 25–30, April 2006. CODEN AALEE5. ISSN 1094-3641 (print), 1557-9476 (electronic).

Tremblay:1976:IDS

[TS76] J. P. Tremblay and P. G. Sorenson. *An Introduction to Data Structures With Applications*. McGraw-Hill, New York, NY, USA, 1976. ISBN 0-07-065150-7. xvi + 704 pp. LCCN QA76.9.D35 .T73.

Tremblay:1984:IDS

[TS84] J. P. Tremblay and P. G. Sorenson. *An Introduction to Data Structures With Applications*. McGraw-Hill, New York, NY, USA, second edition, 1984. ISBN 0-07-065157-4. xviii + 861 pp. LCCN QA76.9.D35 T73 1984. Hashing is covered in section 6–2.4.

Tilchin:1985:EDS

[TS85] O. T. Til'chin and O. L. Shor. Efficient data storage and retrieval organization using the frequency properties of the query stream. *Programming and Computer Software; translation of Programmirovaniye, (Moscow, USSR) Plenum*, 11(6):364–368, November–December 1985. CODEN

PCSODA. ISSN 0361-7688 (print), 1608-3261 (electronic).

Tsai:1994:GHL

[Tsa94] F. C. D. Tsai. Geometric hashing with line features. *Pattern Recognition*, 27(3): 377–??, March 1994. CODEN PTNRA8. ISSN 0031-3203 (print), 1873-5142 (electronic).

Tsai:1996:PAG

[Tsa96] Frank C. D. Tsai. A probabilistic approach to geometric hashing using line features. *Computer vision and image understanding: CVIU*, 63(1):182–195, January 1996. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic).

Tsai:2008:EMS

[Tsa08] Jia-Lun Tsai. Efficient multi-server authentication scheme based on one-way hash function without verification table. *Computers and Security*, 27(3–4): 115–121, May/June 2008. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404808000084`.

Tsoukalos:2015:HTP

[Tso15] Mihalis Tsoukalos. Hash tables — theory and practice. *Linux Journal*, 2015(256): 2:1–2:??, August 2015. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL `http://dl.acm.org/ft_gateway.cfm?id=2830288`.

Turan:2011:SRS

[TSP+11] Turan, M. S., R. Perlner, L. E. Bassham, W. Burr, D. Chang, S. Chang, M. Dworkin, J. Kelsey, J. M. Paul, and R. Peralta. Status report on the Second Round of the SHA-3 Cryptographic Hash Algorithm Competition. NIST Interagency Report 7764, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, February 2011. URL `http:/csrc.nist.gov/groups/ST/hash/sha-3/Round2/documents/Round2_Report_NISTIR_7764.pdf`.

Tsudik:1992:MAOa

[Tsu92a] G. Tsudik. Message authentication with one-way hash functions. *Computer Communication Review*, 22(5): 29–38, October 1, 1992. CODEN CCRED2. ISSN 0146-4833.

Tsudik:1992:MAOb

[Tsu92b] G. Tsudik. Message authentication with one-way hash functions. In IEEE [IEE92a], page ?? Three volumes. IEEE Computer Society order number 2860. IEEE catalog number 92CH3133-6.

Thomlinson:1998:NBP

[TSY98] Matthew W. Thomlinson, Daniel R. Simon, and Bennet Yee. Non-biased pseudo random number generator. United States Patent 5,778,069., July 7, 1998. URL `http:www.google.com/patents/US5778069`.

Tai:1981:CCH

[TT81] K.-C Tai and A. L. Tharp. Computed chaining: a hybrid of direct chaining and open addressing. *Information system*, 6(2):111–116, 1981. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Tharp:1982:PTS

[TT82] Alan L. Tharp and Kuo-Chung Tai. The practicality of text signatures for accelerating string searching. *Software—Practice and Experience*, 12(1):35–44, January 1982. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic). Expands Harrison's work [Har71a].

Tai:1986:CCC

[TT86] K. C. Tai and A. L. Tharp. A comparison of computed chaining to predictors. *IEEE Transactions on Software Engineering*, SE-12(8):870–874, August 1986. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6312990`.

Talia:2010:EDQ

[TT10] Domenico Talia and Paolo Trunfio. Enabling dynamic querying over distributed hash tables. *Journal of Parallel and Distributed Computing*, 70(12):1254–1265, December 2010. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic).

Tian:1993:NHF

[TTY93] Z. Tian, S. Tong, and S. Yang. A new hashing function: Statistical behavior and algorithm. *SIGIR forum*, 27 (1):3–??, Spring 1993. CODEN FASRDV. ISSN 0163-5840.

Torenvliet:1983:ROT

[Tv83] Leen Torenvliet and P. van Emde Boas. The reconstruction and optimization of trie hashing functions. In Schkolnick and Thanos [ST83a], pages 142–156. CODEN VLDBDP.

Teuhola:1991:MSA

[TW91] Jukka Teuhola and Lutz Wegner. Minimal space, average linear time duplicate deletion. *Communications of the Association for Computing Machinery*, 34 (3):62–73, March 1991. CODEN CACMA2. ISSN 0001-

0782 (print), 1557-7317 (electronic).

Tartary:2007:CPH

[TW07] Christophe Tartary and Huaxiong Wang. Combining prediction hashing and MDS codes for efficient multicast stream authentication. *Lecture Notes in CS*, 4586:293–307, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-73458-1_22`.

Tang:2018:CIC

[TWL+18] Min Tang, Tongtong Wang, Zhongyuan Liu, Ruofeng Tong, and Dinesh Manocha. I-cloth: incremental collision handling for GPU-based interactive cloth simulation. *ACM Transactions on Graphics*, 37(6):204:1–204:??, November 2018. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Tzschach:1977:TCS

[TWW77] H. G. Tzschach, Helmut Waldschmidt, and Hermann K.-G. Walter, editors. *Theoretical computer science/3rd GI conference, Darmstadt, March 28–30, 1977*, volume 48 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1977. ISBN 0-387-08138-0. LCCN QA267 .G18 1977.

Tang:2011:SFB

[TWZW11] Zhenjun Tang, Shuozhong Wang, Xinpeng Zhang, and Weimin Wei. Structural feature-based image hashing and similarity metric for tampering detection. *Fundamenta Informaticae*, 106(1): 75–91, January 2011. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Tarjan:1979:SST

[TY79] Robert Endre Tarjan and Andrew Chi-Chih Yao. Storing a sparse table. *Communications of the Association for Computing Machinery*, 22(11):606–611, November 1979. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See also [FKS84].

Tien:1991:CHB

[TY91] J.-Y. Tien and W.-P. Yang. Comments on "hash-based and index-based join algorithms for cube and ring connected multicomputers". *IEEE Transactions on Knowledge and Data Engineering*, 3(3):387–??, September 1, 1991. CODEN ITKEEH. ISSN 1041-4347.

Tang:2003:EDL

[TY03] Hong Tang and Tao Yang. An efficient data location protocol for self-organizing storage clusters. In ACM [ACM03b], page ?? ISBN 1-58113-695-1. LCCN ???? URL `http://www.sc-conference.org/sc2003/inter_cal/intercal_detail.php?eventid=10686#0`; `http://www.sc-conference.org/sc2003/paperpdfs/pap299.pdf`.

Tyma:1996:TJP

[Tym96] Paul Tyma. Tuning Java performance. *Dr. Dobbs Journal*, 21(4):52, 55–56, 58, 90, April 1996. CODEN DDJOEB. ISSN 1044-789X.

Tao:2010:EAN

[TYSK10] Yufei Tao, Ke Yi, Cheng Sheng, and Panos Kalnis. Efficient and accurate nearest neighbor and closest pair search in high-dimensional space. *ACM Transactions on Database Systems*, 35(3):20:1–20:??, July 2010. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Tang:2015:EGF

[TYZO15] Suhua Tang, Yi Yu, Roger Zimmermann, and Sadao Obana. Efficient geo-fencing via hybrid hashing: A combination of bucket selection and in-bucket binary search. *ACM Transactions on Spatial Algorithms and Systems (TSAS)*, 1(2):5:1–5:22, November 2015. CODEN ???? ISSN 2374-0353 (print), 2374-0361 (electronic). URL `http://dl.acm.org/citation.cfm?id=2774219`.

Tillich:1994:GHF

[TZ94a] J.-P. Tillich and G. Zemor. Group-theoretic hash functions. In Cohen [Coh94], pages 90–110. ISBN 3-540-57843-9. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA268 .A397 1994.

Tillich:1994:HS

[TZ94b] J.-P. Tillich and G. Zemor. Hashing with SL2. *Lecture Notes in CS*, 839:40–49, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Thorup:2012:TBI

[TZ12] Mikkel Thorup and Yin Zhang. Tabulation-based 5-independent hashing with applications to linear probing and second moment estimation. *SIAM Journal on Computing*, 41(2):293–331, ???? 2012. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Urvoy:2008:TWS

[UCFL08] Tanguy Urvoy, Emmanuel Chauveau, Pascal Filoche, and Thomas Lavergne. Tracking Web spam with HTML

style similarities. *ACM Transactions on the Web (TWEB)*, 2(1):3:1–3:??, February 2008. CODEN ???? ISSN 1559-1131 (print), 1559-114X (electronic).

Ung:1995:UPR

[UHT95] K. P. Ung, K. C. Hwang, and G. K. Tag. Uniform partitioning of relations using histogram equalization framework: An efficient parallel hash-based join. *Information Processing Letters*, 55(5): 283–289, September 15, 1995. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ugawa:2010:IRB

[UIY10] Tomoharu Ugawa, Hideya Iwasaki, and Taiichi Yuasa. Improved replication-based incremental garbage collection for embedded systems. *SIGPLAN Notices*, 45(8):73–82, August 2010. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Ullman:1970:DHF

[Ull70] Jeffrey D. Ullman. The design of hashing functions. Technical Report 85, Princeton University, Electrical Engineering Department, TR, September 1970. ?? pp.

Ullman:1972:NEH

[Ull72] Jeffrey D. Ullman. A note on the efficiency of hashing functions. *Journal of the Association for Computing Machinery*, 19(3):569–575, July 1972. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). Early work on the problem of finding optimal hash functions for open addressing.

Ullman:1982:PDS

[Ull82] Jeffrey D. Ullman. *Principles of Database Systems*. Computer Science Press, 11 Taft Court, Rockville, MD 20850, USA, second edition, 1982. ISBN 0-7167-8069-0. vii + 484 pp. LCCN QA76.9.D3 U44 1983.

Urdaneta:2011:SDS

[UPV11] Guido Urdaneta, Guillaume Pierre, and Maarten Van Steen. A survey of DHT security techniques. *ACM Computing Surveys*, 43(2): 8:1–8:??, January 2011. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Uchiyama:2009:RIB

[US09] Hideaki Uchiyama and Hideo Saito. Rotated image based photomosaic using combination of principal component hashing. *Lecture Notes in CS*, 5414:668–679, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/`

10.1007/978-3-540-92957-4_58.

USENIX:1990:UCC

[USE90] *USENIX C++ conference proceedings: C++ Conference, San Francisco, California, April 9–11, 1990*. USENIX, San Francisco, CA, USA, 1990.

USENIX:1991:PWU

[USE91] *Proceedings of the Winter 1991 USENIX Conference: January 21-January 25, 1991, Dallas, TX, USA*. USENIX, San Francisco, CA, USA, 1991.

USENIX:2000:PAL

[USE00a] USENIX, editor. *Proceedings of the 4th Annual Linux Showcase and Conference, Atlanta, October 10–14, 2000, Atlanta, Georgia, USA*. USENIX, San Francisco, CA, USA, 2000. ISBN 1-880446-17-0. LCCN ???? URL http://www.usenix.org/publications/library/proceedings/als2000/.

USENIX:2000:PUT

[USE00b] USENIX, editor. *Proceedings of the 7th USENIX Tcl/Tk Conference (Tcl/2k): February 14–18, 2000, Austin, Texas, USA*. USENIX, San Francisco, CA, USA, 2000. ISBN 1-880446-24-3. LCCN ???? URL http://db.usenix.org/publications/library/proceedings/tcl2k/.

Vakhshoori:1985:UHD

[Vak85] Koorosh Vakhshoori. The use of hashing in a database machine. Master's thesis, University of California, Davis, Davis, CA, USA, 1985. 183 pp.

Valduriez:1987:JI

[Val87] Patrick Valduriez. Join indices. *ACM Transactions on Database Systems*, 12(2): 218–246, June 1987. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). Compares join indices with inverted indices, clustered indices, B+ trees, linked lists, and hybrid hash techniques.

Valiant:2015:FCS

[Val15] Gregory Valiant. Finding correlations in subquadratic time, with applications to learning parities and the closest pair problem. *Journal of the Association for Computing Machinery*, 62 (2):13:1–13:??, May 2015. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

vanderPool:1973:OSAb

[van73] J. A. van der Pool. Optimum storage allocation for a file with open addressing. *IBM Journal of Research and Development*, 17(2):106–

114, March 1973. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Vandery:1992:FHN

[Van92] S. Vandery. FFT-hash II is not yet collision-free. In Brickell [Bri92], page ?? ISBN 0-387-57340-2 (New York), 3-540-57340-2 (Berlin). LCCN QA76.9.A25 C79 1992. DM104.00.

vanTrung:1994:CCC

[van94] T. van Trung. A combinatorial characterization of certain universal classes of hash functions. *Journal of Combinatorial Designs*, 2(3):161–??, May 1, 1994. CODEN JDESEU. ISSN 1063-8539.

Gucht:2010:PHE

[Van10] Dirk Van Gucht, editor. *PODS'10: proceedings of the Twenty-Eight ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems: Indianapolis, Indiana, USA, June 6–11, 2011*. ACM Press, New York, NY 10036, USA, 2010. ISBN 1-4503-0033-2. LCCN ????

Vaudenay:1992:FHI

[Vau92] S. Vaudenay. FFT-hash-II is not yet collision-free. In Brickell [Bri92], pages 587–593. ISBN 0-387-57340-2 (New York), 3-540-57340-2 (Berlin). LCCN QA76.9.A25 C79 1992. DM104.00.

Vaudenay:1993:FHI

[Vau93] S. Vaudenay. FFT-Hash-II is not yet collision-free. *Lecture Notes in CS*, 740: 587–593, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vaudenay:2006:ACE

[Vau06] Serge Vaudenay, editor. *Advances in Cryptology — EUROCRYPT 2006: 25th International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28–June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 3-540-34547-7. LCCN ???? URL `http://www.springerlink.com/content/978-3-540-34547-3`.

Vckovski:2000:MTS

[VB00] Andrej Vckovski and Jason Brazile. A multi-threaded server for shared hash table access. In USENIX [USE00b], page ?? ISBN 1-880446-24-3. LCCN ???? URL `http://db.usenix.org/publications/library/proceedings/tcl2k/vckovski.html`.

Vingralek:1994:DFO

[VBW94] Radek Vingralek, Yuri Breit-

bart, and Gerhard Weikum. Distributed file organization with scalable cost/performance. In Snodgrass and Winslett [SW94b], pages 253–264. ISBN 0-89791-639-5. ISSN 0163-5808 (print), 1943-5835 (electronic). LCCN QA 76.9 D3 S53 v.23 no.2 1994. URL `http://www.acm.org/pubs/articles/proceedings/mod/191839/p253-vingralek/p253-vingralek.pdf`; `http://www.acm.org/pubs/citations/proceedings/mod/191839/p253-vingralek/`.

Vitter:1985:OAM

[VC85] Jeffrey Scott Vitter and Wen-Chin Chen. Optimum algorithms for a model of direct chaining. *SIAM Journal on Computing*, 14(2): 490–499, May 1985. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Vitter:1987:DAC

[VC87] Jeffrey Scott Vitter and Wen-Chin Chen. *The Design and Analysis of Coalesced Hashing*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1987. ISBN 0-19-504182-8. xii + 160 pp. LCCN QA76.9.H36 V57 1987. US$29.95.

Vandierendonck:2005:XBH

[VD05] H. Vandierendonck and K. De Bosschere. XOR-based hash functions. *IEEE Transactions on Computers*, 54(7):800–812, July 2005. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1432664`.

Vasudev:2021:SPP

[VD21] Harsha Vasudev and Debasis Das. P^2-SHARP: Privacy preserving secure hash based authentication and revelation protocol in IoVs. *Computer Networks (Amsterdam, Netherlands: 1999)*, 191(??):??, May 22, 2021. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128621001146`.

vandenBraak:2016:CXH

[vdBGLGL+16] Gert-Jan van den Braak, Juan Gómez-Luna, José María González-Linares, Henk Corporaal, and Nicolás Guil. Configurable XOR hash functions for banked scratchpad memories in GPUs. *IEEE Transactions on Computers*, 65(7):2045–2058, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

vanderHoeven:2012:IPI

[vdHvH12] Joris van der Hoeven and Mark van Hoeij, editors. *ISSAC 2012: Proceedings of the*

2012 International Symposium on Symbolic and Algebraic Computation, July 22–25, 2012, Grenoble, France. ACM Press, New York, NY 10036, USA, 2012. ISBN 1-4503-1269-1. LCCN QA76.95 .I59 2012.

vanderPool:1972:OSA

[vdP72] J. A. van der Pool. Optimum storage allocation for initial loading of a file. *IBM Journal of Research and Development*, 16(6):579–586, November 1972. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

vanderPool:1973:OSAa

[vdP73] J. A. van der Pool. Optimum storage allocation for a file in steady state. *IBM Journal of Research and Development*, 17(1):27–38, January 1973. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

deVillers:1974:HSS

[vdSdW74a] E. v. d. S. de Villers and L. B. Wilson. Hashing the subscripts of a sparse matrix. *BIT (Nordisk tidskrift for informationsbehandling)*, 14 (3):347–358, 1974. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

DeVilliers:1974:HSS

[vdSDW74b] E. v. d. S. De Villiers and L. B. Wilson. Hashing the subscripts of a sparse matrix. *BIT (Copenhagen)*, 14 (3):347–358, ???? 1974. CODEN NBITAB.

vanderVegt:2012:PCH

[vdVL12] Steven van der Vegt and Alfons Laarman. A parallel compact hash table. *Lecture Notes in CS*, 7119: 191–204, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-25929-6_18/`.

Veklerov:1985:ADH

[Vek85] Eugene Veklerov. Analysis of dynamic hashing with deferred splitting. *ACM Transactions on Database Systems*, 10(1):90–96, March 1985. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Ventae:1984:FTR

[Ven84] Olli Ventae. *Fast Text Reconstruction Method for the Correction of Imperfect Text*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1984. ISBN 0-8186-0624-X. 446–452 pp. LCCN Q 334 C66 1984. IEEE Service Cent. Piscataway, NJ, USA.

Ventae:1986:GDS

[Ven86] Olli Ventae. N-gram driven search for sentences in a syn-

tactic network. *Proceedings of the International Conference on Acoustics, Speech, and Signal Processing*, pages 1145–1148, 1986. CODEN IPRODJ. ISSN 0736-7791. IEEE Service Cent. Piscataway, NJ, USA.

Vo:1991:FHF

[VFN91] Phong Vo, Glenn Fowler, and Landon Curt Noll. FowlerNollVo hash function. Web document., 1991. URL `https://en.wikipedia.org/wiki/Fowler%E2%80%93Noll%E2%80%93Vo_hash_function#cite_note-2`.

Vidick:1990:PIC

[Vid90] Jean-Luc Vidick, editor. *Proceedings of the 13th International Conference on Research and Development in Information Retrieval, Brussels, Belgium, 5–7 September 1990*. ACM Press, New York, NY 10036, USA, 1990. ISBN 0-89791-408-2. LCCN QA76.9.D3I5588 1990, Z 699 A1 I582 1990.

Viola:2005:EDI

[Vio05] Alfredo Viola. Exact distribution of individual displacements in linear probing hashing. *ACM Transactions on Algorithms*, 1(2): 214–242, October 2005. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

Vitter:1980:TCH

[Vit80a] J. S. Vitter. Tuning the coalesced hashing method to obtain optimum performance. In IEEE-FOCS'80 [IEE80b], pages 238–247.

Vitter:1980:ACHa

[Vit80b] Jeffrey Scott Vitter. *Analysis of Coalescing Hashing*. PhD thesis, Stanford University, Stanford, CA, USA, October 1980. ?? pp. See also technical report [Vit80c].

Vitter:1980:ACHb

[Vit80c] Jeffrey Scott Vitter. Analysis of coalescing hashing. Technical Report STAN-CS-80-817, Stanford University, October 1980. ?? pp. This is the author's Ph.D. thesis, [Vit80b].

Vitter:1981:SMS

[Vit81a] J. S. Vitter. A shared-memory scheme for coalesced hashing. *Information Processing Letters*, 13(2):77–79, November 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Vitter:1981:DAH

[Vit81b] Jeffrey Scott Vitter. Deletion algorithms for hashing that preserve randomness. *Annual Symposium on Foundations of Computer Science (Proceedings)*, pages 127–132, 1981. CODEN ASFPDV. ISSN 0272-5428.

Vitter:1982:DAH

[Vit82a] J. S. Vitter. Deletion algorithms for hashing that preserve randomness. *Journal of Algorithms*, 3(3):261–275, September 1982. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic).

Vitter:1982:ICH

[Vit82b] Jeffrey Scott Vitter. Implementations for coalesced hashing. *Communications of the Association for Computing Machinery*, 25(12):911–926, December 1982. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Vitter:1983:ASP

[Vit83] Jeffrey Scott Vitter. Analysis of the search performance of coalesced hashing. *Journal of the Association for Computing Machinery*, 30(2):231–258, April 1983. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Vitter:1985:EIO

[Vit85] Jeffrey Scott Vitter. An efficient I/O interface for optical disks. *ACM Transactions on Database Systems*, 10(2):129–162, June 1985. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). URL `http://www.acm.org/pubs/articles/journals/tods/1985-10-2/p129-vitter/p129-vitter.pdf`; `http://www.acm.org/pubs/citations/journals/tods/1985-10-2/p129-vitter/`; `http://www.acm.org/pubs/toc/Abstracts/tods/3862.html`.

Vitter:2001:EMA

[Vit01] Jeffrey Scott Vitter. External memory algorithms and data structures: dealing with **massive data**. *ACM Computing Surveys*, 33(2):209–271, June 2001. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Varghese:1987:HHT

[VL87] George Varghese and Tony Lauck. Hashed and hierarchical timing wheels: Data structures for the efficient implementation of a timer facility. In ACM-OSP'87 [ACM87], pages 25–38. ISBN 0-89791-242-x. LCCN QA76.6 .O625 v.21:5. Published as ACM Operating Systems Review, SIGOPS, volume 21, number 5.

vanLeeuwen:1994:GTC

[vL94] Jan van Leeuwen, editor. *Graph-theoretic concepts in computer science: 19th International Workshop, WG '93, Utrecht, The Netherlands, June 16–18, 1993: proceedings*, volume 790 of *Lecture Notes in Com-*

puter Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. CODEN LNCSD9. ISBN 0-86636-292-4 (New York), 3-540-57899-4 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA75.5 .I647 1993. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0790.htm; http://www.springerlink.com/content/978-0-86636-292-4; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=790.

Varghese:1997:HHT

[VL97] George Varghese and Anthony Lauck. Hashed and hierarchical timing wheels: efficient data structures for implementing a timer facility. *IEEE/ACM Transactions on Networking*, 5(6): 824–834, December 1997. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic). URL http://www.acm.org/pubs/citations/journals/ton/1997-5-6/p824-varghese/.

Anonymous:1982:VLD

[VLD82] *Very Large Data Bases: Eighth International Conference on Very Large Data Bases, Mexico City, Mexico, September 8–10, 1982*. Morgan Kaufmann Publishers, San Francisco, CA, 1982. ISBN 0-934613-14-1. LCCN QA76.9.D3 I559 1982.

vonMises:1939:ABG

[vM39] R. von Mises. Über Aufteilungs- und Besetzungswahrscheinlichkeiten. (German) [on partitioning and occupation probabilities]. *İstanbul Üniversitesi Fen Fakültesi Mecmuasi*, 4 (??):145–163, 1939. See also [BC39].

vonMaurich:2012:ESB

[vMG12] Ingo von Maurich and Tim Güneysu. Embedded syndrome-based hashing. *Lecture Notes in CS*, 7668:339–357, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34931-7_20/.

Vaswani:2007:PPP

[VNC07] Kapil Vaswani, Aditya V. Nori, and Trishul M. Chilimbi. Preferential path profiling: compactly numbering interesting paths. *SIGPLAN Notices*, 42(1):351–362, January 2007. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Vidali:2010:CVB

[VNP10] Janoš Vidali, Peter Nose, and Enes Pašalić. Collisions for variants of the BLAKE hash

function. *Information Processing Letters*, 110(14–15): 585–590, July 1, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Viola:1996:ALP

[VP96] A. Viola and P. V. Poblete. The analysis of linear probing hashing with buckets. *Lecture Notes in CS*, 1136: 221–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Viola:1998:ALP

[VP98] Alfredo Viola and Patricio V. Poblete. The analysis of linear probing hashing with buckets. *Algorithmica*, 21(1):37–71, May 1998. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0178-4617&volume=21&issue=1&spage=37`. Fourth European Symposium on Algorithms (Barcelona, 1996).

vanTrung:2014:TBF

[vT14] Tran van Trung. A tight bound for frameproof codes viewed in terms of separating hash families. *Designs, Codes, and Cryptography*, 72(3):713–718, September 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-013-9800-0`.

Valduriez:1984:MHS

[VV84] Patrick Valduriez and Yann Viemont. A multikey hashing scheme using predicate trees. In ACM SIGMOD '84 [ACM84a], pages 107–114. CODEN SRECD8. ISBN 0-89791-128-8. ISSN 0163-5808 (print), 1943-5835 (electronic). LCCN QA76.9.D3 A15 1984.

VanWyk:1986:CHL

[VV86] Christopher J. Van Wyk and Jeffrey Scott Vitter. The complexity of hashing with lazy deletion. *Algorithmica*, 1(1):17–29, January 1986. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

vanOorschot:1994:PCS

[vW94] P. C. van Oorschot and M. J. Wiener. Parallel collision search with application to hash functions and discrete logarithms. In ACM [ACM94a], pages 210–218. ISBN 0-89791-732-4. LCCN ????

Vadhan:2012:CPS

[VZ12] Salil Vadhan and Colin Jia Zheng. Characterizing pseudoentropy and simplifying pseudorandom generator constructions. In ACM [ACM12], pages 817–836.

ISBN 1-4503-1245-4. LCCN ???? URL `http://www.gbv.de/dms/tib-ub-hannover/63314455x`..

Wagner:2000:CYL

[Wag00] David Wagner. Cryptanalysis of the Yi-Lam hash. *Lecture Notes in CS*, 1976: 483–488, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Waldschmidt:1974:OIC

[Wal74] Helmut Waldschmidt. *Optimierungsfragen im Compilerbau*. Carl Hanser, München, Germany, 1974. ISBN 3-446-11895-0. 154 pp. LCCN QA76.6 .W326.

Walker:1988:CSP

[Wal88] Henry M. Walker. *Computer Science 2: Principles of Software Engineering, Data Types, and Algorithms*. Scott, Foresman and Company, Glenview, IL, USA, 1988. ISBN 0-673-39829-3. xvii + 637 pp. LCCN QA76.758 .W35 1989. US$25.00. Textbook treatment of hashing.

Wang:1984:NOT

[Wan84] Patrick Shen-Pei Wang. *New OCR Technique with Learning Capability*. ACM Press, New York, NY 10036, USA, 1984. ISBN 0-89791-127-X. 182–?? pp. LCCN ????

Wang:2005:VCA

[Wan05] Shiuh-Jeng Wang. Vowel-consonant addressing mode on hashing for English letter-oriented keys. *Journal of Discrete Mathematical Sciences and Cryptography*, 8(1):1–25, 2005. CODEN ???? ISSN 0972-0529.

Wang:2014:DRG

[Wan14] Pai-Chou Wang. Dynamic reducts generation using cascading hashes. *International Journal of Foundations of Computer Science*, 25(2):219–??, February 2014. CODEN IFCSEN. ISSN 0129-0541.

Warren:1986:GHR

[War86] Van Warren. Geometric hashing for rendering complex scenes. M.sc. thesis, University of Utah, May 1986. ix + 74 pp.

Warren:2014:IPH

[War14] Michael S. Warren. 2HOT: an improved parallel hashed oct-tree N-body algorithm for cosmological simulation. *Scientific Programming*, 22 (2):109–124, ???? 2014. CODEN SCIPEV. ISSN 1058-9244 (print), 1875-919X (electronic).

Wu:1987:ASM

[WB87] C. T. Wu and Walter A. Burkhard. Associative searching in multiple storage units. *ACM Transactions*

on Database Systems, 12(1): 38–64, March 1987. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic). Discusses interpolation hashing, a multidimensional variant of linear hashing.

White:1990:CSA

[WB90] L. B. White and B. Boashash. Cross spectral analysis of nonstationary processes. *IEEE Transactions on Information Theory*, 36(4):830, 1990.

Wu:2003:HHS

[WB03] Changxun Wu and Randal Burns. Handling heterogeneity in shared-disk file systems. In ACM [ACM03b], page ?? ISBN 1-58113-695-1. LCCN ???? URL `http://www.sc-conference.org/sc2003/inter_cal/inter_cal_detail.php?eventid=10686#1`; `http://www.sc-conference.org/sc2003/paperpdfs/pap132.pdf`.

Wang:2016:CNC

[WBWV16] Sen Wang, Jun Bi, Jianping Wu, and Athanasios V. Vasilakos. CPHR: In-network caching for information-centric networking with partitioning and hash-routing. *IEEE/ACM Transactions on Networking*, 24(5):2742–2755, October 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Wegman:1979:NCA

[WC79] Mark N. Wegman and J. Lawrence Carter. New classes and applications of hash functions. *Annual Symposium on Foundations of Computer Science (Proceedings)*, ??(??):175–182, ???? 1979. CODEN ASFPDV.

Wegman:1981:NHF

[WC81] Mark N. Wegman and J. Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, June 1981. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic).

Wu:1994:AGH

[WC94] T.-C. Wu and C.-C. Chang. Application of geometric hashing to iconic database retrieval. *Pattern Recognition Letters*, 15(9):871–??, September 1, 1994. CODEN PRLEDG. ISSN 0167-8655 (print), 1872-7344 (electronic).

Walker:2007:PHF

[WC07] Robert A. Walker, II and Charles J. Colbourn. Perfect Hash families: constructions and existence. *Journal of Mathematical Cryptology*, 1(2):125–150, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Wang:2022:CLI

[WCW+22] Zhaoguo Wang, Haibo Chen, Youyun Wang, Chuzhe Tang, and Huan Wang. The concurrent learned indexes for multicore data storage. *ACM Transactions on Storage*, 18 (1):8:1–8:35, February 2022. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic). URL `https://dl.acm.org/doi/10.1145/3478289`.

Weng:2012:RIC

[WDP+12] Li Weng, Rony Darazi, Bart Preneel, Benoît Macq, and Ann Dooms. Robust image content authentication using perceptual hashing and watermarking. *Lecture Notes in CS*, 7674:315–326, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-34778-8_29`.

Wolf:1991:EAP

[WDYT91] J. L. Wolf, D. M. Dias, P. S. Yu, and J. Turek. An effective algorithm for parallelizing hash joins in the presence of data skew. In ICDE'91 [ICD91], page 200. ISBN 0-8186-2138-9 (paper), 0-8186-6138-0 (microfiche), 0-8186-9138-7 (hardcover). LCCN QA76.9.D3 I5582 1991.

Webb:1972:DAE

[Web72] D. A. Webb. *The Development and Application of an Evaluation Model for Hash Coding Systems*. Ph.d. thesis, Syracuse University, Syracuse, NY, USA, August 1972.

Weems:1988:SPA

[Wee88] Bob P. Weems. A study of page arrangements for extendible hashing. *Information Processing Letters*, 27 (5):245–248, April 1988. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Wee:2007:OWP

[Wee07] Hoeteck Wee. One-way permutations, interactive hashing and statistically hiding commitments. *Lecture Notes in CS*, 4392: 419–433, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-70936-7_23`.

Wee:2011:TRC

[Wee11] Hoeteck Wee. Threshold and revocation cryptosystems via extractable hash proofs. *Lecture Notes in CS*, 6632:589–609, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_32`.

Wee:2012:DPH

[Wee12] Hoeteck Wee. Dual projective hashing and its applications — lossy trapdoor functions and more. *Lecture Notes in CS*, 7237: 246–262, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_15; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_16/.

Wenzel:1992:WBU

[Wen92] M. Wenzel. Wörterbücher für ein beschränktes universum. (German) [Dictionaries for a limited universe]. Diplomarbeit, Fachbereich Informatik, Universität des Saarlandes, Saarbrücken, Germany, ???? 1992.

Wartik:1992:HA

[WFHC92] Steven Wartik, Edward Fox, Lenwood Heath, and Qi-Fan Chen. Hashing algorithms. In Frakes and Baeza-Yates [FBY92], chapter 13, pages 293–362. ISBN 0-13-463837-9. LCCN QA76.9.D351543 1992. US$56.00.

Wang:2004:CHF

[WFLY04] Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu. Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD. Cryptology ePrint Archive, Report 2004/199, 2004. URL http://eprint.iacr.org/2004/199.pdf; http://www.tcs.hut.fi/~mjos/md5/.

Weiss:2012:MSH

[WFT12] Yair Weiss, Rob Fergus, and Antonio Torralba. Multidimensional spectral hashing. *Lecture Notes in CS*, 7576:340–353, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-33715-4_25.

Wu:2012:PPA

[WFW+12] Shuang Wu, Dengguo Feng, Wenling Wu, Jian Guo, Le Dong, and Jian Zou. (pseudo) preimage attack on round-reduced Grøstl hash function and others. *Lecture Notes in CS*, 7549: 127–145, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34047-5_8/.

Weaver:1994:SAM

[WG94] David L. Weaver and Tom Germond. *The SPARC Architecture Manual: Version 9*. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA, 1994. ISBN 0-13-099227-5. xxii + 357

pp. LCCN QA76.9.A73S648 1992. US$33.00. URL http://www.sparc.org/standards/SPARCV9.pdf.

Wagner:2000:PSU

[WG00] David Wagner and Ian Goldberg. Proofs of security for the Unix password hashing algorithm. *Lecture Notes in CS*, 1976:560–572, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760560.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760560.pdf.

Wegman:1988:CSS

[WGM88] Edward J. Wegman, Donald T. Gantz, and John J. Miller, editors. *Computing Science and Statistics Proceedings of the 20th Symposium on the Interface Fairfax, Virginia, April 1988*. American Statistical Association, Alexandria, VA, USA, 1988. URL http://www.dtic.mil/dtic/tr/fulltext/u2/a208838.pdf.

Weide:1983:MCE

[WH83] Bruce W. Weide and David J. Hogan. *Mapping to Cells: Extension of a Data Structure for Fast Storage and Retrieval*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1983. ISBN 0-387-90835-8. 37–41 pp. LCCN QA276.4 .C58 1982.

Wang:2007:BTS

[WHS+07] Chia-Wei Wang, Hung-Chang Hsiao, Wen-Hung Sun, Chung-Ta King, and Ming-Tsung Sun. Building a tuple space on structured peer-to-peer networks. *The Journal of Supercomputing*, 40(3):213–227, June 2007. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=40&issue=3&spage=213.

Wiederhold:1983:FOD

[Wie83] Gio Wiederhold. *File Organization for Database Design*. McGraw-Hill Computer Science Series, Editor: Richard W. Hamming and Edward A. Feigenbaum. McGraw-Hill, New York, NY, USA, 1983. ?? pp.

Wiener:1986:EVH

[Wie86] Richard S. Wiener. An efficient virtual hash algorithm for a spelling checker. *Journal of Pascal, Ada and Modula-2*, 5(1):23–29, January–February 1986. CODEN JOPAD5, JPAME8. ISSN 0735-1232.

Wiederhold:1987:FOD

[Wie87a] Gio Wiederhold. *File Organisation For Database Design*. McGraw-Hill, New York, NY, USA, 1987. ISBN 0-07-070133-4. xiv + 619 pp. LCCN QA76.9.F5 W53 1987. US$38.95.

Wiedermann:1987:SA

[Wie87b] Juraj Wiedermann. *Searching Algorithms*. B. G. Teubner, Stuttgart, Germany, 1987. ISBN 3-322-00433-3. 123 pp. LCCN QA76.9.D35 W525 1987.

Wiederhold:1989:DD

[Wie89] Gio Wiederhold. *Dateiorganisation in Datenbanken*. McGraw-Hill, New York, NY, USA, 1989. ISBN 3-89028-133-8. ?? pp.

Wiener:1999:ACC

[Wie99] Michael Wiener, editor. *Advances in cryptology — CRYPTO '99: 19th annual international cryptology conference, Santa Barbara, California, USA, August 15–19, 1999 proceedings*, volume 1666 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-66347-9. LCCN QA76.9.A25 C79 1999 Bar.

Williams:1959:HII

[Wil59] F. A. Williams. Handling identifiers as internal symbols in language processors. *Communications of the Association for Computing Machinery*, 2(6):21–24, June 1959. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Williams:1971:SUM

[Wil71] J. G. Williams. Storage utilization in a memory hierarchy when storage assignment is performed by a hashing algorithm. *Communications of the Association for Computing Machinery*, 14 (3):172–5, March 1971. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Willard:1978:NDS

[Wil78] Dan E. Willard. New data structures for orthogonal queries. Technical Report TR-22-78, Centre for Research in Computing Technology, Harvard University, Cambridge, MA, 1978. ?? pp. Published in [Wil85a].

Willett:1979:DRE

[Wil79] Peter Willett. Document retrieval experiments using indexing vocabularies of varying size — 2. hashing, truncation, digram and trigram encoding of index terms. *Journal of Documentation*, 35

(4):296–305, December 1979. CODEN JDOCAS. ISSN 0022-0418 (print), 1758-7379 (electronic).

Willard:1985:NDS

[Wil85a] Dan E. Willard. New data structures for orthogonal range queries. *SIAM Journal on Computing*, 14 (1):232–253, February 1985. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). This paper, together with an earlier report [Wil78], present seven data structures for orthogonal range queries which are more efficient than earlier data structures used for this purpose, such as box array hashing.

Williamson:1985:CCS

[Wil85b] Stanley Gill Williamson. *Combinatorics for Computer Science*. Computer Science Press, 11 Taft Court, Rockville, MD 20850, USA, 1985. ISBN 0-88175-020-4. xliii + 479 pp. LCCN QA164 .W55 1985. US$39.95.

Wildner:1996:CAS

[Wil96] U. Wildner. Compiler assisted self-checking of structural integrity using return address hashing. *Lecture Notes in CS*, 1150:161–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wild:1997:AAB

[Wil97] Fred Wild. Algorithm alley. *Dr. Dobbs Journal*, 22 (3):105–??, March 1997. CODEN DDJOEB. ISSN 1044-789X.

Willard:2000:ECG

[Wil00] Dan E. Willard. Examining computational geometry, Van Emde Boas trees, and hashing from the perspective of the fusion tree. *SIAM Journal on Computing*, 29 (3):1030–1049, June 2000. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/32242`.

Wiley:2003:DHT

[Wil03] Brandon Wiley. Distributed hash tables, Part I. *Linux Journal*, 2003(114):7, October 2003. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

WilsonGarcia:2014:GLD

[Wil14] Edscott Wilson García. GNU `libdbh` (disk-based hash tables). SourceForge software archive., April 9, 2014. URL `http://sourceforge.net/projects/dbh`; `http://www.gnu.org/software/libdbh/`.

Winkowski:1978:SMF

[Win78] J. Winkowski, editor. *Mathematical Foundations of Com-*

puter Science, 1978: proceedings, 7th Symposium, Zakopane, Poland, September 4–8, 1978, volume 64 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1978. ISBN 0-387-08917-9. LCCN QC770 .I55 1978.

Winternitz:1983:POW

[Win83] Robert S. Winternitz. Producing a one-way hash function from DES. In Chaum et al. [CRS83a], pages 203–207. ISBN 0-306-41637-9, 1-4757-0604-9 (print), 1-4757-0602-2. LCCN QA76.9.A25 C791 1983.

Winternitz:1984:SOH

[Win84] Robert S. Winternitz. Secure one-way hash function built from DES. *Proceedings of the Symposium on Security and Privacy*, pages 88–90, 1984. CODEN PSSPEO. ISBN 0-8186-0532-4. IEEE Service Cent. Piscataway, NJ, USA.

Winters:1990:MPHb

[Win90a] Vincent G. Winters. Minimal perfect hashing for large sets of data. In Akl et al. [AFK90], page ?? ISBN 0-387-53504-7 (New York), 3-540-53504-7 (Berlin). LCCN QA75.5 .I578 1990.

Winters:1990:MPHa

[Win90b] Vincent G. Winters. Minimal perfect hashing in polynomial time. *BIT (Nordisk tidskrift for informationsbehandling)*, 30(2):235–244, 1990. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Wirth:1975:AD

[Wir75] Niklaus Wirth. *Algorithmen und Datenstrukturen*. B. G. Teubner, Stuttgart, Germany, 1975. ISBN 3-519-02330-X. 376 pp. LCCN QA76.9.D35 W57. DM26.80.

Wirth:1983:AD

[Wir83] N. Wirth. *Algorithmen und Datenstrukturen*. B. G. Teubner, Stuttgart, Germany, third edition, 1983. ISBN 3-519-02250-8. 320 pp.

Wirth:1986:ADS

[Wir86] Niklaus Wirth. *Algorithms and Data Structures*. Prentice-Hall, Englewood Cliffs, NJ 07632, USA, 1986. ISBN 0-13-022005-1. 288 pp. LCCN QA76.9.D35 W58 1986. US$32.95.

Westergaard:2007:CME

[WKBA07] Michael Westergaard, Lars Michael Kristensen, Gerth Stølting Brodal, and Lars Arge. The ComBack method — extending hash compaction with backtracking. *Lecture Notes in CS*, 4546: 445–464, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.`

springer.com/content/pdf/10.1007/978-3-540-73094-1_26.

Wipke:1978:HFR

[WKO78] W. T. Wipke, S. Krishnan, and G. I. Ouchi. Hash functions for rapid storage and retrieval of chemical structures. *Journal of Chemical Information and Computer Sciences*, 18(1):32–37, February 1978. CODEN JCISD8. ISSN 0095-2338.

Wang:2007:LBP

[WL07] Xiaoming Wang and Dmitri Loguinov. Load-balancing performance of consistent hashing: asymptotic analysis of random node join. *IEEE/ACM Transactions on Networking*, 15(4):892–905, August 2007. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Yau:2009:NTV

[WL12] Zhu Wang and Tiejian Luo. Optimizing hash function number for BF-based object locating algorithm. *Lecture Notes in CS*, 7332:543–552, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-31020-1_65.

Wang:2020:PEF

[WLC20] Kefei Wang, Jian Liu, and Feng Chen. Put an elephant into a fridge: optimizing cache efficiency for in-memory key–value stores. *Proceedings of the VLDB Endowment*, 13(9):1540–1554, May 2020. CODEN ???? ISSN 2150-8097. URL https://dl.acm.org/doi/abs/10.14778/3397230.3397247.

Wang:2008:HBS

[WLLG08] Hongzhi Wang, Jianzhong Li, Jizhou Luo, and Hong Gao. Hash-base subgraph query processing method for graph-structured XML documents. *Proceedings of the VLDB Endowment*, 1(1):478–489, August 2008. CODEN ???? ISSN 2150-8097.

Wang:2019:DDD

[WLWZ19] Yicheng Wang, Yang Liu, Peiyun Wu, and Zhao Zhang. Detect DRAM disturbance error by using disturbance bin counters. *IEEE Computer Architecture Letters*, 18(1):34–37, January/June 2019. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Wang:1993:IHA

[WM93] Y. B. Wang and T. P. Mack. An indexed-hash algorithm for an agrometeorological data management system. *Computers and Elec-*

tronics in Agriculture, 8(2): 105–??, March 1, 1993. CODEN CEAGE6. ISSN 0168-1699.

Wyman:2019:IAT

[WM19] Chris Wyman and Morgan McGuire. Improved alpha testing using hashed sampling. *IEEE Transactions on Visualization and Computer Graphics*, 25(2): 1309–1320, February 2019. CODEN ITVGEA. ISSN 1077-2626 (print), 1941-0506 (electronic), 2160-9306. URL `https://www.computer.org/csdl/trans/tg/2019/02/08010336-abs.html`.

Witten:1994:MGC

[WMB94] Ian H. Witten, Alistair Moffat, and Timothy C. Bell. *Managing Gigabytes: Compressing and Indexing Documents and Images*. Van Nostrand Reinhold, New York, NY, USA, 1994. ISBN 0-442-01863-0. xiv + 429 pp. LCCN TA1637 .W58 1994. US$54.95. The software for full-text indexing described in this book, and errata for the book, are available for anonymous ftp from `munnari.oz.au` in the directory `/pub/mg`.

Witten:1999:MGC

[WMB99] Ian H. Witten, Alistair Moffat, and Timothy C. Bell. *Managing Gigabytes: Compressing and Indexing Documents and Images*. Morgan Kaufmann Publishers, San Francisco, CA, second edition, 1999. ISBN 1-55860-570-3. xxxi + 519 pp. LCCN TA1637 .W58 1994. US$54.95. URL `ftp://ftp.math.utah.edu/pub/mg/`; `ftp://ftp.math.utah.edu/pub/mg/mg-1.3x/bibsearch-1.02.tar.gz`; `ftp://munnari.oz.au:/pub/mg`; `http://www.cs.mu.oz.au/mg/`; `http://www.cs.mu.oz.au/~alistair/arith_coder/`; `https://www.math.utah.edu/pub/mg/`; `https://www.math.utah.edu/pub/mg/mg-1.3x/bibsearch-1.02.tar.gz`; `http://www.mkp.com/books_catalog/1-55860-570-3.asp`.

Woelfel:2001:NBO

[Woe01] Philipp Woelfel. New bounds on the OBDD-size of integer multiplication via universal hashing. *Lecture Notes in CS*, 2010:563–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2010/20100563.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2010/20100563.pdf`.

Woelfel:2005:BOS

[Woe05] Philipp Woelfel. Bounds

on the OBDD-size of integer multiplication via universal hashing. *Journal of Computer and System Sciences*, 71(4):520–534, November 2005. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S002200000500067X`.

Woelfel:2006:CMO

[Woe06a] Philipp Woelfel. A construction method for optimally universal hash families and its consequences for the existence of RBIBDs. *Theoret. Comput. Sci.*, 363(1):76–84, October 25, 2006. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Woelfel:2006:MEM

[Woe06b] Philipp Woelfel. Maintaining external memory efficient hash tables. In Díaz et al. [DJRZ06], pages 508–519. CODEN LNCSD9. ISBN 3-540-38044-2 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA75.5 .I643 2006. URL `http://www.springerlink.com/content/w40104p9224657rk/`.

Wogulis:1989:SAS

[Wog89] James Wogulis. Self-adjusting and split sequence hash tables. *Information Processing Letters*, 30(4): 185–188, February 27, 1989. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Wolverton:1984:PHF

[Wol84] David Alan Wolverton. A perfect hash function for Ada reserved words. *ACM SIGADA Ada Letters*, 4(1): 40–44, July/August 1984. CODEN AALEE5. ISSN 1094-3641 (print), 1557-9476 (electronic).

Wolfowicz:1993:SPR

[Wol93a] W. Wolfowicz, editor. *State and progress of research in cryptography: 3rd Symposium — February 1993, Rome*, PROCEEDINGS OF THE SYMPOSIUM ON STATE AND PROGRESS OF RESEARCH IN CRYPTOGRAPHY 1993; 3rd. [], Rome; Fondazione Ugo Bordoni, 1993.

Wolfowicz:1993:SPS

[Wol93b] William Wolfowicz, editor. *SPRC 93: proceedings of the 3rd Symposium of State and Progress of Research in Cryptography, Rome, 15–16 February, 1993*. Fondazione Ugo Bordoni, Rome, Italy, 1993. LCCN ????

Wood:1989:PQP

[Woo89] D. Wood. Parallel queues and pools, an evaluation. Master's thesis, Courant Institute, New York University,

New York, NY, USA, January 1989. ?? pp. Revised version available as NYU Ultracomputer Note #150.

Weng:2010:IHV

[WP10] Li Weng and Bart Preneel. From image hashing to video hashing. *Lecture Notes in CS*, 5916:662–668, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-11301-7_66`.

Wang:1994:SDP

[WPKK94] Cho-Li Wang, Viktor K. Prasanna, Hyoung J. Kim, and Ashfaq A. Khokhar. Scalable data parallel implementations of object recognition using geometric hashing. *Journal of Parallel and Distributed Computing*, 21 (1):96–109, April 1994. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.idealibrary.com/links/doi/10.1006/jpdc.1994.1044/production; http://www.idealibrary.com/links/doi/10.1006/jpdc.1994.1044/production/pdf`.

Wei:2012:SIV

[WPS+12] Lei Wei, Thomas Peyrin, Przemysław Sokołowski, San Ling, Josef Pieprzyk, and Huaxiong Wang. On the (in)security of IDEA in various hashing modes. *Lecture Notes in CS*, 7549: 163–179, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-34047-5_10/`.

Wah:1990:PIC

[WPY90] Benjamin W. Wah (v.1), David A. Padua (v.2), and Pen-Chung Yew (v.3), editors. *Proceedings of the 1990 International Conference on Parallel Processing, August 13–17, 1990*. Pennsylvania State University Press, University Park, PA, USA, 1990. ISBN 0-271-00728-1. LCCN QA 76.58 I58 1990. Three volumes.

Wolfson:1997:GHO

[WR97] Haim J. Wolfson and Isidore Rigoutsos. Geometric hashing: An overview. *IEEE Computational Science & Engineering*, 4(4):10–21, October/December 1997. CODEN ISCEE4. ISSN 1070-9924 (print), 1558-190X (electronic). URL `http://dlib.computer.org/cs/books/cs1997/pdf/c4010.pdf; http://www.computer.org/cse/cs1998/c4010abs.htm`.

Wright:1983:SFS

[Wri83] William E. Wright. Some file structure considerations

pertaining to magnetic bubble memory. *The Computer Journal*, 26(1):43–51, February 1983. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_26/Issue_01/tiff/43.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_26/Issue_01/tiff/44.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_26/Issue_01/tiff/45.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_26/Issue_01/tiff/46.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_26/Issue_01/tiff/47.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_26/Issue_01/tiff/48.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_26/Issue_01/tiff/49.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_26/Issue_01/tiff/50.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_26/Issue_01/tiff/51.tif.

Wegbreit:1976:PPC

[WS76] Ben Wegbreit and Jay M. Spitzen. Proving properties of complex data structures. *Journal of the Association for Computing Machinery*, 23(2):389–396, April 1976. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Warren:1993:PHO

[WS93] Michael S. Warren and John K. Salmon. A parallel hashed oct-tree N-body algorithm. In IEEE [IEE93], pages 12–21. ISBN 0-8186-4340-4 (paperback), 0-8186-4341-2 (microfiche), 0-8186-4342-0 (hardback), 0-8186-4346-3 (CD-ROM). ISSN 1063-9535. LCCN QA76.5 .S96 1993. URL ftp://ftp.cacr.caltech.edu/nbody/sc93.ps.Z.

Whiting:2003:MPH

[WS03] Douglas L. Whiting and Michael J. Sabin. Montgomery prime hashing for message authentication. In Joye [Joy03], pages 50–67. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C822 2003. URL http://link.springer-ny.com/link/service/series/0558/tocs/t2612.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2612.

Wang:2013:PPC

[WS13] Gaoli Wang and Yanzhao Shen. Preimage and pseudo-collision attacks on step-reduced SM3 hash function. *Information Pro-*

cessing Letters, 113(8):301–306, April 30, 2013. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013000513.

Wang:2012:PAC

[WSSO12] Lei Wang, Yu Sasaki, Kazuo Sakiyama, and Kazuo Ohta. Polynomial-advantage cryptanalysis of 3D cipher and 3D-based hash function. *Lecture Notes in CS*, 7631: 170–181, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34117-5_11/.

Wei:2016:HTH

[WSZ+16] Ying Wei, Yangqiu Song, Yi Zhen, Bo Liu, and Qiang Yang. Heterogeneous translated hashing: a scalable solution towards multi-modal similarity search. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 10(4):36:1–36:??, July 2016. CODEN ???? ISSN 1556-4681 (print), 1556-472X (electronic).

Wu:2007:ASO

[WTN07] Di Wu, Ye Tian, and Kam Wing Ng. An analytical study on optimizing the lookup performance of distributed hash table systems under churn. *Concurrency and Computation: Practice and Experience*, 19(4):543–569, March 25, 2007. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Wu:2009:REL

[WTN09] Di Wu, Ye Tian, and Kam-Wing Ng. Resilient and efficient load balancing in distributed hash tables. *Journal of Network and Computer Applications*, 32(1):45–60, January 2009. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804508000398.

Wang:2013:GNL

[WTZ+13] Yi Wang, Dongzhe Tai, Ting Zhang, Jianyuan Lu, Boyang Xu, Huichen Dai, and Bin Liu. Greedy name lookup for named data networking. *ACM SIGMETRICS Performance Evaluation Review*, 41 (1):359–360, June 2013. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Wu:1984:IHD

[Wu84] C. T. Wu. Interpolation hashing with descriptors. In *Proceedings of the 1984 Conference on Information Sciences and Systems.*, pages 653–657. Princeton Univ, Dep of Electrical Engineering

& Computer Science, Princeton, NJ, USA, 1984.

Wu:1985:DOM

[Wu85] C. Thomas Wu. Data organization method for the parallel execution of relational operations. In *Proceedings — Foundations of Data Organization.*, pages 399–405. Organizing Committee of the Int Conference on Foundations of Data Organization, Jpn, 1985. Kyoto Sangyo Univ. Computer Science Inst, Kyoto, Jpn.

Wu:2005:HC

[Wu05] Chuan-Kun Wu. Hash channels. *Computers and Security*, 24(8):653–661, November 2005. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404805000696`.

Whang:1990:LTP

[WVT90] K. Y. Whang, B. T. Vander Zanden, and H. M. Taylor. A linear-time probabilistic counting algorithm for database applications. *ACM Transactions on Database Systems*, 15 (2):208, June 1990. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Wang:2009:PAH

[WW09] Gaoli Wang and Shaohui Wang. Preimage attack on hash function RIPEMD. *Lecture Notes in CS*, 5451: 274–284, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-00843-6_24`.

Wu:2018:SDH

[WWG+18] Lin Wu, Yang Wang, Zongyuan Ge, Qichang Hu, and Xue Li. Structured deep hashing with convolutional neural networks for fast person re-identification. *Computer vision and image understanding: CVIU*, 167 (??):63–73, February 2018. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1077314217302011`.

Wang:2009:HSEa

[WWZ09] Weiyan Wang, Xiaoling Wang, and Aoying Zhou. Hash-Search: an efficient SLCA-based keyword search algorithm on XML documents. *Lecture Notes in CS*, 5463:496–510, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-00887-0_44`.

Wang:2001:ECP

[WX01] H. Wang and C. Xing. Explicit constructions of perfect

hash families from algebraic curves over finite fields. *Journal of Combinatorial Theory (Series A)*, 93(1):112–124, January 2001. CODEN JCBTA7. ISSN 0097-3165.

Wu:2000:LSH

[WY00] Kun-Lung Wu and Philip S. Yu. Latency-sensitive hashing for collaborative Web caching. *Computer Networks (Amsterdam, Netherlands: 1999)*, 33(1–6):633–644, June 2000. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.elsevier.nl/gej-ng/10/15/22/48/25/69/abstract.html`; `http://www.elsevier.nl/gej-ng/10/15/22/48/25/69/article.pdf`; `http://www9.org/w9cdrom/301/301.html`.

Wu:2002:CRH

[WY02] K-L Wu and P. S. Yu. Controlled replication for hash routing-based Web caching. *International Journal of Computer Systems Science and Engineering*, 17(4/5):??, July/September 2002. CODEN CSSEEI. ISSN 0267-6192.

Wang:2018:TTP

[WYD+18] Weiqing Wang, Hongzhi Yin, Xingzhong Du, Quoc Viet Hung Nguyen, and Xiaofang Zhou. TPM: a temporal personalized model for spatial item recommendation. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 9(6):61:1–61:??, November 2018. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3230706`.

Wolf:1993:PHJ

[WYT93] J. L. Wolf, P. S. Yu, and J. Turek. A parallel hash join algorithm for managing data skew. *IEEE Transactions on Parallel and Distributed Systems*, 4(12):1355–??, December 1, 1993. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Wang:2014:CGR

[WYW14] Zongyue Wang, Hongbo Yu, and Xiaoyun Wang. Cryptanalysis of GOST R hash function. *Information Processing Letters*, 114(12):655–662, December 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019014001458`.

Wang:2005:CSA

[WYY05a] X. Wang, Y. L. Yin, and H. Yu. Collision search attacks on SHA-1. Unpublished (??) research summary., 2005.

Wang:2005:FCFa

[WYY05b] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. Technical report, Shandong University, Shandong, China, June 22, 2005. URL `http://cryptome.org/wang_sha1_v2.zip`.

Wang:2005:FCFb

[WYY05c] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. *Lecture Notes in CS*, 3621:17–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wang:2005:ECS

[WYY05d] Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin. Efficient collision search attacks on SHA-0. In Shoup [Sho05], pages 1–?? CODEN LNCSD9. ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3621`.

Woodruff:1993:HVT

[WZ93] D. L. Woodruff and E. Zemel. Hashing vectors for tabu search. *Annals of Operations Research*, 40(1 / 4): 123–??, May 1, 1993. CODEN AOREEV. ISSN 0254-5330 (print), 1572-9338 (electronic).

Wang:2012:BPS

[WZ12] Wenyuan Wang and Zheng Zhang. Balanced partition scheme for distributed caching systems to solve load imbalance problems. *ACM SIGSOFT Software Engineering Notes*, 37(6):1–6, November 2012. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

Wang:2010:UHT

[WZJS10] Yuliang Wang, Qiuxia Zhao, Liehui Jiang, and Yi Shao. Ultra high throughput implementations for MD5 hash algorithm on FPGA. *Lecture Notes in CS*, 5938: 433–441, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-11842-5_60`.

Wang:2018:SBD

[WZY+18] J. Wang, X. Zhang, J. Yin, R. Wang, H. Wu, and D. Han. Speed up big data analytics by unveiling the storage distribution of sub-datasets. *IEEE Transactions*

on Big Data, 4(2):231–244, June 2018. ISSN 2332-7790.

Xu:2006:TNH

[XBH06] Zhiyong Xu, Laxmi Bhuyan, and Yiming Hu. Tulip: a new hash based cooperative Web caching architecture. *The Journal of Supercomputing*, 35(3):301–320, March 2006. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=35&issue=3&spage=301`.

Xia:2009:APL

[XCCK09] Ye Xia, Shigang Chen, Chunglae Cho, and Vivekanand Korgaonkar. Algorithms and performance of load-balancing with multiple hash functions in massive content distribution. *Computer Networks (Amsterdam, Netherlands: 1999)*, 53(1):110–125, January 16, 2009. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic).

Xue:2019:SEA

[XHZ+19] Kaiping Xue, Peixuan He, Xiang Zhang, Qiudong Xia, David S. L. Wei, Hao Yue, and Feng Wu. A secure, efficient, and accountable edge-based access control framework for information centric networks. *IEEE/ACM Transactions on Networking*, 27(3):1220–1233, June 2019. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Xu:2014:HTM

[XLZC14] Yang Xu, Zhaobo Liu, Zhuoyuan Zhang, and H. Jonathan Chao. High-throughput and memory-efficient multimatch packet classification based on distributed and pipelined hash tables. *IEEE/ACM Transactions on Networking*, 22(3):982–995, June 2014. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Xu:2011:MDP

[XMLC11] Y. Xu, L. Ma, Z. Liu, and H. J. Chao. A multi-dimensional progressive perfect hashing for high-speed string matching. In ACM, editor, *ANCS'11: Proceedings of the 17th ACM/IEEE Symposium on Architectures for Networking and Communications Systems, Brooklyn, NY, USA, October 3–4, 2011*, pages 167–177. ACM Press, New York, NY 10036, USA, 2011. ISBN 0-7695-4521-1.

Xin:2013:LVR

[XNS+13] Xin Xin, Abhishek Nagar, Gaurav Srivastava, Zhu Li, Felix Fernandes, and Aggelos K. Katsaggelos. Large visual repository search with hash collision design optimization. *IEEE MultiMedia*, 20(2):62–71, April/June

2013. CODEN IEMUE4. ISSN 1070-986X.

Xiang:2021:EFT

[XZPG21] Jun Xiang, Ning Zhang, Ruru Pan, and Weidong Gao. Efficient fine-texture image retrieval using deep multi-view hashing. *Computers and Graphics*, 101 (??):93–105, December 2021. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0097849321002156`.

Yamane:1985:HJT

[Yam85] Yasuo Yamane. A hash join technique for relational database systems. In IEEE-FODS'85 [IEE85b], pages 388–398. Kyoto Sangyo Univ. Computer Science Inst, Kyoto, Jpn.

Yang:2005:TFN

[Yan05] JiXian Yang. TWOBLOCK: a fast new hash function, 2005. URL `http://yjxonline.hostrocket.com/Hash2005.pdf`. World-Wide Web document.

Yang:2010:PII

[Yan10] Yixian Yang, editor. *Proceedings 2010 IEEE International Conference on Information Theory and Information Security: December 17–19, 2010, Beijing, China*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 1-4244-6942-2. LCCN QA76.9.A25. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5680738`.

Yao:1978:VLD

[Yao78] S. Bing Yao, editor. *Very large data bases: Fourth International Conference on Very Large Data Bases, West Berlin, Germany, September 13–15, 1978*. ACM Press, New York, NY 10036, USA, 1978.

Yao:1980:NAE

[Yao80] Andrew C. Yao. A note on the analysis of extendible hashing. *Information Processing Letters*, 11(2):84–86, 1980. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Yao:1981:STS

[Yao81] Andrew Chi-Chih Yao. Should tables be sorted? *Journal of the Association for Computing Machinery*, 28(3):615–628, July 1981. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Yao:1983:LBP

[Yao83] Andrew C. Yao. Lower bounds by probabilistic arguments. *Annual Symposium on Foundations of Computer Science (Proceedings)*, pages

420–428, 1983. CODEN ASFPDV. ISBN 0-8186-0508-1. ISSN 0272-5428. IEEE Service Cent. Piscataway, NJ, USA.

Yao:1985:OAK

[Yao85a] Andrew C. Yao. On optimal arrangements of keys with double hashing. *Journal of Algorithms*, 6(2): 253–264, June 1985. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic).

Yao:1985:UHO

[Yao85b] Andrew C. Yao. Uniform hashing is optimal. *Journal of the Association for Computing Machinery*, 32 (3):687–693, July 1985. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/3836.html`. Also published in/as: Stanford Un., CSD, TR-CS-85-1038, Jan. 1985.

Yao:1991:WRA

[Yao91] Andrew C. Yao. Weighted random assignments with application to hashing. In Hsu and Lee [HL91], page 42. ISBN 0-387-54945-5 (New York), 3-540-54945-5 (Berlin). LCCN QA76.9.A43 I57 1991.

Yao:1995:MOK

[Yao95] Andrew Chi-Chih Yao. Minimean optimal key arrangements in hash tables. *Algorithmica*, 14(5):409–428, November 1, 1995. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Yasuda:2007:SIS

[Yas07] Kan Yasuda. "Sandwich" is indeed secure: How to authenticate a message with just one hashing. *Lecture Notes in CS*, 4586: 355–369, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-73458-1_26`.

Yen:1995:PHC

[YB95] I-Ling L. Yen and Farokh B. Bastani. Parallel hashing: Collision resolution strategies and performance. *Journal of Parallel and Distributed Computing*, 31(2):190–198, December 1995. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.idealibrary.com/links/doi/10.1006/jpdc.1995.1158/production`; `http://www.idealibrary.com/links/doi/10.1006/jpdc.1995.1158/production/pdf`.

Yu:2017:FSD

[YBQZ17] Ye Yu, Djamal Belazzougui, Chen Qian, and Qin Zhang. A fast, small, and dynamic

forwarding information base. *ACM SIGMETRICS Performance Evaluation Review*, 45 (1):41–42, June 2017. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Yu:2018:MEU

[YBQZ18] Ye Yu, Djamal Belazzougui, Chen Qian, and Qin Zhang. Memory-efficient and ultra-fast network lookup and forwarding using Othello hashing. *IEEE/ACM Transactions on Networking*, 26(3): 1151–1164, June 2018. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Yang:2012:RHA

[YCJ12] Gaobo Yang, Ning Chen, and Qin Jiang. A robust hashing algorithm based on SURF for video copy detection. *Computers and Security*, 31 (1):33–39, February 2012. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404811001404`.

Yo:1993:OPA

[YCRY93] M.-L. Yo, M.-S. Chen, C. Ravishankar, and P. Yu. On optimal processor allocation to support pipelined hash joins. In Buneman and Jajodia [BJ93], page ?? ISBN 0-89791-592-5. LCCN QA76.A1 A1135 v.22:2.

Yang:1984:DPH

[YD84] W. P. Yang and M. W. Du. A dynamic perfect hash function defined by an extended hash indicator table. In Dayal et al. [DSS84], pages 245–254.

Yang:1985:BMC

[YD85] W. P. Yang and M. W. Du. A backtracking method for constructing perfect hash functions from a set of mapping functions. *BIT (Nordisk tidskrift for informationsbehandling)*, 25(1): 148–164, 1985. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

Yuen:1986:DFO

[YD86a] T. S. Yuen and H. C. Du. Dynamic file organizations for partial match retrieval based on linear hashing. In *Proceedings of the International Conference on Data Engineering*, pages 116–123. IEEE Computer Society, IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, February 1986. ISBN 0-8186-0655-X. LCCN ???? IEEE Service Cent. Piscataway, NJ, USA.

Yuen:1986:DFS

[YD86b] Tak-Sun Yuen and David Huang-Chang Du. Dynamic file structure for partial match retrieval based

on overflow bucket sharing. *IEEE Transactions on Software Engineering*, SE-12 (8):801–810, August 1986. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6312983.

Yang:1983:SPH

[YDT83] W. P. Yang, M. W. Du, and J. C. Tsay. Single-pass perfect hashing for data storage and retrieval. In *Proceedings of the 17th Annual Conference on Information Sciences and Systems.*, pages 470–476. Johns Hopkins Univ, Baltimore, Md, USA, 1983.

Yen:1991:MPH

[Yen91] I.-L. Yen. Massively parallel hash algorithms and performance. In ACM-CSC'91 [ACM91b], pages 21–28. ISBN 0-89791-382-5. LCCN QA76.5 .A137 1991.

Yu:2010:DRF

[YG10] Zhen Yu and Yong Guan. A dynamic en-route filtering scheme for data reporting in wireless sensor networks. *IEEE/ACM Transactions on Networking*, 18(1): 150–163, February 2010. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Yuan:2012:EMR

[YGC+12] Jiangbo Yuan, Guillaume Gravier, Sébastien Campion, Xiuwen Liu, and Hervé Jégou. Efficient mining of repetitions in large-scale TV streams with product quantization hashing. *Lecture Notes in CS*, 7583: 271–280, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-33863-2_27.

Yang:2019:DSA

[YGS+19] T. Yang, S. Gao, Z. Sun, Y. Wang, Y. Shen, and X. Li. Diamond sketch: Accurate per-flow measurement for big streaming data. *IEEE Transactions on Parallel and Distributed Systems*, 30(12): 2650–2662, December 2019. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Yasuda:1989:PAM

[YIAS89] Takuya Yasuda, Satoshi Igarashi, Oichi Atoda, and Nobuo Saito. 'Pattern associative memory' and its use in logic programming language processors. *Systems and computers in Japan*, 20 (11):11–20, November 1989. CODEN SCJAEP. ISSN 0882-1666 (print), 1520-684X (electronic).

Yum:2010:FVH

[YKLH10] Dae Hyun Yum, Jin Seok Kim, Pil Joong Lee, and Sung Je Hong. On fast verification of hash chains. *Lecture Notes in CS*, 5985: 382–396, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-11925-5_26`.

Yao:1983:SSG

[YkWY83] Tien-Shun Yao, Bao ku Wang, and Jing-Sheng Yu. Simulation system of graph composed Chinese character processing. In Anonymous [Ano83], pages 367–378. ISBN 0-87664-739-5. LCCN TA165.M52 1983. Two volumes.

Yi:1997:NHF

[YL97] X. Yi and K.-Y. Lam. A new hash function based on block cipher. *Lecture Notes in CS*, 1270:139–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Yang:2004:ACH

[YL04] Cungang Yang and Celia Li. Access control in a hierarchy using one-way hash functions. *Computers and Security*, 23(8):659–664, December 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404804001919`.

Yen:1990:HTS

[YLB90] I.-L. Yen, D.-R. Leu, and F. B. Bastani. Hash table and sorted array: a case study of multi-entry data structures in massively parallel systems. In Jájá [Jáj90], pages 51–54. ISBN 0-8186-9053-4. LCCN QA76.58 .S95 1990.

Yi:2009:SSG

[YLC+09] Ke Yi, Feifei Li, Graham Cormode, Marios Hadjieleftheriou, George Kollios, and Divesh Srivastava. Small synopses for group-by query verification on outsourced data streams. *ACM Transactions on Database Systems*, 34 (3):15:1–15:??, August 2009. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Yang:2019:NAK

[YLSZ19] Zheng Yang, Junyu Lai, Yingbing Sun, and Jianying Zhou. A novel authenticated key agreement protocol with dynamic credential for WSNs. *ACM Transactions on Sensor Networks*, 15(2):22:1–22:??, April 2019. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3303704`.

Yu:2020:VBG

[YLZ20] Bin Yu, Xiaofeng Li, and He Zhao. Virtual block group: a scalable blockchain model with partial node storage and distributed hash table. *The Computer Journal*, 63(10):1524–1536, October 2020. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/63/10/1524/5828295`.

Yokoyama:1989:NLP

[YMI89] Shoichi Yokoyama, Fumio Motoyoshi, and Hitoshi Isahara. Natural language processing system with a large vocabulary in secondary storage. *Denshi Gijutsu Sogo Kenkyusho Iho/Bulletin of the Electrotechnical Laboratory*, 53(5):52–70, 1989. CODEN DGSKAR. ISSN 0366-9092.

Yamane:1989:DEH

[YNKM89] Y. Yamane, M. Narita, F. Kozakura, and A. Makinouchi. Design and evaluation of a high-speed extended relational database engine, XRDB. In *Proc. of the 1st Intern. Symposium on Database Systems for Advanced Applications, Seoul, Korea*, page ?? ????, ????, April 1989.

Yadan:2009:HJO

[YNW+09] Deng Yadan, Jing Ning, Xiong Wei, Chen Luo, and Chen Hongsheng. Hash join optimization based on shared cache chip multiprocessor. *Lecture Notes in CS*, 5463:293–307, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-00887-0_26`.

Yu:1987:RDI

[YR87] C. T. Yu and C. J. Rijsbergen, editors. *Research and Development in Information Retrieval: Proceedings of the Tenth Annual International ACM SIGIR Conference*. ACM Press, New York, NY 10036, USA, 1987. ISBN 0-89791-232-2. LCCN Z 699 A1 I58 1987. US$19.

Yoon:2004:SUA

[YRY04] Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo. A secure user authentication scheme using hash functions. *Operating Systems Review*, 38(2):62–68, April 2004. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Yum:2009:SLF

[YSEL09] Dae Hyun Yum, Jae Woo Seo, Sungwook Eom, and Pil Joong Lee. Single-layer fractal hash chain traversal with almost optimal complexity. *Lecture Notes in*

CS, 5473:325–339, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-00862-7_22.

Yao:2005:HBL

[YSL05] D. Yao, Cyrus Shahabi, and Per-Åke Larson. Hash-based labeling techniques for storage scaling. *VLDB Journal: Very Large Data Bases*, 14(2):222–237, April 2005. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Yang:2011:NHB

[YSW+11] Kai Yang, Yan Shi, Weili Wu, Xiaofeng Gao, and Jiaofei Zhong. A novel hash-based streaming scheme for energy efficient full-text search in wireless data broadcast. *Lecture Notes in CS*, 6587:372–388, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20149-3_28.

Yaniv:2016:HDC

[YT16] Idan Yaniv and Dan Tsafrir. Hash, don't cache (the page table). *ACM SIGMETRICS Performance Evaluation Review*, 44(1):337–350, June 2016. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Yang:1997:HFM

[YTHC97] Cheng-Hsing Yang, Chia-Chun Tsai, Jan-Ming Ho, and Sao-Jie Chen. Hmap: a fast mapper for EPGAs using extended GBDD hash tables. *ACM Transactions on Design Automation of Electronic Systems.*, 2(2):135–150, January 1997. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic). URL http://www.acm.org/pubs/articles/journals/todaes/1997-2-2/p135-yang/p135-yang.pdf; http://www.acm.org/pubs/citations/journals/todaes/1997-2-2/p135-yang/.

Yu:2006:SST

[YTJ06] Yi Yu, Masami Takata, and Kazuki Joe. Similarity searching techniques in content-based audio retrieval via hashing. *Lecture Notes in CS*, 4351:397–407, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-69423-6_39.

Ytrehus:2006:LFN

[Ytr06] Øyvind Ytrehus, editor. *Coding and Cryptography: International Workshop, WCC 2005, Bergen, Norway, March 14–18, 2005. Revised Selected Papers*, volume 3969 of *Lecture Notes in Com-*

puter Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Yu:1992:IWR

[Yu92] P. S. Yu, editor. *2nd International workshop on research issues on data engineering: transaction and query processing: – February 1992, Tempe, AZ*, INTERNATIONAL WORKSHOP ON RESEARCH ISSUES IN DATA ENGINEERING 1992; 2nd. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. ISBN 0-8186-2660-7, 0-8186-2661-5, 0-8186-2662-3. LCCN QA76.9.D3 I593 1992.

Yu:2018:RHT

[Yu18] Peng Yu. Revisiting hash table performance. Web site., January 13, 2018. URL `https://attractivechaos.wordpress.com/2018/01/13/revisiting-hash-table-performance/`.

Yuan:1992:VLD

[Yua92] Li-Yan Yuan, editor. *Very Large Data Bases: VLDB '92, Proceedings of the 18th International Conference on Very Large Data Bases, August 23–27, 1992, Vancouver, Canada*. Morgan Kaufmann Publishers, San Francisco, CA, 1992. ISBN 1-55860-151-1. LCCN QA76.9.D3 I61 1992.

Yuba:1982:SOP

[Yub82] Toshitsugu Yuba. Studies on optimization problems of key searching. *Denshi Gijutsu Sogo Kenkyusho Kenkyu Hokoku/Researches of the Electrotechnical Laboratory*, ??(823):??, March 1982. CODEN DGSKBS. ISSN 0366-9106.

Yung:2002:ACC

[Yun02] Moti Yung, editor. *Advances in cryptology — CRYPTO 2002: 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18–22, 2002: Proceedings*, volume 2442 of *Lecture Notes in Computer Science and Lecture Notes in Artificial Intelligence*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2002. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t2442.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2442`.

Yuval:1975:FNN

[Yuv75] G. Yuval. Finding near neighbours in K-dimensional space. *Information Processing Letters*, 3(4):113–114, March ??, 1975. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Yang:2009:ILV

[YWH09] Heng Yang, Qing Wang, and Zhoucan He. Indexing large visual vocabulary by randomized dimensions hashing for high quantization accuracy: Improving the object retrieval quality. *Lecture Notes in CS*, 5702:783–790, 2009. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-03767-2_95`.

Young:2001:HRS

[YY01] Adam Young and Moti Yung. Hash to the rescue: Space minimization for PKI directories. *Lecture Notes in CS*, 2015:235–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2015/20150235.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2015/20150235.pdf`.

Yoon:2007:SCH

[YY07] Eun-Jun Yoon and Kee-Young Yoo. A secure chaotic hash-based biometric remote user authentication scheme using mobile devices. *Lecture Notes in CS*, 4537:612–623, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-540-72909-9_68`.

Yen:2000:WOW

[YZ00] Sung-Ming Yen and Yuliang Zheng. Weighted one-way hash chain and its applications. *Lecture Notes in CS*, 1975:135–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1975/19750135.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1975/19750135.pdf`.

Yu:2016:NFC

[YZ16] Qian Yu and Chang N. Zhang. A new and fast cryptographic hash function based on RC4. *Cryptologia*, 40(6):522–540, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Zamora:1980:ADC

[Zam80] Antonio Zamora. Automatic detection and correction of spelling errors in a large data base. *Journal of the American Society for Information Science*, 31(1): 51–57, January 1980. CODEN AISJB6. ISSN 0002-8231 (print), 1097-4571 (electronic).

Zhang:2006:CFS

[ZBB+06] Cheng Zhang, Bhupesh Bansal, Paulo S. Branicio, Rajiv K. Kalia, Aiichiro Nakano, Ashish Sharma, and Priya Vashishta. Collision-free spatial hash functions for structural analysis of billion-vertex chemical bond networks. *Computer Physics Communications*, 175(5): 339–347, September 1, 2006. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465506002311`.

Zobrist:1977:DCO

[ZC77] Albert L. Zobrist and Frederick R. Carlson, Jr. Detection of combined occurrences. *Communications of the Association for Computing Machinery*, 20(1):31–35, January 1977. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Zhu:2012:JLS

[ZC12] Xinglei Zhu and Chang W. Chen. A joint layered scheme for reliable and secure mobile JPEG-2000 streaming. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 8(3):30:1–30:??, July 2012. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Zeng:2019:PKE

[ZCZQ19] Ming Zeng, Jie Chen, Kai Zhang, and Haifeng Qian. Public key encryption with equality test via hash proof system. *Theoret. Comput. Sci.*, 795(??):20–35, November 26, 2019. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397519303822`.

Zollhofer:2015:SBR

[ZDI+15] Michael Zollhöfer, Angela Dai, Matthias Innmann, Chenglei Wu, Marc Stamminger, Christian Theobalt, and Matthias Nießner. Shading-based refinement on volumetric signed distance functions. *ACM Transactions on Graphics*, 34(4):96:1–96:??, August 2015. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Zeller:1991:AHJ

[Zel91] H. Zeller. *Adaptive Hash-Join-Algorithmen (in German)*. Ph.d. thesis, University of Stuttgart, Stuttgart, Germany, November 1991. ?? pp.

Zemor:1991:HFG

[Zem91] G. Zemor. Hash functions and graphs with large girths. In Davies [Dav91], pages 508–511. ISBN 0-387-54620-0 (New York), 3-540-54620-0 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1991.

Zemor:1994:HFC

[Zém94] Gilles Zémor. Hash functions and Cayley graphs. *Designs, Codes, and Cryptography*, 4(4):381–394, 1994. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

Zhang:2006:NGD

[ZF06] Bin Zhang and Dengguo Feng. New guess-and-determine attack on the self-shrinking generator. *Lecture Notes in CS*, 4284: 54–68, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/11935230_4.pdf`.

Zeller:1990:AHJ

[ZG90a] H. Zeller and J. Gray. An adaptive hash join algorithm for multiuser environments. In McLeod et al. [MSDS90], page 186. ISBN 1-55860-149-X. LCCN ???

Zeller:1990:HJA

[ZG90b] H. Zeller and J. Gray. Hash join algorithms in a multiuser environment. In McLeod et al. [MSDS90], page ?? ISBN 1-55860-149-X. LCCN ???

Zhang:2005:ILL

[ZGG05] Hui Zhang, Ashish Goel, and Ramesh Govindan. Improving lookup latency in distributed hash table systems using random sampling. *IEEE/ACM Transactions on Networking*, 13 (5):1121–1134, October 2005. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Zuo:2018:WFC

[ZH18] Pengfei Zuo and Yu Hua. A write-friendly and cache-optimized hashing scheme for non-volatile memory systems. *IEEE Transactions on Parallel and Distributed Systems*, 29(5):985–998, May 2018. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL `https://www.computer.org/csdl/trans/`

td/2018/05/08186236-abs.html.

Zhang:2007:TTI

[Zha07] Rui Zhang. Tweaking TBE/IBE to PKE transforms with Chameleon hash functions. *Lecture Notes in CS*, 4521:323–339, 2007. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-540-72738-5_21.

Zhai:2019:DVP

[Zha19a] Sheping Zhai. Distance variety preserving hashing for large-scale retrieval. *Concurrency and Computation: Practice and Experience*, 31 (12):e4829:1–e4829:??, June 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Zhandry:2019:ME

[Zha19b] Mark Zhandry. The magic of ELFs. *Journal of Cryptology*, 32(3):825–866, July 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9289-9.

Zukowski:2006:ACH

[ZHB06] M. Zukowski, S. Héman, and P. A. Boncz. Architecture-conscious hashing. In Ailamaki et al. [ABM06], pages 6:1–6:8. ISBN 1-59593-466-9. LCCN QA76.9.D3 I58388 2006. URL http://portal.acm.org/toc.cfm?id=1140402.

Zhu:2013:SHF

[ZHC+13] Xiaofeng Zhu, Zi Huang, Hong Cheng, Jiangtao Cui, and Heng Tao Shen. Sparse hashing for fast multimedia search. *ACM Transactions on Information Systems*, 31 (2):9:1–9:??, May 2013. CODEN ATISET. ISSN 1046-8188.

Zheng:1990:PDS

[Zhe90] Yuliang Zheng. *Principles for Designing Secure Block Ciphers and One-Way Hash Functions*. PhD thesis, Yokohama National University, Yokohama, Japan, 1990. ?? pp.

Zheng:1994:RSS

[ZHS94] Yuliang Zheng, T. Hardjono, and J. Seberry. Reusing shares in secret sharing schemes. *The Computer Journal*, 37(3):199–205, ???? 1994. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic).

Zobel:2001:MHT

[ZHW01] Justin Zobel, Steffen Heinz, and Hugh E. Williams. In-memory hash tables for accumulating text vocabularies. *Information Processing Letters*, 80(6):271–277,

December 31, 2001. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.elsevier.com/gej-ng/10/23/20/84/37/27/abstract.html`.

Zuo:2019:LHH

[ZHW19] Pengfei Zuo, Yu Hua, and Jie Wu. Level hashing: a high-performance and flexible-resizing persistent hashing index structure. *ACM Transactions on Storage*, 15(2): 13:1–13:??, June 2019. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3322096`.

Zhou:2021:ELS

[ZHW21] Wei Zhou, Jiankun Hu, and Song Wang. Enhanced locality-sensitive hashing for fingerprint forensics over large multi-sensor databases. *IEEE Transactions on Big Data*, 7(4):759–769, 2021. ISSN 2332-7790.

Zhang:2021:TME

[ZHX+21] Shi Zhang, Jin Huang, Ruliang Xiao, Xin Du, Ping Gong, and Xinhong Lin. Toward more efficient locality-sensitive hashing via constructing novel hash function cluster. *Concurrency and Computation: Practice and Experience*, 33(20):e6355:1–e6355:??, October 25, 2021. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Zuo:2019:WDH

[ZHZ+19] P. Zuo, Y. Hua, M. Zhao, W. Zhou, and Y. Guo. Write deduplication and hash mode encryption for secure non-volatile main memory. *IEEE Micro*, 39(1):44–51, January/February 2019. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Zhang:2009:IBR

[ZJ09] Jianhong Zhang and Cheng Ji. An ID-based and repairing NTRUSign-based anonymous multi-proxy signature scheme. In IEEE, editor, *Proceedings of the International Conference on Computational Intelligence and Software Engineering, 2009. CiSE 2009, December 11–13, 2009, Wuhan, China*, pages 1–?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. ISBN 1-4244-4507-8. LCCN QA76.758 2009. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5362500`. IEEE catalog number CFP0926H.

Zhao:1994:DDBa

[ZJM94a] X. Zhao, R. G. Johnson, and N. J. Martin. DBJ — a dynamic balancing hash join algorithm in multipro-

cessor database systems. *Information system*, 19(1):89–100, January 1994. CODEN INSYD6. ISSN 0306-4379 (print), 1873-6076 (electronic).

Zhao:1994:DDBb

[ZJM94b] X. Zhao, R. G. Johnson, and N. J. Martin. DBJ — a dynamic balancing hash join algorithm in multiprocessor database systems. In Jarke et al. [JBJ94], pages 301–308. ISBN 0-387-57818-8 (New York), 3-540-57818-8 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.D3 I55844 1994. DM80.00.

Zhao:1994:DDBc

[ZJM94c] X. Zhao, R. G. Johnson, and N. J. Martin. DBJ — a dynamic balancing hash join algorithm in multiprocessor database systems. In Jarke et al. [JBJ94], pages 89–100. ISBN 0-387-57818-8 (New York), 3-540-57818-8 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.D3 I55844 1994. DM80.00.

Zee:2008:FFV

[ZKR08] Karen Zee, Viktor Kuncak, and Martin Rinard. Full functional verification of linked data structures. *SIGPLAN Notices*, 43(6):349–361, June 2008. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Zhang:2012:LLF

[ZL12] Donghui Zhang and Per-Åke Larson. LHlf: lock-free linear hashing (poster paper). *SIGPLAN Notices*, 47(8):307–308, August 2012. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). PPOPP '12 conference proceedings.

Zhou:2012:TSC

[ZLC+12] Junfeng Zhou, Guoxiang Lan, Ziyang Chen, Xian Tang, and Jingfeng Guo. Top-down SLCA computation based on hash search. *Lecture Notes in CS*, 7418: 272–283, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-32281-5_27`.

Zhang:2018:AKS

[ZLC+18] Dongxiang Zhang, Yuchen Li, Xin Cao, Jie Shao, and Heng Tao Shen. Augmented keyword search on spatial entity databases. *VLDB Journal: Very Large Data Bases*, 27(2):225–244, April 2018. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Zhu:2020:FMM

[ZLC+20] Lei Zhu, Xu Lu, Zhiyong Cheng, Jingjing Li, and Huaxiang Zhang. Flexible multi-modal hashing for scalable multimedia retrieval. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 11(2):14:1–14:20, March 2020. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3365841`.

Zhang:2007:BHR

[ZLL+07] Zheng Zhang, Qiao Lian, Shiding Lin, Wei Chen, Yu Chen, and Chao Jin. BitVault: a highly reliable distributed data retention platform. *Operating Systems Review*, 41(2):27–36, April 2007. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Zhang:2018:LFT

[ZLLD18] Deli Zhang, Pierre Laborde, Lance Lebanoff, and Damian Dechev. Lock-free transactional transformation for linked data structures. *ACM Transactions on Parallel Computing (TOPC)*, 5(1):6:1–6:??, September 2018. CODEN ???? ISSN 2329-4949 (print), 2329-4957 (electronic).

Zhang:2012:HSP

[ZLY+12] Yijia Zhang, Hongfei Lin, Zhihao Yang, Jian Wang, and Yanpeng Li. Hash subgraph pairwise kernel for protein-protein interaction extraction. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 9(4):1190–1202, July 2012. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Zhang:2013:BET

[ZLY+13] Yijia Zhang, Hongfei Lin, Zhihao Yang, Jian Wang, and Yanpeng Li. Biomolecular event trigger detection using neighborhood hash features. *Journal of Theoretical Biology*, 318(??):22–28, February 7, 2013. CODEN JTBIAP. ISSN 0022-5193 (print), 1095-8541 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S002251931200570X`.

Zheng:1991:SPO

[ZMI91] Y. Zheng, T. Matsumoto, and H. Imai. Structural properties of one-way hash functions. *Lecture Notes in CS*, 537:285–302, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zhu:2016:LEI

[ZNPM16] Erkang Zhu, Fatemeh Nargesian, Ken Q. Pu, and

Renée J. Miller. LSH ensemble: Internet-scale domain search. *Proceedings of the VLDB Endowment*, 9(12): 1185–1196, August 2016. CODEN ???? ISSN 2150-8097.

Zhou:1993:DAH

[ZO93] X. F. Zhou and M. E. Orlowska. A dynamic approach for handling data skew problems in parallel hash join computation. In Anonymous [Ano93c], pages 133–137. ISBN 7-80003-285-X, 0-7803-1233-3, 0-87031-232-5, 0-87031-234-1. LCCN TK5105.5.I327 1993. Five volumes.

Zhao:2013:AAP

[ZO13] Zhen Wei Zhao and Wei Tsang Ooi. APRICOD: an access-pattern-driven distributed caching middleware for fast content discovery of noncontinuous media access. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 9(2): 15:1–15:??, May 2013. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Zobrist:1970:NHMa

[Zob70a] Albert L. Zobrist. A new hashing method with application for game playing. Technical Report 88, Computer Sciences Department, University of Wisconsin, Madison, WI, USA, 1970.

Zobrist:1970:NHMb

[Zob70b] Albert L. Zobrist. A new hashing method with application for game playing. *ICCA Journal*, 13(2):69–73, ???? 1970. ISSN 0920-234X.

Zou:1985:MMC

[Zou85] Youwen Zou. MPHF method for Chinesizing Cobol reserved words. *Hunan Keji Daxue Xuebao/Journal of Hunan Science and Technology University*, 1(1-2):97–104, September 1985. CODEN HKDXEX.

Zheng:1990:HOW

[ZPS90] Y. Zheng, J. Pieprzyk, and J. Seberry. HAVAL — a one-way hashing algorithm with variable length of output. In Seberry and Pieprzyk [SP90], page ?? ISBN 0-387-53000-2 (New York), 3-540-53000-2 (Berlin). LCCN QA76.9.A25 A87 1990.

Zheng:1993:HOWa

[ZPS93a] Y. Zheng, J. Pieprzyk, and J. Seberry. HAVAL — a one-way hashing algorithm with variable length of output. In Seberry and Zheng [SZ93], pages 3.1–3.10. ISBN 0-387-57220-1 (New York), 3-540-57220-1 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 A87 1992.

Zheng:1993:HOWb

[ZPS93b] Y. Zheng, J. Pieprzyk, and J. Seberry. HAVAL — a one-way hashing algorithm with variable length of output. *Lecture Notes in CS*, 718:83–104, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Zhao:2012:HCB

[ZQSH12] Huawei Zhao, Jing Qin, Minglei Shu, and Jiankun Hu. A hash chains based key management scheme for wireless sensor networks. *Lecture Notes in CS*, 7672: 296–308, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-35362-8_23`.

Zhou:2008:RTS

[ZRL+08] Kun Zhou, Zhong Ren, Stephen Lin, Hujun Bao, Baining Guo, and Heung-Yeung Shum. Real-time smoke rendering using compensated ray marching. *ACM Transactions on Graphics*, 27 (3):36:1–36:??, August 2008. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Zezula:1991:DPS

[ZRT91] P. Zezula, F. Rabitti, and P. Tiberio. Dynamic partitioning of signature files. *ACM Transactions on Information Systems*, 9(4):336–369, October 1991. CODEN ATISET. ISSN 1046-8188. URL `http://www.acm.org:80`.

Zukowski:2021:TPO

[Zuk21] Marcin Zukowski. Technical perspective: Optimistically compressed hash tables & strings in the USSR. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 50(1): 59, June 2021. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic). URL `https://dl.acm.org/doi/10.1145/3471485.3471499`.

Zhang:2005:ISS

[ZW05] Jianhong Zhang and Yumin Wang. An improved signature scheme without using one-way Hash functions. *Applied Mathematics and Computation*, 170(2): 905–908, November 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Zhang:2010:LCH

[ZWCL10] Dell Zhang, Jun Wang, Deng Cai, and Jinsong Lu. Laplacian co-hashing of terms and documents. *Lecture Notes in CS*, 5993:577–580, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/`

10.1007/978-3-642-12275-0_51.

Zhang:2017:LBP

[ZWH17] Jiaming Zhang, Shuhui Wang, and Qingming Huang. Location-based parallel tag completion for geo-tagged social image retrieval. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 8(3):38:1–38:??, April 2017. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic).

Zhang:2014:FFS

[ZWT+14] Yong-Dong Zhang, Yu Wang, Sheng Tang, Steven C. H. Hoi, and Jin-Tao Li. FSpH: Fitted spectral hashing for efficient similarity search. *Computer vision and image understanding: CVIU*, 124(??):3–11, July 2014. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic). URL http://www.sciencedirect.com/science/article/pii/S1077314214000241.

Zou:2012:PAS

[ZWW+12] Jian Zou, Wenling Wu, Shuang Wu, Bozhan Su, and Le Dong. Preimage attacks on step-reduced SM3 hash function. *Lecture Notes in CS*, 7259:375–390, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-31912-9_25.

Zhang:2021:LCF

[ZWY21] Donglin Zhang, Xiao-Jun Wu, and Jun Yu. Label consistent flexible matrix factorization hashing for efficient cross-modal retrieval. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 17 (3):90:1–90:18, August 2021. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/doi/10.1145/3446774.

Zhang:2019:SPB

[ZXL19] Rui Zhang, Rui Xue, and Ling Liu. Security and privacy on blockchain. *ACM Computing Surveys*, 52(3): 51:1–51:??, July 2019. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3316481.

Zhou:2020:NUI

[ZYWM20] Yanwei Zhou, Bo Yang, Tao Wang, and Yi Mu. Novel updatable identity-based hash proof system and its applications. *Theoret. Comput. Sci.*, 804(??): 1–28, January 12, 2020. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397519306607.

Zhao:1983:PMC

[ZZ83] Hejun Zhao and Yuefang Zhang. Practical microcomputer management system of an automated stereowarehouse. *Chi Hsieh Kung Ch'eng Hsueh Pao/Chinese Journal of Mechanical Engineering*, 19(3):22–31, September 1983. CODEN CHHKA2. ISSN 0577-6686.

Zhou:2018:DSH

[ZZLZ18] Ke Zhou, Jiangfeng Zeng, Yu Liu, and Fuhao Zou. Deep sentiment hashing for text retrieval in social CIoT. *Future Generation Computer Systems*, 86(??): 362–371, September 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X18302383`.

Zhang:2021:POP

[ZZLZ21] Zheng Zhang, Xiaofeng Zhu, Guangming Lu, and Yudong Zhang. Probability ordinal-preserving semantic hashing for large-scale image retrieval. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 15 (3):37:1–37:22, May 2021. CODEN ???? ISSN 1556-4681 (print), 1556-472X (electronic). URL `https://dl.acm.org/doi/10.1145/3442204`.

Zhang:2017:NLR

[ZZM17] Leyou Zhang, Jingxia Zhang, and Yi Mu. Novel leakage-resilient attribute-based encryption from hash proof system. *The Computer Journal*, 60(4):541–554, March 23, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `https://academic.oup.com/comjnl/article/60/4/541/2608069`.