-

A Bibliography of Publications on Cryptography: 2010–2019

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/

09 April 2024
Version 1.527

Title word cross-reference

BCEO19, BCEO20, BBB$^+$16a, BSSV12, BHG12, BKPW12, BRT12, BHH$^+$15, BBKL19, BS13b, BFK$^+$10, Bon12, BSJ15, BF19, Boy13, BKJP12, BDH11, BCF$^+$14, But17, CMLS15, CLL16, CGMO14, CKHP19, CMRH17, CCM17, CSH$^+$18, CZLC12a, CZLC12b, CLHC12, CCZC13, CLY14, CZLC14, CST$^+$17, CZCD18, CLND19, CGL$^+$12, CDD13, CGY$^+$13, CD12, Chi12, CK18, CD16b, CDLW19, CHH$^+$19, DSMM14, DHT$^+$19, DL17, DS19, DA12, DLZ$^+$16b, EM12, EKB$^+$16, EFGT18, FM15, FHH10b, FHR14, FZT14, FGRQ18, FGM10, FYD$^+$19, FR15, FVS17, FP19, FSX12b, FSX12c, FSX12a, GT19, GWWC15, GDLL18, GZZ$^+$13, GSW$^+$16, GV14b, GI12, GY13, GDCC16, GVW15, GJJ15, GJZ17, GRRZ18, HZC$^+$12, HSMY12, HSM14, HBC$^+$19, HEP$^+$11, HIJ$^+$19, HL10a, HZX15, HWZP18, HCPLSB12, HKL$^+$12]. **Based** [HG12, HMR12, HSA14, HWS$^+$19, HPO$^+$15, HKR$^+$18, HGT15, HCL$^+$14, HLN$^+$10, Hül13, HRS16, HBG$^+$17, HEC$^+$12, HM19, HP12, HP17, JTZ$^+$16, JP19, JHHN12, JEA$^+$15, JKHeY12, KMZS19, KS18b, KZG10, KK12, KKA15, Kha10, KLY$^+$12, KSSY12, KPKS12, KHRG19, KRB12, KAK18, KS15, LMGC17, LMG$^+$18, LYY$^+$18a, LYX$^+$19, LTKP16, LSL12a, LKBK19, LSL12b, LW11b, LW11c, LW12, LHF12, LJLC12, LYZ$^+$13, LHL$^+$14, LTH$^+$15, LLC$^+$15, LDZ16, LTZY16, LLZ$^+$17, LLLH18, LPL15, LSLW15, LAL$^+$15, LH11c, Lin15, LYL$^+$18, LP12, LNWZ19, LNZ$^+$13, LCCJ13, LWCJ14, LNXY15, LHL15, LW16, LPO$^+$17, LHW18, LLD19, LZZ$^+$19a, LGPRH14, LDB$^+$15, LD13, LSC12, LBR12, LLH18, MWZ12, Ma17a, MLO17, MEFO12, MCDB12, MVV12, MD12b, MBC15, MKN13, MZ17b, MCS$^+$15, MMS17b, MKF$^+$16, MCF17, Men13a, MST18, Mor12, MSKRJ17, MKAA17, Muf16, NIS15, NC12, NXH$^+$17, NDR$^+$19, NXB13, NLLJ12, NLY15, pNyWyY$^+$14]. **Based** [OTD10, PB12, PSSK19, PTT16, PYM$^+$15, PDNH15, PPS12b, PYS18, PG12, PAS13b, PNRC17, QJC$^+$18, QF19, RVH$^+$16, RSR$^+$19, RZZ$^+$15, RS16, Rao17, RR11, RDZ$^+$16, RVRSCM12, RW12, RJV$^+$18, SBS18, SSW12, Sar18a, SS13, Sen17, SJLK18, SXH$^+$19, SJ12, SGP$^+$12, SPG$^+$19, SP15b, SSA13, SRAA17, SNCK18, SH15, SGH15, TB18, TKR14, TWZ11, TW12, TWZ$^+$12, TYM$^+$17, TSH17, TT12, TTH15, TFS19, TC10, VDB$^+$16, VGA15, VGA19, Vle12, WY10, Wan10, WSSO12, WgMW12, WYW$^+$13, Wan14, WZCC18, yWXyZ$^+$18, WDCL18, WLH15, WHLH17, WCL$^+$18, WT10b, WMS$^+$12, WZCH19, XNG$^+$14, XNRG15, XXZ12, XMLC13, XLQ09, XQL11, Xio12, XGLM14, XWLJ16, XJW$^+$16, XJR$^+$17, XHX$^+$17, XHZ$^+$19, YE12, YZLC12, YZX$^+$12, YGFL15, YHSW19, YTS12, Ye10, Ye14, YH16, YTH17, YYO15, Y$^+$17, YKNS12, YHK$^+$10, YMWS11, YKC$^+$11, YFK$^+$12, YCZY12, ZSP$^+$19, ZPM$^+$15, ZJ11, ZXZ$^+$11, ZDL12, ZLH$^+$12]. **Based** [ZQQ15, ZMW16, ZXYL16, ZWWW17, ZZM17, ZWZ17b, ZYZ$^+$19, ZPW16, ZHW15, ZVG16, ZPXX17, ZGCZ18, ZYM18, ZYH$^+$19, ZHL15, AMN18, AGLW16, AaBT16, ARL13, AY14a, AHS14, AAL19, AAT16, AA14, ASO14, AIA$^+$18a, AIM$^+$19, AKG13, ASVE13, ACA$^+$16, ARG19, AM19, Ara13, ATI$^+$10, ACC$^+$13, AHL$^+$12, BK19, AVAH18, BS15, BDM18, BDL$^+$19, BBBP13, BD18, BGAD12, BAAS13, BBTC20, BDM$^+$19, BOB13, BWR12a, BW13, BWA13, BMM12, BZD16a, BC18, BTK15, BBB16b, BK12b, CPPT18, CML$^+$18, CXX$^+$19, CFL13, CFY$^+$10, CCLL11, CTL12, CLSW12, CNF$^+$18, CRS$^+$18, CG12b, CSZ$^+$11, CHX13, CSS$^+$13, CW14a, CLC$^+$19, CWZ19, CXWT19, CCMB19, CTHP13, CJP12, CJP15, CCG10, CTL13, Cho14, Con12, CHL19, dCCSM$^+$12, Cra11, CDL18, DSCS12, DGMT19, DZ14, DLN13, Dra16, uHAN$^+$18, EZ15, FH13, FG19, Far14, FA14a, FA14b, FIO15]. **based** [Fay16, FLYL16b, FHZW18, FMC19,

References

Akyildiz:2014:OTB

[AA14] Ersan Akyildiz and Muhammad Ashraf. An overview of trace based public key cryptography over finite fields. *Journal of Computational and Applied Mathematics*, 259 (part B)(??):599–621, March 15, 2014. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042713005669.

Abouaroek:2019:NAU

[AA19] Musaeed Abouaroek and Khaleel Ahmad. Node authentication using NTRU algorithm in opportunistic network. *Scalable Computing: Practice and Experience*, 20(1):83–92, ???? 2019. CODEN ???? ISSN 1895-1767. URL https://www.scpe.org/index.php/scpe/article/view/1481.

Aditya:2019:ISF

[AAA+19] B. P. Aditya, U. G. K. Avaneesh, K. Adithya, Akshay Murthy, R. Sandeep, and B. Kavyashree. Invisible semi-fragile watermarking and steganography of digital videos for content authentication and data hiding. *International Journal of Image and Graphics (IJIG)*, 19(3):??, 2019. ISSN 0219-4678. URL https://www.worldscientific.com/doi/10.1142/S0219467819500153.

Applebaum:2017:AC

[AAB17] Benny Applebaum, Jonathan Avron, and Chris Brzuska. Arithmetic cryptography. *Journal of the ACM*, 64 (2):10:1–10:??, June 2017. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Abo-alian:2016:KDB

[AaBT16] Alshaimaa Abo-alian, Nagwa L. Badr, and M. F. Tolba. Keystroke dynamics-based user authentication service for cloud computing. *Concurrency and Computation: Practice and Ex-*

perience, 28(9):2567–2585, June 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Ambrosin:2016:FAB

[AAC+16] Moreno Ambrosin, Arman Anzanpour, Mauro Conti, Tooska Dargahi, Sanaz Rahimi Moosavi, Amir M. Rahmani, and Pasi Liljeberg. On the feasibility of attribute-based encryption on Internet of Things devices. *IEEE Micro*, 36(6):25–35, November/December 2016. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL https://www.computer.org/csdl/mags/mi/2016/06/mmi2016060025-abs.html.

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://malicioussha1.github.io/.

Ahmad:2019:PQE

[AAH+19] Awais Ahmad, Mudassar Ahmad, Muhammad Asif Habib, Shahzad Sarwar, Junaid Chaudhry, Muhammad Ahsan Latif, Saadat Hanif Dar, and Muhammad Shahid. Parallel query execution over encrypted data in database-as-a-service (DaaS). *The Journal of Supercomputing*, 75(4):2269–2288, April 2019. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Akdogan:2019:SKA

[AAL19] Dilara Akdogan, Duygu Karaoglan Altop, and Albert Levi. Secure key agreement based on ordered biometric features. *Computer Networks (Amsterdam, Netherlands: 1999)*, 163(??):Article 106885, ???? 2019. CODEN ????. ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128618313975.

Arora:2012:ILM

[AARJ12] Divya Arora, Najwa Aaraj, Anand Raghunathan, and Niraj K. Jha. INVISIOS: a lightweight, minimally intrusive secure execution environment. *ACM*

Transactions on Embedded Computing Systems, 11 (3):60:1–60:??, September 2012. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Al-Azzam:2018:SRC

[AASSAA18] Saad Al-Azzam, Ahmad Sharieh, Azzam Sleit, and Nedaa Al-Azzam. Securing robot communication using packet encryption distribution. *Network Security*, 2018(2):8–14, February 2018. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485818300151`.

Akleylek:2016:SPM

[AAT16] Sedat Akleylek, Erdem Alkim, and Zaliha Yüce Tok. Sparse polynomial multiplication for lattice-based cryptography with small complexity. *The Journal of Supercomputing*, 72(2):438–450, February 2016. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://link.springer.com/article/10.1007/s11227-015-1570-1`.

Aghili:2018:ISA

[AATM18] Seyed Farhad Aghili, Maede Ashouri-Talouki, and Hamid Mala. DoS, impersonation and de-synchronization attacks against an ultra-lightweight RFID mutual authentication protocol for IoT. *The Journal of Supercomputing*, 74(1):509–525, January 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Acar:2018:SHE

[AAUC18] Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys*, 51(4):79:1–79:??, September 2018. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Alizadeh:2016:AMC

[AAZ+16] Mojtaba Alizadeh, Saeid Abolfazli, Mazdak Zamani, Sabariah Baharun, and Kouichi Sakurai. Authentication in mobile cloud computing: a survey. *Journal of Network and Computer Applications*, 61(??):59–80, February 2016. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804515002258`.

Abdalla:2010:PCL

[AB10a] Michel Abdalla and Paulo S. L. M. Barreto, editors. *Progress in cryptology — Latincrypt 2010: first international conference on cryptology and information security in Latin America, Puebla, Mexico, August 8–11, 2010, proceedings*, volume 6212 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-14711-9 (softcover). LCCN ????

Atallah:2010:ATC

[AB10b] Mikhail J. Atallah and Marina Blanton, editors. *Algorithms and theory of computation handbook. Special topics and techniques*, volume 2 of *Chapman and Hall/CRC applied algorithms and data structures series*. Chapman and Hall/CRC, Boca Raton, FL, USA, second edition, 2010. ISBN 1-58488-820-2. ???? pp. LCCN QA76.9.A43 A433 2010. URL http://www.crcnetbase.com/isbn/9781584888208.

Anand:2015:ICL

[AB15] Kapil Anand and Rajeev Barua. Instruction-cache locking for improving embedded systems performance. *ACM Transactions on Embedded Computing Systems*, 14(3):53:1–53:??, April 2015. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

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].

Abbate:2012:RGWa

[Abb12] Janet Abbate. *Recoding Gender: Women's Changing Participation in Computing*. History of computing. MIT Press, Cambridge, MA, USA, 2012. ISBN 0-262-01806-3 (hardcover), 0-262-30546-1 (e-book), 1-283-95309-9. x + 247 pp. LCCN QA76.9.W65 A33 2012. URL http://mitpress.mit.edu/9780262018067.

Alleaume:2014:UQK

[ABB+14] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger. Using quantum key distribution for cryptographic purposes: a survey. *Theoretical Computer Science*, 560 (part 1)(??):62–81, December 4, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397514006963`.

Athmani:2019:EED

[ABB19a] Samir Athmani, Azeddine Bilami, and Djallel Eddine Boubiche. EDAK: An efficient dynamic authentication and key management mechanism for heterogeneous WSNs. *Future Generation Computer Systems*, 92(??):789–799, March 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X17315388`.

Avoine:2019:SDB

[ABB+19b] Gildas Avoine, Muhammed Ali Bingöl, Ioana Boureanu, Srdjan Capkun, Gerhard Hancke, Süleyman Kardas, Chong Hee Kim, Cédric Lauradoux, Benjamin Martin, Jorge Munilla, Alberto Peinado, Kasper Bonne Rasmussen, Dave Singelée, Aslan Tchamkerten, Rolando Trujillo-Rasua, and Serge Vaudenay. Security of distance-bounding: a survey. *ACM Computing Surveys*, 51(5):94:1–94:??, January 2019. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3264628`.

Almeida:2013:CCA

[ABBD13] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, and François Dupressoir. Certified computer-aided cryptography: Efficient provably secure machine code from high-level implementations. In ????, editor, *ACM Conference on Computer and Communications Security*, pages 1217–1230. ACM Press, New York, NY 10036, USA, 2013. ISBN ???? LCCN ???? URL `????`.

Arnold:2012:ICC

[ABC+12] T. W. Arnold, C. Buscaglia, F. Chan, V. Condorelli, J. Dayka, W. Santiago-Fernandez, N. Hadzic, M. D. Hocker, M. Jordan, T. E. Morris, and

K. Werner. IBM 4765 cryptographic coprocessor. *IBM Journal of Research and Development*, 56(1): 10:1–10:13, ???? 2012. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Ateniese:2017:LCS

[ABC+17] Giuseppe Ateniese, Giuseppe Bianchi, Angelo T. Capossele, Chiara Petrioli, and Dora Spenza. Low-cost standard signatures for energy-harvesting wireless sensor networks. *ACM Transactions on Embedded Computing Systems*, 16(3): 64:1–64:??, July 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Agrawal:2018:RLR

[ABC+18] Megha Agrawal, Tarun Kumar Bansal, Donghoon Chang, Amit Kumar Chauhan, Seokhie Hong, Jinkeon Kang, and Somitra Kumar Sanadhya. RCB: leakage-resilient authenticated encryption via re-keying. *The Journal of Supercomputing*, 74(9):4173–4198, September 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Ambrosin:2017:OBB

[ABCL17] Moreno Ambrosin, Paolo Braca, Mauro Conti, and Riccardo Lazzeretti. ODIN: Obfuscation-based privacy-preserving consensus algorithm for decentralized information fusion in smart device networks. *ACM Transactions on Internet Technology (TOIT)*, 18(1): 6:1–6:??, December 2017. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Adrian:2015:IFS

[ABD+15] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelink, and Paul Zimmermann. Imperfect forward secrecy: How Diffie–Hellman fails in practice. Report, INRIA Paris-Rocquencourt [and others], Rocquencourt, France, May 21, 2015. 13 pp. URL `https://weakdh.org/`; `https://weakdh.org/imperfect-forward-secrecy.pdf`.

Adrian:2019:IFS

[ABD+19] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel

Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. Imperfect forward secrecy: how Diffie–Hellman fails in practice. *Communications of the Association for Computing Machinery*, 62 (1):106–114, January 2019. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `https://cacm.acm.org/magazines/2019/1/233523/fulltext`.

Agosta:2015:OPP

[ABDP15] Giovanni Agosta, Alessandro Barenghi, Alessandro Di Federico, and Gerardo Pelosi. OpenCL performance portability for general-purpose computation on graphics processor units: an exploration on cryptographic primitives. *Concurrency and Computation: Practice and Experience*, 27(14):3633–3660, September 25, 2015. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Abe:2010:ACA

[Abe10] Masayuki Abe, editor. *Advances in cryptology — Asiacrypt 2010: 16th international conference on the theory and application of cryptology and information security, Singapore, December 5–9, 2010. Proceedings*, volume 6477 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-17372-1 (softcover). LCCN ????

Abe:2012:TBG

[Abe12] Masayuki Abe. Tools over bilinear groups for modular design of cryptographic tasks. *Lecture Notes in Computer Science*, 7496:1, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/accesspage/chapter/10.1007/978-3-642-33272-2_1`.

Arriaga:2012:JSS

[ABF12] Afonso Arriaga, Manuel Barbosa, and Pooya Farshim. On the joint security of signature and encryption schemes under randomness reuse: Efficiency and security amplification. *Lecture Notes in Computer Science*, 7341:206–223, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31284-7_13/`.

Almeida:2014:COS

[ABF+14] José Bacelar Almeida,

Manuel Barbosa, Jean-Christophe Filliâtre, Jorge Sousa Pinto, and Bárbara Vieira. CAOVerif: an open-source deductive verification platform for cryptographic software implementations. *Science of Computer Programming*, 91 (part B)(??):216–233, October 1, 2014. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S016764231200189X`.

Ananth:2013:SFP

[ABGR13] Prabhanjan Ananth, Raghav Bhaskar, Vipul Goyal, and Vanishree Rao. On the (in)security of Fischlin's paradigm. *Lecture Notes in Computer Science*, 7785:202–221, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-36594-2_12/`.

Avoine:2016:SSP

[ABHC+16] Gildas Avoine, Antonin Beaujeant, Julio Hernandez-Castro, Louis Demay, and Philippe Teuwen. A survey of security and privacy issues in ePassport protocols. *ACM Computing Surveys*, 48(3):47:1–47:??, February 2016. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Aid:2013:DIO

[ABJ13] Matthew M. Aid, William Burr, and Thomas R. Johnson, editors. *"Disreputable if Not Outright Illegal": the National Security Agency versus Martin Luther King, Muhammad Ali, Art Buchwald, Frank Church, et al.: Newly Declassified History Divulges Names of Prominent Americans Targeted by NSA during Vietnam Era*, volume 441 of *National Security Archive Electronic Briefing Book*. National Security Archive, Washington, DC, USA, 2013. LCCN JZ5630. URL `http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB441/`.

Acar:2013:SPA

[ABK13] Tolga Acar, Mira Belenkiy, and Alptekin Küpçü. Single password authentication. *Computer Networks (Amsterdam, Netherlands: 1999)*, 57(13):2597–2614, September 9, 2013. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128613001667`.

Archer:2018:KDR

[ABL+18] David W. Archer, Dan

Bogdanov, Yehuda Lindell, Liina Kamm, Kurt Nielsen, Jakob Illeborg Pagter, Nigel P. Smart, and Rebecca N. Wright. From keys to databases — real-world applications of secure multi-party computation. *The Computer Journal*, 61(12):1749–1771, December 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/12/1749/5095655.

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.

Archer:2016:MPP

[ABPP16] David W. Archer, Dan Bogdanov, Benny Pinkas, and Pille Pullonen. Maturity and performance of programmable secure computation. *IEEE Security & Privacy*, 14(5):48–56, September/October 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/05/msp2016050048-abs.html.

Arapinis:2012:RET

[ABR12] Myrto Arapinis, Sergiu Bursuc, and Mark D. Ryan. Reduction of equational theories for verification of trace equivalence: Re-encryption, associativity and commutativity. *Lecture Notes in Computer Science*, 7215: 169–188, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28641-4_10/.

Arapinis:2013:PSC

[ABR13] Myrto Arapinis, Sergiu

Bursuc, and Mark Ryan. Privacy-supporting cloud computing by in-browser key translation. *Journal of Computer Security*, 21 (6):847–880, ???? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Atighehchi:2015:NME

[ABR15] Kevin Atighehchi, Alexis Bonnecaze, and Gabriel Risterucci. New models for efficient authenticated dictionaries. *Computers & Security*, 53(??):203–214, September 2015. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404815000607.

AlMashrafi:2012:AIM

[ABS+12] Mufeed AlMashrafi, Harry Bartlett, Leonie Simpson, Ed Dawson, and Kenneth Koon-Ho Wong. Analysis of indirect message injection for MAC generation using stream ciphers. *Lecture Notes in Computer Science*, 7372: 138–151, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31448-3_11/.

Aldaya:2019:MTA

[ABSSS19] Alejandro Cabrera Aldaya, Billy Bob Brumley, Alejandro J. Cabrera Sarmiento, and Santiago Sánchez-Solano. Memory tampering attack on binary GCD based inversion algorithms. *International Journal of Parallel Programming*, 47 (4):621–640, August 2019. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic).

Applebaum:2010:PKC

[ABW10] Benny Applebaum, Boaz Barak, and Avi Wigderson. Public-key cryptography from different assumptions. In ACM [ACM10], pages 171–180. ISBN 1-60558-817-2. LCCN QA 76.6 .A152 2010. URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Alzubi:2016:SCC

[ACA+16] O. A. Alzubi, T. M. Chen, J. A. Alzubi, H. Rashaideh, and N. Al-Najdawi. Secure channel coding schemes based on algebraic–geometric codes over Hermitian curves. *J.UCS: Journal of Universal Computer Science*, 22 (4):552–??, ???? 2016. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL http://www.jucs.org/jucs_22_

4/secure_channel_coding_schemes.

Arias-Cabarcos:2015:BIP

[ACAT+15] Patricia Arias-Cabarcos, Florina Almenarez, Ruben Trapero, Daniel Diaz-Sanchez, and Andres Marin. Blended identity: Pervasive IdM for continuous authentication. *IEEE Security & Privacy*, 13(3):32–39, May/June 2015. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://www.computer.org/csdl/mags/sp/2015/03/msp2015030032-abs.html.

Armando:2013:AFB

[ACC+13] Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuéllar, Giancarlo Pellegrino, and Alessandro Sorniotti. An authentication flaw in browser-based single sign-on protocols: Impact and remediations. *Computers & Security*, 33(??):41–58, March 2013. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404812001356.

Arnold:2015:NGH

[ACD+15] T. W. Arnold, M. Check, E. A. Dames, J. Dayka, S. Dragone, D. Evans, W. Santiago Fernandez, M. D. Hocker, R. Kisley, T. E. Morris, J. Petreshock, and K. Werner. The next generation of highly reliable and secure encryption for the IBM z13. *IBM Journal of Research and Development*, 59(4–5):6:1–6:13, July/September 2015. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Anastasiadis:2018:BTA

[ACD18] M. Anastasiadis, N. Chatzis, and K. A. Draziotis. Birthday type attacks to the Naccache–Stern knapsack cryptosystem. *Information Processing Letters*, 138(??):35–38, October 2018. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019018301273.

Amoah:2016:FMA

[ACF16] Raphael Amoah, Seyit Camtepe, and Ernest Foo. Formal modelling and analysis of DNP3 secure authentication. *Journal of Network and Computer Applications*, 59(??):345–360, January 2016. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804515001228.

Ardagna:2010:ECP

[ACK+10] Claudio A. Ardagna, Jan Camenisch, Markulf Kohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, Pierangela Samarati, Dieter Sommer, and Mario Verdicchio. Exploiting cryptography for privacy-enhanced access control: A result of the PRIME Project. *Journal of Computer Security*, 18 (1):123–160, ???? 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Arias-Cabarcos:2019:SAA

[ACKB19] Patricia Arias-Cabarcos, Christian Krupitzer, and Christian Becker. A survey on adaptive authentication. *ACM Computing Surveys*, 52(4):80:1–80:??, September 2019. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3336117`.

ACM:2010:PAI

[ACM10] ACM, editor. *Proceedings of the 2010 ACM International Symposium on Theory of Computing: June 5–8, 2010, Cambridge, MA, USA*. ACM Press, New York, NY 10036, USA, 2010. ISBN 1-60558-817-2. LCCN QA 76.6 .A152 2010. URL `http://www.gbv.de/dms/tib-ub-hannover/63314455x.`.

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.`.

Avoine:2012:PFS

[ACM12] Gildas Avoine, Xavier Carpent, and Benjamin Martin. Privacy-friendly synchronized ultralightweight authentication protocols in the storm. *Journal of Network and Computer Applications*, 35(2):826–843, March 2012. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804511002335`.

Austrin:2017:ICT

[ACM+17] Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, and Karn Seth. On the impossibility of cryptography with tamperable randomness. *Algorithmica*, 79 (4):1052–1101, December 2017. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Aceto:2019:MME

[ACMP19] Giuseppe Aceto, Domenico Ciuonzo, Antonio Montieri, and Antonio Pescapè. MIMETIC: Mobile encrypted traffic classification using multimodal deep learning. *Computer Networks (Amsterdam, Netherlands: 1999)*, 165(??):Article 106944, December 24, 2019. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128619304669.

Aczel:2011:SWL

[Acz11] Amir D. Aczel. *A Strange Wilderness: the Lives of the Great Mathematicians*. Sterling, New York, NY, USA, 2011. ISBN 1-4027-8584-4 (hardback), 1-4027-9085-6 (e-book). xix + 284 pp. LCCN QA21 .A29 2011.

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).

Aizatulin:2012:VCC

[AD12] Mihhail Aizatulin and François Dupressoir. Verifying cryptographic code in C: Some experience and the Csec challenge. *Lecture Notes in Computer Science*, 7140:1–20, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29420-4_1/.

Anyanwu:2010:DCS

[ADD10] Matthew N. Anyanwu, Lih-Yuan Deng, and Dipankar Dasgupta. Design of cryptographically strong generator by linearly generated sequences. Report ??, The University of Memphis, Memphis, TN 38152, USA, January 12, 2010. URL http://ais.cs.memphis.edu/files/papers/Mathew-security-paper.pdf.

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).

Aliberti:2016:RPS

[ADG16] Giulio Aliberti, Roberto Di Pietro, and Stefano Guarino. Reliable and perfectly secret communication over the generalized Ozarow–Wyner's wire-tap channel. *Computer Networks (Amsterdam, Netherlands: 1999)*, 109 (part 1)(??):21–30, November 9, 2016. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128616302146.

Attasena:2017:SSC

[ADH17] Varunya Attasena, Jérôme Darmont, and Nouria Harbi. Secret sharing for cloud data security: a survey. *VLDB Journal: Very Large Data Bases*, 26(5): 657–681, October 2017. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Abraham:2019:DPL

[ADH19] Ittai Abraham, Danny Dolev, and Joseph Y. Halpern. Distributed protocols for leader election: a game-theoretic perspective. *ACM Transactions on Economics and Computation*, 7(1):4:1–4:??, February 2019. CODEN ???? ISSN 2167-8375 (print), 2167-8383 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3303712.

Adikari:2011:HBT

[ADI11] Jithra Adikari, Vassil S. Dimitrov, and Laurent Imbert. Hybrid binary-ternary number system for elliptic curve cryptosystems. *IEEE Transactions on Computers*, 60(2):254–265, February 2011. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Abdalla:2012:LBH

[ADM12] Michel Abdalla, Angelo De Caro, and Karina Mochetti. Lattice-based hierarchical inner product encryption. *Lecture Notes in Computer Science*, 7533:121–138, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33481-8_7/.

Abro:2019:LEE

[ADM19] Adeel Abro, Zhongliang Deng, and Kamran Ali Memon. A lightweight elliptic-Elgamal-based authentication scheme for secure device-to-device communication. *Future Internet*, 11(5):108, May 07, 2019. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/11/5/108.

Andrychowicz:2016:SMC

[ADMM16] Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. Secure multiparty computations on Bitcoin. *Communications of the Association for Computing Machinery*, 59(4): 76–84, April 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2016/4/200175/fulltext`.

Araldo:2018:CEC

[ADR18] Andrea Araldo, Gyorgy Dan, and Dario Rossi. Caching encrypted content via stochastic cache partitioning. *IEEE/ACM Transactions on Networking*, 26(1):548–561, February 2018. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Anandakumar:2018:RHA

[ADSH18] N. Nalla Anandakumar, M. Prem Laxman Das, Somitra K. Sanadhya, and Mohammad S. Hashmi. Reconfigurable hardware architecture for authenticated key agreement protocol over binary Edwards curve. *ACM Transactions on Reconfigurable Technology and Systems*, 11 (2):12:1–12:??, November 2018. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Ahmed:2017:IRD

[AEH17] Kareem Ahmed and Ibrahim El-Henawy. Increasing robustness of Data Encryption Standard by integrating DNA cryptography. *International Journal of Computer Applications*, 39(2):91–105, 2017. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.1080/1206212X.2017.1289690`.

Attrapadung:2015:RGS

[AEHS15] Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, and Yusuke Sakai. Revocable group signature with constant-size revocation list. *The Computer Journal*, 58 (10):2698–2715, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/10/2698`.

Aminifar:2018:OME

[AEP18] Amir Aminifar, Petru Eles, and Zebo Peng. Optimization of message encryption for real-time applications in embedded systems. *IEEE Transactions on Computers*, 67(5):748–754, May 2018. CODEN

ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL https://ieeexplore.ieee.org/document/8125122/.

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.

Antonopoulos:2017:DIS

[AGH+17] Timos Antonopoulos, Paul Gazzillo, Michael Hicks, Eric Koskinen, Tachio Terauchi, and Shiyi Wei. Decomposition instead of self-composition for proving the absence of timing channels. *ACM SIGPLAN Notices*, 52(6):362–375, June 2017. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Akinyele:2014:MGA

[AGHP14] Joseph A. Akinyele, Matthew Green, Susan Hohenberger, and Matthew Pagano. Machine-generated algorithms, proofs and software for the batch verification of digital signature schemes. *Journal of Computer Security*, 22(6):867–912, ???? 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Abdullaziz:2016:AAI

[AGLW16] Osamah Ibrahiem Abdullaziz, Vik Tor Goh, Huo-Chong Ling, and Kok-Sheik Wong. AIPISteg: an active IP identification based steganographic method. *Journal of Network and Computer Applications*, 63(??):150–158, March 2016. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S108480451600059X.

Ahani:2015:SRB

[AGW15] S. Ahani, S. Ghaemmaghami, and Z. J. Wang. A sparse representation-based wavelet domain speech steganography method. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 23(1): 80–91, January 2015. CODEN ???? ISSN 2329-9290.

Allender:2019:NIN

[AH19] Eric Allender and Shuichi Hirahara. New insights on the (non-)hardness of circuit minimization and related problems. *ACM Transactions on Computation Theory*, 11 (4):27:1–27:??, September 2019. CODEN ???? ISSN 1942-3454 (print), 1942-3462 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3349616`.

Ahmadzadeh:2018:HPE

[AHG18] Armin Ahmadzadeh, Omid Hajihassani, and Saeid Gorgin. A high-performance and energy-efficient exhaustive key search approach via GPU on DES-like cryptosystems. *The Journal of Supercomputing*, 74(1):160–182, January 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Attrapadung:2012:ABE

[AHL+12] Nuttapong Attrapadung, Javier Herranz, Fabien Laguillaumie, Benoît Libert, Elie de Panafieu, and Carla Ràfols. Attribute-based encryption schemes with constant-size ciphertexts. *Theoretical Computer Science*, 422(1):15–38, March 9, 2012. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397511009649`.

Ali:2018:ECM

[AHM+18] Zulfiqar Ali, M. Shamim Hossain, Ghulam Muhammad, Ihsan Ullah, Hamid Abachi, and Atif Alamri. Edge-centric multimodal authentication system using encrypted biometric templates. *Future Generation Computer Systems*, 85(??):76–87, August 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X17328741`.

Akhtar:2018:BSI

[AHN+18] Z. Akhtar, A. Hadid, M. S. Nixon, M. Tistarelli, J. Dugelay, and S. Marcel. Biometrics: In search of identity and security (Q&A). *IEEE MultiMedia*, 25(3):22–35, July/September 2018. CODEN IEMUE4. ISSN 1070-986x

(print), 1941-0166 (electronic).

Appelbaum:2013:SSG

[AHS13] J. Appelbaum, J. Horchert, and C. Stöcker. Shopping for spy gear: Catalog advertises NSA toolbox. *Der Spiegel*, ??(??):??, December 29, 2013. URL http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

Ak:2014:ICS

[AHS14] Murat Ak, Turgut Hanoymak, and Ali Aydin Selçuk. IND-CCA secure encryption based on a Zheng–Seberry scheme. *Journal of Computational and Applied Mathematics*, 259 (part B)(??):529–535, March 15, 2014. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042713003403.

Au:2020:SIC

[AHWB20] Man Ho Au, Jinguang Han, Qianhong Wu, and Colin Boyd. Special issue on cryptographic currency and blockchain technology. *Future Generation Computer Systems*, 107(??):758–759, June 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19314840.

Aiash:2015:FAA

[Aia15] Mahdi Aiash. A formal analysis of authentication protocols for mobile devices in next generation networks. *Concurrency and Computation: Practice and Experience*, 27 (12):2938–2953, August 25, 2015. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Ali:2018:CBR

[AIA+18a] Zulfiqar Ali, Muhammad Imran, Mansour Alsulaiman, Muhammad Shoaib, and Sana Ullah. Chaos-based robust method of zero-watermarking for medical signals. *Future Generation Computer Systems*, 88(??):400–412, November 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18304709.

Ali:2018:ZWA

[AIA+18b] Zulfiqar Ali, Muhammad Imran, Mansour Alsulaiman, Tanveer Zia, and Muhammad Shoaib. A zero-watermarking algorithm for privacy protection in biomedical signals.

Future Generation Computer Systems, 82(??):290–303, May 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17322975.

Amin:2016:DAP

[AIB+16] Ruhul Amin, SK Hafizul Islam, G. P. Biswas, Muhammad Khurram Khan, Lu Leng, and Neeraj Kumar. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 101 (??):42–62, June 4, 2016. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128616000207.

Altakrori:2019:AAA

[AIF+19] Malik H. Altakrori, Farkhund Iqbal, Benjamin C. M. Fung, Steven H. H. Ding, and Abdallah Tubaishat. Arabic authorship attribution: an extensive study on Twitter posts. *ACM Transactions on Asian and Low-Resource Language Information Processing (TALLIP)*, 18(1):5:1–5:??, January 2019. CODEN ???? ISSN 2375-4699 (print), 2375-4702 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3236391.

Applebaum:2014:HGA

[AIK14] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. How to garble arithmetic circuits. *SIAM Journal on Computing*, 43(2): 905–929, ???? 2014. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Amin:2018:UAP

[AIKC18] Ruhul Amin, S. K. Hafizul Islam, Neeraj Kumar, and Kim-Kwang Raymond Choo. An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. *Journal of Network and Computer Applications*, 104 (??):133–144, February 15, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804517304058.

Ali:2019:PRD

[AIM+19] Zulfiqar Ali, Muhammad Imran, Sally McClean, Naveed Khan, and Muhammad Shoaib. Protection of records and data authentication based on secret shares and watermarking. *Future Generation Computer Systems*, 98(??):331–341, September 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18328802.

Alhanahnah:2016:MTI

[AJA16] Mohannad J. Alhanahnah, Arshad Jhumka, and Sahel Alouneh. A multidimension taxonomy of insider threats in cloud computing. *The Computer Journal*, 59(11):1612–1622, November 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/11/1612.

Alam:2018:AFC

[AJYG18] Badiul Alam, Zhe Jin, Wun-She Yap, and Bok-Min Goi. An alignment-free cancelable fingerprint template for bio-cryptosystems. *Journal of Network and Computer Applications*, 115(??):20–32, August 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518301450.

Ashraf:2014:MTG

[AK14a] Muhammad Ashraf and Baris Bülent Kirlar. Message transmission for GH-public key cryptosystem. *Journal of Computational and Applied Mathematics*, 259 (part B)(??):578–585, March 15, 2014. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042713005499.

Azarderakhsh:2014:NDP

[AK14b] R. Azarderakhsh and K. Karabina. A new double point multiplication algorithm and its application to binary elliptic curves with endomorphisms. *IEEE Transactions on Computers*, 63(10):2614–2619, October 2014. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Almulla:2013:CKE

[AKG13] M. Almulla, A. Kanso, and M. Ghebleh. A concurrent key exchange protocol based on commuting matrices. *Concurrency and Computation: Practice and Experience*, 25(5):743–751, April 10, 2013. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Anada:2017:CGS

[AKK+17] Hiroaki Anada, Junpei Kawamoto, Chenyutao Ke, Kirill Morozov, and Kouichi Sakurai. Cross-group secret sharing scheme for secure usage of cloud storage over different providers and regions. *The Journal of Supercomputing*, 73(10): 4275–4301, October 2017. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Alabdulatif:2017:PPA

[AKKY17] Abdulatif Alabdulatif, Heshan Kumarage, Ibrahim Khalil, and Xun Yi. Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption. *Journal of Computer and System Sciences*, 90(??):28–45, December 2017. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000017300284.

Afanasyev:2011:PPN

[AKM+11] Mikhail Afanasyev, Tadayoshi Kohno, Justin Ma, Nick Murphy, Stefan Savage, Alex C. Snoeren, and Geoffrey M. Voelker. Privacy-preserving network forensics. *Communications of the Association for Computing Machinery*, 54(5):78–87, May 2011. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Andrysco:2015:SFP

[AKM+15] Marc Andrysco, David Kohlbrenner, Keaton Mowery, Ranjit Jhala, Sorin Lerner, and Hovav Shacham. On subnormal floating point and abnormal timing. In IEEE [IEE15], pages 623–639. ISBN 1-4673-6949-7 (print), 1-4673-6950-0 (e-book). ISSN 1081-6011 (print), 2375-1207 (electronic). LCCN QA76.9.A25. URL http://www.gbv.de/dms/tib-ub-hannover/836112652.pdf.

Armknecht:2012:STH

[AKP12] Frederik Armknecht, Stefan Katzenbeisser, and Andreas Peter. Shift-type homomorphic encryption and its application to fully homomorphic encryption. *Lecture Notes in Computer Science*, 7374:234–251, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31410-0_15/.

Arfaoui:2019:CAA

[AKS19] Amel Arfaoui, Ali Kribeche, and Sidi-Mohammed Senouci. Context-aware anonymous authentication protocols in the Internet of Things dedicated to e-health applications. *Computer Networks*

(Amsterdam, Netherlands: 1999), 159(??):23–36, August 4, 2019. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128619300465.

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.

Aiash:2015:IAA

[AL15] Mahdi Aiash and Jonathan Loo. An integrated authentication and authorization approach for the network of information architecture. *Journal of Network and Computer Applications*, 50(??):73–79, April 2015. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804514001349.

Aldrich:2011:GUS

[Ald11] Richard J. (Richard James) Aldrich. *GCHQ: the uncensored story of Britain's most secret intelligence agency*. HarperPress, London, UK, 2011. ISBN 0-00-727847-0 (hardcover), 0-00-731265-2 (paperback), 0-00-731266-0 (paperback). 666 + 16 pp. LCCN JN329.I6 A43 2011; UB251.G7 A54 2010.

Au:2018:PPP

[ALL+18] Man Ho Au, Kaitai Liang, Joseph K. Liu, Rongxing Lu, and Jianting Ning. Privacy-preserving personal data operation on mobile cloud: Chances and challenges over advanced persistent threat. *Future Generation Computer Systems*, 79 (part 1)(??):337–349, 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17312864.

Alomair:2012:AEH

[Alo12] Basel Alomair. Authenticated encryption: How reordering can impact performance. *Lecture Notes in Computer Science*, 7341:84–99, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31284-7_6/.

Alpar:2018:BTA

[Alp18] Orcan Alpar. Biometric touchstroke authentication by fuzzy proximity of touch locations. *Future Generation Computer Systems*, 86(??):71–80, September 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17326055.

Asharov:2013:FCF

[ALR13] Gilad Asharov, Yehuda Lindell, and Tal Rabin. A full characterization of functions that imply fair coin tossing and ramifications to fairness. *Lecture Notes in Computer Science*, 7785:243–262, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_14/.

Alzahrani:2019:SAC

[Alz19] Naif Saeed Alzahrani. *A Secure Anti-Counterfeiting System Using Near Field Communication, Public Key Cryptography, Blockchain, and Bayesian Games*. Ph.D., Portland State University, Portland, OR, USA, 2019. 176 pp. URL http://search.proquest.com/pqdtglobal/docview/2305527274.

Araghi:2019:EHI

[AM19] Tanya Koohpayeh Araghi and Azizah Abd Manaf. An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD. *Future Generation Computer Systems*, 101(??):1223–1246, December 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19310842.

Awad:2016:SSZ

[AMH+16] Amro Awad, Pratyusa Manadhata, Stuart Haber, Yan Solihin, and William Horne. Silent shredder: Zero-cost shredding for secure non-volatile main memory controllers. *ACM SIGPLAN Notices*, 51(4):263–276, April 2016. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Arnedo-Moreno:2010:JRA

[AMHJ10] Joan Arnedo-Moreno and Jordi Herrera-Joancomartí. JXTA resource access control by means of advertisement encryption. *Future Generation Computer Systems*, 26(1):21–28, January 2010. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Arsalan:2012:IRW

[AMK12] Muhammad Arsalan, Sana Ambreen Malik, and Asifullah Khan. Intelligent reversible watermarking in integer wavelet domain for medical images. *The Journal of Systems and Software*, 85(4):883–894, April 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211002858.

Ahir:2017:LAR

[AMKA17] Prashant Ahir, Mehran Mozaffari-Kermani, and Reza Azarderakhsh. Lightweight architectures for reliable and fault detection Simon and Speck cryptographic algorithms on FPGA. *ACM Transactions on Embedded Computing Systems*, 16(4):109:1–109:??, August 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Aghili:2019:SSL

[AMKC19] Seyed Farhad Aghili, Hamid Mala, Pallavi Kaliyar, and Mauro Conti. SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT. *Future Generation Computer Systems*, 101(??):621–634, December 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19304777.

Abarzua:2018:ASC

[AMMV18] Rodrigo Abarzúa, Santi Martínez, Valeria Mendoza, and Javier Valera. Avoiding side-channel attacks by computing isogenous and isomorphic elliptic curves. *Mathematics in Computer Science*, 12(3):295–307, September 2018. CODEN ???? ISSN 1661-8270 (print), 1661-8289 (electronic).

Abbasinezhad-Mood:2018:DHI

[AMN18] Dariush Abbasinezhad-Mood and Morteza Nikooghadam. Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. *Future Generation Computer Systems*, 84(??):47–57, July 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17315376.

Adj:2013:WDC

[AMORH13] Gora Adj, Alfred Menezes, Thomaz Oliveira, and Francisco Rodriguez-Henriquez. Weakness of $\mathbf{F}_{3^{6509}}$ for discrete logarithm cryptography. Report, University of Waterloo, Waterloo, ON, Canada, July 15, 2013. 25 pp. URL http://crypto.2013.rump.cr.yp.to/; http://eprint.iacr.org/2013/446.

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.

Ahmadian:2010:PDS

[AMS+10] Zahra Ahmadian, Javad Mohajeri, Mahmoud Salmasizadeh, Risto M. Hakala, and Kaisa Nyberg. A practical distinguisher for the Shannon cipher. *The Journal of Systems and Software*, 83(4):543–547, April 2010. CODEN JSSODM. ISSN 0164-1212.

Aghili:2019:LLT

[AMSPL19] Seyed Farhad Aghili, Hamid Mala, Mohammad Shojafar, and Pedro Peris-Lopez. LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. *Future Generation Computer Systems*, 96(??):410–424, July 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18331297.

Alvarez:2012:CAB

[ÁMVZ12] Rafael Álvarez, Francisco Martínez, José-Francisco Vicent, and Antonio Zamora. Cryptographic applications of 3 × 3 block upper triangular matrices. *Lecture Notes in Computer Science*, 7209:97–104, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28931-6_10/.

Albrecht:2012:SDL

[AN12] Alexander Albrecht and Felix Naumann. Schema decryption for large extract-transform-load systems. *Lecture Notes in Computer Science*, 7532:116–125, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34002-4_9/.

Arshad:2015:SAI

[AN15] Hamed Arshad and Morteza Nikooghadam. Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol. *The Journal of Supercomputing*, 71(8):3163–3180, August 2015. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-015-1434-8.

Aga:2017:ISM

[AN17] Shaizeen Aga and Satish Narayanasamy. InvisiMem: Smart memory defenses for memory bus side channel. *ACM SIGARCH Computer Architecture News*, 45(2):94–106, May 2017. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Anawis:2014:ARR

[Ana14] Mark Anawis. Applications for randomness: Random numbers have been shown to be valuable in sampling, simulations, modeling, data encryption, gambling and even musical composition. *Scientific Computing*, 31(11):28–30, November 2014. CODEN SCHRCU. ISSN 1930-5753 (print), 1930-6156 (electronic). URL http://digital.scientificcomputing.com/scientificcomputing/hpc_source_sc14_special_edition. Special issue for Supercomputing 2014 (SC14), defining the market: 30 years of high-performance computing (1984–2014).

Anderson:2013:MNF

[And13] David Anderson. Max Newman: forgotten man of early British computing. *Communications of the Association for Computing Machinery*, 56(5):29–31, May 2013. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Anderson:2019:QCN

[And19] Mark Anderson. Quantum cryptography needs a reboot: A failed security product could someday power large-scale quantum computing — [news]. *IEEE Spectrum*, 56(10):9–10, October 2019. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anghelescu:2016:FIP

[Ang16] Petre Anghelescu. FPGA implementation of programmable cellular automata encryption algorithm for network communications. *International Journal of Com-*

puter Systems Science and Engineering, 31(5):??, September 2016. CODEN CSSEEI. ISSN 0267-6192.

Anonymous:2010:NDS

[Ano10a] 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:2010:MML

[Ano10b] Anonymous. Mirror, mirror .... *IEEE Spectrum*, 47(2):11, February 2010. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Anonymous:2011:AIS

[Ano11a] Anonymous, editor. *ACIS international symposium on cryptography, and network security, data mining and knowledge discovery, e-commerce and its applications, and embedded systems*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. ISBN 0-7695-4332-4. LCCN ????

Anonymous:2011:AXL

[Ano11b] Anonymous. *ANSI X9.98-2010: Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry*. American National Standards Institute, 1430 Broadway, New York, NY 10018, USA, April 2011. US$100. URL `http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.98-2010`.

Anonymous:2011:MCB

[Ano11c] Anonymous. Memorial for codebreakers at Bletchley Park. *BBC News*, April 27, 2011. URL `http://www.bbc.co.uk/news/uk-england-beds-bucks-herts-13208090`.

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:CFF

[Ano13a] Anonymous. Crypto flaw

found in Android. *Network Security*, 2013(7): 2, July 2013. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485813700771.

Anonymous:2013:CRR

[Ano13b] Anonymous. CryptoLocker runs rampant, but drops ransom price. *Network Security*, 2013(12):2, December 2013. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485813701302.

Anonymous:2013:DSS

[Ano13c] 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.

Anonymous:2013:NCI

[Ano13d] Anonymous. NSA has cracked Internet encryption protocols. *Network Security*, 2013(9):1–2, September 2013. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485813700977.

Anonymous:2013:SSD

[Ano13e] Anonymous. Simple steps to data encryption. *Network Security*, 2013(9):4, September 2013. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485813701004.

Anonymous:2013:SIS

[Ano13f] Anonymous. Special issue on "Security and identity architecture for the future Internet". *Computer Networks (Amsterdam, Netherlands: 1999)*, 57(10):2215–2217, July 5, 2013. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128613001795.

Anonymous:2014:CSL

[Ano14a] Anonymous. CryptoLocker success leads to more malware. *Network Security*, 2014(1):20, January 2014. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485814700121.

Anonymous:2014:ERE

[Ano14b] Anonymous. Encryption on the rise, but not enough. *Network Security*, 2014(2): 1–2, February 2014. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485814700145.

Anonymous:2014:TPC

[Ano14c] Anonymous. TrueCrypt project cancelled by its developers. *Network Security*, 2014(6):1–2, June 2014. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485814700546.

Anonymous:2015:BSU

[Ano15a] Anonymous. Blind signatures using offline repositories provide new level of security. *Scientific Computing*, ??(??):??, May 15, 2015. CODEN SCHRCU. ISSN 1930-5753 (print), 1930-6156 (electronic). URL http://www.scientificcomputing.com/news/2015/05/blind-signatures-using-offline-repositories-provide-new-level-security.

Anonymous:2015:BRDa

[Ano15b] Anonymous. Book review: *Digital Identity Management*, Maryline Laurent and Samia Bouzefrane. ISTE Press/Elsevier. ISBN 978-1-78548-004-1. *Network Security*, 2015(9): 4, September 2015. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485815300787.

Anonymous:2015:CEB

[Ano15c] Anonymous. Cryptography for everyone: Bringing end-to-end encryption to the masses. *Scientific Computing*, ??(??):??, March 17, 2015. URL http://www.scientificcomputing.com/news/2015/03/cryptography-everyone-bringing-end-end-encryption-masses.

Anonymous:2015:QCS

[Ano15d] Anonymous. Quantum cryptography security hole revealed, energy-time entanglement vulnerable to attack. *Scientific Computing*, ??(??):??, December 12, 2015. CODEN SCHRCU. ISSN 1930-5753 (print), 1930-6156 (electronic). URL http://www.scientificcomputing.com/news/2015/12/quantum-cryptography-security-hole-revealed-energy-time-entanglement-vulnerable-attack. See research article [JEA+15].

Anonymous:2015:UGB

[Ano15e] Anonymous. UK Government battles tech firms over encryption. *Network Security*, 2015(11):1–2, November 2015. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485815300945.

Anonymous:2016:BRBa

[Ano16a] Anonymous. Book review: *Bitcoin and Cryptocurrency Technologies*, Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder. *Network Security*, 2016(8):4, August 2016. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485816300745.

Anonymous:2016:CPSd

[Ano16b] Anonymous. Call for papers special issue on postquantum cryptography. *IEEE Security & Privacy*, 14(4):63, July/August 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/04/msp2016040063.pdf.

Anonymous:2016:CPSe

[Ano16c] Anonymous. Call for papers special issue on postquantum cryptography. *IEEE Security & Privacy*, 14(5):57, September/October 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/05/msp2016050057.pdf.

Anonymous:2016:EMT

[Ano16d] Anonymous. The Enigma machine takes a quantum leap. *R&D Magazine*, ??(??):??, September 7, 2016. URL http://www.rdmag.com/news/2016/09/enigma-machine-takes-quantum-leap. News story on quantum data locking research in [LCW+16, LHA+16].

Anonymous:2016:FVM

[Ano16e] Anonymous. Facsimile of the Voynich Manuscript now available to citizen cryptographers. Web document, November 16, 2016. URL http://hyperallergic.com/335505/voynich-manuscript-facsimile-published-yale-university/.

Anonymous:2016:GUP

[Ano16f] Anonymous. Generating unclonable patterns to fight counterfeiting. *Scientific Computing*, ??(??):??, June 13, 2016. URL http://www.

scientificcomputing.com/news/2016/06/generating-unclonable-patterns-fight-counterfeiting.

Anonymous:2016:IICd

[Ano16g] Anonymous. Introducing IEEE Collabratec. *IEEE Computer Architecture Letters*, 15(1):66, January/June 2016. ISSN 1556-6056 (print), 1556-6064 (electronic).

Anonymous:2016:MBE

[Ano16h] Anonymous. More battles over encryption & surveillance. *Network Security*, 2016(1):2, January 2016. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485816300022.

Anonymous:2016:SWT

[Ano16i] Anonymous. Smith wins Test of Time award for paper. Penn State News, January 18, 2016. URL http://news.psu.edu/story/387916/2016/01/18/academics/smith-wins-test-time-award-paper.

Anonymous:2016:SIR

[Ano16j] Anonymous. Special issue on real-world cryptography call for papers house advertisement. *IEEE Security & Privacy*, 14(1):62, January/February 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Anonymous:2017:BA

[Ano17a] Anonymous. BitErrant attack. Web site, March 6, 2017. URL http://biterrant.io/. The story describes how SHA-1 collision attacks could lead to bogus, and malware, file downloads via BitTorrent: the obvious solution, which should have been adopted long ago, is to use multiple checksum algorithms, and require all to match before concluding that two files are in fact identical.

Anonymous:2017:BRM

[Ano17b] Anonymous. Book review: *The Mathematics of Secrets*, by Joshua Holden. Princeton University Press. ISBN 978-0-691-14175-6. *Network Security*, 2017(3):4, March 2017. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485817300247.

Anonymous:2017:CCS

[Ano17c] Anonymous. Cybernetica case study: Solving the Estonian ID-card case. Web news story., December 13, 2017.

URL https://cyber.ee/en/news/cybernetica-case-study-solving-the-estonian-id-card-case/. The story describes a poor choice of generating large (about 1024 bits) primes p and q that led to crackable RSA cryptography. The solution for Estonia was to switch to elliptic-curve cryptography that was also supported by the cards.

Anonymous:2017:HDQ

[Ano17d] Anonymous. High-dimensional quantum encryption performed in real-world city conditions for first time. *Scientific Computing*, ??(??):??, August 24, 2017. CODEN SCHRCU. ISSN 1930-5753 (print), 1930-6156 (electronic). URL https://www.scientificcomputing.com/news/2017/08/high-dimensional-quantum-encryption-performed-real-world-city-conditions-first-time.

Anonymous:2017:MBH

[Ano17e] Anonymous. Mathematician breaks down how to defend against quantum computing attacks. *Research & Development*, ??(??):??, February 2, 2017. CODEN REDEEA. ISSN 0746-9179. URL http://www.rdmag.com/news/2017/02/mathematician-breaks-down-how-defend-against-quantum-computing-attacks.

Anonymous:2017:RV

[Ano17f] Anonymous. ROCA vulnerability. Wikipedia article., October 2017. URL https://en.wikipedia.org/wiki/ROCA_vulnerability. The ROCA vulnerability affects millions of smartcards, and devices using TPM (Trusted Platform Modules). It allows recovery of the private key from knowledge of the RSA public key, and thus, facilitates malicious cloning of the cards, and decrypting of some encrypted filesystems.

Anonymous:2019:GES

[Ano19a] Anonymous. Guest editorial: Special issue on Information Systems Security, Privacy, Security and Cryptography (ICISSP 2017 and SECRYPT 2017). *Computers & Security*, 86(??):419, September 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404819301233.

Anonymous:2019:HCC

[Ano19b] Anonymous. The history of cryptography and codes. *British Journal for the History of Mathematics*, 34(1):71–72, 2019.

CODEN ???? ISSN 2637-5494. URL http://www.tandfonline.com/doi/full/10.1080/17498430.2018.1542200.

Anonymous:2019:PBT

[Ano19c] Anonymous. Preface: Blockchain: From technology to solutions. *IBM Journal of Research and Development*, 63(2–3):1–2, March/May 2019. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Anthes:2014:FTI

[Ant14] Gary Anthes. French team invents faster code-breaking algorithm. *Communications of the Association for Computing Machinery*, 57(1):21–23, January 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Andriotis:2013:JSD

[AOT13] Panagiotis Andriotis, George Oikonomou, and Theo Tryfonas. JPEG steganography detection with Benford's Law. *Digital Investigation*, 9(3–4):246–257, 2013. ISSN 1742-2876. URL http://www.sciencedirect.com/science/article/pii/S1742287613000066.

Agarwal:2010:BRW

[AP10] Parag Agarwal and Balakrishnan Prabhakaran. Blind robust watermarking of 3D motion data. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 6(1):2:1–2:??, February 2010. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

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).

AlFardan:2013:LTB

[AP13] Nadhem AlFardan and Kenny Paterson. Lucky thirteen: Breaking the TLS and DTLS record protocols. Report ??, Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK, February 4, 2013. 18 pp. URL http://www.isg.rhul.ac.uk/tls/; http://www.isg.rhul.ac.uk/tls/TLStiming.pdf.

Abellan:2018:FCQ

[AP18] C. Abellan and V. Pruneri. The future of cybersecurity is quantum. *IEEE Spec-*

trum, 55(7):30–35, July 2018. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Ali:2018:SUA

[APK+18] Rifaqat Ali, Arup Kumar Pal, Saru Kumari, Marimuthu Karuppiah, and Mauro Conti. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. *Future Generation Computer Systems*, 84(??):200–215, July 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17303862.

Alcaide:2013:AAP

[APMCR13] Almudena Alcaide, Esther Palomar, José Montero-Castillo, and Arturo Ribagorda. Anonymous authentication for privacy-preserving IoT target-driven applications. *Computers & Security*, 37(??): 111–123, September 2013. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404813000904.

Applebaum:2013:GXG

[App13] Benny Applebaum. Garbling XOR gates "for free" in the standard model. *Lecture Notes in Computer Science*, 7785: 162–181, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_10/.

Applebaum:2014:CCP

[App14] Benny Applebaum. *Cryptography in Constant Parallel Time*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2014. ISBN 3-642-17366-7, 3-642-17367-5 (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xvi + 193 + 3 pp. LCCN QA76.9.M35; TK5102.94 QA76.9.A25.

Appel:2015:VCP

[App15] Andrew W. Appel. Verification of a cryptographic primitive: SHA-256. *ACM Transactions on Programming Languages and Systems*, 37(2):7:1–7:??, April 2015. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic).

Albrecht:2015:FBR

[APPVP15] Martin R. Albrecht, Davide Papini, Kenneth G. Paterson, and Ricardo Villanueva-Polanco. Factoring 512-bit RSA moduli for fun (and a profit of $9,000). Report, Information Security Group Royal Holloway, University of London, London, UK, March 13, 2015. 3 pp. URL `https://martinralbrecht.files.wordpress.com/2015/03/freak-scan1.pdf`.

Al-Qarni:2012:EII

[AQD12] Garsah Farhan Al-Qarni and Farzin Deravi. Explicit integration of identity information from skin regions to improve face recognition. *Lecture Notes in Computer Science*, 7325:30–37, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31298-4_4/`.

Al-Qurishi:2018:EKA

[AQRH+18] Muhammad Al-Qurishi, Sk Md Mizanur Rahman, M. Shamim Hossain, Ahmad Almogren, Majed Alrubaian, Atif Alamri, Mabrook Al-Rakhami, and B. B. Gupta. An efficient key agreement protocol for Sybil-precaution in online social networks. *Future Generation Computer Systems*, 84(??):139–148, July 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X17306623`.

Arai:2013:MDH

[Ara13] Kohei Arai. Method for data hiding based on LeGall 5/3 (Cohen–Daubechies–Feauveau: CDF 5/3) wavelet with data compression and random scanning of secret imagery data. *International Journal of Wavelets, Multiresolution and Information Processing*, 11(4):1360006, 18, 2013. CODEN IJWMIP. ISSN 0219-6913 (print), 1793-690X (electronic).

Arab:2019:IEM

[ARG19] Alireza Arab, Mohammad Javad Rostami, and Behnam Ghavami. An image encryption method based on chaos system and AES algorithm. *The Journal of Supercomputing*, 75(10):6663–6682, October 2019. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://link.springer.com/content/pdf/10.1007/s11227-019-02878-7.pdf`.

Adj:2014:SRC

[ARH14] G. Adj and F. Rodriguez-Henriquez. Square root computation over even extension fields. *IEEE Trans-*

actions on Computers, 63 (11):2829–2841, November 2014. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Altawy:2018:SLT

[ARH+18a] 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).

AlTawy:2018:TCM

[ARH+18b] Riham AlTawy, Raghvendra Rohit, Morgan He, Kalikinkar Mandal, Gangqiang Yang, and Guang Gong. Towards a cryptographic minimal design: The sLiSCP family of permutations. *IEEE Transactions on Computers*, 67(9):1341–1358, ???? 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `https://ieeexplore.ieee.org/document/8305605/`.

Agudo:2013:PAC

[ARL13] Isaac Agudo, Ruben Rios, and Javier Lopez. A privacy-aware continuous authentication scheme for proximity-based access control. *Computers & Security*, 39 (part B)(??): 117–126, November 2013. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404813000874`.

Abdulrahman:2015:NRR

[ARM15a] E. A. H. Abdulrahman and A. Reyhani-Masoleh. New regular radix-8 scheme for elliptic curve scalar multiplication without precomputation. *IEEE Transactions on Computers*, 64(2):438–451, February 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Azarderakhsh:2015:PHS

[ARM15b] Reza Azarderakhsh and Arash Reyhani-Masoleh. Parallel and high-speed computations of elliptic curve cryptography using hybrid-double multipliers. *IEEE Transactions on Parallel and Distributed Systems*, 26(6): 1668–1677, June 2015. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL `http://csdl.computer.org/csdl/trans/td/2015/06/06814322-abs.html`.

Armasu:2019:IFA

[Arm19] Lucian Armasu. Intel follows AMD's lead on full memory encryption. Web site, May 27, 2019. URL https://www.tomshardware.com/news/intel-mktme-amd-memory-encryption,39467.html.

Ambrose:2012:RII

[ARP12] Jude A. Ambrose, Roshan G. Ragel, and Sri Parameswaran. Randomized instruction injection to counter power analysis attacks. *ACM Transactions on Embedded Computing Systems*, 11 (3):69:1–69:??, September 2012. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Alghamdi:2019:RAM

[ARWK19] Wael Alghamdi, Mohsen Rezvani, Hui Wu, and Salil S. Kanhere. Routing-aware and malicious node detection in a concealed data aggregation for WSNs. *ACM Transactions on Sensor Networks*, 15(2):18:1–18:??, April 2019. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3293537.

Asharov:2016:LPI

[AS16] Gilad Asharov and Gil Segev. Limits on the power of indistinguishability obfuscation and functional encryption. *SIAM Journal on Computing*, 45 (6):2117–2176, ???? 2016. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Artemenko:2017:PGO

[AS17] Sergei Artemenko and Ronen Shaltiel. Pseudorandom generators with optimal seed length for non-Boolean poly-size circuits. *ACM Transactions on Computation Theory*, 9(2):6:1–6:??, May 2017. CODEN ???? ISSN 1942-3454 (print), 1942-3462 (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).

Asharov:2014:TCC

[Ash14] Gilad Asharov. Towards characterizing complete fairness in secure two-party computation. *Lecture Notes in Computer Sci-*

ence, 8349:291–316, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_13/.

Al-Sinani:2012:UCB

[ASM12] Haitham S. Al-Sinani and Chris J. Mitchell. A universal client-based identity management tool. *Lecture Notes in Computer Science*, 7163:49–74, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29804-2_4/.

Ahmadi:2011:SKC

[ASN11] Hadi Ahmadi and Reihaneh Safavi-Naini. Secret keys from channel noise. *Lecture Notes in Computer Science*, 6632:266–283, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_16.

Ahmadi:2012:SKE

[ASN12] Hadi Ahmadi and Reihaneh Safavi-Naini. Secret key establishment over noisy channels. *Lecture Notes in Computer Science*, 6888:132–147, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27901-0_11/.

Ali:2014:ALD

[ASO14] Syed Taha Ali, Vijay Sivaraman, and Diethelm Ostry. Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring. *Future Generation Computer Systems*, 35(??):80–90, June 2014. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X13001866.

Asaar:2015:IBM

[ASS15] Maryam Rajabzadeh Asaar, Mahmoud Salmasizadeh, and Willy Susilo. An identity-based multi-proxy multi-signature scheme without bilinear pairings and its variants. *The Computer Journal*, 58(4):1021–1039, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/1021.

Alharbi:2018:CME

[ASV+18] Rawan Alharbi, Tammy Stump, Nilofar Vafaie, Angela Pfammatter, Bonnie Spring, and Nabil Alshurafa. I can't be myself: Effects of wearable cameras on the capture of authentic behavior in the wild. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2(3):1–40, September 2018. CODEN ???? ISSN 2474-9567 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3264900.

Alsulaiman:2013:IVB

[ASVE13] Fawaz A. Alsulaiman, Nizar Sakr, Julio J. Valdés, and Abdulmotaleb El Saddik. Identity verification based on handwritten signatures with haptic information using genetic programming. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 9(2): 11:1–11:??, May 2013. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Altman:2010:AAP

[AT10] Alon Altman and Moshe Tennenholtz. An axiomatic approach to personalized ranking systems. *Journal of the ACM*, 57(4):26:1–26:35, April 2010. CODEN JACOAH. ISSN 0004-5411.

Azimpourkivi:2017:CBT

[ATC17] Mozhgan Azimpourkivi, Umut Topkara, and Bogdan Carbunar. Camera based two factor authentication through mobile and wearable devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 1(3):1–37, September 2017. CODEN ???? ISSN 2474-9567 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3131904.

Aste:2017:BTF

[ATD17] Tomaso Aste, Paolo Tasca, and Tiziana Di Matteo. Blockchain technologies: The foreseeable impact on society and industry. *Computer*, 50(9): 18–28, September 2017. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL https://www.computer.org/csdl/mags/co/2017/09/mco2017090018-abs.html.

Argyropoulos:2010:BTP

[ATI+10] Savvas Argyropoulos, Dimitrios Tzovaras, Dimosthenis Ioannidis, Yannis Damousis, Michael G. Strintzis, Martin Braun, and Serge Boverie. Biometric template protection in multimodal authentication systems based on error correcting codes. *Journal of Computer Security*, 18(1):161–185, ???? 2010. CODEN JCSIET. ISSN

0926-227X (print), 1875-8924 (electronic).

Au:2011:PPT

[ATK11] M. Ho Au, P. P. Tsang, and A. Kapadia. PEREA: Practical TTP-free revocation of repeatedly misbehaving anonymous users. *ACM Transactions on Information and System Security*, 14(4):29:1–29:??, December 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Al-Tariq:2017:SFP

[ATKH+17] Abdullah Al-Tariq, Abu Raihan Mostofa Kamal, Md. Abdul Hamid, M. Abdullah-Al-Wadud, Mohammad Mehedi Hassan, and Sk Md. Mizanur Rahman. A scalable framework for protecting user identity and access pattern in untrusted Web server using forward secrecy, public key encryption and Bloom filter. *Concurrency and Computation: Practice and Experience*, 29(23):??, December 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Alam:2015:ACF

[ATS15] Shahid Alam, Issa Traore, and Ibrahim Sogukpinar. Annotated control flow graph for metamorphic malware detection. *The Computer Journal*, 58 (10):2608–2621, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/10/2608`.

Aslan:2016:DEM

[AUMT16] Ilhan Aslan, Andreas Uhl, Alexander Meschtscherjakov, and Manfred Tscheligi. Design and exploration of mid-air authentication gestures. *ACM Transactions on Interactive Intelligent Systems (TIIS)*, 6(3): 23:1–23:??, October 2016. CODEN ???? ISSN 2160-6455 (print), 2160-6463 (electronic).

Abdalla:2012:LRS

[AV12] Michel Abdalla and Jill-Jênn Vie. Leakage-resilient spatial encryption. *Lecture Notes in Computer Science*, 7533:78–99, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-33481-8_5/`.

Abdou:2018:SLV

[AV18] Abdelrahman Abdou and P. C. Van Oorschot. Server location verification (SLV) and server location pinning: Augmenting TLS authentication. *ACM Transactions on Privacy and Security (TOPS)*, 21(1):1:1–1:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3139294`.

Badawi:2018:ASS

[AVAH18] Ahmad Al Badawi, Bharadwaj Veeravalli, Khin Mi Mi Aung, and Brahim Hamadicharef. Accelerating subset sum and lattice based public-key cryptosystems with multi-core CPUs and GPUs. *Journal of Parallel and Distributed Computing*, 119(??):179–190, September 2018. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731518302831`.

Altaf:2015:LPM

[AW15] Muhammad Shoaib Bin Altaf and David A. Wood. LogCA: A performance model for hardware accelerators. *IEEE Computer Architecture Letters*, 14(2): 132–135, July/December 2015. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Altaf:2017:LHL

[AW17] Muhammad Shoaib Bin Altaf and David A. Wood. LogCA: a high-level performance model for hardware accelerators. *ACM SIGARCH Computer Architecture News*, 45(2): 375–388, May 2017. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Awad:2017:OLO

[AWSS17] Amro Awad, Yipeng Wang, Deborah Shands, and Yan Solihin. ObfusMem: a low-overhead access obfuscation for trusted memories. *ACM SIGARCH Computer Architecture News*, 45(2): 107–119, May 2017. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Anzala-Yamajako:2012:RAC

[AY12a] Alexandre Anzala-Yamajako. Review of *Algorithmic Cryptanalysis*, by Antoine Joux. *ACM SIGACT News*, 43(4):13–16, December 2012. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Anzala-Yamajako:2012:RBC

[AY12b] Alexandre Anzala-Yamajako. Review of *Algorithmic Cryptanalysis*, by Antoine Joux. *ACM SIGACT News*, 43(4):13–16, December 2012. CODEN SIGNDM. ISSN 0163-5700

(print), 1943-5827 (electronic).

Ahmad:2014:RTN

[AY14a] 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.

AlTawy:2014:IDR

[AY14b] Riham AlTawy and Amr M. Youssef. Integral distinguishers for reduced-round Stribog. *Information Processing Letters*, 114(8): 426–431, August 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019014000428.

Aysu:2015:FRT

[AYS15] Aydin Aysu, Bilgiday Yuce, and Patrick Schaumont. The future of real-time security: Latency-optimized lattice-based digital signatures. *ACM Transactions on Embedded Computing Systems*, 14(3): 43:1–43:??, May 2015. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Au:2014:SMV

[AYSZ14] Man Ho Au, Guomin Yang, Willy Susilo, and Yunmei Zhang. (Strong) multi-designated verifiers signatures secure against rogue key attack. *Concurrency and Computation: Practice and Experience*, 26(8): 1574–1592, June 10, 2014. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Ayub:2012:BRB

[Ayu12] Abu Mohammad Omar Shehab Uddin Ayub. Book review: *The Cryptoclub: Using Mathematics to Make and Break Secret Codes*, by Janet Beissinger and Vera Pless. *ACM SIGACT News*, 43(1):9–14, March 2012. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [BP06].

Apavatjrut:2012:EEA

[AZF+12] Anya Apavatjrut, Wassim Znaidi, Antoine Fraboulet, Claire Goursaud, Katia Jaffrès-Runser, Cédric Lauradoux, and Marine Minier. Energy efficient authentication strategies for network coding. *Concurrency and Computation: Practice and Experience*, 24(10):1086–1107, July 2012. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Alshammari:2011:CET

[AZH11] Riyad Alshammari and A. Nur Zincir-Heywood. Can encrypted traffic be identified without port numbers, IP addresses and payload inspection? *Computer Networks (Amsterdam, Netherlands: 1999)*, 55(6):1326–1350, April 25, 2011. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128610003695`.

Alavi:2014:RQE

[AZPC14] Zohreh Alavi, Lu Zhou, James Powers, and Keke Chen. RASP-QS: efficient and confidential query services in the cloud. *Proceedings of the VLDB Endowment*, 7(13):1685–1688, August 2014. CODEN ???? ISSN 2150-8097.

Barcellos:2018:RSP

[BA18] M. Barcellos and D. F. Aranha. Research in security and privacy in Brazil. *IEEE Security & Privacy*, 16(6):14–21, November/ December 2018. ISSN 1540-7993 (print), 1558-4046 (electronic).

Behnia:2013:IEB

[BAAS13] S. Behnia, A. Akhavan, A. Akhshani, and A. Samsudin. Image encryption based on the Jacobian elliptic maps. *The Journal of Systems and Software*, 86(9):2429–2438, September 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121213001283`.

Blaner:2013:IPP

[BAB+13] B. Blaner, B. Abali, B. M. Bass, S. Chari, R. Kalla, S. Kunkel, K. Lauricella, R. Leavens, J. J. Reilly, and P. A. Sandon. IBM POWER7+ processor on-chip accelerators for cryptography and active memory expansion. *IBM Journal of Research and Development*, 57(6):3:1–3:16, November–December 2013. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Brennan:2012:ASC

[BAG12] Michael Brennan, Sadia Afroz, and Rachel Greenstadt. Adversarial stylometry: Circumventing authorship recognition to preserve privacy and anonymity. *ACM Transactions on Information and System Security*, 15 (3):12:1–12:??, November

2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bai:2010:RKI

[Bai10] L. Bai. A reliable (K, N) image secret sharing scheme with low information overhead. *International Journal of Computer Applications*, 32(1): 9–14, 2010. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.1080/1206212X.2010.11441955`.

Bailin:2012:ERG

[Bai12] David Bailin. Essay review: The geese that never cackled. *Secret Days: Codebreaking in Bletchley Park*, by Asa Briggs. ISBN 978-1-84832-615-6, Scope: review. Level: general readership. *Contemporary Physics*, 53(3):256–262, 2012. CODEN CTPHAF. ISSN 0010-7514 (print), 1366-5812 (electronic).

Berbecaru:2010:FSM

[BAL10] Diana Berbecaru, Luca Albertalli, and Antonio Lioy. The ForwardDiffsig scheme for multicast authentication. *IEEE/ACM Transactions on Networking*, 18 (6):1855–1868, December 2010. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Barbay:2012:BRB

[Bar12] Jérémy Barbay. Book review: *Understanding and Applying Cryptography and Data Security*, by Adam J. Elbirt. *ACM SIGACT News*, 43(1):18–21, March 2012. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [Elb09].

Barthe:2015:HAC

[Bar15] Gilles Barthe. High-assurance cryptography: Cryptographic software we can trust. *IEEE Security & Privacy*, 13(5):86–89, September/October 2015. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `http://csdl.computer.org/csdl/mags/sp/2015/05/msp2015050086-abs.html`.

Barker:2016:RKM

[Bar16a] Elaine Barker. Recommendation for key management. Part 1: General. xi + 147, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, January 2016. URL `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf`.

Bartkewitz:2016:LPL

[Bar16b] Timo Bartkewitz. Leakage prototype learning for profiled differential side-channel cryptanalysis. *IEEE Transactions on Computers*, 65(6):1761–1774, June 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Bard:2019:DWG

[Bar19] Gregory V. Bard. Determining whether a given cryptographic function is a permutation of another given cryptographic function — a problem in intellectual property. *Theoretical Computer Science*, 800(??):3–14, December 31, 2019. CODEN TCSDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397519306395.

Batey:2010:DMW

[Bat10] Mavis Batey. *Dilly: the man who broke Enigmas*. Biteback, London, UK, 2010. ISBN 1-906447-15-2 (paperback). 256 (est.) pp. LCCN ???? US$9.99.

Bax:2014:PPD

[Bax14] Stephen Bax. A proposed partial decoding of the Voynich script. Web report, Centre for Research in English Language Learning and Assessment (CRELLA), University of Bedfordshire, Luton, Bedfordshire, UK, LU1 3JU, January 2014. 62 pp. URL http://stephenbax.net/wp-content/uploads/2014/01/Voynich-a-provisional-partial-decoding-BAX.pdf.

Baylis:2010:CC

[Bay10] John Baylis. Codes, not ciphers. *The Mathematical Gazette*, 94(531):412–425, November 2010. CODEN MAGAAS. ISSN 0025-5572.

Bulygin:2010:OSS

[BB10] Stanislav Bulygin and Michael Brickenstein. Obtaining and solving systems of equations in key variables only for the small variants of AES. *Mathematics in Computer Science*, 3(2):185–200, April 2010. CODEN ???? ISSN 1661-8270 (print), 1661-8289 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=1661-8270&volume=3&issue=2&spage=185.

Bennett:2014:QCP

[BB14] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560 (part 1)(??):7–11, December 4, 2014. CODEN TCSDI. ISSN 0304-3975

(print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397514004241.

Barenghi:2016:FBS

[BBB+16a] Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, Gerardo Pelosi, Stefano Sanfilippo, and Ruggero Susella. A fault-based secret key retrieval method for ECDSA: Analysis and countermeasure. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 13(1):8:1–8:??, December 2016. CODEN ???? ISSN 1550-4832.

Boumerzoug:2016:LKM

[BBB16b] Hayette Boumerzoug, Boucif Amar Bensaber, and Ismail Biskri. A lightweight key management scheme based on an Adelson-Velskii and Landis tree and elliptic curve cryptography for wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 28(6):1831–1847, April 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Benyamina:2019:ANE

[BBB19] Zakarya Benyamina, Khelifa Benahmed, and Fateh Bounaama. ANEL: a novel efficient and lightweight authentication scheme for vehicular ad hoc networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 164(??):Article 106899, December 9, 2019. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128619306012.

Barenghi:2013:FIT

[BBBP13] Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, and Gerardo Pelosi. A fault induction technique based on voltage underfeeding with application to attacks against AES and RSA. *The Journal of Systems and Software*, 86(7):1864–1878, July 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121213000320.

Baldi:2013:ULC

[BBC+13] Marco Baldi, Marco Bianchi, Franco Chiaraluce, Joachim Rosenthal, and Davide Schipani. Using LDGM codes and sparse syndromes to achieve digital signatures. *Lecture Notes in Computer Science*, 7932:1–15, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.

com/chapter/10.1007/978-3-642-38616-9_1/.

Barak:2014:OEF

[BBC+14] Boaz Barak, Nir Bitansky, Ran Canetti, Yael Tauman Kalai, Omer Paneth, and Amit Sahai. Obfuscation for evasive functions. *Lecture Notes in Computer Science*, 8349:26–51, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_2/.

Barthe:2019:SLN

[BBCL19] Gilles Barthe, Gustavo Betarte, Juan Diego Campo, and Carlos Luna. System-level non-interference of constant-time cryptography. Part I: Model. *Journal of Automated Reasoning*, 63(1):1–51, June 2019. CODEN JAREEW. ISSN 0168-7433 (print), 1573-0670 (electronic). URL http://link.springer.com/article/10.1007/s10817-017-9441-5.

Baillot:2019:ICC

[BBD19] Patrick Baillot, Gilles Barthe, and Ugo Dal Lago. Implicit computational complexity of subrecursive definitions and applications to cryptographic proofs. *Journal of Automated Reasoning*, 63(4):813–855, December 2019. CODEN JAREEW. ISSN 0168-7433 (print), 1573-0670 (electronic). URL http://link.springer.com/article/10.1007/s10817-019-09530-2.

Beurdouche:2017:MSU

[BBDL+17] Benjamin Beurdouche, Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, and Jean Karim Zinzindohoue. A messy state of the union: taming the composite state machines of TLS. *Communications of the Association for Computing Machinery*, 60(2):99–107, February 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2017/2/212438/fulltext.

Barenghi:2016:PPE

[BBDP16] Alessandro Barenghi, Michele Beretta, Alessandro Di Federico, and Gerardo Pelosi. A privacy-preserving encrypted OSN with stateless server interaction: the snake design. *Computers & Security*, 63(??):67–84, November 2016. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404816301031.

Beimel:2014:MLS

[BBEPT14] Amos Beimel, Aner Ben-Efraim, Carles Padró, and Ilya Tyomkin. Multi-linear secret-sharing schemes. *Lecture Notes in Computer Science*, 8349:394–418, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_17/`.

Bernstein:2017:SRD

[BBG+17] Daniel J. Bernstein, Joachim Breitner, Daniel Genkin, Leon Groot Bruinderink, Nadia Heninger, Tanja Lange, Christine van Vredendaal, and Yuval Yarom. Sliding right into disaster: Left-to-right sliding windows leak, June 28, 2017. URL `http://eprint.iacr.org/2017/627.pdf`.

Boldi:2012:IUG

[BBGT12] Paolo Boldi, Francesco Bonchi, Aristides Gionis, and Tamir Tassa. Injecting uncertainty in graphs for identity obfuscation. *Proceedings of the VLDB Endowment*, 5(11):1376–1387, July 2012. CODEN ???? ISSN 2150-8097.

Bingol:2019:EPP

[BBKL19] Muhammed Ali Bingöl, Osman Biçer, Mehmet Sabir Kiraz, and Albert Levi. An efficient 2-party private function evaluation protocol based on half gates. *The Computer Journal*, 62(4):598–613, April 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/62/4/598/5259181`.

Bollman:2015:PWI

[BBM15] Dorothy Bollman, Alcibiades Bustillo, and Einstein Morales. Parallel watermarking of images in the frequency domain. *Scalable Computing: Practice and Experience*, 16 (2):205–217, ???? 2015. CODEN ???? ISSN 1895-1767. URL `https://www.scpe.org/index.php/scpe/article/view/1090`.

Behrad:2020:NSA

[BBTC20] Shanay Behrad, Emmanuel Bertin, Stéphane Tuffin, and Noel Crespi. A new scalable authentication and access control mechanism for 5g-based IoT. *Future Generation Computer Systems*, 108(??):46–61, July 2020. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X19310143`.

Bernstein:2011:PCI

[BC11] Daniel J. Bernstein and Sanjit Chatterjee, editors. *Progress in Cryptology — INDOCRYPT 2011: 12th International Conference on Cryptology in India, Chennai, India, December 11–14. Proceedings*, volume 7107 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011. CODEN LNCSD9. ISBN 3-642-25577-9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/978-3-642-25577-9`.

Basin:2014:KYE

[BC14] David Basin and Cas Cremers. Know your enemy: Compromising adversaries in protocol analysis. *ACM Transactions on Information and System Security*, 17(2):7:1–7:??, November 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Bao:2016:LPP

[BC16] Haiyong Bao and Le Chen. A lightweight privacy-preserving scheme with data integrity for smart grid communications. *Concurrency and Computation: Practice and Experience*, 28(4):1094–1110, March 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Bocu:2018:HEB

[BC18] R. Bocu and C. Costache. A homomorphic encryption-based system for securely managing personal health metrics data. *IBM Journal of Research and Development*, 62(1):1:1–1:10, ???? 2018. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL `http://ieeexplore.ieee.org/document/8269765/`.

Balagurusamy:2019:CA

[BCC+19] V. S. K. Balagurusamy, C. Cabral, S. Coomaraswamy, E. Delamarche, D. N. Dillenberger, G. Dittmann, D. Friedman, O. Gökçe, N. Hinds, J. Jelitto, A. Kind, A. D. Kumar, F. Libsch, J. W. Ligman, S. Munetoh, C. Narayanaswami, A. Narendra, A. Paidimarri, M. A. P. Delgado, J. Rayfield, C. Subramanian, and R. Vaculin. Crypto anchors. *IBM Journal of Research and Development*, 63(2–3):4:1–4:12, March/May 2019. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Bichsel:2012:DMA

[BCD+12] Patrik Bichsel, Jan Camenisch, Bart De Decker, Jorn Lapon, and Vincent Naessens. Data-minimizing authentication goes mobile. *Lecture Notes in Computer Science*, 7394:55–71, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32805-3_5/.

Boche:2017:CQA

[BCDN17] Holger Boche, Minglai Cai, Christian Deppe, and Janis Nötzel. Classical-quantum arbitrarily varying wiretap channel: Secret message transmission under jamming attacks. *Journal of Mathematical Physics*, 58 (10):102203, October 2017. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427.

Badrignans:2010:SSA

[BCE+10] Benoît Badrignans, David Champagne, Reouven Elbaz, Catherine Gebotys, and Lionel Torres. SARFUM: Security architecture for remote FPGA update and monitoring. *ACM Transactions on Reconfigurable Technology and Systems*, 3(2):8:1–8:??, May 2010. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Balfanz:2012:FA

[BCE+12] Dirk Balfanz, Richard Chow, Ori Eisen, Markus Jakobsson, Steve Kirsch, Scott Matsumoto, Jesus Molina, and Paul van Oorschot. The future of authentication. *IEEE Security & Privacy*, 10(1): 22–27, January/February 2012. ISSN 1540-7993 (print), 1558-4046 (electronic).

Bugliesi:2015:ART

[BCEM15] Michele Bugliesi, Stefano Calzavara, Fabienne Eigner, and Matteo Maffei. Affine refinement types for secure distributed programming. *ACM Transactions on Programming Languages and Systems*, 37(4): 11:1–11:??, August 2015. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic).

Bana:2019:VMC

[BCEO19] Gergei Bana, Rohit Chadha, Ajay Kumar Eeralla, and Mitsuhiro Okada. Verification methods for the computationally complete symbolic attacker based on indistinguishability. *ACM Transactions on Computational Logic*, 21(1):2:1–2:??, October 2019. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic).

Bana:2020:VMC

[BCEO20] Gergei Bana, Rohit Chadha, Ajay Kumar Eeralla, and Mitsuhiro Okada. Verification methods for the computationally complete symbolic attacker based on indistinguishability. *ACM Transactions on Computational Logic*, 21(1):2:1–2:44, January 2020. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic).

Buhrman:2014:PBQ

[BCF+14] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, ???? 2014. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Bahri:2016:CCO

[BCF16] Leila Bahri, Barbara Carminati, and Elena Ferrari. COIP-continuous, operable, impartial, and privacy-aware identity validity estimation for OSN profiles. *ACM Transactions on the Web (TWEB)*, 10(4):23:1–23:??, December 2016. CODEN ???? ISSN 1559-1131 (print), 1559-114X (electronic).

Bugliesi:2015:CPB

[BCFK15] Michele Bugliesi, Stefano Calzavara, Riccardo Focardi, and Wilayat Khan. CookiExt: Patching the browser against session hijacking attacks. *Journal of Computer Security*, 23 (4):509–537, ???? 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Benedetto:2010:DQE

[BCG10] Francesco Benedetto, Alberto Curcio, and Gaetano Giunta. Dynamic QoS evaluation of multimedia contents in wireless networks by “double-boomerang” watermarking. *Future Internet*, 2 (1):60–73, March 08, 2010. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/2/1/60`.

Bahi:2012:SCS

[BCG12a] Jacques M. Bahi, Jean-François Couchot, and Christophe Guyeux. Steganography: a class of secure and robust algorithms. *The Computer Journal*, 55(6):653–666, June 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/55/6/653.full.pdf+html.

Borghoff:2012:PLL

[BCG+12b] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, and Miroslav Knezevic. PRINCE — a low-latency block cipher for pervasive computing applications. *Lecture Notes in Computer Science*, 7658:208–225, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34961-4_14/.

Blais:2019:DTL

[BCG19] Eric Blais, Clément L. Canonne, and Tom Gur. Distribution testing lower bounds via reductions from communication complexity. *ACM Transactions on Computation Theory*, 11(2):6:1–6:??, April 2019. CODEN ???? ISSN 1942-3454 (print), 1942-3462 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3305270.

Baelde:2012:TPR

[BCGAPM12] David Baelde, Pierre Courtieu, David Gross-Amblard, and Christine Paulin-Mohring. Towards provably robust watermarking. *Lecture Notes in Computer Science*, 7406:201–216, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32347-8_14/.

Bahi:2011:ECS

[BCGH11] Jacques M. Bahi, Raphaël Couturier, Christophe Guyeux, and Pierre-Cyrille Héam. Efficient and cryptographically secure generation of chaotic pseudorandom numbers on GPU. *arxiv.org*, ??(??):??, December 22, 2011. URL http://arxiv.org/abs/1112.5239.

Barthe:2012:CACa

[BCGK12] Gilles Barthe, Juan Manuel Crespo, Benjamin Grégoire, and César Kunz. Computer-aided cryptographic proofs. *Lecture Notes in Computer Science*, 7406:11–27, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32347-8_2/.

Beunardeau:2016:WBC

[BCGN16] Marc Beunardeau, Aisling Connolly, Remi Geraud, and David Naccache. White-box cryptography: Security in an insecure environment. *IEEE Security & Privacy*, 14(5):

88–92, September/October 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/05/msp2016050088-abs.html.

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/8e135695937bfe03e467e215177eec79d7dd.pdf. Cryptology ePrint Archive Report 2016/027 Version: 20160601:225540. See [AB17].

Belleville:2019:ASP

[BCHC19] Nicolas Belleville, Damien Couroussé, Karine Heydemann, and Henri-Pierre Charles. Automated software protection for the masses against side-channel attacks. *ACM Transactions on Architecture and Code Optimization*, 15(4):47:1–47:??, January 2019. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic).

Batina:2019:ISI

[BCHL19] Lejla Batina, Sherman S. M. Chow, Gerhard Hancke, and Zhe Liu. Introduction to the special issue on cryptographic engineering for Internet of Things: Security foundations, lightweight solutions, and attacks. *ACM Transactions on Embedded Computing Systems*, 18(3):22:1–22:??, June 2019. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3322641.

Bitansky:2013:SNI

[BCI$^+$13] Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Omer Paneth, and Rafail Ostrovsky. Succinct non-interactive arguments via linear interactive proofs. *Lecture Notes in Computer Science*, 7785:315–333, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_18/.

Brandenburger:2017:DTC

[BCK17] Marcus Brandenburger, Christian Cachin, and Nikola Knezević. Don't trust the cloud, verify: Integrity and consistency for cloud object stores. *ACM Transactions on Privacy and Security (TOPS)*, 20(3):8:1–8:??, August 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Bitansky:2017:VGB

[BCKP17] Nir Bitansky, Ran Canetti, Yael Tauman Kalai, and Omer Paneth. On virtual grey box obfuscation for general circuits. *Algorithmica*, 79(4):1014–1051, December 2017. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Bernstein:2014:CKR

[BCL14] Daniel J. Bernstein, Chitchanok Chuengsatiansup, and Tanja Lange. Curve41417: Karatsuba revisited. Report, Department of Computer Science, University of Illinois at Chicago, and Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, Chicago, IL 60607-7045, USA and P.O. Box 513, 5600 MB Eindhoven, The Netherlands, July 6, 2014. 19 pp. URL `http://cr.yp.to/ecdh/curve41417-20140706.pdf`.

Basin:2012:PRI

[BCM12] David Basin, Cas Cremers, and Simon Meier. Provably repairing the ISO/IEC 9798 standard for entity authentication. *Lecture Notes in Computer Science*, 7215:129–148, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-28641-4_8/`.

Basin:2013:PRI

[BCM13] David Basin, Cas Cremers, and Simon Meier. Provably repairing the ISO/IEC 9798 standard for entity authentication. *Journal of Computer Security*, 21(6):817–846, ???? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Basin:2015:ISC

[BCM+15] David Basin, Cas Cremers, Kunihiko Miyazaki, Sasa Radomirovic, and Dai Watanabe. Improving the security of cryptographic protocol standards. *IEEE Security & Privacy*, 13 (3):24–31, May/June 2015. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `http://www.computer.org/csdl/mags/sp/2015/03/msp2015030024-abs.html`.

Boche:2019:SMT

[BCND19] Holger Boche, Minglai Cai, Janis Nötzel, and Christian Deppe. Secret message transmission over quantum channels under adversarial quantum noise: Secrecy capacity and superactivation. *Journal of Mathematical Physics*, 60 (6):062202, June 2019. CODEN JMAPAQ. ISSN

0022-2488 (print), 1089-7658 (electronic), 1527-2427.

Bicakci:2013:LSS

[BCO13] Kemal Bicakci, Bruno Crispo, and Gabriele Oligeri. LAKE: a server-side authenticated key-establishment with low computational workload. *ACM Transactions on Internet Technology (TOIT)*, 13(2):5:1–5:??, December 2013. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Botta:2014:PCI

[BCP14a] Marco Botta, Davide Cavagnino, and Victor Pomponiu. Protecting the content integrity of digital imagery with fidelity preservation: An improved version. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 10(3):29:1–29:??, April 2014. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Boyle:2014:EO

[BCP14b] Elette Boyle, Kai-Min Chung, and Rafael Pass. On extractability obfuscation. *Lecture Notes in Computer Science*, 8349: 52–73, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_3/.

Basso:2011:BWC

[BCPV11] Alessandro Basso, Davide Cavagnino, Victor Pomponiu, and Annamaria Vernone. Blind watermarking of color images using Karhunen–Loève transform keying. *The Computer Journal*, 54(7):1076–1090, July 2011. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/54/7/1076.full.pdf+html.

Bessani:2013:DDS

[BCQ+13] Alysson Bessani, Miguel Correia, Bruno Quaresma, Fernando André, and Paulo Sousa. DepSky: Dependable and secure storage in a cloud-of-clouds. *ACM Transactions on Storage*, 9(4):12:1–12:??, November 2013. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic).

Blasco:2016:SWB

[BCTPL16] Jorge Blasco, Thomas M. Chen, Juan Tapiador, and Pedro Peris-Lopez. A survey of wearable biometric recognition systems. *ACM Computing Surveys*, 49

(3):43:1–43:??, November 2016. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Biddle:2012:GPL

[BCV12] Robert Biddle, Sonia Chiasson, and P. C. Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, 44(4): 19:1–19:??, August 2012. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Barker:2015:RKM

[BD15] Elaine Barker and Quynh Dang. Recommendation for key management. Part 3: Application-specific key management guidance. NIST Special Publication 800-57 Part 3 Revision 1, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, January 2015. vii + 94 pp. URL https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-57pt3r1.pdf.

Baruah:2018:TFA

[BD18] Barnana Baruah and Subhasish Dhal. A two-factor authentication scheme against FDM attack in IFTTT based smart home system. *Computers & Security*, 77(??):21–35, August 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818302402.

Belkacem:2014:DCM

[BDB14] Samia Belkacem, Zohir Dibi, and Ahmed Bouridane. DCT coefficients modelling for image watermarking. *International Journal of Computer Applications*, 36(4):155–163, 2014. ISSN 1206-212X (print), 1925-7074 (electronic). URL https://www.tandfonline.com/doi/full/10.2316/Journal.202.2014.4.202-4017.

Bruguera:2019:GEI

[BdD19] J. D. Bruguera and F. de Dinechin. Guest Editors introduction: Special section on computer arithmetic. *IEEE Transactions on Computers*, 68(7):951–952, July 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Bender:2012:DSP

[BDFK12] Jens Bender, Özgür Dagdelen, Marc Fischlin, and Dennis Kügler. Domain-specific pseudonymous signatures for the German identity card. *Lecture Notes in Computer Science*, 7483:104–119, 2012. CODEN LNCSD9. ISSN

0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33383-5_7/.

Bhasin:2015:EFB

[BDGH15] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Wei He. Exploiting FPGA block memories for protected cryptographic implementations. *ACM Transactions on Reconfigurable Technology and Systems*, 8(3):16:1–16:??, May 2015. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Buchmann:2011:XPF

[BDH11] Johannes Buchmann, Eeik Dahmen, and Andreas Hülsing. XMSS — a practical forward secure signature scheme based on minimal security assumptions. *Lecture Notes in Computer Science*, 7071: 117–129, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL https://link.springer.com/chapter/10.1007/978-3-642-25405-5_8.

Backstrom:2011:WAT

[BDK11] Lars Backstrom, Cynthia Dwork, and Jon Kleinberg. Wherefore art thou R3579X?: anonymized social networks, hidden patterns, and structural steganography. *Communications of the Association for Computing Machinery*, 54(12):133–141, December 2011. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

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].

Bernstein:2011:HSH

[BDL+11] D. Bernstein, N. Duif, T. Lange, P. Schwabe, and B. Yang. High-speed high-security signatures. *Journal of Cryptographic Engineering*, 2(2):77–89, September 2011. URL http://ed25519.cr.yp.to/ed25519-20110926.pdf.

Barbareschi:2019:PBM

[BDL+19] Mario Barbareschi, Alessandra De Benedictis, Erasmo La Montagna, Antonino Mazzeo, and Nicola Mazzocca. A PUF-based mutual authentication scheme for cloud-edges IoT systems. *Future Generation Computer Systems*, 101(??):246–261, December 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19301293.

Barbareschi:2018:PBH

[BDM18] Mario Barbareschi, Alessandra De Benedictis, and Nicola Mazzocca. A PUF-based hardware mutual authentication protocol. *Journal of Parallel and Distributed Computing*, 119(??):107–120, September 2018. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731518302582.

Belkhouja:2019:BBA

[BDM+19] Taha Belkhouja, Xiaojiang Du, Amr Mohamed, Abdulla K. Al-Ali, and Mohsen Guizani. Biometric-based authentication scheme for implantable medical devices during emergency situations. *Future Generation Computer Systems*, 98(??):109–119, September 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18325792.

Bossuet:2016:EPA

[BDMLN16] Lilian Bossuet, Nilanjan Datta, Cuauhtemoc Mancillas-López, and Mridul Nandi. ELmD: A pipelineable authenticated encryption and its hardware implementation. *IEEE Transactions on Computers*, 65 (11):3318–3331, November 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Bendlin:2011:SHE

[BDOZ11] Rikke Bendlin, Ivan Damgaård, Claudio Orlandi, and Sarah Zakarias. Semi-homomorphic encryption and multiparty computation. *Lecture Notes in Computer Science*, 6632: 169–188, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_11.

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.

Boldyreva:2012:SSE

[BDPS12] Alexandra Boldyreva, Jean Paul Degabriele, Kenneth G. Paterson, and Martijn Stam. Security of symmetric encryption in the presence of ciphertext fragmentation. *Lecture Notes in Computer Science*, 7237: 682–699, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_39; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_40/.

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/.

Bitansky:2013:WFS

[BDSG+13] Nir Bitansky, Dana Dachman-Soled, Sanjam Garg, Abhishek Jain, Yael Tauman Kalai, Adriana López-Alt, and Daniel Wichs. Why "Fiat–Shamir for proofs" lacks a proof. *Lecture Notes in Computer Science*, 7785:182–201, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_11/.

Bottarelli:2018:PCW

[BEB+18] Mirko Bottarelli, Gregory Epiphaniou, Dhouha Kbaier Ben Ismail, Petros Karadimas, and Haider Al-Khateeb. Physical characteristics of wireless communication channels for secret key establishment: a survey of the research. *Computers & Security*, 78(??):454–476, September 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818300841.

Beebe:2017:MFC

[Bee17] Nelson H. F. Beebe. *The Mathematical-Function Computation Handbook: Programming Using the MathCW Portable Software Library*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2017. ISBN 3-319-64109-3 (hardcover), 3-319-64110-7 (e-book). xxxvi + 1114 pp. LCCN QA75.5-76.95. URL http://www.springer.com/us/book/9783319641096.

Bellovin:2015:WRC

[Bel15] Steven M. Bellovin. What a real cybersecurity bill should address. *IEEE Security & Privacy*, 13(3): 92, May/June 2015. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://www.computer.org/csdl/mags/sp/2015/03/msp2015030092.html.

Bellovin:2016:EEE

[Bel16] Steven M. Bellovin. Easy email encryption. *IEEE Security & Privacy*, 14(6): 96, November/December 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/06/msp2016060096.html.

Bellovin:2018:UAE

[Bel18a] Steven M. Bellovin. Usenet, authentication, and engineering (or: Early design decisions for Usenet). Web article., February 23, 2018. URL https://www.cs.columbia.edu/~smb/blog/2018-02/2018-02-23.html.

Beltran:2018:IAA

[Bel18b] Marta Beltrán. Identifying, authenticating and authorizing smart objects and end users to cloud services in Internet of Things. *Computers & Security*, 77(??):595–611, August 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818301366.

Bellovin:2019:LI

[Bel19] S. M. Bellovin. Layered insecurity. *IEEE Security & Privacy*, 17(3):96–95, May/June 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Bajard:2016:MFA

[BEM16] Jean-Claude Bajard, Julien Eynard, and Nabil Merkiche. Multi-fault attack detection for RNS cryptographic architecture. In Montuschi et al. [MSH+16], pages 16–23. ISBN 1-5090-1615-5. ISSN 1063-6889. LCCN QA76.9.C62 S95 2016. URL http://ieeexplore.ieee.org/servlet/opac?punumber=7562813.

Berghel:2012:ITF

[Ber12] Hal Berghel. Identity theft and financial fraud: Some strangeness in the proportions. *Computer*, 45(1):86–89, January 2012. CODEN CPTRB4. ISSN 0018-9162.

Bera:2014:QC

[Ber14] Subhendu Bera. Quantum cryptography. *Linux Journal*, 2014(237):1:1–1:??, January 2014. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Berghel:2016:CKF

[Ber16a] Hal Berghel. Coda in the key of F2654hD4. *Computer*, 49(9):104–109, September 2016. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL https://www.computer.org/csdl/mags/co/2016/09/mco2016090104.html.

Berghel:2016:DJT

[Ber16b] Hal Berghel. Douglas Jones on today's voting machines. *Computer*, 49 (10):84–89, October 2016. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL https://www.computer.org/csdl/mags/co/2016/10/mco2016100084.html.

Berghel:2016:S

[Ber16c] Hal Berghel. Secretocracy. *Computer*, 49(2):63–67, February 2016. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/csdl/mags/co/2016/02/mco2016020063.html.

Berghel:2017:ELR

[Ber17] Hal Berghel. Equifax and the latest round of identity theft roulette. *Computer*, 50(12):72–76, December 2017. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL https://www.computer.org/csdl/mags/co/2017/12/mco2017120072.html.

Berretti:2018:IAS

[Ber18] Stefano Berretti. Improved audio steganalytic feature and its applications in audio forensics. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 14(2):43:1–43:??, May 2018. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Bouman:2011:SAW

[BF11] Niek J. Bouman and Serge Fehr. Secure authentication from a weak key, without leaking information. *Lecture Notes in Computer Science*, 6632: 246–265, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_15.

Bas:2012:BLK

[BF12] Patrick Bas and Teddy Furon. Are 128 bits Long keys possible in watermarking? *Lecture Notes in Computer Science*, 7394:191, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-32805-3_15.

Bos:2019:ACI

[BF19] J. W. Bos and S. J. Friedberger. Arithmetic considerations for isogeny-based cryptography. *IEEE Transactions on Computers*, 68(7):979–990, July 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Bhargavan:2012:VCI

[BFCZ12] Karthikeyan Bhargavan, Cédric Fournet, Ricardo Corin, and Eugen Zalinescu. Verified cryptographic implementations for TLS. *ACM Transactions on Information and System Security*, 15(1):3:1–3:??, March 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Barthe:2014:PRV

[BFG+14] Gilles Barthe, Cédric Fournet, Benjamin Grégoire, Pierre-Yves Strub, Nikhil Swamy, and Santiago Zanella-Béguelin. Probabilistic relational verification for cryptographic implementations. *ACM SIGPLAN Notices*, 49(1):193–205, January 2014. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). POPL '14 conference proceedings.

Bobba:2010:ABM

[BFK+10] Rakesh Bobba, Omid Fatemieh, Fariba Khan, Arindam Khan, Carl A. Gunter, Himanshu Khurana, and Manoj Prabhakaran. Attribute-based messaging: Access control and confidentiality. *ACM Transactions on Information and System Security*, 13(4):31:1–31:??, December 2010. CODEN ATISBQ. ISSN 1094-9224

(print), 1557-7406 (electronic).

Bhargavan:2016:MVP

[BFK16] Karthikeyan Bhargavan, Cedric Fournet, and Markulf Kohlweiss. miTLS: Verifying protocol implementations against real-world attacks. *IEEE Security & Privacy*, 14(6):18–25, November/December 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `https://www.computer.org/csdl/mags/sp/2016/06/msp2016060018-abs.html`.

Beimel:2012:SSS

[BFM12] Amos Beimel, Oriol Farràs, and Yuval Mintz. Secret sharing schemes for very dense graphs. *Lecture Notes in Computer Science*, 7417:144–161, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32009-5_10/`.

Berger:2016:EGF

[BFMT16] Thierry P. Berger, Julien Francq, Marine Minier, and Gaël Thomas. Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput. *IEEE Transactions on Computers*, 65(7):2074–2089, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Boldyreva:2014:MEW

[BG14] Alexandra Boldyreva and Paul Grubbs. Making encryption work in the cloud. *Network Security*, 2014(10):8–10, October 2014. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485814701011`.

Battistello:2012:TBA

[BGAD12] Patrick Battistello, Joaquin Garcia-Alfaro, and Cyril Delétré. Transaction-based authentication and key agreement protocol for inter-domain VoIP. *Journal of Network and Computer Applications*, 35(5):1579–1597, September 2012. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804512000653`.

Barthe:2012:CACb

[BGB12] Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin. Computer-aided cryptographic proofs. *Lecture Notes in Computer Science*, 7460:1–2, 2012.

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/accesspage/chapter/10.1007/978-3-642-33125-1_1`.

Balagani:2018:IAC

[BGE+18] Kiran S. Balagani, Paolo Gasti, Aaron Elliott, Azriel Richardson, and Mike O'Neal. The impact of application context on privacy and performance of keystroke authentication systems. *Journal of Computer Security*, 26(4):543–556, ???? 2018. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bossuet:2013:AFS

[BGG+13] Lilian Bossuet, Michael Grand, Lubos Gaspar, Viktor Fischer, and Guy Gogniat. Architectures of flexible symmetric key crypto engines — a survey: From hardware coprocessor to multi-crypto-processor system on chip. *ACM Computing Surveys*, 45(4):41:1–41:??, August 2013. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Boudot:2019:BFD

[BGG+19] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann. 795-bit factoring and discrete logarithms. Cado-nfs-discuss mailing list., December 2, 2019. URL `https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2019-December/001139.html`.

Barak:2010:IPO

[BGI+10] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. Report, Weizmann Institute, Rehovot 7610001, Israel, July 29, 2010. 54 pp. URL `http://www.wisdom.weizmann.ac.il/~oded/PS/obf4.pdf`.

Barak:2012:IPO

[BGI+12] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. *Journal of the ACM*, 59(2):6:1–6:48, April 2012. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Barbulescu:2013:QPA

[BGJT13] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. Report, Inria, CNRS, University of Lorraine; Foundation UPMC — LIP 6, CNRS UMR 7606; CryptoExperts, Lorraine, France; Paris, France; Paris, France, November 25, 2013. 16 pp. URL http://eprint.iacr.org/2013/400.pdf.

Barbulescu:2014:HQP

[BGJT14] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. *Lecture Notes in Computer Science*, 8441:1–16, 2014.

Barthe:2012:ACA

[BGK12] Gilles Barthe, Benjamin Grégoire, and César Kunz. Automation in computer-aided cryptography: Proofs, attacks and designs. *Lecture Notes in Computer Science*, 7679:7–8, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-35308-6_3.

Biswas:2017:STC

[BGN17] Arnab Kumar Biswas, Dipak Ghosal, and Shishir Nagaraja. A survey of timing channels and countermeasures. *ACM Computing Surveys*, 50(1):6:1–6:??, April 2017. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Borcea:2017:PEE

[BGP+17] Cristian Borcea, Arnab 'Bobby" Deb Gupta, Yuriy Polyakov, Kurt Rohloff, and Gerard Ryan. PICADOR: End-to-end encrypted publish–subscribe information distribution with proxy re-encryption. *Future Generation Computer Systems*, 71(??):177–191, June 2017. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16303983.

Brakerski:2014:LFH

[BGV14] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory*, 6(3):13:1–13:??, July 2014. CODEN ???? ISSN 1942-3454 (print), 1942-3462 (electronic).

Barkatullah:2015:GCF

[BH15] Javed Barkatullah and Timo Hanke. Goldstrike 1: CoinTerra's first-generation cryptocurrency mining processor for Bitcoin. *IEEE Micro*, 35(2):68–76, March/April 2015. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL http://www.computer.org/csdl/mags/mi/2015/02/mmi2015020068-abs.html.

Breitner:2019:BNS

[BH19] Joachum Breitner and Nadia Heninger. Biased nonce sense: lattice attacks against weak ECDSA signatures in cryptocurrencies. In I. Godberg and T. Moore, editors, *Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers*, volume 11598 of *Lecture Notes in Computer Science*, pages 3–20. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2019. URL https://www.springerprofessional.de/en/biased-nonce-sense-lattice-attacks-against-weak-ecdsa-signatures/17265526.

Bhattacharjee:2016:SWC

[Bha16] Yudhijit Bhattacharjee. *The spy who couldn't spell: a dyslexic traitor, an unbreakable code, and the FBI's hunt for America's stolen secrets*. New American Library, New York, NY, USA, 2016. ISBN 1-59240-900-8 (hardcover), 0-698-40409-2. ???? pp. LCCN JK468.I6 B48 2016.

Blasco:2012:FAS

[BHCdFR12] Jorge Blasco, Julio Cesar Hernandez-Castro, José María de Fuentes, and Benjamín Ramos. A framework for avoiding steganography usage over HTTP. *Journal of Network and Computer Applications*, 35(1):491–501, January 2012. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804511001901.

Behnia:2012:SEI

[BHG12] Rouzbeh Behnia, Swee-Huay Heng, and Che-Sheng Gan. Short and efficient identity-based undeniable signature scheme. *Lecture Notes in Computer Science*, 7449:143–148, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/

10.1007/978-3-642-32287-7_12/.

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 Computer Science*, 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.

Benhamouda:2019:SPD

[BHH19] F. Benhamouda, S. Halevi, and T. Halevi. Supporting private data on Hyperledger Fabric with secure multiparty computation. *IBM Journal of Research and Development*, 63(2–3): 3:1–3:8, March/May 2019. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Bosch:2014:SPS

[BHJP14] Christoph Bösch, Pieter Hartel, Willem Jonker, and Andreas Peter. A survey of provably secure searchable encryption. *ACM Computing Surveys*, 47(2):18:1–18:??, November 2014. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Berman:2013:HPR

[BHKN13] Itay Berman, Iftach Haitner, Ilan Komargodski, and Moni Naor. Hardness preserving reductions via cuckoo hashing. *Lecture Notes in Computer Science*, 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:2018:CFC

[BHT18] Itay Berman, Iftach Haitner, and Aris Tentes. Coin flipping of any constant bias implies one-way functions. *Journal of the ACM*, 65(3):14:1–14:??, March 2018. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Bonneau:2015:PEI

[BHvOS15] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. Passwords and the evolution of imperfect authentication. *Communications of the Association for Computing Machinery*, 58(7):78–87, July 2015. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://

cacm.acm.org/magazines/2015/7/188731/fulltext.

Biagioli:2012:CCS

[Bia12] Mario Biagioli. From ciphers to confidentiality: secrecy, openness and priority in science. *British Journal for the History of Science*, 45(2):213–233, June 2012. CODEN BJHSAT. ISSN 0007-0874 (print), 1474-001X (electronic).

Biggs:2008:CII

[Big08] Norman Biggs. *Codes: An introduction to Information Communication and Cryptography*. Springer undergraduate mathematics series. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 1-84800-273-4 (e-book), 1-84800-272-6 (paperback). x + 273 pp. LCCN QA268 .B496 2008eb.

Beimel:2014:CCW

[BIKK14] Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. *Lecture Notes in Computer Science*, 8349: 317–342, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_14/.

Biswas:2017:SAT

[Bis17] Arnab Kumar Biswas. Source authentication techniques for network-on-chip router configuration packets. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 13(2):28:1–28:??, March 2017. CODEN ???? ISSN 1550-4832.

Bauer:2010:RVC

[BJ10a] Andreas Bauer and Jan Jürjens. Runtime verification of cryptographic protocols. *Computers & Security*, 29(3):315–330, May 2010. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404809001047.

Brumley:2010:CAI

[BJ10b] B. B. Brumley and K. U. Jarvinen. Conversion algorithms and implementations for Koblitz curve cryptography. *IEEE Transactions on Computers*, 59(1):81–92, January 2010. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5255226.

Boche:2016:DSK

[BJ16] H. Boche and G. Janßen. Distillation of secret-key from a class of compound memoryless quantum sources. *Journal of Mathematical Physics*, 57 (8):082201, August 2016. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427.

Bouraoui:2017:HAE

[BJCHA17] Hasna Bouraoui, Chadlia Jerad, Anupam Chattopadhyay, and Nejib Ben Hadj-Alouane. Hardware architectures for embedded speaker recognition applications: a survey. *ACM Transactions on Embedded Computing Systems*, 16(3): 78:1–78:??, July 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Bogdanov:2012:UTC

[BJL12] Dan Bogdanov, Roman Jagomägis, and Sven Laur. A universal toolkit for cryptographically secure privacy-preserving data mining. *Lecture Notes in Computer Science*, 7299: 112–126, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-30428-6_9/.

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).

Brubaker:2014:UFA

[BJR+14] Chad Brubaker, Suman Jana, Baishakhi Ray, Sarfraz Khurshid, and Vitaly Shmatikov. Using frankencerts for automated adversarial testing of certificate validation in SSL/TLS implementations. In ????, editor, *IEEE Symposium on Security and Privacy*, page ?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2014. ISBN ???? LCCN ???? URL ????.

Boldyreva:2012:NPG

[BK12a] 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.

Bouti:2012:SCB

[BK12b] Adil Bouti and Jörg Keller. Securing cloud-based computations against malicious providers. *Operating Systems Review*, 46(2):38–42, July 2012. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Babamir:2019:DDB

[BK19] Faezeh Sadat Babamir and Murvet Kirci. Dynamic digest based authentication for client-server systems using biometric verification. *Future Generation Computer Systems*, 101(??):112–126, December 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19304480.

Bhuyan:2014:DDD

[BKBK14] Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita. Detecting distributed denial of service attacks: Methods, tools and future directions. *The Computer Journal*, 57(4):537–556, April 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/57/4/537.full.pdf+html.

Braun:2012:ULA

[BKJP12] Bastian Braun, Stefan Kucher, Martin Johns, and Joachim Posegga. A user-level authentication scheme to mitigate Web session-based vulnerabilities. *Lecture Notes in Computer Science*, 7449:17–29, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32287-7_2/.

Brakerski:2010:OHB

[BKKV10] Z. Brakerski, Y. T. Kalai, J. Katz, and V. Vaikuntanathan. Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In IEEE [IEE10], pages 501–510. ISBN 1-4244-8525-8. LCCN ???? URL http://ieeexplore.ieee.org/servlet/opac?punumber=5669376. IEEE Computer Society Order Number P4244.

Bogdanov:2013:SDS

[BKL+13] Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede. SPONGENT: The design space of lightweight cryptographic hashing. *IEEE Transactions on Computers*, 62(10):2041–2053, October 2013. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Bogdanov:2012:KAC

[BKLS12] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, and Francois-Xavier Standaert. Key-alternating ciphers in a provable setting: Encryption using a small number of public permutations. *Lecture Notes in Computer Science*, 7237:45–62, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_4`; `http://link.springer.com/chapter/10.1007/978-3-642-29011-4_5/`.

Bogdanov:2018:IEA

[BKLS18] Dan Bogdanov, Liina Kamm, Sven Laur, and Ville Sokk. Implementation and evaluation of an algorithm for cryptographically private principal component analysis on genomic data. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 15 (5):1427–1432, September 2018. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Bellare:2012:IBL

[BKPW12] Mihir Bellare, Eike Kiltz, Chris Peikert, and Brent Waters. Identity-based (lossy) trapdoor functions and applications. *Lecture Notes in Computer Science*, 7237:228–245, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_14`; `http://link.springer.com/chapter/10.1007/978-3-642-29011-4_15/`.

Bogdanov:2011:BCF

[BKR11] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. Report, Microsoft Research, Redmon, WA, USA, 2011. URL `http://research.microsoft.com/en-us/projects/cryptanalysis/aes.aspx`; `http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf`; `http://rump2011.cr.yp.to/d41bd80f6680cfd2323e53fbb9a62a81.pdf`. To appear at ASIACRYPT 2011.

Bogatov:2019:CEO

[BKR19] Dmytro Bogatov, George Kollios, and Leonid Reyzin.

A comparative evaluation of order-revealing encryption schemes and secure range-query protocols. *Proceedings of the VLDB Endowment*, 12(8): 933–947, April 2019. CODEN ???? ISSN 2150-8097.

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 (IJFCS)*, 29(3):357–??, April 2018. CODEN IFCSEN. ISSN 0129-0541.

Bothe:2013:EPS

[BKV13] Suvarna Bothe, Panagiotis Karras, and Akrivi Vlachou. eSkyline: processing skyline queries over encrypted data. *Proceedings of the VLDB Endowment*, 6(12):1338–1341, August 2013. CODEN ???? ISSN 2150-8097.

Bernstein:2010:PCA

[BL10] Daniel J. Bernstein and Tanja Lange, editors. *Progress in cryptology — Africacrypt 2010: third international conference on cryptology in Africa, Stellenbosch, South Africa, May 3–6, 2010. proceedings*, volume 6055 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-12677-4 (softcover). LCCN ????

Byun:2011:SMC

[BL11] Jin Wook Byun and Dong Hoon Lee. On a security model of conjunctive keyword search over encrypted relational database. *The Journal of Systems and Software*, 84(8):1364–1372, August 2011. CODEN JSSODM. ISSN 0164-1212.

Bai:2012:SSR

[BL12] Yu Bai and Yanlong Liu. A synchronization strengthen RFID authentication protocol based on key array. *Lecture Notes in Computer Science*, 7530: 113–119, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33478-8_15/.

Bernstein:2014:HEC

[BL14] Daniel J. Bernstein and Tanja Lange. Hyper-and-elliptic-curve cryptography. *LMS Journal of Computation and Mathematics*, 17(A):181–202, 2014. CO-

DEN ???? ISSN 1461-1570.

Bidgoly:2015:MQV

[BL15] Amir Jalaly Bidgoly and Behrouz Tork Ladani. Modelling and quantitative verification of reputation systems against malicious attackers. *The Computer Journal*, 58(10):2567–2582, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2567.

Bidgoly:2016:MQV

[BL16] Amir Jalaly Bidgoly and Behrouz Tork Ladani. Modeling and quantitative verification of trust systems against malicious attackers. *The Computer Journal*, 59(7):1005–1027, July 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/7/1005.

Bernstein:2017:SCS

[BL17] Daniel J. Bernstein and Tanja Lange. SafeCurves: choosing safe curves for elliptic-curve cryptography. Web site., January 22, 2017. URL https://safecurves.cr.yp.to/.

Blanchette:2012:BPC

[Bla12] Jean-François Blanchette. *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents*. MIT Press, Cambridge, MA, USA, 2012. ISBN 0-262-01751-2 (hardcover). 276 pp. LCCN K2269.5 .B58 2012.

Blaze:2016:UHR

[Bla16] Matt Blaze. US House of Representatives, Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, Hearing on “Deciphering the Debate over Encryption”. Web document, April 19, 2016. URL http://docs.house.gov/meetings/IF/IF02/20160419/104812/HHRG-114-IF02-Wstate-BlazeM-20160419-U3.pdf.

Benzaid:2016:FAW

[BLAN+16] Chafika Benzaid, Karim Lounis, Ameer Al-Nemrat, Nadjib Badache, and Mamoun Alazab. Fast authentication in wireless sensor networks. *Future Generation Computer Systems*, 55(??):362–375, February 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X14001393.

Bai:2019:LMD

[BLL+19] Tong Bai, Jinzhao Lin, Guoquan Li, Huiqian Wang, Peng Ran, Zhangyong Li, Dan Li, Yu Pang, Wei Wu, and Gwanggil Jeon. A lightweight method of data encryption in BANs using electrocardiogram signal. *Future Generation Computer Systems*, 92(??):800–811, March 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X17310361`.

Buchmann:2017:PCS

[BLM17a] Johannes Buchmann, Kristin Lauter, and Michele Mosca. Postquantum cryptography — state of the art. *IEEE Security & Privacy*, 15(4):12–13, July/August 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `https://www.computer.org/csdl/mags/sp/2017/04/msp2017040012.html`.

Buchmann:2017:PCU

[BLM17b] Johannes Buchmann, Kristin Lauter, and Michele Mosca. Postquantum cryptography — state of the art. *IEEE Security & Privacy*, 15(4):12–13, July/August 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `https://www.computer.org/csdl/mags/sp/2017/04/msp2017040012.html`.

Buchmann:2018:PCP

[BLM18] J. Buchmann, K. Lauter, and M. Mosca. Postquantum cryptography, part 2. *IEEE Security & Privacy*, 16(5):12–13, September/October 2018. ISSN 1540-7993 (print), 1558-4046 (electronic).

Bernstein:2016:DES

[BLN16] Daniel J. Bernstein, Tanja Lange, and Ruben Niederhagen. Dual EC: A standardized back door. In Ryan et al. [RNQ16], pages 256–281. ISBN 3-662-49300-4 (paperback); 3-662-49301-2 (e-book). LCCN QA76.9.A25. URL `http://link.springer.com/book/10.1007/978-3-662-49301-4`.

Blomer:2012:TKG

[Blö12] Johannes Blömer. Turing und Kryptografie. (German) [Turing and cryptography]. *Informatik Spektrum*, 35(4):261–270, August 2012. CODEN INSKDW. ISSN 0170-6012 (print), 1432-122X (electronic). URL `http://www.springerlink.com/content/703t016671n87094/`. Special Issue: Alan Turing.

Blondeau:2015:IDA

[Blo15] Céline Blondeau. Impossible differential attack on 13-round Camellia-192. *Information Processing Letters*, 115(9):660–666, September 2015. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019015000472.

Bernstein:2012:SIN

[BLS12] Daniel J. Bernstein, Tanja Lange, and Peter Schwabe. The security impact of a new cryptographic library. *Lecture Notes in Computer Science*, 7533:159–176, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33481-8_9/.

Buchanan:2015:FIW

[BLU+15] William J. Buchanan, David Lanc, Elochukwu Ukwandu, Lu Fan, Gordon Russell, and Owen Lo. The future Internet: a world of secret shares. *Future Internet*, 7(4):445–464, November 24, 2015. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/7/4/445.

Bestavros:2017:PSU

[BLV17] Azer Bestavros, Andrei Lapets, and Mayank Varia. Privacy and security: User-centric distributed solutions for privacy-preserving analytics. *Communications of the Association for Computing Machinery*, 60(2):37–39, February 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2017/2/212427/fulltext.

Burmester:2011:LRA

[BM11] Mike Burmester and Jorge Munilla. Lightweight RFID authentication with forward and backward security. *ACM Transactions on Information and System Security*, 14(1):11:1–11:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Birajdar:2013:DIF

[BM13] Gajanan K. Birajdar and Vijay H. Mankar. Digital image forgery detection using passive techniques: A survey. *Digital Investigation*, 10(3):226–245, 2013. ISSN 1742-2876. URL http://www.sciencedirect.com/science/article/pii/S1742287613000364.

Bard:2015:PRO

[BM15] Gregory V. Bard and Theodore McDonnough.

Plaintext recovery for one-time pads used twice. *ACM Communications in Computer Algebra*, 49(1):17–18, March 2015. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Bhattacharya:2018:UPC

[BM18] Sarani Bhattacharya and Debdeep Mukhopadhyay. Utilizing performance counters for compromising public key ciphers. *ACM Transactions on Privacy and Security (TOPS)*, 21(1):5:1–5:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3156015.

Benamara:2016:ICA

[BMB16] Oualid Benamara, Fatiha Merazka, and Kamel Betina. An improvement of a cryptanalysis algorithm. *Information Processing Letters*, 116(2):192–196, February 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019015001398.

Baldwin:2010:AFI

[BMBS10] Adrian Baldwin, Marco Casassa-Mont, Yolanta Beres, and Simon Shiu. Assurance for federated identity management. *Journal of Computer Security*, 18(4):541–572, ???? 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bartoli:2019:VEW

[BMDT19] Alberto Bartoli, Eric Medvet, Andrea De Lorenzo, and Fabiano Tarlao. Viewpoint: Enterprise wi-fi: we need devices that are secure by default. *Communications of the Association for Computing Machinery*, 62(5):33–35, May 2019. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL https://cacm.acm.org/magazines/2019/5/236421/fulltext.

Biswas:2012:IBA

[BMM12] Subir Biswas, Jelena Misić, and Vojislav Misić. An identity-based authentication scheme for safety messages in WAVE-enabled VANETs. *International Journal of Parallel, Emergent and Distributed Systems: IJPEDS*, 27(6):541–562, 2012. CODEN ???? ISSN 1744-5760 (print), 1744-5779 (electronic).

Backes:2012:GCP

[BMP12] Michael Backes, Matteo Maffei, and Kim Pecina. G2C: Cryptographic protocols from goal-driven specifications. *Lecture*

Notes in Computer Science, 6993:57–77, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27375-9_4/.

Banik:2012:DFA

[BMS12] Subhadeep Banik, Subhamoy Maitra, and Santanu Sarkar. A differential fault attack on the grain family of stream ciphers. *Lecture Notes in Computer Science*, 7428: 122–139, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33027-8_8/.

Babamir:2014:AKP

[BN14] Faezeh Sadat Babamir and Ali Norouzi. Achieving key privacy and invisibility for unattended wireless sensor networks in healthcare. *The Computer Journal*, 57(4):624–635, April 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/57/4/624.full.pdf+html.

Buckley:2015:RVV

[BNA15] N. Buckley, A. K. Nagar, and S. Arumugam. On real-valued visual cryptographic basis matrices. *J.UCS: Journal of Universal Computer Science*, 21 (12):1536–??, ???? 2015. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL http://www.jucs.org/jucs_21_12/on_real_valued_visual.

Bailis:2017:RPC

[BNMH17] Peter Bailis, Arvind Narayanan, Andrew Miller, and Song Han. Research for practice: Cryptocurrencies, blockchains, and smart contracts; hardware for deep learning. *Communications of the Association for Computing Machinery*, 60(5):48–51, May 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2017/5/216321/fulltext.

Baskaran:2019:TEL

[BNNH19] Annie Gilda Roselin Arockia Baskaran, Priyadarsi Nanda, Surya Nepal, and Sean He. Testbed evaluation of lightweight authentication protocol (LAUP) for 6LoWPAN wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 31 (23):e4868:1–e4868:??, December 10, 2019. CODEN CCPEBO. ISSN 1532-0626

(print), 1532-0634 (electronic).

Bunder:2017:GAR

[BNST17] Martin Bunder, Abderrahmane Nitaj, Willy Susilo, and Joseph Tonien. A generalized attack on RSA type cryptosystems. *Theoretical Computer Science*, 704(??):74–81, December 15, 2017. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397517306643.

Biryukov:2014:DEA

[BNY14] Alex Biryukov, Jorge Nakahara, Jr., and Hamdi Murat Yildirim. Differential entropy analysis of the IDEA block cipher. *Journal of Computational and Applied Mathematics*, 259 (part B)(??):561–570, March 15, 2014. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042713003981.

Ben-Othman:2013:IHN

[BOB13] Jalel Ben-Othman and Yesica I. Saavedra Benitez. IBC-HWMP: a novel secure identity-based cryptography-based scheme for Hybrid Wireless Mesh Protocol for IEEE 802.11s. *Concurrency and Computation: Practice and Experience*, 25(5):686–700, April 10, 2013. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Bohme:2010:ASS

[Böh10] Rainer Böhme. *Advanced Statistical Steganalysis*, volume 0 of *Information Security and Cryptography*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-14312-1, 3-642-14313-X (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xv + 285 pp. LCCN QA76.9.A25 B64 2010; TA1637-1638; Z104 .B68 2010. URL http://www.springerlink.com/content/978-3-642-14313-7.

Boneh:2012:PBC

[Bon12] Dan Boneh. Pairing-based cryptography: Past, present, and future. *Lecture Notes in Computer Science*, 7658:1, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-34961-4_1.

Boneh:2019:ACK

[Bon19] Dan Boneh. Attacking cryptographic key exchange with precomputation: technical perspective. *Communications of the Association for Computing Machinery*, 62(1): 105, January 2019. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL https://cacm.acm.org/magazines/2019/1/233522/fulltext.

Bailey:2014:UIA

[BOP14] Kyle O. Bailey, James S. Okolica, and Gilbert L. Peterson. User identification and authentication using multi-modal behavioral biometrics. *Computers & Security*, 43(??):77–89, June 2014. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404814000340.

Borghoff:2010:CLC

[Bor10] Julia Borghoff. *Cryptanalysis of lightweight ciphers*. Ph.D. thesis, Department of Mathematics, Technical University of Denmark, Lyngby, Denmark, 2010. x + 198 pp.

Bowyer:2011:WSD

[Bow11] Kevin W. Bowyer. What surprises do identical twins have for identity science? *Computer*, 44(7):100–102, July 2011. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Boyen:2013:ABF

[Boy13] Xavier Boyen. Attribute-based functional encryption on lattices. *Lecture Notes in Computer Science*, 7785:122–142, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_8/.

Boyce:2016:BOT

[Boy16] Griffin Boyce. Bake in .onion for tear-free and stronger Website authentication. *IEEE Security & Privacy*, 14(2):15–21, March/April 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Beissinger:2006:CUM

[BP06] Janet Beissinger and Vera Pless. *The Cryptoclub: Using Mathematics to Make and Break Secret Codes*. A. K. Peters, Ltd., Wellesley, MA, USA, 2006. ISBN 1-56881-223-X. xvi + 199 pp. LCCN QA40.5 .B45 2006. URL http://www.loc.gov/catdir/toc/ecip067/2006002743.html.

Burns:2010:SCR

[BP10] Randal Burns and Zachary Peterson. Security constructs for regulatory-compliant storage. *Communications of the Association for Computing Machinery*, 53(1):126–130, January 2010. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Bohli:2011:RAP

[BP11] Jens-Matthias Bohli and Andreas Pashalidis. Relations among privacy notions. *ACM Transactions on Information and System Security*, 14(1):4:1–4:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

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).

Bencsath:2012:CSD

[BPBF12] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, and Márk Félegyházi. The cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet*, 4(4):971–1003, November 06, 2012. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/4/4/971`.

Brooke:2010:DCX

[BPP10] Phillip J. Brooke, Richard F. Paige, and Christopher Power. Document-centric XML workflows with fragment digital signatures. *Software—Practice and Experience*, 40(8):655–672, July 2010. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Bellare:2014:SSEa

[BPR14a] Mihir Bellare, Kenneth Paterson, and Phillip Rogaway. Security of symmetric encryption against mass surveillance. Cryptology ePrint Archive report 2014/438, Department of Computer Science and Engineering, University of California San Diego, San Diego, CA, USA, 2014. URL `http://eprint.iacr.org`.

Bellare:2014:SSEb

[BPR14b] Mihir Bellare, Kenneth Paterson, and Phillip Rogaway. Security of symmetric encryption against mass surveillance. In ????, editor, *Advances in Cryptology – CRYPTO 2014*, pages 1–19. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2014. ISBN ???? LCCN ???? URL ????.

Boneh:2016:BCR

[BPS16] Dan Boneh, Kenny Paterson, and Nigel P. Smart. Building a community of real-world cryptographers. *IEEE Security & Privacy*, 14(6):7–9, November/December 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/06/msp2016060007.html.

Balsa:2017:TIC

[BPSD17] Ero Balsa, Cristina Pérez-Solà, and Claudia Diaz. Towards inferring communication patterns in online social networks. *ACM Transactions on Internet Technology (TOIT)*, 17(3):32:1–32:??, July 2017. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Brakerski:2014:VBB

[BR14] Zvika Brakerski and Guy N. Rothblum. Virtual black-box obfuscation for all circuits via generic graded encoding. *Lecture Notes in Computer Science*, 8349:1–25, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_1/; http://link.springer.com/content/pdf/bfm:978-3-642-54242-8/1.pdf.

Barker:2019:TUC

[BR19] Elaine Barker and Allen Roginsky. Transitioning the use of cryptographic algorithms and key lengths. NIST Special Publication 800-131A Revision 2, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, March 2019. iv + 27 pp.

Brakerski:2013:WHB

[Bra13] Zvika Brakerski. When homomorphism becomes a liability. *Lecture Notes in Computer Science*, 7785:143–161, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_9/.

Bradbury:2015:BSB

[Bra15] D. Bradbury. In blocks [security Bitcoin]. *Engineering Technology*, 10(2):68–71, March 2015. ISSN 1750-9637 (print), 1750-9645 (electronic).

Brewster:2018:RCF

[Bre18] R. Brewster. Re-creating the first flip-flop — a fundamental component of computers turns 100 [resources hands on]. *IEEE Spectrum*, 55(6):13–14, June 2018. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Briggs:2011:SDC

[Bri11] Asa Briggs. *Secret days: code-breaking in Bletchley Park*. Frontline Books, London, UK, 2011. ISBN 1-84832-615-7. xix + 202 + 26 pp. LCCN D810.C88 B75 2011.

Broemeling:2011:AES

[Bro11] Lyle D. Broemeling. An account of early statistical inference in Arab cryptology. *The American Statistician*, 65(4):255–257, November 2011. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Brooks:2012:QCE

[Bro12] M. Brooks. Quantum cash and the end of counterfeiting. *IEEE Spectrum*, 49(6): 58–59, June 2012. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Brook:2017:LSR

[Bro17] Chris Brook. `libgcrypt` 'sliding right' attack allows recovery of RSA-1024 keys. Web blog., July 5, 2017. URL `https://threatpost.com/libgcrypt-sliding-right-attack-allows-recovery-of-rsa-1024-keys/126675/`. See [BBG+17].

Broumandnia:2019:MCM

[Bro19] Ali Broumandnia. The 3D modular chaotic map to digital color image encryption. *Future Generation Computer Systems*, 99(??):489–499, October 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X19300214`.

Becker:2013:SDL

[BRPB13] Georg T. Becker, Francesco Regazzoni, Christof Paar, and Wayne P. Burleson. Stealthy dopant-level hardware trojans? Report, University of Massachusetts (Amherst, USA); TU Delft (The Netherlands); ALaRI (University of Lugano, Switzerland); Horst Görtz Institut for IT-Security, Ruhr-Universität Bochum (Bochum, Germany), June 7, 2013. 18 pp. URL `http://people.umass.edu/gbecker/BeckerChes13.pdf`.

Benaloh:2015:EEV

[BRR+15] Josh Benaloh, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa

Teague, and Poorvi L. Vora. End-to-end verifiability. *arxiv.org*, ??(??):??, April 15, 2015. URL `http://arxiv.org/abs/1504.03778`.

Bag:2017:BBW

[BRS17] S. Bag, S. Ruj, and K. Sakurai. Bitcoin block withholding attack: Analysis and mitigation. *IEEE Transactions on Information Forensics and Security*, 12(8):1967–1978, August 2017. ISSN 1556-6013 (print), 1556-6021 (electronic).

Bellare:2012:MIS

[BRT12] Mihir Bellare, Thomas Ristenpart, and Stefano Tessaro. Multi-instance security and its application to password-based cryptography. *Lecture Notes in Computer Science*, 7417: 312–329, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32009-5_19/`.

Brumley:2012:SFI

[Bru12] Billy Bob Brumley. Secure and fast implementations of two involution ciphers. *Lecture Notes in Computer Science*, 7127: 269–282, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-27937-9_19/`.

Bachrach:2011:ISS

[BS11] Mayra Bachrach and Frank Y. Shih. Image steganography and steganalysis. *WIREs Computational Statistics*, 3(5):251–259, May/June 2011. CODEN ???? ISSN 1939-0068 (print), 1939-5108 (electronic).

Bergsma:2012:PAW

[BS12] Timothy T. Bergsma and Michael S. Smith. `Sumo`: An authenticating Web application with an embedded R session. *The R Journal*, 4(1):60–63, June 2012. CODEN ???? ISSN 2073-4859. URL `http://journal.r-project.org/archive/2012-1/RJournal_2012-1_Bergsma+Smith.pdf`.

Bajaj:2013:CSE

[BS13a] Sumeet Bajaj and Radu Sion. CorrectDB: SQL engine with practical query authentication. *Proceedings of the VLDB Endowment*, 6(7):529–540, May 2013. CODEN ???? ISSN 2150-8097.

Birrell:2013:FIM

[BS13b] Eleanor Birrell and Fred B. Schneider. Federated identity management systems:

A privacy-based characterization. *IEEE Security & Privacy*, 11(5):36–48, September/October 2013. ISSN 1540-7993 (print), 1558-4046 (electronic).

Bhattacherjee:2014:CAT

[BS14] Sanjay Bhattacherjee and Palash Sarkar. Concrete analysis and trade-offs for the (complete tree) layered subset difference broadcast encryption scheme. *IEEE Transactions on Computers*, 63(7):1709–1722, July 2014. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Bagheri:2015:NNA

[BS15] Kadijeh Bagheri and Mohammad-Reza Sadeghi. A new non-associative cryptosystem based on NTOW public key cryptosystem and octonions algebra. *ACM Communications in Computer Algebra*, 49(1):13, March 2015. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Bronzino:2019:ISV

[BSA+19] Francesco Bronzino, Paul Schmitt, Sara Ayoubi, Guilherme Martins, Renata Teixeira, and Nick Feamster. Inferring streaming video quality from encrypted traffic: Practical models and deployment experience. *Proceedings of the ACM on Measurement and Analysis of Computing Systems (POMACS)*, 3(3):56:1–56:25, December 2019. CODEN ???? ISSN 2476-1249. URL https://dl.acm.org/doi/10.1145/3366704.

Bala:2019:SAG

[BSBB19] Suman Bala, Gaurav Sharma, Himani Bansal, and Tarunpreet Bhatia. On the security of authenticated group key agreement protocols. *Scalable Computing: Practice and Experience*, 20(1):93–99, ???? 2019. CODEN ???? ISSN 1895-1767. URL https://www.scpe.org/index.php/scpe/article/view/1440.

Bendiab:2019:FNF

[BSBG19] Keltoum Bendiab, Stavros Shiaeles, Samia Boucherkha, and Bogdan Ghita. FCMDT: a novel fuzzy cognitive maps dynamic trust model for cloud federated identity management. *Computers & Security*, 86(??):270–290, September 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818312252.

Ben-Sasson:2017:SZK

[BSCTV17] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and

Madars Virza. Scalable zero knowledge via cycles of elliptic curves. *Algorithmica*, 79(4):1102–1160, December 2017. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Boorghany:2015:CIL

[BSJ15] Ahmad Boorghany, Siavash Bayat-Sarmadi, and Rasool Jalili. On constrained implementation of lattice-based cryptographic primitives and schemes on smart cards. *ACM Transactions on Embedded Computing Systems*, 14(3):42:1–42:??, April 2015. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Bojinov:2014:NMC

[BSR+14] Hristo Bojinov, Daniel Sanchez, Paul Reber, Dan Boneh, and Patrick Lincoln. Neuroscience meets cryptography: crypto primitives secure against rubber hose attacks. *Communications of the Association for Computing Machinery*, 57(5):110–118, May 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Basin:2011:AIS

[BSS11] David Basin, Patrick Schaller, and Michael Schläpfer. *Applied information security: a hands-on approach*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011. ISBN 3-642-24473-4 (hardcover). xiv + 202 pp. LCCN QA76.9.A25 B37 2011.

Beaulieu:2013:SSF

[BSS+13] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. Report, National Security Agency, 9800 Savage Road, Fort Meade, MD 20755, USA, June 19, 2013. 45 pp. URL `https://eprint.iacr.org/2013/404.pdf`; `https://www.schneier.com/crypto-gram/archives/2018/0515.html`; `https://www.wikitribune.com/story/2018/04/20/business/exclusive-nsa-encryption-plan-for-internet-of-things-rejected-by-international-body/67004/`.

Batina:2012:HEB

[BSSV12] Lejla Batina, Stefaan Seys, Dave Singelée, and Ingrid Verbauwhede. Hierarchical ECC-based RFID authentication protocol. *Lecture Notes in Computer Science*, 7055:183–201, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-

3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-25286-0_12/.

Broustis:2012:GAN

[BSV12] Ioannis Broustis, Ganapathy S. Sundaram, and Harish Viswanathan. Group authentication: a new paradigm for emerging applications. *Bell Labs Technical Journal*, 17(3):157–173, December 2012. CODEN BLTJFD. ISSN 1089-7089 (print), 1538-7305 (electronic).

Boneh:2012:FEN

[BSW12] Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: a new vision for public-key cryptography. *Communications of the Association for Computing Machinery*, 55(11):56–64, November 2012. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Biskup:2012:RBR

[BT12] Joachim Biskup and Cornelia Tadros. Revising belief without revealing secrets. *Lecture Notes in Computer Science*, 7153:51–70, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28472-4_4/.

Braeken:2018:AAA

[BT18] A. Braeken and Abdellah Touhafi. AAA — autonomous anonymous user authentication and its application in V2G. *Concurrency and Computation: Practice and Experience*, 30(12), June 25, 2018. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic). URL https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.4303.

Bosch:2012:SDR

[BTHJ12] Christoph Bösch, Qiang Tang, Pieter Hartel, and Willem Jonker. Selective document retrieval from encrypted database. *Lecture Notes in Computer Science*, 7483:224–241, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33383-5_14/.

Bouabana-Tebibel:2015:PSE

[BTK15] Thouraya Bouabana-Tebibel and Abdellah Kaci. Parallel search over encrypted data under attribute based encryption on the cloud computing. *Computers & Security*, 54(??):77–91, October 2015. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404815000577.

Blasco:2015:HDT

[BTPLST15] Jorge Blasco, Juan E. Tapiador, Pedro Peris-Lopez, and Guillermo Suarez-Tangil. Hindering data theft with encrypted data trees. *The Journal of Systems and Software*, 101(??):147–158, March 2015. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121214002775.

Brocardo:2015:AVM

[BTW15] Marcelo Luiz Brocardo, Issa Traore, and Isaac Woungang. Authorship verification of e-mail and tweet messages applied for continuous authentication. *Journal of Computer and System Sciences*, 81(8):1429–1440, December 2015. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000014001834.

Buchmann:2010:EKG

[Buc10] Johannes Buchmann. *Einführung in die Kryptographie. (German) [Introduction to Cryptography]*. Springer-Lehrbuch. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-11186-6. xxiv + 280 pp. LCCN ???? URL http://www.springer.com/mathematics/numbers/book/978-3-642-11185-3; http://www.springerlink.com/content/j5g004.

Budiansky:2016:CWN

[Bud16] Stephen Budiansky. *Code warriors: NSA's codebreakers and the secret intelligence war against the Soviet Union*. Alfred A. Knopf, New York, NY, USA, 2016. ISBN 0-385-35266-2, 0-385-35267-0. xxi + 389 + 16 pp. LCCN UB256.U6 B83 2016.

Bulygin:2010:AOP

[Bul10a] Stanislav Bulygin. Abstract only: Polynomial system solving for decoding linear codes and algebraic cryptanalysis parametric polynomial system discussion: canonical comprehensive. *ACM Communications in Computer Algebra*, 44(2):72, June 2010. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Bulygin:2010:CAC

[Bul10b] Stanislav Bulygin. *Com-*

puter algebra in coding theory and cryptanalysis. Südwestdeutscher Verlag für Hochschulschriften, Saarbrücken, Germany, 2010. ISBN 3-8381-0948-1. ???? pp. LCCN ????

Bultan:2018:SCA

[Bul18] Tevfik Bultan. Side-channel analysis via symbolic execution and model counting. *ACM SIGSOFT Software Engineering Notes*, 43(4):55, October 2018. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

Burke:2011:AMD

[Bur11] Colin Burke. Agnes Meyer Driscoll vs. the Enigma and the Bombe. Report, University of Maryland, Baltimore County, 1000 Hilltop Circle Baltimore, MD 21250, USA, January 7, 2011. 132 pp. URL `https://userpages.umbc.edu/~burke/driscoll1-2011.pdf`.

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`.

Brakerski:2011:EFH

[BV11] Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In IEEE [IEE11b], pages 97–106. ISBN 1-4577-1843-X. LCCN ????

Brakerski:2014:EFH

[BV14] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on Computing*, 43(2):831–871, ???? 2014. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Bitansky:2018:IOF

[BV18] Nir Bitansky and Vinod Vaikuntanathan. Indistinguishability obfuscation from functional encryption. *Journal of the ACM*, 65(6):39:1–39:??, November 2018. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3234511`.

Bayrak:2012:AII

[BVIB12] Ali Galip Bayrak, Nikola Velickovic, Paolo Ienne, and Wayne Burleson. An architecture-independent instruction shuffler to protect against side-channel attacks. *ACM Transactions on Architecture and Code Optimization*, 8(4): 20:1–20:??, January 2012. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic).

Baek:2013:SPK

[BVS+13] Joonsang Baek, Quang Hieu Vu, Abdulhadi Shoufan, Andrew Jones, and Duncan S. Wong. Stateful public-key encryption schemes forward-secure against state exposure. *The Computer Journal*, 56(4):497–507, April 2013. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/56/4/497.full.pdf+html`.

Bogdanov:2012:ZCL

[BW12] Andrey Bogdanov and Meiqin Wang. Zero-correlation linear cryptanalysis with reduced data complexity. *Lecture Notes in Computer Science*, 7549: 29–48, 2012.

Bhatnagar:2013:BIW

[BW13] Gaurav Bhatnagar and Q. M. Jonathan Wu. Biometrics inspired watermarking based on a fractional dual tree complex wavelet transform. *Future Generation Computer Systems*, 29(1):182–195, January 2013. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X1200129X`.

Bai:2016:ALC

[BW16] Kunpeng Bai and Chuankun Wu. An AES-like cipher and its white-box implementation. *The Computer Journal*, 59(7):1054–1065, July 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/59/7/1054`.

Bhatnagar:2013:SRI

[BWA13] Gaurav Bhatnagar, Q. M. Jonathan Wu, and Pradeep K. Atrey. Secure randomized image watermarking based on singular value decomposition. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 10(1):4:1–4:??, December 2013. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Baek:2016:EGC

[BWLA16] Joonsang Baek, Duncan S. Wong, Jin Li, and Man Ho Au. Efficient generic construction of CCA-secure identity-based encryption from randomness extraction. *The Computer Journal*, 59(4):508–521, April 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/4/508.

Bhatnagar:2012:IVE

[BWR12a] Gaurav Bhatnagar, Q. M. Jonathan Wu, and Balasubramanian Raman. Image and video encryption based on dual space-filling curves. *The Computer Journal*, 55(6): 667–685, June 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/55/6/667.full.pdf+html.

Bhatnagar:2012:NRA

[BWR12b] Gaurav Bhatnagar, Q. M. Jonathan Wu, and Balasubramanian Raman. A new robust adjustable logo watermarking scheme. *Computers & Security*, 31(1):40–58, February 2012. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404811001398.

Buhren:2019:IUP

[BWS19] Robert Buhren, Christian Werling, and Jean-Pierre Seifert. Insecure until proven updated: Analyzing AMD SEV's remote attestation. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security — CCS '19*, pages 1–13. ACM Press, New York, NY 10036, USA, 2019. URL https://arxiv.org/abs/1908.11680.

Bai:2019:HAF

[BYDC19] Xu Bai, Jiajia Yang, Qiong Dai, and Zhaolin Chen. A hybrid ARM-FPGA cluster for cryptographic algorithm acceleration. *Concurrency and Computation: Practice and Experience*, 31(24):e5257:1–e5257:??, December 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Bao:2010:ISC

[BYL10] Feng Bao, Moti Yung, and Dongdai Lin, editors. *Information security and cryptology: 5th international conference, INSCRYPT 2009, Beijing, China, December 12–15, 2009. revised selected papers*, volume 6151 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-16341-6 (softcover). LCCN ????

Bo:2016:ETK

[BZD16a] Yang Bo, Mingwu Zhang, and Jun-Qiang Du. An error-tolerant keyword search scheme based on public-key encryption in secure cloud computing. *Concurrency and Computation: Practice and Experience*, 28 (4):1083–1093, March 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Bock:2016:NDA

[BZD+16b] Hanno Böck, Aaron Zauner, Sean Devlin, Juraj Somorovsky, and Philipp Jovanovic. Nonce-disrespecting adversaries: practical forgery attacks on GCM in TLS. In *10th Usenix Workshop on Offensive Technologies*, pages 1–11. USENIX, Berkeley, CA, USA, August 2016. URL `https://www.usenix.org/conference/woot16/workshop-program/presentation/bock`.

Staff:2014:KYS

[CAC14] CACM Staff. Know your steganographic enemy. *Communications of the Association for Computing Machinery*, 57(5): 8, May 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Caldwell:2013:INP

[Cal13] Tracey Caldwell. Identity — the new perimeter. *Network Security*, 2013(4):14–18, April 2013. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485813700515`.

Chakraborty:2019:TIP

[CAM19] Nilesh Chakraborty, Vijay S. Anand, and Samrat Mondal. Towards identifying and preventing behavioral side channel attack on recording attack resilient unaided authentication services. *Computers & Security*, 84(??):193–205, July 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404818302062`.

Carter:2010:TB

[Car10] Frank Carter. The Turing Bombe. *Rutherford Journal*, 3(??):??, ???? 2010. CODEN ???? ISSN 1177-1380. URL `http://rutherfordjournal.org/article030108.html`.

Carlson:2011:JRW

[Car11] Elliot Carlson. *Joe Rochefort's war: the odyssey of the codebreaker who outwitted Yamamoto at Midway*. Naval Institute

Press, Annapolis, MD, US, 2011. ISBN 1-61251-060-4 (hardcover). ???? pp. LCCN D774.M5 C28 2011.

Casselman:2010:VC

[Cas10] Bill Casselman. Visible cryptography. *Notices of the American Mathematical Society*, 57(3):378–379, March 2010. CODEN AMNOAN. ISSN 0002-9920 (print), 1088-9477 (electronic). URL `http://www.ams.org/notices/201003/`.

Cass:2015:SE

[Cas15] Stephen Cass. A simple Enigma. *IEEE Spectrum*, 52(1):19–20, January 2015. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Courtois:2019:RRR

[CATB19] J. Courtois, L. Abbas-Turki, and J. Bajard. Resilience of randomized RNS arithmetic with respect to side-channel leaks of cryptographic computation. *IEEE Transactions on Computers*, 68 (12):1720–1730, December 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Chang:2019:KCS

[CBJX19] Jinyong Chang, Genqing Bian, Yanyan Ji, and Maozhi Xu. On the KDM–CCA security from partial trapdoor one-way family in the random oracle model. *The Computer Journal*, 62(8):1232–1245, August 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/62/8/1232/5492772`.

Cho:2016:MAT

[CBJY16] Haehyun Cho, Jiwoong Bang, Myeongju Ji, and Jeong Hyun Yi. Mobile application tamper detection scheme using dynamic code injection against repackaging attacks. *The Journal of Supercomputing*, 72(9):3629–3645, September 2016. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://link.springer.com/article/10.1007/s11227-016-1763-2`.

Cheneau:2010:SIP

[CBL10] Tony Cheneau, Aymen Boudguiga, and Maryline Laurent. Significantly improved performances of the cryptographically generated addresses thanks to ECC and GPGPU. *Computers & Security*, 29(4):419–431, June 2010. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://`

www.sciencedirect.com/science/article/pii/S0167404809001461.

Cobb:2013:LMS

[CBL13] William E. Cobb, Rusty O. Baldwin, and Eric D. Laspe. Leakage mapping: a systematic methodology for assessing the side-channel information leakage of cryptographic implementations. *ACM Transactions on Information and System Security*, 16(1):2:1–2:??, June 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chang:2018:DMU

[CBO+18] Doohwang Chang, Ganapati Bhat, Umit Ogras, Bertan Bakkaloglu, and Sule Ozev. Detection mechanisms for unauthorized wireless transmissions. *ACM Transactions on Design Automation of Electronic Systems*, 23(6):70:1–70:??, December 2018. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Chattopadhyay:2019:QIL

[CBRZ19] Sudipta Chattopadhyay, Moritz Beck, Ahmed Rezine, and Andreas Zeller. Quantifying the information leakage in cache attacks via symbolic execution. *ACM Transactions on Embedded Computing Systems*, 18(1):7:1–7:??, February 2019. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3288758.

Cachin:2010:EKS

[CC10] Christian Cachin and Jan Camenisch. Encrypting keys securely. *IEEE Security & Privacy*, 8(4):66–69, July/August 2010. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Chang:2014:RRT

[CC14] Chin-Chen Chang and Ting-Fang Cheng. A reliable real-time multicast authentication protocol with provable accuracy. *Fundamenta Informaticae*, 131(2):167–186, April 2014. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Chen:2019:IAS

[CCC19] Yi-Cheng Chen, Yueh-Peng Chou, and Yung-Chen Chou. An image authentication scheme using Merkle tree mechanisms. *Future Internet*, 11(7):149, July 06, 2019. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/11/7/149.

Chadha:2016:AVE

[CCCK16] Rohit Chadha, Vincent Cheval, Stefan Ciobâca, and Steve Kremer. Automated verification of equivalence properties of cryptographic protocols. *ACM Transactions on Computational Logic*, 17(4):23:1–23:??, November 2016. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic).

Chretien:2015:SPP

[CCD15] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. From security protocols to pushdown automata. *ACM Transactions on Computational Logic*, 17(1):3:1–3:??, December 2015. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic).

Chretien:2019:TMF

[CCDD19] Rémy Chrétien, Véronique Cortier, Antoine Dallon, and Stéphanie Delaune. Typing messages for free in security protocols. *ACM Transactions on Computational Logic*, 21(1):1:1–1:??, October 2019. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3343507`.

Chretien:2020:TMF

[CCDD20] Rémy Chrétien, Véronique Cortier, Antoine Dallon, and Stéphanie Delaune. Typing messages for free in security protocols. *ACM Transactions on Computational Logic*, 21(1):1:1–1:52, January 2020. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3343507`.

Chen:2017:LAA

[CCF17] Min Chen, Shigang Chen, and Yuguang Fang. Lightweight anonymous authentication protocols for RFID systems. *IEEE/ACM Transactions on Networking*, 25(3):1475–1488, June 2017. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Carota:2012:FFI

[CCFM12] Serenella Carota, Flavio Corradini, Damiano Falcioni, and Maria Laura Maggiulli. FedCohesion: Federated identity management in the Marche region. *Lecture Notes in Computer Science*, 7452:112–124, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32701-8_11/`.

Chou:2010:PSO

[CCG10] Cheng-Fu Chou, William C. Cheng, and Leana Golubchik. Performance study of online batch-based digital signature schemes. *Journal of Network and Computer Applications*, 33(2):98–114, March 2010. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804509001374.

Checkoway:2016:SAJ

[CCG+16] Stephen Checkoway, Shaanan Cohney, Christina Garman, Matthew Green, Nadia Heninger, Jacob Maskiewicz, Eric Rescorla, Hovav Shacham, and Ralf-Philipp Weinmann. A systematic analysis of the Juniper Dual EC incident. Cryptology ePrint Archive, Report 2016/376., April 14, 2016. URL https://eprint.iacr.org/2016/376.

Chadha:2012:AVE

[CCK12] Rohit Chadha, Ştefan Ciobâcă, and Steve Kremer. Automated verification of equivalence properties of cryptographic protocols. *Lecture Notes in Computer Science*, 7211: 108–127, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28869-2_6/.

Chatterjee:2016:TAD

[CCKM16] Urbi Chatterjee, Rajat Subhra Chakraborty, Hitesh Kapoor, and Debdeep Mukhopadhyay. Theory and application of delay constraints in arbiter PUF. *ACM Transactions on Embedded Computing Systems*, 15(1):10:1–10:??, February 2016. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Chou:2013:UGS

[CCL+13] Yao-Hsin Chou, Shuo-Mao Chen, Yu-Ting Lin, Chi-Yuan Chen, and Han-Chieh Chao. Using GHZ-state for multiparty quantum secret sharing without code table. *The Computer Journal*, 56(10):1167–1175, October 2013. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/56/10/1167.full.pdf+html.

Cao:2019:AML

[CCL+19] Nanyuan Cao, Zhenfu Cao, Zhen Liu, Xiaolei Dong, and Xiaopeng Zhao. All-but-many lossy trapdoor functions under decisional RSA subgroup assumption and application. *The Computer Journal*, 62(8):1148–1157, August 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/8/1148/5369686.

Chang:2011:SFW

[CCLL11] Chin-Chen Chang, Kuo-Nan Chen, Chin-Feng Lee, and Li-Jen Liu. A secure fragile watermarking scheme based on chaos-and-Hamming code. *The Journal of Systems and Software*, 84(9):1462–1470, September 2011. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211000549.

Cascudo:2015:SSN

[CCM+15] Ignacio Cascudo, Ronald Cramer, Diego Mirandola, Carles Padró, and Chaoping Xing. On secret sharing with nonlinear product reconstruction. *SIAM Journal on Discrete Mathematics*, 29(2):1114–1131, ???? 2015. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Chatterjee:2017:PBS

[CCM17] Urbi Chatterjee, Rajat Subhra Chakraborty, and Debdeep Mukhopadhyay. A PUF-based secure communication protocol for IoT. *ACM Transactions on Embedded Computing Systems*, 16(3):67:1–67:??, July 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Chikouche:2019:PPC

[CCMB19] Noureddine Chikouche, Pierre-Louis Cayrel, El Hadji Modou Mboup, and Brice Odilon Boidje. A privacy-preserving code-based authentication protocol for Internet of Things. *The Journal of Supercomputing*, 75(12):8231–8261, December 2019. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Cho:2014:DGA

[CCS14] Michael Cheng Yi Cho, Pokai Chen, and Shiuhpyng Winston Shieh. Dmail: A globally authenticated email service. *Computer*, 47(5):88–91, May 2014. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Chen:2011:EAA

[CCSW11] Tien-Ho Chen, Yen-Chiu Chen, Wei-Kuan Shih, and Hsin-Wen Wei. An efficient anonymous authentication protocol for mobile pay-TV. *Journal of Net-*

work and Computer Applications, 34(4):1131–1137, July 2011. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804510002031.

Chu:2014:KAC

[CCT+14] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng. Key-aggregate cryptosystem for scalable data sharing in cloud storage. *IEEE Transactions on Parallel and Distributed Systems*, 25(2):468–477, February 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Chen:2010:ALD

[CCW+10] Songqing Chen, Shiping Chen, Xinyuan Wang, Zhao Zhang, and Sushil Jajodia. An application-level data transparent authentication scheme without communication overhead. *IEEE Transactions on Computers*, 59(7):943–954, July 2010. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5453339.

Chen:2013:WSB

[CCZC13] Guoming Chen, Qiang Chen, Dong Zhang, and Yiqun Chen. A watermarking scheme based on compressive sensing and Bregman iteration. *International Journal of Computer Applications*, 35(4):173–180, 2013. ISSN 1206-212X (print), 1925-7074 (electronic). URL https://www.tandfonline.com/doi/full/10.2316/Journal.202.2013.4.202-3844.

Chiasson:2012:MWB

[CD12] Sonia Chiasson and Chris Deschamps. The MVP Web-based authentication framework. *Lecture Notes in Computer Science*, 7397:16–24, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32946-3_2/.

Canard:2016:HPP

[CD16a] S. Canard and J. Devigne. Highly privacy-protecting data sharing in a tree structure. *Future Generation Computer Systems*, 62(??):119–127, September 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16300036.

Cui:2016:RDA

[CD16b] Hui Cui and Robert H.

Deng. Revocable and decentralized attribute-based encryption. *The Computer Journal*, 59(8):1220–1235, August 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/59/8/1220`.

Criswell:2014:VGP

[CDA14] John Criswell, Nathan Dautenhahn, and Vikram Adve. Virtual Ghost: protecting applications from hostile operating systems. *ACM SIGARCH Computer Architecture News*, 42(1):81–96, March 2014. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Cheng:2013:DVB

[CDD13] Yueqiang Cheng, Xuhua Ding, and Robert H. Deng. DriverGuard: Virtualization-based fine-grained protection on I/O flows. *ACM Transactions on Information and System Security*, 16(2):6:1–6:??, September 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ciriani:2010:CFE

[CDF+10] Valentina Ciriani, Sabrina De Capitani Di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. Combining fragmentation and encryption to protect privacy in data storage. *ACM Transactions on Information and System Security*, 13(3):22:1–22:??, July 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Ciriani:2010:TPA

[CDFS10] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, and Pierangela Samarati. *Theory of Privacy and Anonymity*, chapter 18, pages 1–35. Volume 2 of Atallah and Blanton [AB10b], second edition, 2010. ISBN 1-58488-820-2. LCCN QA76.9.A43 A433 2010. URL `http://www.crcnetbase.com/doi/abs/10.1201/9781584888215-c18`.

Choo:2016:CCT

[CDFZ16] Kim-Kwang Raymond Choo, Josep Domingo-Ferrer, and Lei Zhang. Cloud cryptography: Theory, practice and future research directions. *Future Generation Computer Systems*, 62(??):51–53, September 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X16300942`.

Cao:2012:ITM

[CDGC12] Zhen Cao, Hui Deng, Zhi Guan, and Zhong Chen. Information-theoretic modeling of false data filtering schemes in wireless sensor networks. *ACM Transactions on Sensor Networks*, 8(2):14:1–14:??, March 2012. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Chari:2010:DSC

[CDK+10] Suresh Chari, Vincenzo V. Diluoffo, Paul A. Karger, Elaine R. Palmer, Tal Rabin, Josyula R. Rao, Pankaj Rohatgi, Helmut Scherzer, Michael Steiner, and David C. Toll. Designing a side channel resistant random number generator. In Gollmann et al. [GLIC10], pages 49–64. ISBN 3-642-12509-3 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.S62 C36 2010. URL `http://www.informatik.uni-trier.de/~ley/db/conf/cardis/cardis2010.html#ChariDKPRRRSST10`.

Cui:2018:ABC

[CDL18] Hui Cui, Robert H. Deng, and Yingjiu Li. Attribute-based cloud storage with secure provenance over encrypted data. *Future Generation Computer Systems*, 79 (part 2)(??):461–472, 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X17322835`.

Cui:2019:ABS

[CDLW19] H. Cui, R. H. Deng, Y. Li, and G. Wu. Attribute-based storage supporting secure deduplication of encrypted data in cloud. *IEEE Transactions on Big Data*, 5(3):330–342, September 2019. ISSN 2332-7790.

Coras:2016:AML

[CDPLCA16] Florin Coras, Jordi Domingo-Pascual, Darrel Lewis, and Albert Cabellos-Aparicio. An analytical model for Loc/ID mappings caches. *IEEE/ACM Transactions on Networking*, 24(1):506–516, February 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Costello:2014:CAS

[CDSLY14] Craig Costello, Alyson Deines-Schartz, Kristin Lauter, and Tonghai Yang. Constructing abelian surfaces for cryptography via Rosenhain invariants. *LMS Journal of Computation and Mathematics*, 17(A): 157–180, 2014. CODEN ???? ISSN 1461-1570.

Cremers:2019:SAG

[CDWM19] Cas Cremers, Martin Dehnel-Wild, and Kevin Milner. Secure authentication in the grid: a formal analysis of DNP3 SAv5. *Journal of Computer Security*, 27(2):203–232, ???? 2019. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Culnane:2019:KKR

[CEL+19] C. Culnane, A. Essex, S. J. Lewis, O. Pereira, and V. Teague. Knights and knaves run elections: Internet voting and undetectable electoral fraud. *IEEE Security & Privacy*, 17(4):62–70, July/August 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Ceruzzi:2014:HFT

[Cer14] P. E. Ceruzzi. Are historians failing to tell the real story about the history of computing? *IEEE Annals of the History of Computing*, 36(3):94–95, July 2014. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic).

Cerf:2015:CTN

[Cer15] Vinton G. Cerf. Cerf's up: There is nothing new under the sun. *Communications of the Association for Computing Machinery*, 58(2):7, February 2015. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2015/2/182649/fulltext`.

Cerf:2018:CSA

[Cer18] Vinton G. Cerf. Cerf's up: Self-authenticating identifiers. *Communications of the Association for Computing Machinery*, 61(12): 5, December 2018. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `https://cacm.acm.org/magazines/2018/12/232883/fulltext`.

Chang-Fong:2016:CSC

[CFE16] N. Chang-Fong and A. Essex. The cloudier side of cryptographic end-to-end verifiable voting: A security analysis of Helios. In ACM, editor, *Proceedings of the 32nd Annual Conference on Computer Security Applications (ACSAC 16: 5–9 December 2016, Hilton Los Angeles Universal City, Los Angeles, CA, USA)*. ACM Press, New York, NY 10036, USA, 2016. ISBN 1-4503-4771-1.

Crampton:2017:CEI

[CFG+17] Jason Crampton, Naomi Farley, Gregory Gutin, Mark Jones, and Bertram Poettering. Cryptographic enforcement of information flow policies without public information via tree partitions. *Journal of Computer Security*, 25(6):511–535, ???? 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Carter:2013:SSA

[CFH+13] Kyle Carter, Adam Foltzer, Joe Hendrix, Brian Huffman, and Aaron Tomb. SAW: the software analysis workbench. *ACM SIGADA Ada Letters*, 33(3):15–18, December 2013. CODEN AALEE5. ISSN 1094-3641 (print), 1557-9476 (electronic).

Centenaro:2013:TBA

[CFL13] Matteo Centenaro, Riccardo Focardi, and Flaminia L. Luccio. Type-based analysis of key management in PKCS#11 cryptographic devices. *Journal of Computer Security*, 21(6):971–1007, ???? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Checkoway:2014:PED

[CFN+14] Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, and Hovav Schacham. On the practical exploitability of Dual EC in TLS implementations. In ????, editor, *USENIX Security Symposium*, page ?? USENIX, Berkeley, CA, USA, 2014. ISBN ???? LCCN ???? URL `????`.

Cevallos:2012:USR

[CFOR12] Alfonso Cevallos, Serge Fehr, Rafail Ostrovsky, and Yuval Rabani. Unconditionally-secure robust secret sharing with compact shares. *Lecture Notes in Computer Science*, 7237:195–208, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_12; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_13/`.

Carstensen:2011:AAA

[CFR11] Celine Carstensen, Benjamin Fine, and Gerhard Rosenberger. *Abstract algebra: applications to Galois theory, algebraic geometry, and cryptography*, volume 11 of *Sigma series in pure mathematics*. Walter de Gruyter, New York, NY, USA, 2011. ISBN 3-11-025008-X. ???? pp. LCCN QA162 .C375 2011.

Calzavara:2017:SWJ

[CFST17] Stefano Calzavara, Riccardo Focardi, Marco

Squarcina, and Mauro Tempesta. Surviving the Web: a journey into Web session security. *ACM Computing Surveys*, 50 (1):13:1–13:??, April 2017. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Celesti:2016:ALT

[CFVP16] Antonio Celesti, Maria Fazio, Massimo Villari, and Antonio Puliafito. Adding long-term availability, obfuscation, and encryption to multi-cloud storage systems. *Journal of Network and Computer Applications*, 59(??):208–218, January 2016. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804514002288`.

Choo:2017:EDF

[CFXY17] Kim-Kwang Raymond Choo, Yunsi Fei, Yang Xiang, and Yu Yu. Embedded device forensics and security. *ACM Transactions on Embedded Computing Systems*, 16(2):50:1–50:??, April 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Chang:2010:PRN

[CFY+10] Weiling Chang, Binxing Fang, Xiaochun Yun, Shupeng Wang, and Xiangzhan Yu. A pseudo-random number generator based on LZSS. In *2010 Data Compression Conference (DCC)*, page 524. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5453503`.

Chen:2010:IFA

[CFZ+10] Lanxiang Chen, Dan Feng, Yu Zhang, Lingfang Zeng, and Zhongying Niu. Integrating FPGA/ASIC into cryptographic storage systems to avoid re-encryption. *International Journal of Parallel, Emergent and Distributed Systems: IJPEDS*, 25(2):105–122, 2010. CODEN ???? ISSN 1744-5760 (print), 1744-5779 (electronic).

Camenisch:2012:EAA

[CG12a] Jan Camenisch and Thomas Groß. Efficient attributes for anonymous credentials. *ACM Transactions on Information and System Security*, 15(1):4:1–4:??, March 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Che:2012:WAM

[CG12b] Xiangjiu Che and Zhanheng Gao. Watermarking algorithm for 3D mesh based on multi-scale radial basis functions. *International Journal of Parallel, Emergent and Distributed Systems: IJPEDS*, 27(2): 133–141, 2012. CODEN ???? ISSN 1744-5760 (print), 1744-5779 (electronic).

Cheraghchi:2014:NMC

[CG14a] Mahdi Cheraghchi and Venkatesan Guruswami. Non-malleable coding against bit-wise and split-state tampering. *Lecture Notes in Computer Science*, 8349: 440–464, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_19/.

Corrigan-Gibbs:2014:KS

[CG14b] Henry Corrigan-Gibbs. Keeping secrets. *Stanford Magazine*, ??(??):??, November/December 2014. URL https://alumni.stanford.edu/get/page/magazine/article/?article_id=74801.

Chaudhuri:2010:PIC

[CGB+10] Pranay Chaudhuri, Sukumar Ghosh, Raj Kumar Buyya, Jian-Nong Cao, and Oeepak Oahiya, editors. *Proceedings of the 2010 1st International Conference on Parallel Distributed and Grid Computing (PDGC), Jaypee University of Information Technology Waknaghat, Solan, HP, India, 28–30 October, 2010*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 1-4244-7675-5. LCCN ????

Caballero-Gil:2012:LAR

[CGCGPDMG12] C. Caballero-Gil, P. Caballero-Gil, A. Peinado-Domínguez, and J. Molina-Gil. Lightweight authentication for RFID used in VANETs. *Lecture Notes in Computer Science*, 6928:493–500, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-27579-1_64.

Chmiel:2012:EPC

[CGCS12] Krzysztof Chmiel, Anna Grocholewska-Czurylo, and Janusz Stoklosa. Evaluation of PP-1 cipher resistance against differential and linear cryptanalysis in comparison to a DES-like cipher. *Fundamenta Informaticae*, 114(3–4):239–269, August 2012. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Coull:2011:ACO

[CGH11] Scott E. Coull, Matthew Green, and Susan Hohenberger. Access controls for oblivious and anonymous systems. *ACM Transactions on Information and System Security*, 14(1): 10:1–10:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cohney:2017:PSR

[CGH17] Shaanan Cohney, Matthew D. Green, and Nadia Heninger. Practical state recovery attacks against legacy RNG implementations. Report, University of Pennsylvania and The Johns Hopkins University, College Park, PA and Baltimore, MD, October 23, 2017. 15 pp. URL `https://duhkattack.com/paper.pdf`.

Curtmola:2011:SSE

[CGKO11] Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions and efficient constructions. *Journal of Computer Security*, 19(5):895–934, ???? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cheng:2012:PAI

[CGL+12] Pengqi Cheng, Yan Gu, Zihong Lv, Jianfei Wang, Wenlei Zhu, Zhen Chen, and Jiwei Huang. A performance analysis of identity-based encryption schemes. *Lecture Notes in Computer Science*, 7222: 289–303, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32298-3_19/`.

Chandran:2014:PBC

[CGMO14] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position-based cryptography. *SIAM Journal on Computing*, 43 (4):1291–1341, ???? 2014. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Cheng:2013:NIB

[CGY+13] Xiangguo Cheng, Lifeng Guo, Jia Yu, Huiran Ma, and Yuexiu Wu. A new identity-based group signature scheme. *International Journal of Computer Applications*, 35(1): 1–5, 2013. CODEN IJCAFW. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.2316/Journal.202.2013.1.202-3136`.

Chen:2010:NUP

[CH10] Tzung-Her Chen and Jyun-Ci Huang. A novel user-participating authentication scheme. *The Journal of Systems and Software*, 83(5):861–867, May 2010. CODEN JSSODM. ISSN 0164-1212.

Chang:2011:DEQ

[CH11] Tao-Ku Chang and Gwan-Hwan Hwang. Developing an efficient query system for encrypted XML documents. *The Journal of Systems and Software*, 84(8): 1292–1305, August 2011. CODEN JSSODM. ISSN 0164-1212.

Chan:2013:OCK

[Cha13a] Aldar C.-F. Chan. On optimal cryptographic key derivation. *Theoretical Computer Science*, 489–490(??):21–36, June 10, 2013. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397513002843.

Chang:2013:MPQ

[Cha13b] Mei-Chu Chang. On a matrix product question in cryptography. *Linear Algebra and its Applications*, 439(7):1742–1748, October 1, 2013. CODEN LAAPAW. ISSN 0024-3795 (print), 1873-1856 (electronic). URL http://www.sciencedirect.com/science/article/pii/S002437951300339X.

Chappell:2013:PMI

[Cha13c] Brian Chappell. Privilege management — the industry's best kept secret. *Network Security*, 2013(10): 12–14, October 2013. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485813701144.

Chen:2011:CCI

[Che11] Liqun Chen, editor. *Cryptography and Coding: 13th IMA International Conference, IMACC 2011, Oxford, UK, December 12–15. Proceedings*, volume 7089 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011. CODEN LNCSD9. ISBN 3-642-25515-9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/978-3-642-25515-1.

Cheswick:2013:RP

[Che13] William Cheswick. Rethinking passwords. *Communications of the Association for Computing Machinery*, 56(2):40–44, February 2013. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Chen:2015:SSS

[Che15] Yu-Chi Chen. SPEKS: Secure server-designation public key encryption with keyword search against keyword guessing attacks. *The Computer Journal*, 58 (4):922–933, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/922.

Chen:2017:CSQ

[Che17] Lidong Chen. Cryptography standards in quantum time: New wine in an old wineskin? *IEEE Security & Privacy*, 15(4): 51–57, July/August 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2017/04/msp2017040051-abs.html.

Chen:2018:ESA

[Che18] Yung-Chih Chen. Enhancements to SAT attack: Speedup and breaking cyclic logic encryption. *ACM Transactions on Design Automation of Electronic Systems*, 23(4):52:1–52:??, July 2018. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Courtois:2013:BRC

[CHH+13] N. T. Courtois, D. Hulme, K. Hussain, J. A. Gawinecki, and M. Grajek. On bad randomness and cloning of contactless payment and building smart cards. In *Proceedings of the IEEE Security and Privacy Workshops*, pages 105–110. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2013.

Cui:2019:CPA

[CHH+19] Yuzhao Cui, Qiong Huang, Jianye Huang, Hongbo Li, and Guomin Yang. Ciphertext-policy attribute-based encrypted data equality test and classification. *The Computer Journal*, 62(8):1166–1177, August 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/8/1166/5480373.

Chen:2012:SRF

[CHHW12] Fan Chen, Hongjie He, Yaoran Huo, and Hongxia Wang. Self-recovery fragile watermarking scheme with variable watermark payload. *Lecture Notes in Computer Science*, 7128:

142–155, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32205-1_13/.

Chien:2012:IAM

[Chi12] Hung-Yu Chien. Improved anonymous multi-receiver identity-based encryption. *The Computer Journal*, 55(4):439–446, April 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/55/4/439.full.pdf+html. See comment on insecurity [Wan14].

Chien:2013:CRC

[Chi13a] Hung-Yu Chien. Combining Rabin cryptosystem and error correction codes to facilitate anonymous authentication with untraceability for low-end devices. *Computer Networks (Amsterdam, Netherlands: 1999)*, 57(14):2705–2717, October 4, 2013. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128613001898.

Chirgwin:2013:ABB

[Chi13b] R. Chirgwin. Android bug batters Bitcoin wallets. *The Register*, ??(??): ??, ???? 2013. URL ????.

Chien:2016:GAI

[Chi16] Hung-Yu Chien. A generic approach to improving Diffie–Hellman key agreement efficiency for thin clients. *The Computer Journal*, 59(4):592–601, April 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/4/592.

Conti:2019:BUB

[CHL19] Mauro Conti, Muhammad Hassan, and Chhagan Lal. BlockA*uth*: BlockChain based distributed producer authentication in ICN. *Computer Networks (Amsterdam, Netherlands: 1999)*, 164(??):Article 106888, December 9, 2019. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128619308308.

Chmielowiec:2010:FPR

[Chm10] Andrzej Chmielowiec. Fixed points of the RSA encryption algorithm. *Theoretical Computer Science*, 411(1): 288–292, January 1, 2010. CODEN TCSCDI. ISSN

0304-3975 (print), 1879-2294 (electronic).

Cohen:2018:WCC

[CHN+18] Aloni Cohen, Justin Holmgren, Ryo Nishimaki, Vinod Vaikuntanathan, and Daniel Wichs. Watermarking cryptographic capabilities. *SIAM Journal on Computing*, 47(6):2157–2202, ???? 2018. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Choudary:2010:SCD

[Cho10] Omar S. Choudary. The Smart Card detective: a hand-held EMV interceptor. M. Phil. dissertation in Advance Computer Science, Computer Laboratory, Darwin College, University of Cambridge, Cambridge, UK, June 2010. 57 pp. URL http://www.cl.cam.ac.uk/~osc22/docs/mphil_acs_osc22.pdf; http://www.cl.cam.ac.uk/~osc22/scd/; http://www.lightbluetouchpaper.org/2010/10/19/the-smart-card-detective-a-hand-held-emv-interceptor/.

Chou:2014:EMA

[Cho14] Jue-Sam Chou. An efficient mutual authentication RFID scheme based on elliptic curve cryptography. *The Journal of Supercomputing*, 70(1):75–94, October 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-013-1073-x.

Chen:2011:SEI

[CHS11] Tien-Ho Chen, Han-Cheng Hsiang, and Wei-Kuan Shih. Security enhancement on an improvement on two remote user authentication schemes using smart cards. *Future Generation Computer Systems*, 27(4):377–380, April 2011. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Cooke:2015:FSM

[CHS15] Patrick Cooke, Lu Hao, and Greg Stitt. Finite-state-machine overlay architectures for fast FPGA compilation and application portability. *ACM Transactions on Embedded Computing Systems*, 14(3):54:1–54:??, April 2015. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Chu:2016:BEE

[Chu16] Jennifer Chu. The beginning of the end for encryption schemes? *Scientific Computing*, ??(??):??, March 7, 2016. CODEN

SCHRCU. ISSN 1930-5753 (print), 1930-6156 (electronic). URL http://www.scientificcomputing.com/news/2016/03/beginning-end-encryption-schemes.

Chen:2013:ATK

[CHX13] Qian Chen, Haibo Hu, and Jianliang Xu. Authenticating top-k queries in location-based services with confidentiality. *Proceedings of the VLDB Endowment*, 7(1):49–60, September 2013. CODEN ???? ISSN 2150-8097.

Cilardo:2011:EPT

[Cil11] Alessandro Cilardo. Exploring the potential of threshold logic for cryptography-related operations. *IEEE Transactions on Computers*, 60(4):452–462, April 2011. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Cheng:2013:EHM

[CJ13] Chi Cheng and Tao Jiang. An efficient homomorphic MAC with small key size for authentication in network coding. *IEEE Transactions on Computers*, 62(10):2096–2100, October 2013. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). See comments [LCLL15, Kim15].

Cao:2014:SCI

[CJFH14] Yan-Pei Cao, Tao Ju, Zhao Fu, and Shi-Min Hu. Shapes and cryptography: Interactive image-guided modeling of extruded shapes. *Computer Graphics Forum*, 33(7):101–110, October 2014. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Cheon:2016:ANP

[CJL16] Jung Hee Cheon, Jinhyuck Jeong, and Changmin Lee. An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero. *LMS Journal of Computation and Mathematics*, 19(A):255–266, 2016. CODEN ???? ISSN 1461-1570. URL https://www.cambridge.org/core/product/230ECFEEE6AF4D8027FF3E13998D560C.

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.

Choi:2019:PTE

[CJW+19] Hoyul Choi, Jongmin Jeong, Simon S. Woo, Kyungtae Kang, and Junbeom Hur. Password typographical error resilience in honey encryption. *Computers & Security*, 87(??):Article 101411, November 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818311246.

Chang:2019:GTS

[CJXX19] Jinyong Chang, Yanyan Ji, Maozhi Xu, and Rui Xue. General transformations from single-generation to multi-generation for homomorphic message authentication schemes in network coding. *Future Generation Computer Systems*, 91(??):416–425, February 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17330170.

Cui:2013:OSL

[CJZ13] T. Cui, C. Jin, and G. Zhang. Observations of skipjack-like structure with SP/SPS round function. *J.UCS: Journal of Universal Computer Science*, 19(16):2453–??, ???? 2013. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL http://www.jucs.org/jucs_19_16/observations_of_skipjack_like.

Chandra:2011:AST

[CK11] Shalini Chandra and Raees Ahmad Khan. Availability state transition model. *ACM SIGSOFT Software Engineering Notes*, 36(3):1–3, May 2011. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

Chailloux:2017:PLQ

[CK17] André Chailloux and Iordanis Kerenidis. Physical limitations of quantum cryptographic primitives or optimal bounds for quantum coin flipping and bit commitment. *SIAM Journal on Computing*, 46(5): 1647–1677, ???? 2017. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Chung:2018:ERN

[CK18] Heewon Chung and Myungsun Kim. Encoding of rational numbers and their homomorphic computations for FHE-based applications. *International Journal of Foundations of Computer Science (IJFCS)*, 29(6):??, September 2018. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054118500193.

Chang:2019:PPN

[CKHP19] Sang-Yoon Chang, Sristi Lakshmi Sravana Kumar, Yih-Chun Hu, and Younghee Park. Power-positive networking: Wireless-charging-based networking to protect energy against battery DoS attacks. *ACM Transactions on Sensor Networks*, 15(3):27:1–27:??, August 2019. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3317686.

Chase:2013:SMN

[CKLM13] Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn. Succinct malleable NIZKs and an application to compact shuffles. *Lecture Notes in Computer Science*, 7785: 100–119, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_6/.

Chuang:2011:LMA

[CL11] Ming-Chin Chuang and Jeng-Farn Lee. A lightweight mutual authentication mechanism for network mobility in IEEE 802.16e wireless networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 55(16):3796–3809, November 10, 2011. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128611002052.

Colin:2016:CTC

[CL16] Alexei Colin and Brandon Lucia. Chain: tasks and channels for reliable intermittent programs. *ACM SIGPLAN Notices*, 51(10): 514–530, October 2016. CODEN SINODQ. ISSN 0362-1340 (print), 1523-

2867 (print), 1558-1160 (electronic).

Claxson:2018:SVE

[Cla18] Nick Claxson. Securing VoIP: encrypting today's digital telephony systems. *Network Security*, 2018(11):11–13, November 2018. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485818301120.

Calegari:2019:WPH

[CLB19] Patrice Calegari, Marc Levrier, and Paweł Balczyński. Web portals for high-performance computing: a survey. *ACM Transactions on the Web (TWEB)*, 13(1):5:1–5:??, February 2019. CODEN ???? ISSN 1559-1131 (print), 1559-114X (electronic).

Chen:2019:BBS

[CLC+19] Lanxiang Chen, Wai-Kong Lee, Chin-Chen Chang, Kim-Kwang Raymond Choo, and Nan Zhang. Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems*, 95(??):420–429, June 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18314134.

Comon-Lundh:2010:DSP

[CLCZ10] Hubert Comon-Lundh, Véronique Cortier, and Eugen Zălinescu. Deciding security properties for cryptographic protocols. application to key cycles. *ACM Transactions on Computational Logic*, 11(2):9:1–9:??, January 2010. CODEN ???? ISSN 1529-3785.

Chang:2011:RSB

[CLF11] Chin-Chen Chang, Chih-Yang Lin, and Yi-Hsuan Fan. Reversible steganography for BTC-compressed images. *Fundamenta Informaticae*, 109(2):121–134, April 2011. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Chen:2017:PGF

[CLF+17] Yajing Chen, Shengshuo Lu, Cheng Fu, David Blaauw, Ronald Dreslinski, Jr., Trevor Mudge, and Hun-Seok Kim. A programmable Galois field processor for the Internet of Things. *ACM SIGARCH Computer Architecture News*, 45(2):55–68, May 2017. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Chong:2013:ASG

[CLH13] Song-Kong Chong, Cheng-Chi Lee, and Min-Shiang Hwang. An authentication scheme for the global mobility network. *Parallel Processing Letters*, 23(3): 1350009, September 2013. CODEN PPLTEE. ISSN 0129-6264 (print), 1793-642X (electronic).

Chen:2016:RPR

[CLH+16] Zhenhua Chen, Shundong Li, Qiong Huang, Yilei Wang, and Sufang Zhou. A restricted proxy re-encryption with keyword search for fine-grained data access control in cloud storage. *Concurrency and Computation: Practice and Experience*, 28(10):2858–2876, July 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Chen:2012:NCB

[CLHC12] Yu Chen, Song Luo, Jianbin Hu, and Zhong Chen. A novel commutative blinding identity based encryption scheme. *Lecture Notes in Computer Science*, 6888:73–89, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-27901-0_7/`.

Chen:2013:TSE

[CLHJ13] Te-Yu Chen, Cheng-Chi Lee, Min-Shiang Hwang, and Jinn-Ke Jan. Towards secure and efficient user authentication scheme using smart card for multi-server environments. *The Journal of Supercomputing*, 66(2):1008–1032, November 2013. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://link.springer.com/article/10.1007/s11227-013-0966-z`.

Chande:2016:NSC

[CLL16] Manoj Kumar Chande, Cheng-Chi Lee, and Chun-Ta Li. A new self-certified convertible authenticated encryption scheme based on discrete logarithm problem. *Parallel Processing Letters*, 26(4):1650018, December 2016. CODEN PPLTEE. ISSN 0129-6264 (print), 1793-642X (electronic).

Cao:2012:SRH

[CLM+12] Jin Cao, Hui Li, Maode Ma, Yueyu Zhang, and Chengzhe Lai. A simple and robust handover authentication between HeNB and eNB in LTE networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 56(8):2119–2131, May 24, 2012. CODEN

???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S138912861200076X.

Chen:2019:IBS

[CLND19] Jiahui Chen, Jie Ling, Jianting Ning, and Jintai Ding. Identity-based signature schemes for multivariate public key cryptosystems. *The Computer Journal*, 62(8):1132–1147, August 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/8/1132/5369678.

Canetti:2013:PCC

[CLP13a] Ran Canetti, Huijia Lin, and Omer Paneth. Public-coin concurrent zero-knowledge in the global hash model. *Lecture Notes in Computer Science*, 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/.

Castro:2013:RAM

[CLP+13b] P. C. Castro, J. W. Ligman, M. Pistoia, J. Ponzo, G. S. Thomas, and U. Topkara. Runtime adaptive multi-factor authentication for mobile devices. *IBM Journal of Research and Development*, 57(6):8:1–8:17, November–December 2013. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Chang:2012:PRS

[CLSW12] Shih-Ying Chang, Yue-Hsun Lin, Hung-Min Sun, and Mu-En Wu. Practical RSA signature scheme based on periodical rekeying for wireless sensor networks. *ACM Transactions on Sensor Networks*, 8(2):13:1–13:??, March 2012. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Cui:2016:KAS

[CLW16] Baojiang Cui, Zheli Liu, and Lingyu Wang. Key-Aggregate Searchable Encryption (KASE) for group data sharing via cloud storage. *IEEE Transactions on Computers*, 65(8):2374–2385, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Chen:2014:CDP

[CLY14] Liqun Chen, Hoon Wei Lim, and Guomin Yang. Cross-domain password-based authenticated key exchange revisited. *ACM Transactions on Information and System Security*, 16(4):15:1–15:??, April 2014. CODEN

ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cao:2018:CUP

[CLY18] Kaidi Cao, Jing Liao, and Lu Yuan. CariGANs: unpaired photo-to-caricature translation. *ACM Transactions on Graphics*, 37 (6):244:1–244:??, November 2018. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Cheng:2017:ISK

[CLZ+17] Longwang Cheng, Wei Li, Li Zhou, Chunsheng Zhu, Jibo Wei, and Yantao Guo. Increasing secret key capacity of OFDM systems: a geometric program approach. *Concurrency and Computation: Practice and Experience*, 29(16), August 25, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Cremers:2011:OSV

[CM11] Cas Cremers and Sjouke Mauw. *Operational Semantics and Verification of Security Protocols*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011. ISBN 3-540-78635-X (print), 3-540-78636-8 (e-book), 3-642-43053-8. ISSN 1619-7100 (print), 2197-845X (electronic). xiii + 172 + 59 pp. LCCN QA76.9.A25 C74 2012; QA76.9.D35. URL `http://www.springerlink.com/content/978-3-540-78636-8`.

Cozzens:2013:MEE

[CM13] Margaret B. Cozzens and Steven J. Miller. *The mathematics of encryption: an elementary introduction*, volume 29 of *Mathematical world*. American Mathematical Society, Providence, RI, USA, 2013. ISBN 0-8218-8321-6 (paperback). xvii + 332 pp. LCCN QA268 .C697 2013.

Cui:2014:SSA

[CMA14] Hui Cui, Yi Mu, and Man Ho Au. Signcryption secure against linear related-key attacks. *The Computer Journal*, 57(10):1472–1483, October 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/57/10/1472`.

Checkoway:2018:WDL

[CMG+18] Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, and Hovav Shacham. Where did I leave my keys?: lessons from the Juniper Dual EC incident. *Communications of the Association for Computing Machinery*, 61(11):148–155, November 2018. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL https://cacm.acm.org/magazines/2018/11/232227/fulltext.

Coles:2016:NAU

[CML16] Patrick J. Coles, Eric M. Metodiev, and Norbert Lütkenhaus. Numerical approach for unstructured quantum key distribution. *Nature Communications*, 7:11712, May 2016. CODEN NCAOBW. ISSN 2041-1723 (electronic). URL http://www.nature.com/ncomms/2016/160520/ncomms11712/full/ncomms11712.html; http://www.scientificcomputing.com/news/2016/05/computing-secret-unbreakable-key.

Cao:2018:EEG

[CML+18] Jin Cao, Maode Ma, Hui Li, Yulong Fu, and Xuefeng Liu. EGHR: Efficient group-based handover authentication protocols for mMTC in 5G wireless networks. *Journal of Network and Computer Applications*, 102(??):1–16, January 15, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804517303776.

Chakraborty:2013:EHI

[CMLRHS13] Debrup Chakraborty, Cuauhtemoc Mancillas-Lopez, Francisco Rodriguez-Henriquez, and Palash Sarkar. Efficient hardware implementations of BRW polynomials and tweakable enciphering schemes. *IEEE Transactions on Computers*, 62(2):279–294, February 2013. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Chakraborty:2015:SSC

[CMLS15] D. Chakraborty, C. Mancillas-Lopez, and P. Sarkar. STES: A stream cipher based low cost scheme for securing stored data. *IEEE Transactions on Computers*, 64(9):2691–2707, ???? 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Chen:2017:VME

[CMMS17] Jiageng Chen, Rashed Mazumder, Atsuko Miyaji, and Chunhua Su. Variable message encryption through blockcipher compression function. *Concur-*

rency and Computation: Practice and Experience, 29(7):??, April 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Cao:2016:OMA

[CMO+16] Xiaolin Cao, Ciara Moore, Máire O'Neill, Elizabeth O'Sullivan, and Neil Hanley. Optimised multiplication architectures for accelerating fully homomorphic encryption. *IEEE Transactions on Computers*, 65 (9):2794–2806, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Chatterjee:2017:IPB

[CMRH17] Sanjit Chatterjee, Alfred Menezes, and Francisco Rodríguez-Henríquez. On instantiating pairing-based protocols with elliptic curves of embedding degree one. *IEEE Transactions on Computers*, 66(6): 1061–1070, June 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/document/7762073/`.

Chen:2012:FAA

[CN12] Yuanmi Chen and Phong Q. Nguyen. Faster algorithms for approximate common divisors: Breaking fully-homomorphic-encryption challenges over the integers. *Lecture Notes in Computer Science*, 7237: 502–519, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_29`; `http://link.springer.com/chapter/10.1007/978-3-642-29011-4_30/`.

Chaudhry:2018:IRB

[CNF+18] Shehzad Ashraf Chaudhry, Husnain Naqvi, Mohammad Sabzinejad Farash, Taeshik Shon, and Muhammad Sher. An improved and robust biometrics-based three factor authentication scheme for multi-server environments. *The Journal of Supercomputing*, 74(8):3504–3520, August 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

CNRS:2014:NAS

[CNR14] CNRS. New algorithm shakes up cryptography. *Scientific Computing*, May 15, 2014. URL `http://www.scientificcomputing.com/news/2014/05/new-algorithm-shakes-cryptography`. See [BGJT14].

Coron:2012:PKC

[CNT12] Jean-Sébastien Coron, David

Naccache, and Mehdi Tibouchi. Public key compression and modulus switching for fully homomorphic encryption over the integers. *Lecture Notes in Computer Science*, 7237:446–464, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_26; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_27/.

Chin:2011:ACS

[CO11] Shiu-Kai Chin and Susan Beth Older. *Access control, security, and trust: a logical approach*. Chapman and Hall/CRC cryptography and network security. Chapman and Hall/CRC, Boca Raton, FL, USA, 2011. ISBN 1-58488-862-8. ???? pp. LCCN QA76.9.A25 C446 2011.

Collie:2017:CBI

[Col17] Craig Collie. *Code Breakers: Inside the Shadow World of Signals Intelligence in Australia's Two Bletchley Parks*. Allen and Unwin, Sydney, NSW, Australia, 2017. ISBN 1-74269-977-4 (e-book), 1-74331-210-5 (paperback). ix + 389 + 16 pp. LCCN D810.C88.

Conitzer:2010:AP

[Con10] Vincent Conitzer. *Auction Protocols*, chapter 16, pages 1–19. Volume 2 of Atallah and Blanton [AB10b], second edition, 2010. ISBN 1-58488-820-2. LCCN QA76.9.A43 A433 2010. URL http://www.crcnetbase.com/doi/abs/10.1201/9781584888215-c16.

Constantin:2012:RSN

[Con12] Lucian Constantin. Researchers set new cryptanalysis world record for pairing-based cryptography. *Network World*, June 19, 2012. ISSN 0887-7661 (print), 1944-7655 (electronic). URL http://www.networkworld.com/news/2012/061912-researchers-set-new-cryptanalysis-world-260338.html.

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.

Connolly:2018:FE

[Con18] Aisling Connolly. Freedom of encryption. *IEEE Security & Privacy*, 16(1):102–103, January/February 2018. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `https://www.computer.org/csdl/mags/sp/2018/01/msp2018010102.html`.

Copeland:2006:CSB

[Cop06] B. Jack Copeland, editor. *Colossus: the secrets of Bletchley Park's codebreaking computers*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 2006. ISBN 0-19-284055-X (hardcover), 0-19-957814-1 (paperback). xvi + 462 + 16 pp. LCCN D810.C88 C66 2006. URL `http://www.colossus-computer.com/`.

Copeland:2010:CBG

[Cop10a] B. Jack Copeland. Colossus: Breaking the German 'Tunny' code at Bletchley Park. An illustrated history. *Rutherford Journal*, 3(??):??, ???? 2010. CODEN ???? ISSN 1177-1380. URL `http://rutherfordjournal.org/article030109.html`.

Copeland:2010:CSB

[Cop10b] B. Jack Copeland, editor. *Colossus: the secrets of Bletchley Park's codebreaking computers*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 2010. ISBN 0-19-284055-X (hardcover), 0-19-957814-1 (paperback). xvi + 462 + 16 pp. LCCN D810.C88 C66 2010. URL `http://www.colossus-computer.com/`.

Chung:2014:RRS

[COP+14] Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Muthuramakrishnan Venkitasubramaniam, and Ivan Visconti. 4-round resettably-sound zero knowledge. *Lecture Notes in Computer Science*, 8349:192–216, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_9/`.

Cordova:2014:EBS

[Cor14a] Tim Cordova. Encrypted backup solution: Home Paranoia Edition. *Linux Journal*, 2014(237):3:1–3:??, January 2014. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Corthesy:2014:SSD

[Cor14b] Sébastien Corthésy. Smartphones set out to decipher cryptographic system. *Scientific Computing*, August 25, 2014. URL http://www.scientificcomputing.com/news/2014/08/smartphones-set-out-decipher-cryptographic-system. The article describes use of thousands of mobile phones to attempt a parallel brute-force attack on elliptic-curve and RSA algorithms, in a research project by Ramasany Gowthami and Arjen Lenstra at the LACAL laboratory at EPFL, Lausanne, Switzerland.

Courtland:2012:VCG

[Cou12a] Rachel Courtland. Virtual currency gets real. *IEEE Spectrum*, 49(6):52–53, June 2012. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Coutinho:2012:RPT

[Cou12b] S. C. Coutinho. Review of *Primality Testing and Integer Factorization in Public Key Cryptography* by Song Y. Yan. *ACM SIGACT News*, 43(2):33–35, June 2012. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Claessen:2013:SPN

[CP13] Koen Claessen and Michał H. Pałka. Splittable pseudorandom number generators using cryptographic hashing. *ACM SIGPLAN Notices*, 48(12):47–58, December 2013. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). Haskell '14 conference proceedings.

Canard:2018:NTC

[CPPT18] S. Canard, D. H. Phan, D. Pointcheval, and V. C. Trinh. A new technique for compacting ciphertext in multi-channel broadcast encryption and attribute-based encryption. *Theoretical Computer Science*, 723(??):51–72, May 2, 2018. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397518301427.

Chung:2016:NBB

[CPS16] Kai-Min Chung, Rafael Pass, and Karn Seth. Non-black-box simulation from one-way functions and applications to resettable security. *SIAM Journal on Computing*, 45(2):415–458, ???? 2016. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Chen:2018:RLF

[CQX18] Yu Chen, Baodong Qin, and Haiyang Xue. Regular lossy functions and their applications in leakage-resilient cryptography. *Theoretical Computer Science*, 739(??):13–38, August 29, 2018. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397518302937`.

Chevalier:2010:CSC

[CR10] Yannick Chevalier and Michaël Rusinowitch. Compiling and securing cryptographic protocols. *Information Processing Letters*, 110(3):116–122, January 1, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chen:2012:DCC

[CR12] Jian Chen and Jeffrey S. Rosenthal. Decrypting classical cipher text using Markov chain Monte Carlo. *Statistics and Computing*, 22(2):397–413, March 2012. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1007/s11222-011-9232-5`.

Crampton:2011:PEC

[Cra11] Jason Crampton. Practical and efficient cryptographic enforcement of interval-based access control policies. *ACM Transactions on Information and System Security*, 14(1):14:1–14:??, May 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Cramer:2012:TCT

[Cra12] Ronald Cramer, editor. *Theory of Cryptography: 9th Theory of Cryptography Conference, TCC 2012, Taormina, Sicily, Italy, March 19–21. Proceedings*, volume 7194 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. CODEN LNCSD9. ISBN 3-642-28913-4. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/978-3-642-28913-2`.

Craver:2014:UCC

[Cra14] Scott Craver. The underhanded C contest. Web site, 2014. URL `http://underhanded.xcott.com/`.

Clear:2012:CPA

[CRE+12] Michael Clear, Karl Reid, Desmond Ennis, Arthur Hughes, and Hitesh Tewari. Collaboration-preserving authenticated encryption for operational transformation systems. *Lecture Notes in Computer Science*, 7483:204–223, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33383-5_13/.

Crichlow:2016:RSE

[Cri16] Ramon Crichlow. Rock-solid encrypted video streaming using SSH tunnels and the BeagleBone Black. *Linux Journal*, 2016(264):1:1–1:??, April 2016. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://dl.acm.org/ft_gateway.cfm?id=2933362.

Crawford:2013:FCT

[CRS13] Heather Crawford, Karen Renaud, and Tim Storer. A framework for continuous, transparent mobile device authentication. *Computers & Security*, 39 (part B)(??):127–136, November 2013. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404813000886.

Chauhan:2018:PCD

[CRS+18] Jagmohan Chauhan, Jathushan Rajasegaran, Suranga Seneviratne, Archan Misra, Aruna Seneviratne, and Youngki Lee. Performance characterization of deep learning models for breathing-based authentication on resource-constrained devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2(4):1–24, December 2018. CODEN ???? ISSN 2474-9567 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3287036.

Culnane:2015:VVV

[CRST15] Chris Culnane, Peter Y. A. Ryan, Steve Schneider, and Vanessa Teague. vVote: a verifiable voting system. *ACM Transactions on Information and System Security*, 18(1):3:1–3:??, June 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Caranay:2010:ESP

[CS10] Perlas C. Caranay and Renate Scheidler. An efficient seventh power residue symbol algorithm. *International Journal of Number Theory (IJNT)*, 6 (8):1831–1853, December 2010. ISSN 1793-0421 (print), 1793-7310 (electronic). URL https://www.worldscientific.com/doi/10.1142/S1793042110003770.

Chhabra:2011:NSN

[CS11] Siddhartha Chhabra and

Yan Solihin. i-NVMM: a secure non-volatile main memory system with incremental encryption. *ACM SIGARCH Computer Architecture News*, 39(3): 177–188, June 2011. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Clark:2012:RLA

[CS12] Liat Clark and Ian Steadman. The rich legacy of Alan Turing. Wired UK Web site., June 18, 2012. URL `http://www.wired.com/wiredscience/2012/06/alan-turing-legacy/`.

Chapin:2014:SRP

[CS14] Peter Chapin and Christian Skalka. SpartanRPC: Remote procedure call authorization in wireless sensor networks. *ACM Transactions on Information and System Security*, 17(2):5:1–5:??, November 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Chattaraj:2018:NTS

[CSD18] Durbadal Chattaraj, Monalisa Sarma, and Ashok Kumar Das. A new two-server authentication and key agreement protocol for accessing secure cloud services. *Computer Networks (Amsterdam, Netherlands: 1999)*, 131(??):144–164, February 11, 2018. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S1389128617304255`.

Chauhan:2018:BBA

[CSH+18] Jagmohan Chauhan, Suranga Seneviratne, Yining Hu, Archan Misra, Aruna Seneviratne, and Youngki Lee. Breathing-based authentication on resource-constrained IoT devices using recurrent neural networks. *Computer*, 51(5): 60–67, May 2018. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `https://www.computer.org/csdl/mags/co/2018/05/mco2018050060-abs.html`.

Chadwick:2014:AFI

[CSL+14] David W. Chadwick, Kristy Siu, Craig Lee, Yann Fouillat, and Damien Germonville. Adding federated identity management to OpenStack. *Journal of Grid Computing*, 12(1):3–27, March 2014. CODEN ???? ISSN 1570-7873 (print), 1572-9184 (electronic). URL `http://link.springer.com/article/10.1007/s10723-013-9283-2`; `http://link.springer.com/content/`

pdf/10.1007/s10723-013-9283-2.pdf.

Chen:2013:RWM

[CSS+13] Xianyi Chen, Xingming Sun, Huiyu Sun, Zhili Zhou, and Jianjun Zhang. Reversible watermarking method based on asymmetric-histogram shifting of prediction errors. *The Journal of Systems and Software*, 86(10):2620–2626, October 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S016412121300126X.

Chen:2017:SIE

[CST+17] Chin-Ling Chen, Jungpil Shin, Yu-Ting Tsai, Aniello Castiglione, and Francesco Palmieri. Securing information exchange in VANETs by using pairing-based cryptography. *International Journal of Foundations of Computer Science (IJFCS)*, 28(6):781–??, September 2017. CODEN IFCSEN. ISSN 0129-0541.

Ciegis:2016:ADP

[CSTR16] Raimondas Ciegis, Vadimas Starikovicius, Natalija Tumanova, and Minvydas Ragulskis. Application of distributed parallel computing for dynamic visual cryptography. *The Journal of Supercomputing*, 72(11):4204–4220, November 2016. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Chong:2015:SID

[CSV15] Stephen Chong, Christian Skalka, and Jeffrey A. Vaughan. Self-identifying data for fair use. *Journal of Data and Information Quality (JDIQ)*, 5(3):11:1–11:??, February 2015. CODEN ???? ISSN 1936-1955.

Chow:2012:EPV

[CSW12] Yang-Wai Chow, Willy Susilo, and Duncan S. Wong. Enhancing the perceived visual quality of a size invariant visual cryptography scheme. *Lecture Notes in Computer Science*, 7618:10–21, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34129-8_2/.

Chen:2018:SIA

[CSYY18] Jiageng Chen, Chunhua Su, Kuo-Hui Yeh, and Moti Yung. Special issue on advanced persistent threat. *Future Generation Computer Systems*, 79 (part 1)(??):243–246, 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17324913.

Chen:2011:IBT

[CSZ+11] Xiaofeng Chen, Willy Susilo, Fangguo Zhang, Haibo Tian, and Jin Li. Identity-based trapdoor mercurial commitments and applications. *Theoretical Computer Science*, 412 (39):5498–5512, September 9, 2011. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Chen:2011:ARI

[CT11a] Chien-Chang Chen and Yao-Hong Tsai. Adaptive reversible image watermarking scheme. *The Journal of Systems and Software*, 84(3):428–434, March 2011. CODEN JSSODM. ISSN 0164-1212.

Chen:2011:TVS

[CT11b] Tzung-Her Chen and Kai-Hsiang Tsao. Threshold visual secret sharing by random grids. *The Journal of Systems and Software*, 84 (7):1197–1208, July 2011. CODEN JSSODM. ISSN 0164-1212.

Canard:2018:CPK

[CT18] Sébastien Canard and Viet Cuong Trinh. Certificateless public key cryptography in the standard model. *Fundamenta Informaticae*, 161(3):219–248, ???? 2018. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Calzavara:2015:SLA

[CTC+15] Stefano Calzavara, Gabriele Tolomei, Andrea Casini, Michele Bugliesi, and Salvatore Orlando. A supervised learning approach to protect client authentication on the Web. *ACM Transactions on the Web (TWEB)*, 9(3):15:1–15:??, June 2015. CODEN ???? ISSN 1559-1131 (print), 1559-114X (electronic).

Chin:2013:SMB

[CTHP13] Ji-Jian Chin, Syh-Yuan Tan, Swee-Huay Heng, and Raphael C.-W. Phan. On the security of a modified Beth identity-based identification scheme. *Information Processing Letters*, 113(14–16):580–583, July/ August 2013. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013001324.

Chang:2012:GBP

[CTL12] Ting-Yi Chang, Cheng-Jung Tsai, and Jyun-Hao Lin. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *The Journal of Systems and Software*, 85(5):1157–1165, May 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211003256.

Chou:2013:TIB

[CTL13] Chih-Ho Chou, Kuo-Yu Tsai, and Chung-Fu Lu. Two ID-based authenticated schemes with key agreement for mobile environments. *The Journal of Supercomputing*, 66(2): 973–988, November 2013. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-013-0962-3.

Crenne:2013:CMS

[CVG+13] Jérémie Crenne, Romain Vaslin, Guy Gogniat, Jean-Philippe Diguet, Russell Tessier, and Deepak Unnikrishnan. Configurable memory security in embedded systems. *ACM Transactions on Embedded Computing Systems*, 12(3): 71:1–71:??, March 2013. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Calmon:2014:ITM

[CVM14] Flavio P. Calmon, Mayank Varia, and Muriel Médard. On information-theoretic metrics for symmetric-key encryption and privacy. In ????, editor, *Proceedings of the 52nd Annual Allerton Conference on Communication, Control, and Computing, 2014*, page ?? ????, ????, 2014. URL http://www.mit.edu/~flavio/Documents/Calmon_Allerton13.pdf.

Choi:2012:LTF

[CW12a] Seung Geol Choi and Hoeteck Wee. Lossy trapdoor functions from homomorphic reproducible encryption. *Information Processing Letters*, 112(20):794–798, October 31, 2012. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019012002001.

Chung:2012:CBI

[CW12b] Yu-Fang Chung and Zhen-Yu Wu. Casting ballots over Internet connection against bribery and coercion. *The Computer Journal*, 55(10):1169–1179, October 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/55/10/1169.full.pdf+html.

Chen:2014:SBB

[CW14a] Chien-Chang Chen and Wei-Jie Wu. A secure Boolean-based multi-secret image sharing scheme. *The Journal of Systems and Software*, 92(??):107–114, June 2014. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121214000181.

Chen:2014:DSE

[CW14b] Jie Chen and Hoeteck Wee. Doubly spatial encryption from DBDH. *Theoretical Computer Science*, 543(??):79–89, July 10, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397514004277.

Cao:2014:PPM

[CWL+14] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou. Privacy-preserving multi-keyword ranked search over encrypted cloud data. *IEEE Transactions on Parallel and Distributed Systems*, 25(1):222–233, January 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Chen:2016:EPN

[CWL16] Yu-Jia Chen, Li-Chun Wang, and Chen-Hung Liao. Eavesdropping prevention for network coding encrypted cloud storage systems. *IEEE Transactions on Parallel and Distributed Systems*, 27(8):2261–2273, August 2016. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL http://csdl.computer.org/csdl/trans/td/2016/08/07289458-abs.html.

Chen:2012:IDC

[CWP12] Jiazhe Chen, Meiqin Wang, and Bart Preneel. Impossible differential cryptanalysis of the lightweight block ciphers TEA, XTEA and HIGHT. *Lecture Notes in Computer Science*, 7374:117–137, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31410-0_8/.

Chen:2012:CKS

[CWWL12] Zhenhua Chen, Chunying Wu, Daoshun Wang, and Shundong Li. Conjunctive keywords searchable encryption with efficient pairing, constant ciphertext and short trapdoor. *Lecture Notes in Computer Science*, 7299:

176–189, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-30428-6_15/.

Chen:2016:WPM

[CWXW16] Zhide Chen, Meng Wang, Li Xu, and Wei Wu. Worm propagation model in mobile network. *Concurrency and Computation: Practice and Experience*, 28 (4):1134–1144, March 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Chen:2019:MBR

[CWZ19] Lele Chen, Gaoli Wang, and GuoYan Zhang. MILP-based related-key rectangle attack and its application to GIFT, Khudra, MIBS. *The Computer Journal*, 62(12):1805–1821, December 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/12/1805/5587703.

Cao:2013:SIPa

[CWZL13] Jian Cao, Jie Wang, Haiyan Zhao, and Minglu Li. Special issue papers: An event view specification approach for Supporting Service process collaboration. *Concurrency and Computation: Practice and Experience*, 25(13):1943–1966, September 10, 2013. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Chen:2019:WBS

[CXWT19] Yu-Chi Chen, Xin Xie, Peter Shaojui Wang, and Raylin Tso. Witness-based searchable encryption with optimal overhead for cloud-edge computing. *Future Generation Computer Systems*, 100(??):715–723, November 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19301086.

Cao:2019:PPS

[CXX+19] Yang Cao, Yonghui Xiao, Li Xiong, Liquan Bai, and Masatoshi Yoshikawa. PriSTE: protecting spatiotemporal event privacy in continuous location-based services. *Proceedings of the VLDB Endowment*, 12(12):1866–1869, August 2019. CODEN ???? ISSN 2150-8097.

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).

Chen:2015:TCP

[CZ15a] Shangdi Chen and Xiaolian Zhang. Three constructions of perfect authentication codes from projective geometry over finite fields. *Applied Mathematics and Computation*, 253(??):308–317, February 15, 2015. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300314017494.

Cheng:2015:OMU

[CZ15b] Rong Cheng and Fangguo Zhang. Obfuscation for multi-use re-encryption and its application in cloud computing. *Concurrency and Computation: Practice and Experience*, 27(8):2170–2190, June 10, 2015. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Cai:2019:UMD

[CZ19] Hongyun Cai and Fuzhi Zhang. An unsupervised method for detecting shilling attacks in recommender systems by mining item relationship and identifying target items. *The Computer Journal*, 62(4):579–597, April 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/4/579/5255729.

Chen:2018:ERS

[CZCD18] Siyuan Chen, Peng Zeng, Kim-Kwang Raymond Choo, and Xiaolei Dong. Efficient ring signature and group signature schemes based on q-ary identification protocols. *The Computer Journal*, 61(4):545–560, April 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/4/545/4656252.

Chen:2012:FSD

[CZF12] Cheng Chen, Zhenfeng Zhang, and Dengguo Feng. Fully secure doubly-spatial encryption under simple assumptions. *Lecture Notes in Computer Science*, 7496:253–263, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33272-2_16/.

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 Computer Science*, 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 Computer Science*, 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.

Dharwadkar:2010:SSG

[DA10] Nagaraj V. Dharwadkar and B. B. Amberker. Steganographic scheme for gray-level image using pixel neighborhood and LSB substitution. *International Journal of Image and Graphics (IJIG)*, 10 (4):589–607, October 2010. CODEN ???? ISSN 0219-4678.

Djebbar:2012:ASB

[DA12] Fatiha Djebbar and Beghdad Ayad. Audio steganalysis based on lossless data-compression techniques. *Lecture Notes in Computer Science*, 7618:1–9, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34129-8_1/.

Darivandpour:2018:ESP

[DA18] Javad Darivandpour and Mikhail J. Atallah. Efficient and secure pattern matching with wildcards using lightweight cryptography. *Computers & Security*, 77(??):666–674, August 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S016740481830021X.

Danezis:2012:FCDb

[Dan12] George Danezis, editor. *Financial Cryptography and Data Security: 15th International Conference, FC 2011, Gros Islet, St. Lucia, February 28 — March 4, 2011, Revised Selected Papers*, volume 7035 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. CODEN LNCSD9. ISBN 3-642-27575-3. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/978-3-642-27575-3`.

Davies:2011:IST

[Dav11] Joshua Dennis Davies. *Implementing SSL/TLS using cryptography and PKI*. John Wiley and Sons, Inc., New York, NY, USA, 2011. ISBN 0-470-92041-6 (paperback). ???? pp. LCCN ????

Demirhan:2016:CRP

[DB16] Haydar Demirhan and Nihan Bitirim. `CryptRndTest`: an R package for testing the cryptographic randomness. *The R Journal*, 8(1):233–247, August 2016. ISSN 2073-4859. URL `https://journal.r-project.org/archive/2016/RJ-2016-016`.

Diong:2012:DAU

[DBPS12] Mouhamadou L. Diong, Patrick Bas, Chloé Pelle, and Wadih Sawaya. Document authentication using 2D codes: Maximizing the decoding performance using statistical inference. *Lecture Notes in Computer Science*, 7394:39–54, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32805-3_4/`.

Djath:2019:HAR

[DBT19] Libey Djath, Karim Bigou, and Arnaud Tisserand. Hierarchical approach in RNS base extension for asymmetric cryptography. In Takagi et al. [TBL19], pages 46–53. ISBN 1-72813-366-1. ISSN 1063-6889.

Dou:2018:OHR

[DCA18] Yi Dou, Henry C B Chan, and Man Ho Au. Order-hiding range query over encrypted data without search pattern leakage. *The Computer Journal*, 61(12):1806–1824, December 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/61/12/1806/5065094`.

Dou:2019:DTE

[DCA19] Y. Dou, H. C. B. Chan, and M. H. Au. A distributed trust evaluation protocol with privacy protection for intercloud. *IEEE Transactions on Parallel and Distributed Systems*, 30(6): 1208–1221, June 2019. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Dacosta:2012:OTC

[DCAT12] Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad, and Patrick Traynor. One-time cookies: Preventing session hijacking attacks with stateless authentication tokens. *ACM Transactions on Internet Technology (TOIT)*, 12(1):1:1–1:??, June 2012. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Cordeiro:2016:MPG

[dCCSB+16] Weverton Luis da Costa Cordeiro, Flávio Roberto Santos, Marinho Pilla Barcelos, Luciano Paschoal Gaspary, Hanna Kavalionak, Alessio Guerrieri, and Alberto Montresor. Making puzzles green and useful for adaptive identity management in large-scale distributed systems. *Computer Networks (Amsterdam, Netherlands: 1999)*, 95(??):97–114, February 11, 2016. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128615004818`.

Cordeiro:2012:IMB

[dCCSM+12] Weverton Luis da Costa Cordeiro, Flávio Roberto Santos, Gustavo Huff Mauch, Marinho Pilla Barcelos, and Luciano Paschoal Gaspary. Identity management based on adaptive puzzles to protect P2P systems from Sybil attacks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 56(11):2569–2589, July 31, 2012. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128612001417`.

Ding:2018:NPH

[DCM18] Kaimeng Ding, Shiping Chen, and Fan Meng. A novel perceptual hash algorithm for multispectral image authentication. *Algorithms (Basel)*, 11(1), January 2018. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL `https://www.mdpi.com/1999-4893/11/1/6`.

DePrisco:2013:CVC

[DD13] Roberto De Prisco and Alfredo De Santis. Color visual cryptography schemes for black and white secret images. *Theoretical Computer Science*, 510(??):62–86, October 28, 2013. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397513006750`.

DArco:2014:MIC

[DDD14] P. D'Arco, R. De Prisco, and A. De Santis. Measure-independent characterization of contrast optimal visual cryptography schemes. *The Journal of Systems and Software*, 95(??):89–99, September 2014. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121214000995`.

Didier:2019:RAP

[DDE+19] Laurent-Stephane Didier, Fangan-Yssouf Dosso, Nadia El Mrabet, Jeremy Marrez, and Pascal Véron. Randomization of arithmetic over polynomial modular number system. In Takagi et al. [TBL19], pages 199–206. ISBN 1-72813-366-1. ISSN 1063-6889.

DaRolt:2013:NDS

[DDFR13] Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, and Bruno Rouzeyre. A novel differential scan attack on advanced DFT structures. *ACM Transactions on Design Automation of Electronic Systems*, 18(4):58:1–58:??, October 2013. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Dreier:2015:BFP

[DDL15] Jannik Dreier, Jean-Guillaume Dumas, and Pascal Lafourcade. Brandt's fully private auction protocol revisited. *Journal of Computer Security*, 23(5):587–610, ???? 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Datta:2017:SFH

[DDM17] Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay. Strongly full-hiding inner product encryption. *Theoretical Computer Science*, 667(??):16–50, March 8, 2017. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397516307526`.

Castro:2016:FVB

[DDR+16] Stephan De Castro, Jean-Max Dutertre, Bruno Rouzeyre, Giorgio Di Natale, and Marie-Lise Flottes. Frontside versus backside laser injection: a comparative study. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 13(1):7:1–7:??, December 2016. CODEN ???? ISSN 1550-4832.

Danezis:2012:FCDa

[DDS12] George Danezis, Sven Dietrich, and Kazue Sako, editors. *Financial Cryptography and Data Security: FC 2011 Workshops, RLCPS and WECSR 2011, Rodney Bay, St. Lucia, February 28 — March 4, 2011, Revised Selected Papers*, volume 7126 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. CODEN LNCSD9. ISBN 3-642-29888-5. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/978-3-642-29888-2`.

Dai:2019:SAM

[DDY+19] Hua Dai, Xuelong Dai, Xun Yi, Geng Yang, and Haiping Huang. Semantic-aware multi-keyword ranked search scheme over encrypted cloud data. *Journal of Network and Computer Applications*, 147 (??):??, December 1, 2019. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804519303029`.

DeOliveiraNunes:2019:SSC

[DEL19] Ivan De Oliveira Nunes, Karim Eldefrawy, and Tancrède Lepoint. SNUSE: a secure computation approach for large-scale user re-enrollment in biometric authentication systems. *Future Generation Computer Systems*, 98(??):259–273, September 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X1833098X`.

derhans:2010:USC

[der10] der.hans. Use SSH to cross a suspect host securely. *Linux Journal*, 2010(191): 3:1–3:??, March 2010. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Desmedt:2010:CF

[Des10a] Yvo Desmedt. *Cryptographic Foundations*, chapter 9, pages 1–15. Volume 2 of Atallah and Blanton [AB10b], second edition, 2010. ISBN 1-58488-820-2. LCCN QA76.9.A43 A433 2010. URL `http://www.crcnetbase.com/doi/abs/10.1201/9781584888215-c9`.

Desmedt:2010:ES

[Des10b] Yvo Desmedt. *Encryption Schemes*, chapter 10, pages 1–30. Volume 2 of Atallah and Blanton [AB10b], second edition, 2010. ISBN 1-58488-820-2. LCCN QA76.9.A43 A433 2010. URL `http://www.crcnetbase.com/doi/abs/10.1201/9781584888215-c10`.

Dew:2011:BRB

[Dew11] Nicholas Dew. Book review: *The Information Master: Jean-Baptiste Colbert's Secret State Intelligence System*. *Isis*, 102(4): 765, December 2011. CODEN ISISA4. ISSN 0021-1753 (print), 1545-6994 (electronic). URL `http://www.jstor.org/stable/10.1086/664857`.

Durmuth:2011:DEN

[DF11] Markus Dürmuth and David Mandell Freeman. Deniable encryption with negligible detection probability: An interactive construction. *Lecture Notes in Computer Science*, 6632: 610–626, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_33`.

DuPont:2016:ECC

[DF16] Quinn DuPont and Bradley Fidler. Edge cryptography and the codevelopment of computer networks and cybersecurity. *IEEE Annals of the History of Computing*, 38(4):55–73, ???? 2016. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic).

DeCapitaniDiVimercati:2010:EPR

[DFJ+10] Sabrina De Capitani Di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. Encryption policies for regulating access to outsourced data. *ACM Transactions on Database Systems*, 35(2):12:1–12:??, April 2010. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

DeCapitanidiVimercati:2017:AMM

[DFJ+17] Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Giovanni Livraga, Stefano Paraboschi, and Pierangela Samarati. An authorization model for multi provider queries. *Proceedings of the VLDB Endowment*, 11(3):256–268, November 2017. CODEN ???? ISSN 2150-8097.

Deng:2017:LLH

[DFKC17] Zhaoxia Deng, Ariel Feldman, Stuart A. Kurtz, and Frederic T. Chong. Lemonade from lemons: Harnessing device wearout to create limited-use security architectures. *ACM SIGARCH Computer Architecture News*, 45(2): 361–374, May 2017. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Ding:2012:CLS

[DG12] Lin Ding and Jie Guan. Cryptanalysis of Loiss stream cipher. *The Computer Journal*, 55 (10):1192–1201, October 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/55/10/1192.full.pdf+html`.

Djuric:2015:FSF

[DG15] Zoran Djuric and Dragan Gasevic. FEIPS: a secure fair-exchange payment system for Internet transactions. *The Computer Journal*, 58(10):2537–2556, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/10/2537`.

Dutta:2017:EFC

[DG17] Tanima Dutta and Hari Prabhat Gupta. An efficient framework for compressed domain watermarking in P frames of high-efficiency video coding (HEVC)-encoded video. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 13(1):12:1–12:??, January 2017. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Dickens:2018:SCI

[DGFH18] Bernard Dickens III, Haryadi S. Gunawi, Ariel J. Feldman, and Henry Hoffmann. StrongBox: Confidentiality, integrity, and performance using stream ciphers for full drive encryption. *ACM SIGPLAN Notices*, 53(2):708–721, February 2018. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Dupressoir:2014:GGP

[DGJN14] François Dupressoir, Andrew D. Gordon, Jan Jürjens, and David A. Naumann. Guiding a general-purpose C verifier to prove cryptographic protocols. *Journal of Computer Security*, 22(5):823–866, ???? 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Drucker:2018:FMB

[DGK18] Nir Drucker, Shay Gueron, and Vlad Krasnov. Fast multiplication of binary polynomials with the forthcoming vectorized VPCLMULQDQ instruction. In Tenca and Takagi [TT18], pages 115–119. ISBN 1-5386-2612-8 (USB), 1-5386-2665-9. ISSN 2576-2265. LCCN QA76.9.C62. IEEE catalog number CFP18121-USB.

Dolev:2019:AAC

[DGL19] Shlomi Dolev, Niv Gilboa, and Ximing Li. Accumulating automata and cascaded equations automata for communicationless information theoretically secure multi-party computation. *Theoretical Computer Science*, 795(??):81–99, November 26, 2019. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397519303883.

Ding:2012:NRR

[DGlS12] L. Ding, J. Guan, and W. l. Sun. New results of related-key attacks on all Py-family of stream ciphers. *J.UCS: Journal of Universal Computer Science*, 18(12):1741–??, ???? 2012. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_18_12/new_results_of_related.

Demay:2019:PSS

[DGMT19] Grégory Demay, Peter Gaži, Ueli Maurer, and Björn Tackmann. Per-session security: Password-based cryptography revisited. *Journal of Computer Security*, 27(1):75–111, ???? 2019. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Drimer:2010:DBP

[DGP10] Saar Drimer, Tim Güneysu, and Christof Paar. DSPs, BRAMs, and a pinch of logic: Extended recipes for AES on FPGAs. *ACM Transactions on Reconfigurable Technology and Systems*, 3(1):3:1–3:??, January 2010. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Dubeuf:2016:EPA

[DHB16] Jeremy Dubeuf, David Hely, and Vincent Beroulle. ECDSA passive attacks, leakage sources, and common design mistakes. *ACM Transactions on Design Automation of Electronic Systems*, 21(2):31:1–31:??, January 2016. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Dodis:2010:CAC

[DHLAW10] Y. Dodis, K. Haralambiev, A. Lopez-Alt, and D. Wichs. Cryptography against continuous memory attacks. In IEEE [IEE10], pages 511–520. ISBN 1-4244-8525-8. LCCN ???? URL http://ieeexplore.ieee.org/servlet/opac?punumber=5669376. IEEE Computer Society Order Number P4244.

Dang:2019:SBS

[DHT+19] Van Tuyen Dang, Truong Thu Huong, Nguyen Huu Thanh, Pham Ngoc Nam, Nguyen Ngoc Thanh, and Alan Marshall. SDN-based SYN proxy — a solution to enhance performance of attack mitigation under TCP SYN flood. *The Computer Journal*, 62(4):518–534, April 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/4/518/5183521.

Driessen:2013:ESA

[DHW+13] Benedikt Driessen, Ralf Hund, Carsten Willems, Christof Paar, and Thorsten Holz. An experimental security analysis of two satphone standards. *ACM Transactions on Information and System Security*, 16(3):10:1–10:??, November 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Diem:2012:UES

[Die12] Claus Diem. On the use of expansion series for stream ciphers. *LMS Journal of Computation and Mathematics*, 15:326–340, 2012. CODEN ???? ISSN 1461-1570.

Drosou:2012:SAH

[DIMT12] Anastasios Drosou, Dimosthenis Ioannidis, Konstantinos Moustakas, and Dimitrios Tzovaras. Spatiotemporal analysis of human activities for biometric authentication. *Computer Vision and Image Understanding: CVIU*, 116(3):411–421, March 2012. CODEN CVIUF4. ISSN 1077-3142 (print), 1090-235X (electronic). URL http://www.sciencedirect.com/science/article/pii/S1077314211002098.

Dinoor:2010:PIM

[Din10] Shlomi Dinoor. Privileged identity management: securing the enterprise. *Network Security*, 2010(12):4–6, December 2010. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485810701446.

Dong:2019:FOI

[DJ19] Shi Dong and Raj Jain. Flow online identification method for the encrypted Skype. *Journal of Network and Computer Applications*, 132(??):75–85, April 15, 2019. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804519300074`.

Ding:2015:CWF

[DJG+15] Lin Ding, Chenhui Jin, Jie Guan, Shaowu Zhang, Ting Cui, Dong Han, and Wei Zhao. Cryptanalysis of WG family of stream ciphers. *The Computer Journal*, 58(10):2677–2685, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/10/2677`.

Domnitser:2012:NMC

[DJL+12] Leonid Domnitser, Aamer Jaleel, Jason Loew, Nael Abu-Ghazaleh, and Dmitry Ponomarev. Non-monopolizable caches: Low-complexity mitigation of cache side channel attacks. *ACM Transactions on Architecture and Code Optimization*, 8(4):35:1–35:??, January 2012. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic).

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`.

Delfs:2007:ICP

[DK07] Hans Delfs and Helmut Knebl. *Introduction to Cryptography: Principles and Applications*, volume 1 of *Information Security and Cryptography*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2007. ISBN 3-540-49243-7 (hardcover), 3-540-49244-5. ISSN 1619-7100 (print), 2197-845X (electronic). xvi + 367 pp. LCCN QA76.9A25 D44 2007; QA76.9.D35. URL `http://www.springerlink.com/content/gm2886`.

Dolev:2012:ATC

[DK12] Shlomi Dolev and Marina

Kopeetsky. Anonymous transactions in computer networks. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 7(2):26:1–26:??, July 2012. CODEN ???? ISSN 1556-4665 (print), 1556-4703 (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`.

Delimitrou:2016:SID

[DK16a] Christina Delimitrou and Christos Kozyrakis. Security implications of data mining in cloud scheduling. *IEEE Computer Architecture Letters*, 15(2):109–112, July/December 2016. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Dorre:2016:ELO

[DK16b] Felix Dörre and Vladimir Klebanov. Entropy loss and output predictability in the Libgcrypt PRNG. Report CVE-2016-6313, Karlsruhe Institute of Technology, Karlsruhe, Germany, August 18, 2016. 2 pp. URL `http://formal.iti.kit.edu/~klebanov/pubs/libgcrypt-cve-2016-6313.pdf`.

Doychev:2017:RAS

[DK17] Goran Doychev and Boris Köpf. Rigorous analysis of software countermeasures against cache attacks. *ACM SIGPLAN Notices*, 52(6):406–421, June 2017. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Durumeric:2014:MH

[DKA+14] Zakir Durumeric, James Kasten, David Adrian, J. Alex Halderman, Michael Bailey, Frank Li, Nicholas Weaver, Johanna Amann, Jethro Beekman, Mathias Payer, et al. The matter of Heartbleed. In ????, editor, *ACM Internet Measurement Conference*, page ?? ACM Press, New York, NY 10036, USA, 2014. ISBN ???? LCCN ???? URL `????`.

Dolev:2016:MCG

[DKL+16] Shlomi Dolev, Ephraim Korach, Ximing Li, Yin Li, and Galit Uzan. Magnifying computing gaps: Establishing encrypted communication over unidirectional channels. *Theoretical Computer Science*, 636(??):17–26, July 11, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397516300718.

Dobre:2019:PWR

[DKL+19] D. Dobre, G. O. Karame, W. Li, M. Majuntke, N. Suri, and M. Vukoli . Proofs of writing for robust storage. *IEEE Transactions on Parallel and Distributed Systems*, 30 (11):2547–2566, November 2019. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Doychev:2015:CTS

[DKMR15] Goran Doychev, Boris Köpf, Laurent Mauborgne, and Jan Reineke. CacheAudit: a tool for the static analysis of cache side channels. *ACM Transactions on Information and System Security*, 18(1):4:1–4:??, June 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Dodis:2012:MAR

[DKPW12] Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, and Daniel Wichs. Message authentication, revisited. *Lecture Notes in Computer Science*, 7237: 355–374, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_21; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_22/.

Dunkelman:2012:MCE

[DKS12] Orr Dunkelman, Nathan Keller, and Adi Shamir. Minimalism in cryptography: The Even–Mansour scheme revisited. *Lecture Notes in Computer Science*, 7237:336–354, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_20; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_21/.

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).

DeLuca:2015:SUS

[DL15] Alexander De Luca and Janne Lindqvist. Is secure and usable Smartphone authentication asking too much? *Computer*, 48(5):64–68, May 2015. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/csdl/mags/co/2015/05/mco2015050064-abs.html.

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).

Deng:2019:DMS

[DLGT19] Cheng Deng, Zhao Li, Xinbo Gao, and Dacheng Tao. Deep multi-scale discriminative networks for double JPEG compression forensics. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 10(2):20:1–20:??, February 2019. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3301274.

Degefa:2016:PSE

[DLK+16] Fikadu B. Degefa, Donghoon Lee, Jiye Kim, Younsung Choi, and Dongho Won. Performance and security enhanced authentication and key agreement protocol for SAE/LTE network. *Computer Networks (Amsterdam, Netherlands: 1999)*, 94(??):145–163, January 15, 2016. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128615004211.

Djaziri-Larbi:2018:WDA

[DLMM+18] Sonia Djaziri-Larbi, Gaël Mahé, Imen Mezghani, Monia Turki, and Mériem Jaïdane. Watermark-driven acoustic echo cancellation. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 26(2):367–378, ???? 2018. CODEN ???? ISSN 2329-9290. URL http://ieeexplore.ieee.org/document/8122007/.

Dong:2013:PRS

[DLN13] Qi Dong, Donggang Liu, and Peng Ning. Providing DoS resistance for signature-based broadcast authentication in sensor networks. *ACM Transactions on Embedded Computing Systems*, 12(3): 73:1–73:??, March 2013. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

DiPietro:2016:CLD

[DLV16] Roberto Di Pietro, Flavio Lombardi, and Antonio Villani. CUDA leaks: a detailed hack for CUDA and a (partial) fix. *ACM Transactions on Embedded Computing Systems*, 15(1):15:1–15:??, February 2016. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Dodis:2011:SSC

[DLWW11] Y. Dodis, A. Lewko, B. Waters, and D. Wichs. Storing secrets on continually leaky devices. In IEEE [IEE11b], pages 688–697. ISBN 1-4577-1843-X. LCCN ????

Dai:2016:MLR

[DLZ16a] Shuguang Dai, Huige Li, and Fangguo Zhang. Memory leakage-resilient searchable symmetric encryption. *Future Generation Computer Systems*, 62(??):76–84, September 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X15003404.

Duan:2016:SDC

[DLZ+16b] Li Duan, Dongxi Liu, Yang Zhang, Shiping Chen, Ren Ping Liu, Bo Cheng, and Junliang Chen. Secure data-centric access control for smart grid services based on publish/subscribe systems. *ACM Transactions on Internet Technology (TOIT)*, 16(4):23:1–23:??, December 2016. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

DeCarneDeCarnavalet:2015:LSE

[DM15] Xavier De Carné De Carnavalet and Mohammad Mannan. A large-scale evaluation of high-impact password strength meters. *ACM Transactions on Information and System Security*, 18(1):1:1–1:??, June 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Daneshgar:2018:SSS

[DM18] Amir Daneshgar and Fahimeh Mohebbipoor. A secure self-synchronized stream cipher. *The Computer Journal*, 61(8):1180–1201, August 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://

academic.oup.com/comjnl/article/61/8/1180/5005423.

DeMarsico:2019:SGR

[DM19] Maria De Marsico and Alessio Mecca. A survey on gait recognition via wearable sensors. *ACM Computing Surveys*, 52 (4):86:1–86:??, September 2019. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3340293.

Dong:2018:SSM

[DMD18] Yao Dong, Ana Milanova, and Julian Dolby. SecureMR: secure mapreduce using homomorphic encryption and program partitioning. *ACM SIGPLAN Notices*, 53(1):389–390, January 2018. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

DiPietro:2010:HKS

[DMM10] Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei. Hierarchies of keys in secure multicast communications. *Journal of Computer Security*, 18(5):839–860, ???? 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Drozdz:2019:SCC

[DMO+19] Stanisław Drozdz, Ludovico Minati, Paweł Oświecimka, Marek Stanuszek, and Marcin Watorek. Signatures of the crypto-currency market decoupling from the Forex. *Future Internet*, 11(7):154, July 10, 2019. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/11/7/154.

Diesburg:2016:TLA

[DMS+16] Sarah Diesburg, Christopher Meyers, Mark Stanovich, An-I Andy Wang, and Geoff Kuenning. TrueErase: Leveraging an auxiliary data path for per-file secure deletion. *ACM Transactions on Storage*, 12(4):18:1–18:??, August 2016. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic).

Dwivedi:2018:DLR

[DMSD18] Ashutosh Dhar Dwivedi, Pawel Morawiecki, Rajani Singh, and Shalini Dhar. Differential-linear and related key cryptanalysis of round-reduced scream. *Information Processing Letters*, 136(??):5–8, August 2018. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019018300656.

Dimitrakakis:2015:ELA

[DMV15] Christos Dimitrakakis, Aikaterini Mitrokotsa, and Serge Vaudenay. Expected loss analysis for authentication in constrained channels. *Journal of Computer Security*, 23(3):309–329, ???? 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Demme:2012:SCV

[DMWS12] John Demme, Robert Martin, Adam Waksman, and Simha Sethumadhavan. Side-channel vulnerability factor: a metric for measuring information leakage. *ACM SIGARCH Computer Architecture News*, 40(3): 106–117, June 2012. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic). ISCA '12 conference proceedings.

David:2012:UCO

[DN12] Bernardo Machado David and Anderson C. A. Nascimento. Universally composable oblivious transfer from lossy encryption and the McEliece assumptions. *Lecture Notes in Computer Science*, 7412:80–99, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32284-6_5/.

Donovan:2014:ATM

[Don14] Peter W. Donovan. Alan Turing, Marshall Hall, and the alignment of WW2 Japanese Naval intercepts. *Notices of the American Mathematical Society*, 61(3):258–264, March 2014. CODEN AMNOAN. ISSN 0002-9920 (print), 1088-9477 (electronic). URL http://www.ams.org/notices/201403/rnoti-p258.pdf.

Doroz:2015:AFH

[DOS15] Y. Doroz, E. Ozturk, and B. Sunar. Accelerating fully homomorphic encryption in hardware. *IEEE Transactions on Computers*, 64(6):1509–1521, ???? 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Duncan:2012:CAI

[DP12] Christian A. Duncan and Vir V. Phoha. On the complexity of aggregating information for authentication and profiling. *Lecture Notes in Computer Science*, 7122:58–71, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28879-1_5/.

Ding:2017:CSM

[DP17] Jintai Ding and Albrecht Petzoldt. Current state of multivariate cryptography. *IEEE Security & Privacy*, 15(4):28–36, July/August 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `https://www.computer.org/csdl/mags/sp/2017/04/msp2017040028-abs.html`.

Das:2016:CWM

[DPCM16] Aveek K. Das, Parth H. Pathak, Chen-Nee Chuah, and Prasant Mohapatra. Characterization of wireless multidevice users. *ACM Transactions on Internet Technology (TOIT)*, 16(4):29:1–29:??, December 2016. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Dziembowski:2018:NMC

[DPW18] Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. Non-malleable codes. *Journal of the ACM*, 65(4): 20:1–20:??, August 2018. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Dong:2012:NCV

[DQFL12] Deshuai Dong, Longjiang Qu, Shaojing Fu, and Chao Li. New constructions of vectorial Boolean functions with good cryptographic properties. *International Journal of Foundations of Computer Science (IJFCS)*, 23(3):749–??, April 2012. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Daemen:2010:FYA

[DR10] Joan Daemen and Vincent Rijmen. The first 10 years of advanced encryption. *IEEE Security & Privacy*, 8(6):72–74, November/December 2010. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Duong:2011:CWC

[DR11] Thai Duong and J. Rizzo. Cryptography in the Web: The case of cryptographic design flaws in ASP.NET. Unknown, May 2011.

Dautrich:2012:SLU

[DR12] Jonathan L. Dautrich and Chinya V. Ravishankar. Security limitations of using secret sharing for data outsourcing. *Lecture Notes in Computer Science*, 7371: 145–160, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31540-4_12/`.

Draziotis:2016:EDL

[Dra16] Konstantinos A. Draziotis. (EC)DSA lattice attacks based on Coppersmith's method. *Information Processing Letters*, 116(8): 541–545, August 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019016300436.

Dong:2011:SSE

[DRD11] Changyu Dong, Giovanni Russello, and Naranker Dulay. Shared and searchable encrypted data for untrusted servers. *Journal of Computer Security*, 19 (3):367–397, ???? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Dasgupta:2016:TDA

[DRN16] Dipankar Dasgupta, Arunava Roy, and Abhijit Nag. Toward the design of adaptive selection strategies for multi-factor authentication. *Computers & Security*, 63(??):85–116, November 2016. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S016740481630102X.

Dixon:2016:NTO

[DRS16] Lucas Dixon, Thomas Ristenpart, and Thomas Shrimpton. Network traffic obfuscation and automated Internet censorship. *IEEE Security & Privacy*, 14(6):43–53, November/December 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/06/msp2016060043-abs.html.

delRey:2012:EDI

[dRSdlVC12] A. Martín del Rey, G. Rodríguez Sánchez, and A. de la Villa Cuenca. Encrypting digital images using cellular automata. *Lecture Notes in Computer Science*, 7209:78–88, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28931-6_8/.

Dini:2011:LLA

[DS11] Gianluca Dini and Ida M. Savino. LARK: a lightweight authenticated ReKeying scheme for clustered wireless sensor networks. *ACM Transactions on Embedded Computing Systems*, 10 (4):41:1–41:??, November 2011. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Dixit:2019:FBD

[DS19] Umesh D. Dixit and M. S.

Shirdhonkar. Fingerprint-based document image retrieval. *International Journal of Image and Graphics (IJIG)*, 19(2): ??, 2019. ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S0219467819500086`.

Das:2015:DCS

[DSB15] Debasish Das, Utpal Sharma, and D. K. Bhattacharyya. Detection of cross-site scripting attack under multiple scenarios. *The Computer Journal*, 58(4):808–822, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/4/808`.

Das:2016:MPU

[DSB16] Jayita Das, Kevin Scott, and Sanjukta Bhanja. MRAM PUF: Using geometric and resistive variations in MRAM cells. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 13(1):2:1–2:??, December 2016. CODEN ???? ISSN 1550-4832.

Das:2012:DPB

[DSCS12] Ashok Kumar Das, Pranay Sharma, Santanu Chatterjee, and Jamuna Kanta Sing. A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *Journal of Network and Computer Applications*, 35(5):1646–1656, September 2012. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804512000926`.

Deng:2018:SFE

[DSLB18] Lih-Yuan Deng, Jyh-Jen Horng Shiau, Henry Horng-Shing Lu, and Dale Bowman. Secure and Fast Encryption (SAFE) with classical random number generators. *ACM Transactions on Mathematical Software*, 44(4):45:1–45:17, August 2018. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `https://dl.acm.org/citation.cfm?id=3212673`.

Dachman-Soled:2014:COF

[DSMM14] Dana Dachman-Soled, Mohammad Mahmoody, and Tal Malkin. Can optimally-fair coin tossing be based on one-way functions? *Lecture Notes in Computer Science*, 8349:217–239, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_10/`.

Dodis:2014:HEY

[DSSDW14] Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs. How to eat your entropy and have it too — optimal recovery strategies for compromised RNGs. Report, Dept. of Computer Science, New York University; Dept. of Computer Science and Applied Mathematics, Weizmann Institute; Dept. of Computer Science, Northeastern University, New York, NY, USA; Tel Aviv, Israel; Boston, MA, USA, March 3, 2014. 27 pp. URL http://eprint.iacr.org/2014/167; https://www.schneier.com/fortuna.html.

Dodis:2017:HEY

[DSSDW17] Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs. How to eat your entropy and have it too: Optimal recovery strategies for compromised RNGs. *Algorithmica*, 79(4):1196–1232, December 2017. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Dini:2013:HHS

[DT13] Gianluca Dini and Marco Tiloca. HISS: a HIghly Scalable Scheme for group rekeying. *The Computer Journal*, 56(4):508–525, April 2013. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/56/4/508.full.pdf+html.

Drosatos:2017:PET

[DTE17] George Drosatos, Aimilia Tasidou, and Pavlos S. Efraimidis. Privacy-enhanced television audience measurements. *ACM Transactions on Internet Technology (TOIT)*, 17(1):10:1–10:??, March 2017. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Deng:2012:VIA

[DTZZ12] Aidong Deng, Jianeng Tang, Li Zhao, and Cairong Zou. The variable-interval arithmetic coding using asymptotic deterministic randomness for data compression and encryption. *Journal of Statistical Computation and Simulation*, 82(10):1545–1555, 2012. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Dunkelman:2012:MEK

[Dun12a] Orr Dunkelman. From multiple encryption to knapsacks — efficient dissection of composite problems. *Lecture Notes in*

Computer Science, 7668: 16, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-34931-7_2.

Dunkelman:2012:TCC

[Dun12b] Orr Dunkelman, editor. *Topics in Cryptology — CT-RSA 2012: The Cryptographers' Track at the RSA Conference 2012, San Francisco, CA, USA, February 27 — March 2, 2012. Proceedings*, volume 7178 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. CODEN LNCSD9. ISBN 3-642-27953-8. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/978-3-642-27953-9.

Durcheva:2015:SAI

[Dur15] Mariana Durcheva. Some applications of idempotent semirings in public key cryptography. *ACM Communications in Computer Algebra*, 49(1):19, March 2015. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

David:2012:PRE

[DW12] C. David and J. Wu. Pseudoprime reductions of elliptic curves. *Canadian Journal of Mathematics = Journal canadien de mathématiques*, 64(1):81–101, February 2012. CODEN CJMAAB. ISSN 0008-414X (print), 1496-4279 (electronic).

Dorn:2012:ECE

[DWB12] Michael Dorn, Peter Wackersreuther, and Christian Böhm. Efficient comparison of encrypted biometric templates. *Lecture Notes in Computer Science*, 7449:129–142, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32287-7_11/.

Dong:2012:KKD

[DWWZ12] Le Dong, Wenling Wu, Shuang Wu, and Jian Zou. Known-key distinguisher on round-reduced 3D block cipher. *Lecture Notes in Computer Science*, 7115:55–69, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27890-7_5/.

Dong:2012:NDI

[DWZ12] Huanhe Dong, Xiangrong Wang, and Wencai Zhao. A new 4-dimensional implicit vector-form loop algebra with arbitrary constants and the corresponding computing formula of constant γ in the Variation identity. *Applied Mathematics and Computation*, 218(22):10998–11008, July 15, 2012. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300312004602.

Dai:2018:OPC

[DWZ18] Wei Dai, William Whyte, and Zhenfei Zhang. Optimizing polynomial convolution for NTRUEncrypt. *IEEE Transactions on Computers*, 67(11):1572–1583, ???? 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL https://ieeexplore.ieee.org/document/8303667/.

Deng:2014:CCC

[DXA14] Robert H. Deng, Yang Xiang, and Man Ho Au. Cryptography in cloud computing. *Future Generation Computer Systems*, 30 (??):90, January 2014. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X13002197.

Deng:2016:NCS

[DXWD16] Jiang Deng, Chunxiang Xu, Huai Wu, and Liju Dong. A new certificateless signature with enhanced security and aggregation version. *Concurrency and Computation: Practice and Experience*, 28(4):1124–1133, March 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Dodis:2013:OWE

[DY13] Yevgeniy Dodis and Yu Yu. Overcoming weak expectations. *Lecture Notes in Computer Science*, 7785: 1–22, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_1/; http://link.springer.com/content/pdf/bfm:978-3-642-36594-2/1.pdf.

Dyakonov:2019:WWU

[Dya19] M. Dyakonov. When will useful quantum computers be constructed? Not in the foreseeable future, this physicist argues. Here's why: The case against: Quantum computing. *IEEE Spectrum*, 56(3):24–29, March 2019.

CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Dong:2015:SSS

[DYZ+15] Xin Dong, Jiadi Yu, Yanmin Zhu, Yingying Chen, Yuan Luo, and Minglu Li. SECO: Secure and scalable data collaboration services in cloud computing. *Computers & Security*, 50(??):91–105, May 2015. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404815000048`.

Deng:2014:TNI

[DZ14] Lunzhi Deng and Jiwen Zeng. Two new identity-based threshold ring signature schemes. *Theoretical Computer Science*, 535(??):38–45, May 22, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397514002692`.

Dong:2016:EPP

[DZC16] Xiaolei Dong, Jun Zhou, and Zhenfu Cao. Efficient privacy-preserving temporal and spacial data aggregation for smart grid communications. *Concurrency and Computation: Practice and Experience*, 28 (4):1145–1160, March 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Doss:2012:MDA

[DZS+12] Robin Doss, Wanlei Zhou, Saravanan Sundaresan, Shui Yu, and Longxiang Gao. A minimum disclosure approach to authentication and privacy in RFID systems. *Computer Networks (Amsterdam, Netherlands: 1999)*, 56(15):3401–3416, October 15, 2012. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128612002447`.

Delledonne:2018:CDA

[DZS+18] Lorenzo Delledonne, Vittorio Zaccaria, Ruggero Susella, Guido Bertoni, and Filippo Melzani. CASCA: a design automation approach for designing hardware countermeasures against side-channel attacks. *ACM Transactions on Design Automation of Electronic Systems*, 23(6):69:1–69:??, December 2018. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Dent:2010:PS

[DZY10] Alexander W. Dent, Yuliang Zheng, and Moti

Yung, editors. *Practical Signcryption*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 1-282-98107-2, 3-540-89411-X (e-book), 3-540-89409-8 (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xviii + 274 pp. LCCN QA76.9.A25 P735 2010. URL http://www.springerlink.com/content/978-3-540-89411-7.

Eslami:2011:SIS

[EA11] Z. Eslami and J. Zarepour Ahmadabadi. Secret image sharing with authentication-chaining and dynamic embedding. *The Journal of Systems and Software*, 84(5):803–809, May 2011. CODEN JSSODM. ISSN 0164-1212.

Erguler:2012:PAI

[EA12] Imran Erguler and Emin Anarim. Practical attacks and improvements to an efficient radio frequency identification authentication protocol. *Concurrency and Computation: Practice and Experience*, 24(17):2069–2080, December 10, 2012. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Ekberg:2012:AEP

[EAA12] Jan-Erik Ekberg, Alexandra Afanasyeva, and N. Asokan. Authenticated encryption primitives for size-constrained trusted computing. *Lecture Notes in Computer Science*, 7344:1–18, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-30921-2_1/.

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.

Elrabaa:2019:PPP

[EAAA19] Muhammad E. S. Elrabaa, Mohamed A. Al-Asli, and Marwan H. Abu-Amara. A protection and pay-per-use licensing scheme for on-cloud FPGA circuit IPs. *ACM Transactions on Reconfigurable Technology and Systems*, 12(3):13:1–13:??, September 2019. CODEN

???? ISSN 1936-7406 (print), 1936-7414 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3329861.

Erbagci:2019:SHE

[EAB+19] Burak Erbagci, Nail Etkin Can Akkaya, Mudit Bhargava, Rachel Dondero, and Ken Mai. Secure hardware-entangled field programmable gate arrays. *Journal of Parallel and Distributed Computing*, 131(??):81–96, September 2019. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731519302618.

Ermis:2017:KAP

[EBAÇ17] Orhan Ermis, Serif Bahtiyar, Emin Anarim, and M. Ufuk Çaglayan. A key agreement protocol with partial backward confidentiality. *Computer Networks (Amsterdam, Netherlands: 1999)*, 129 (part 1)(??):159–177, December 24, 2017. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128617303596.

Egele:2013:ESC

[EBFK13] Manuel Egele, David Brumley, Yanick Fratantonio, and Christopher Kruegel. An empirical study of cryptographic misuse in Android applications. In ????, editor, *ACM Conference on Computer and Communications Security*, pages 73–84. ACM Press, New York, NY 10036, USA, 2013. ISBN ???? LCCN ???? URL ????.

Esiner:2017:QRI

[ED17] Ertem Esiner and Anwitaman Datta. On query result integrity over encrypted data. *Information Processing Letters*, 122 (??):34–39, June 2017. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019017300327.

Esiner:2019:TFA

[ED19] Ertem Esiner and Anwitaman Datta. Two-factor authentication for trusted third party free dispersed storage. *Future Generation Computer Systems*, 90(??):291–306, January 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17322859.

Edwards:2014:NRP

[Edw14] Chris Edwards. News: Researchers probe security through obscurity. *Communications of the Association for Computing Machinery*, 57(8):11–13, August 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Edwards:2017:NSQ

[Edw17] Chris Edwards. News: Secure quantum communications. *Communications of the Association for Computing Machinery*, 60(2):15–17, February 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2017/2/212424/fulltext`.

El-Emam:2013:NSA

[EEAZ13] Nameer N. El-Emam and Rasheed Abdul Shaheed Al-Zubidy. New steganography algorithm to conceal a large amount of secret message using hybrid adaptive neural networks with modified adaptive genetic algorithm. *The Journal of Systems and Software*, 86(6):1465–1481, June 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121212003317`.

Espitau:2018:LAF

[EFGT18] Thomas Espitau, Pierre-Alain Fouque, Benoît Gérard, and Mehdi Tibouchi. Loop-abort faults on lattice-based signature schemes and key exchange protocols. *IEEE Transactions on Computers*, 67(11):1535–1549, November 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `https://ieeexplore.ieee.org/document/8354897/`.

Eisenbarth:2012:CIP

[EGG+12] Thomas Eisenbarth, Zheng Gong, Tim Güneysu, Stefan Heyse, and Sebastiaan Indesteege. Compact implementation and performance evaluation of block ciphers in ATtiny devices. *Lecture Notes in Computer Science*, 7374:172–187, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31410-0_11/`.

El-Hadedy:2019:RPR

[EHKSS19] Mohamed El-Hadedy, Amit Kulkarni, Dirk Stroobandt, and Kevin Skadron. Reco-Pi: a reconfigurable cryptoprocessor for π-cipher. *Journal of Parallel and Distributed Computing*, 133(??):420–431, November 2019. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731517301636.

Eisenbarth:2010:CCE

[Eis10] Thomas Eisenbarth. *Cryptography and cryptanalysis for embedded systems*, volume 11 of *IT-Security*. Europäischer Universitätsverlag, Berlin, Germany, 2010. ISBN 3-89966-344-6. xiv + 193 pp. LCCN ????

Esiner:2016:FFB

[EKB+16] Ertem Esiner, Adilet Kachkeev, Samuel Braunfeld, Alptekin Küpçü, and Öznur Özkasap. FlexDPDP: Flexlist-based optimized dynamic provable data possession. *ACM Transactions on Storage*, 12(4):23:1–23:??, August 2016. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic).

Emura:2019:PPA

[EKOS19] Keita Emura, Hayato Kimura, Toshihiro Ohigashi, and Tatsuya Suzuki. Privacy-preserving aggregation of time-series data with public verifiability from simple assumptions and its implementations. *The Computer Journal*, 62(4):614–630, April 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/4/614/5263983.

Engels:2013:NLL

[EKP+13] Susanne Engels, Elif Bilge Kavun, Christof Paar, Tolga Yalcin, and Hristina Mihajloska. A non-linear/linear instruction set extension for lightweight ciphers. In IEEE [IEE13], pages 67–75. ISBN 0-7695-4957-8. ISSN 1063-6889. LCCN QA76.9.C62 S95 2013.

Elbirt:2009:UAC

[Elb09] Adam J. Elbirt. *Understanding and Applying Cryptography and Data Security*. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 2009. ISBN 1-4200-6160-7. xxvii + 637 pp. LCCN QA76.9.A25 E43 2009. URL http://www.loc.gov/catdir/toc/ecip0821/2008028154.html.

ElBansarkhani:2012:ELB

[EM12] Rachid El Bansarkhani and Mohammed Meziani. An efficient lattice-based secret sharing construction. *Lecture Notes in Computer Science*, 7322: 160–168, 2012. CODEN LNCSD9. ISSN

0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-30955-7_14/.

Ermoshina:2019:SRC

[EM19] Ksenia Ermoshina and Francesca Musiani. "Standardising by running code": the Signal protocol and *de facto* standardisation in end-to-end encrypted messaging. *Internet Histories*, 3(3–4):343–363, 2019. CODEN ???? ISSN 2470-1483. URL http://www.tandfonline.com/doi/full/10.1080/24701475.2019.1654697.

Embar:2014:PWO

[EMW14] Maya Embar, Louis F. McHugh IV, and William R. Wesselman. Printer watermark obfuscation. In *Proceedings of the 3rd Annual Conference on Research in Information Technology*, RIIT '14, pages 15–20. ACM Press, New York, NY 10036, USA, 2014. ISBN 1-4503-2711-7.

English:2015:SME

[Eng15] Rosanne English. Simulating and modelling the effectiveness of graphical password intersection attacks. *Concurrency and Computation: Practice and Experience*, 27(12):3089–3107, August 25, 2015. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Evtyushkin:2016:UMC

[EPAG16] Dmitry Evtyushkin, Dmitry Ponomarev, and Nael Abu-Ghazaleh. Understanding and mitigating covert channels through branch predictors. *ACM Transactions on Architecture and Code Optimization*, 13(1):10:1–10:??, April 2016. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic).

Eberz:2016:LLE

[ERLM16] Simon Eberz, Kasper B. Rasmussen, Vincent Lenders, and Ivan Martinovic. Looks like Eve: Exposing insider threats using eye movement biometrics. *ACM Transactions on Privacy and Security (TOPS)*, 19(1):1:1–1:??, August 2016. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

El-Razouk:2015:NHI

[ERRMG15] H. El-Razouk, A. Reyhani-Masoleh, and Guang Gong. New hardware implementations of WG and WG-StreamCiphers using polynomial basis. *IEEE Transactions on Computers*, 64(7):2020–2035, July 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

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).

Engels:2012:HLA

[ESS12] Daniel Engels, Markku-Juhani O. Saarinen, and Peter Schweitzer. The Hummingbird-2 lightweight authenticated encryption algorithm. *Lecture Notes in Computer Science*, 7055: 19–31, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-25286-0_2/`.

Ebadi:2015:DPN

[ESS15] Hamid Ebadi, David Sands, and Gerardo Schneider. Differential privacy: Now it's getting personal. *ACM SIGPLAN Notices*, 50(1): 69–81, January 2015. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Essex:2017:DDU

[Ess17] Aleksander Essex. Detecting the detectable: Unintended consequences of cryptographic election verification. *IEEE Security & Privacy*, 15(3): 30–38, May/June 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `https://www.computer.org/csdl/mags/sp/2017/03/msp2017030030-abs.html`.

Everett:2012:EC

[Eve12] Bernard Everett. The encryption conundrum. *Network Security*, 2012(4):15–18, April 2012. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485812700272`.

Everett:2016:SES

[Eve16] Cath Everett. Should encryption software be banned? *Network Security*, 2016(8):14–17, August 2016. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485816300782`.

Eibach:2010:OGB

[EVP10] Tobias Eibach, Gunnar Völkel, and Enrico Pilz. Optimising Gröbner bases on Bivium. *Mathematics in Computer Science*, 3(2): 159–172, April 2010. CODEN ???? ISSN 1661-8270 (print), 1661-8289 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=1661-8270&volume=3&issue=2&spage=159.

Eldib:2014:FVS

[EWS14] Hassan Eldib, Chao Wang, and Patrick Schaumont. Formal verification of software countermeasures against side-channel attacks. *ACM Transactions on Software Engineering and Methodology*, 24(2):11:1–11:??, December 2014. CODEN ATSMER. ISSN 1049-331X (print), 1557-7392 (electronic).

Eyal:2017:BTT

[Eya17] Ittay Eyal. Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities. *Computer*, 50(9):38–49, September 2017. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL https://www.computer.org/csdl/mags/co/2017/09/mco2017090038-abs.html.

Enos:2015:IBS

[EZ15] Graham Enos and Yuliang Zheng. An ID-based signcryption scheme with compartmented secret sharing for unsigncryption. *Information Processing Letters*, 115(2):128–133, February 2015. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019014001537.

Emmart:2018:FME

[EZW18] Niall Emmart, Fangyu Zhengt, and Charles Weems. Faster modular exponentiation using double precision floating point arithmetic on the GPU. In Tenca and Takagi [TT18], pages 130–137. ISBN 1-5386-2612-8 (USB), 1-5386-2665-9. ISSN 2576-2265. LCCN QA76.9.C62. IEEE catalog number CFP18121-USB.

Farash:2014:ECC

[FA14a] Mohammad Sabzinejad Farash and Mahmoud Ahmadian Attari. An efficient client–client password-based authentication scheme with provable security. *The Journal of Supercomputing*, 70(2):1002–1022, November 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-014-1273-z.

Farash:2014:SEI

[FA14b] Mohammad Sabzinejad Farash and Mahmoud Ahmadian Attari. A secure and efficient identity-based authenticated key exchange protocol for mobile client-server networks. *The Journal of Supercomputing*, 69(1):395–411, July 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-014-1170-5.

Fahd:2018:CPA

[FAA+18] Shah Fahd, Mehreen Afzal, Haider Abbas, Waseem Iqbal, and Salman Waheed. Correlation power analysis of modes of encryption in AES and its countermeasures. *Future Generation Computer Systems*, 83(??):496–509, June 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17311822.

Faal:2019:MVE

[Faa19] Hossein Teimoori Faal. A multiset version of even-odd permutations identity. *International Journal of Foundations of Computer Science (IJFCS)*, 30 (5):683–691, August 2019. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054119500163.

Fagone:2017:WWS

[Fag17] Jason Fagone. *The woman who smashed codes: a true story of love, spies, and the unlikely heroine who outwitted America's enemies*. Dey Street Books, New York, New York, 2017. ISBN 0-06-243048-3 (hardcover). xvi + 444 pp. LCCN Z103.4.U6.

Fairley:2019:EWC

[Fai19] P. Fairley. Ethereum will cut back its absurd energy use. *IEEE Spectrum*, 56(1):29–32, January 2019. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Farash:2014:CIE

[Far14] Mohammad Sabzinejad Farash. Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography. *The Journal of Supercomputing*, 70(2):987–1001, November 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-014-1272-0.

Fay:2016:ICM

[Fay16] Robin Fay. Introducing the counter mode of operation to Compressed Sensing based encryption. *Information Processing Letters*, 116(4):279–283, April 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019015001945`.

Fischlin:2012:PKC

[FBM12] Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors. *Public Key Cryptography — PKC 2012: 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21–23. Proceedings*, volume 7293 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. CODEN LNCSD9. ISBN 3-642-30056-1. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/978-3-642-30056-1`.

Ferretti:2014:DCI

[FCM14] Luca Ferretti, Michele Colajanni, and Mirco Marchetti. Distributed, concurrent, and independent access to encrypted cloud databases. *IEEE Transactions on Parallel and Distributed Systems*, 25(2):437–446, February 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Fuglerud:2011:SIA

[FD11] Kristin Fuglerud and Øystein Dale. Secure and inclusive authentication with a talking mobile one-time-password client. *IEEE Security & Privacy*, 9(2):27–34, March/April 2011. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Fang:2019:PPO

[FDY+19] Hongyu Fang, Sai Santosh Dayapule, Fan Yao, Miloš Doroslovački, and Guru Venkataramani. PrODACT: Prefetch-obfuscator to defend against cache timing channels. *International Journal of Parallel Programming*, 47(4):571–594, August 2019. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic).

Fehr:2010:QC

[Feh10] Serge Fehr. Quantum cryptography. *Foundations of Physics*, 40(5):494–531, May 2010. CODEN FNDPA4. ISSN 0015-9018 (print), 1572-9516 (electronic). URL `http://link.springer.com/article/10.1007/s10701-010-9408-4`.

Feigenbaum:2019:PSE

[Fei19] Joan Feigenbaum. Privacy and security: Encryption and surveillance. *Communications of the Association for Computing Machinery*, 62(5):27–29, May 2019. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL https://cacm.acm.org/magazines/2019/5/236419/fulltext.

Felten:2013:LBA

[Fel13] Edward Felten. The Linux backdoor attempt of 2003. Web site., 2013. URL https://freedom-to-tinker.com/blog/felten/the-linux-backdoor-attempt-of-2003/.

Faugere:2010:CLR

[FES10] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In Watt [Wat10], pages 257–264. ISBN 1-4503-0150-9. LCCN QA76.95 .I59 2010.

Fleischmann:2012:MFA

[FFL12] Ewan Fleischmann, Christian Forler, and Stefan Lucks. McOE: a family of almost foolproof on-line authenticated encryption schemes. *Lecture Notes in Computer Science*, 7549:196–215, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34047-5_12/.

Fan:2019:OVG

[FG19] Hua Fan and Wojciech Golab. Ocean Vista: gossip-based visibility control for speedy geo-distributed transactions. *Proceedings of the VLDB Endowment*, 12(11):1471–1484, July 2019. CODEN ???? ISSN 2150-8097.

Feng:2010:CTS

[FGM10] Tao Feng, Yongguo Gao, and Jianfeng Ma. Changeable threshold signature scheme based on lattice theory. In IEEE, editor, *Proceedings of the 2010 International Conference on E-Business and E-Government (ICEE), Guangzhou, China, 7–9 May 2010*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 0-7695-3997-1. LCCN ???? URL http://ieeexplore.ieee.org/servlet/opac?punumber=5589107.

Farras:2012:LTM

[FGMP12] Oriol Farràs, Ignacio Gracia, Sebastià Martín, and Carles Padró. Linear threshold multisecret sharing schemes. *Information Processing Letters*, 112 (17–18):667–673, September 30, 2012. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019012001378.

Faugere:2014:MCA

[FGPGP14] Jean-Charles Faugère, Domingo Gómez-Pérez, Jaime Gutierrez, and Ludovic Perret. Mathematical and computer algebra techniques in cryptology. *Journal of Symbolic Computation*, 64 (??):1–2, August 2014. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic). URL http://www.sciencedirect.com/science/article/pii/S0747717113001673.

Fan:2017:SSP

[FGR+17] Jingyuan Fan, Chaowen Guan, Kui Ren, Yong Cui, and Chunming Qiao. SPABox: Safeguarding privacy during deep packet inspection at a MiddleBox. *IEEE/ACM Transactions on Networking*, 25 (6):3753–3766, December 2017. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Fan:2018:MBP

[FGRQ18] Jingyuan Fan, Chaowen Guan, Kui Ren, and Chunming Qiao. Middlebox-based packet-level redundancy elimination over encrypted network traffic. *IEEE/ACM Transactions on Networking*, 26(4): 1742–1753, August 2018. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Fan:2013:CPP

[FH13] Chun-I Fan and Shi-Yuan Huang. Controllable privacy preserving search based on symmetric predicate encryption in cloud storage. *Future Generation Computer Systems*, 29(7):1716–1724, September 2013. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X1200101X.

Fan:2010:PSN

[FHH10a] Chun-I Fan, Pei-Hsiu Ho, and Ruei-Hau Hsu. Provably secure nested one-time secret mechanisms for fast mutual authentication and key exchange in mobile communications. *IEEE/ACM Transactions on Networking*, 18(3):996–1009, June 2010. CODEN IEANEP. ISSN 1063-6692

(print), 1558-2566 (electronic).

Fan:2010:AMI

[FHH10b] Chun-I Fan, Ling-Ying Huang, and Pei-Hsiu Ho. Anonymous multireceiver identity-based encryption. *IEEE Transactions on Computers*, 59(9):1239–1249, September 2010. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5396332.

Farras:2017:IRN

[FHKP17] Oriol Farràs, Torben Brandt Hansen, Tarik Kaced, and Carles Padró. On the information ratio of non-perfect secret sharing schemes. *Algorithmica*, 79(4):987–1013, December 2017. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Faz-Hernandez:2019:HPI

[FHLD19] Armando Faz-Hernández, Julio López, and Ricardo Dahab. High-performance implementation of elliptic curve cryptography using vector instructions. *ACM Transactions on Mathematical Software*, 45(3):25:1–25:??, July 2019. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL https://dl.acm.org/citation.cfm?id=3309759.

Faz-Hernandez:2018:FSI

[FHLOJRH18] Armando Faz-Hernández, Julio López, Eduardo Ochoa-Jiménez, and Francisco Rodríguez-Henríquez. A faster software implementation of the supersingular isogeny Diffie–Hellman key exchange protocol. *IEEE Transactions on Computers*, 67(11):1622–1636, November 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL https://ieeexplore.ieee.org/document/8100879/.

Forne:2010:PAA

[FHM+10] Jordi Forné, Francisca Hinarejos, Andrés Marín, Florina Almenárez, Javier Lopez, Jose A. Montenegro, Marc Lacoste, and Daniel Díaz. Pervasive authentication and authorization infrastructures for mobile users. *Computers & Security*, 29(4):501–514, June 2010. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404809000911.

Fahl:2012:WEM

[FHM+12] Sascha Fahl, Marian Harbach, Thomas Muders, Lars Baumgärtner, Bernd Freisleben, and Matthew Smith. Why Eve and Mallory love Android: An analysis of Android SSL (in)security. In ????, editor, *ACM Conference on Computer and Communications Security*, pages 50–61. ACM Press, New York, NY 10036, USA, 2012. ISBN ???? LCCN ???? URL ????.

Fan:2014:ASA

[FHR14] Chun-I Fan, Vincent Shi-Ming Huang, and He-Ming Ruan. Arbitrary-state attribute-based encryption with dynamic membership. *IEEE Transactions on Computers*, 63(8):1951–1961, August 2014. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Fawzi:2013:LDN

[FHS13] Omar Fawzi, Patrick Hayden, and Pranab Sen. From low-distortion norm embeddings to explicit uncertainty relations and efficient information locking. *Journal of the ACM*, 60 (6):44:1–44:??, November 2013. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Florencio:2016:PSD

[FHV16] Dinei Florêncio, Cormac Herley, and Paul C. Van Oorschot. Pushing on string: the 'don't care' region of password strength. *Communications of the Association for Computing Machinery*, 59(11):66–74, November 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2016/11/209115/fulltext.

Feng:2018:ABB

[FHZW18] Qi Feng, Debiao He, Sherali Zeadally, and Huaqun Wang. Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment. *Future Generation Computer Systems*, 84(??):239–251, July 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17309020.

Fidler:2018:CCN

[Fid18] Bradley Fidler. Cryptography, capitalism, and national security. *IEEE Annals of the History of Computing*, 40(4):80–84, October/December 2018. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic). URL https://ieeexplore.ieee.org/document/8620680/.

Farash:2015:PSE

[FIO15] Mohammad Sabzinejad Farash, Sk Hafizul Islam, and Mohammad S. Obaidat. A provably secure and efficient two-party password-based explicit authenticated key exchange protocol resistance to password guessing attacks. *Concurrency and Computation: Practice and Experience*, 27(17):4897–4913, December 10, 2015. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Fisher:2015:CS

[Fis15] Charles Fisher. Cipher security. *Linux Journal*, 2015 (257):2:1–2:??, September 2015. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL `http://dl.acm.org/ft_gateway.cfm?id=2846057`.

Fei:2012:GTK

[FJHJ12] Han Fei, Qin Jing, Zhao Huawei, and Hu Jiankun. A general transformation from KP-ABE to searchable encryption. *Lecture Notes in Computer Science*, 7672:165–178, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-35362-8_14/`.

Fotiadis:2019:TRF

[FK19] Georgios Fotiadis and Elisavet Konstantinou. TNFS resistant families of pairing-friendly elliptic curves. *Theoretical Computer Science*, 800 (??):73–89, December 31, 2019. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397519306462`.

Fanti:2015:SVS

[FKOV15] Giulia Fanti, Peter Kairouz, Sewoong Oh, and Pramod Viswanath. Spy vs. spy: Rumor source obfuscation. *ACM SIGMETRICS Performance Evaluation Review*, 43(1):271–284, June 2015. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Fehr:2013:FCC

[FKS+13] Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou, and Vassilis Zikas. Feasibility and completeness of cryptographic tasks in the quantum world. *Lecture Notes in Computer Science*, 7785:281–296, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-36594-2_16/`.

Fan:2013:CEM

[FLH13] Chun-I Fan, Yi-Hui Lin, and Ruei-Hau Hsu. Complete EAP method: User efficient and forward secure authentication protocol for IEEE 802.11 wireless LANs. *IEEE Transactions on Parallel and Distributed Systems*, 24(4): 672–680, April 2013. CODEN ITDSEO. ISSN 1045-9219.

Fan:2014:RRS

[FLL+14] Kai Fan, Jie Li, Hui Li, Xiaohui Liang, Xuemin (Sherman) Shen, and Yintang Yang. RSEL: revocable secure efficient lightweight RFID authentication scheme. *Concurrency and Computation: Practice and Experience*, 26(5):1084–1096, April 10, 2014. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

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.

Forler:2012:DAC

[FLW12] Christian Forler, Stefan Lucks, and Jakob Wenzel. Designing the API for a cryptographic library. *Lecture Notes in Computer Science*, 7308:75–88, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-30598-6_6/.

Fei:2016:PPA

[FLYL16a] Xiongwei Fei, Kenli Li, Wangdong Yang, and Keqin Li. Practical parallel AES algorithms on cloud for massive users and their performance evaluation. *Concurrency and Computation: Practice and Experience*, 28(16):4246–4263, November 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Fei:2016:SEF

[FLYL16b] Xiongwei Fei, Kenli Li, Wangdong Yang, and Keqin Li. A secure and efficient file protecting system based on SHA3 and parallel AES. *Parallel Computing*, 52(??):106–132, February 2016. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167819116000028.

Feng:2012:CAO

[FLZ+12] Hui Feng, Hefei Ling, Fuhao Zou, Weiqi Yan, and Zhengding Lu. A collusion attack optimization strategy for digital fingerprinting. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 8(2S):36:1–36:??, September 2012. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Fallahpour:2015:AWB

[FM15] M. Fallahpour and D. Megias. Audio watermarking based on Fibonacci numbers. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 23(8):1273–1282, August 2015. CODEN ???? ISSN 2329-9290.

Ferrag:2018:SCN

[FMA+18] Mohamed Amine Ferrag, Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos, and Helge Janicke. Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, 101(??):55–82, January 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804517303521.

Fomichev:2019:PZI

[FMA+19] Mikhail Fomichev, Max Maass, Lars Almon, Alejandro Molina, and Matthias Hollick. Perils of zero-interaction security in the Internet of Things. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 3(1):1–38, March 2019. CODEN ???? ISSN 2474-9567 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3314397.

Farwa:2018:FAI

[FMB+18] Shabieh Farwa, Nazeer Muhammad, Nargis Bibi, Sajjad A. Haider, Syed R. Naqvi, and Sheraz Anjum. Fresnelet approach for image encryption in the algebraic frame. *Applied Mathematics and Computation*, 334(??):343–355, October 1, 2018. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300318302868. See retraction notice [?].

Ferretti:2019:FBS

[FMC19] Luca Ferretti, Mirco Marchetti, and Michele Colajanni. Fog-based secure communications for low-power IoT devices. *ACM Transactions on Internet Technology (TOIT)*, 19(2):27:1–27:??, April 2019. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3284554`.

Faust:2014:CNM

[FMNV14] Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, and Daniele Venturi. Continuous non-malleable codes. *Lecture Notes in Computer Science*, 8349:465–488, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_20/`.

Feng:2012:USD

[FMS12a] XiaoXiao Feng, Koichi Matsumoto, and Shigeo Sugimoto. Uncovering the secrets of Daoism *Fus* using digital Dao-Fa Hui-Yuan. *Lecture Notes in Computer Science*, 7634:1–10, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-34752-8_1/`.

Fraczek:2012:MSI

[FMS12b] W. Fraczek, W. Mazurczyk, and K. Szczypiorski. Multilevel steganography: Improving hidden communication in networks. *J.UCS: Journal of Universal Computer Science*, 18 (14):1967–??, ???? 2012. CODEN ???? ISSN 0948-6968. URL `http://www.jucs.org/jucs_18_14/multilevel_steganography_improving_hidden`.

Fernandez-Mir:2012:SRA

[FMTR12] Albert Fernàndez-Mir and Rolando Trujillo-Rasua. A scalable RFID authentication protocol supporting ownership transfer and controlled delegation. *Lecture Notes in Computer Science*, 7055: 147–162, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-25286-0_10/`.

Ferreira:2015:LPA

[FNP+15] Anselmo Ferreira, Luiz C. Navarro, Giuliano Pinheiro, Jefersson A. dos Santos, and Anderson Rocha. Laser printer attribution: Exploring new features and beyond. *Forensic Science International*, 247

(0):105–125, 2015. ISSN 0379-0738. URL http://www.sciencedirect.com/science/article/pii/S0379073814005064. See also [?].

Fu:2018:LUA

[FNWL18] Xingbing Fu, Xuyun Nie, Ting Wu, and Fagen Li. Large universe attribute based access control with efficient decryption in cloud storage system. *The Journal of Systems and Software*, 135(??):157–164, January 2018. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121217302510.

Fokkink:2012:TCG

[Fok12] Robbert Fokkink. Tossing coins to guess a secret number. *American Mathematical Monthly*, 119(4):337–339, April 2012. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic). URL http://www.jstor.org/stable/pdfplus/10.4169/amer.math.monthly.119.04.337.pdf.

Folger:2016:TQH

[Fol16] Tim Folger. Technology: The quantum hack. *Scientific American*, 314(2):48–55, February 2016. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.nature.com/scientificamerican/journal/v314/n2/full/scientificamerican0216-48.html; http://www.nature.com/scientificamerican/journal/v314/n2/pdf/scientificamerican0216-48.pdf.

Fox:2013:RLQ

[Fox13] Margalit Fox. *The Riddle of the Labyrinth: the Quest to Crack an Ancient Code*. HarperCollins College Publishers, New York, NY, USA, 2013. ISBN 0-06-222883-8. xx + 363 pp. LCCN P1038 .F69 2013. URL http://en.wikipedia.org/wiki/Linear_B_script.

Fotiou:2019:NBS

[FP19] Nikos Fotiou and George C. Polyzos. Name-based security for information-centric networking architectures. *Future Internet*, 11(11): 232, November 01, 2019. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/11/11/232.

Faigl:2014:PEC

[FPBG14] Zoltán Faigl, Jani Pellikka, László Bokor, and Andrei Gurtov. Performance evaluation of current and emerging authentication schemes for future 3GPP network architectures. *Com-*

puter Networks (Amsterdam, Netherlands: 1999), 60(??):60–74, February 26, 2014. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128613004180.

Faust:2012:PLR

[FPS12] Sebastian Faust, Krzysztof Pietrzak, and Joachim Schipper. Practical leakage-resilient symmetric cryptography. *Lecture Notes in Computer Science*, 7428: 213–232, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33027-8_13/.

Fu:2015:TVG

[FPY15] Dong Lai Fu, Xin Guang Peng, and Yu Li Yang. Trusted validation for geolocation of cloud data. *The Computer Journal*, 58(10):2595–2607, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2595.

Feng:2018:ALA

[FQZF18] Wei Feng, Yu Qin, Shijun Zhao, and Dengguo Feng. AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS. *Computer Networks (Amsterdam, Netherlands: 1999)*, 134(??):167–182, April 7, 2018. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128618300471.

Fiore:2015:EIB

[FR15] Ugo Fiore and Francesco Rossi. Embedding an identity-based short signature as a digital watermark. *Future Internet*, 7(4):393–404, October 23, 2015. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/7/4/393.

Fathimal:2016:SSS

[FR16] P. Mohamed Fathimal and P. Arockia Jansi Rani. *K* out of *N* secret sharing scheme for multiple color images with steganography and authentication. *International Journal of Image and Graphics (IJIG)*, 16(2):1650010, April 2016. CODEN ???? ISSN 0219-4678.

Frattolillo:2015:WPP

[Fra15] Franco Frattolillo. Watermarking protocols: Problems, challenges and a possible solution. *The Computer Journal*, 58(4):944–

960, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/944.

Frattolillo:2016:BFM

[Fra16] Franco Frattolillo. A buyer-friendly and mediated watermarking protocol for Web context. *ACM Transactions on the Web (TWEB)*, 10(2):9:1–9:??, May 2016. CODEN ???? ISSN 1559-1131 (print), 1559-114X (electronic).

Frey:2010:ABC

[Fre10] Gerhard Frey. The arithmetic behind cryptography. *Notices of the American Mathematical Society*, 57(3):366–374, March 2010. CODEN AMNOAN. ISSN 0002-9920 (print), 1088-9477 (electronic). URL http://www.ams.org/notices/201003/.

Fernandes:2017:ITS

[FREP17] Earlence Fernandes, Amir Rahmati, Kevin Eykholt, and Atul Prakash. Internet of Things security research: A rehash of old ideas or new intellectual challenges? *IEEE Security & Privacy*, 15(4):79–84, July/August 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2017/04/msp2017040079-abs.html.

Fridrich:2010:SDM

[Fri10a] Jessica Fridrich. *Steganography in digital media: principles, algorithms, and applications*. Cambridge University Press, Cambridge, UK, 2010. ISBN 0-521-19019-3 (hardcover). xxii + 437 + 4 pp. LCCN QA76.9.A25 F75 2010.

Frikken:2010:SMC

[Fri10b] Keith B. Frikken. *Secure Multiparty Computation*, chapter 14, pages 1–16. Volume 2 of Atallah and Blanton [AB10b], second edition, 2010. ISBN 1-58488-820-2. LCCN QA76.9.A43 A433 2010. URL http://www.crcnetbase.com/doi/abs/10.1201/9781584888215-c14.

Fridrich:2012:MTS

[Fri12] Jessica Fridrich. Modern trends in steganography and steganalysis. *Lecture Notes in Computer Science*, 7128:1, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-32205-1_1.

Fritsch:2013:CPE

[Fri13] Lothar Fritsch. The clean privacy ecosystem of the future Internet. *Future Internet*, 5(1):34–45, January 14, 2013. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/5/1/34.

Fu:2016:EPS

[FRS+16] Zhangjie Fu, Kui Ren, Jiangang Shu, Xingming Sun, and Fengxiao Huang. Enabling personalized search over encrypted outsourced data with efficiency improvement. *IEEE Transactions on Parallel and Distributed Systems*, 27 (9):2546–2559, September 2016. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL https://www.computer.org/csdl/trans/td/2016/09/07349214-abs.html.

Frauchiger:2013:TRR

[FRT13] Daniela Frauchiger, Renato Renner, and Matthias Troyer. True randomness from realistic quantum devices. *arXiv.org*, ??(??): ??, November 13, 2013. URL http://arxiv.org/abs/1311.4547.

Forbes:2015:CTC

[FS15] Michael A. Forbes and Amir Shpilka. Complexity theory column 88: Challenges in polynomial factorization. *ACM SIGACT News*, 46(4):32–49, December 2015. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Fugkeaw:2018:SSA

[FS18] Somchart Fugkeaw and Hiroyuki Sato. Scalable and secure access control policy update for outsourced big data. *Future Generation Computer Systems*, 79 (part 1)(??):364–373, 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17312426.

Fang:2011:ICP

[FSGW11] Liming Fang, Willy Susilo, Chunpeng Ge, and Jiandong Wang. Interactive conditional proxy re-encryption with fine grain policy. *The Journal of Systems and Software*, 84 (12):2293–2302, December 2011. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211001579.

Fang:2012:CCS

[FSGW12] Liming Fang, Willy Susilo, Chunpeng Ge, and Jiandong Wang. Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search. *Theoretical Computer Science*, 462(1):39–58, November 30, 2012. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397512007906.

Ferguson:2010:CED

[FSK10] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. *Cryptography Engineering: Design Principles and Practical Applications*. John Wiley and Sons, Inc., New York, NY, USA, 2010. ISBN 0-470-47424-6 (paperback). xxix + 353 pp. LCCN QA76.9.A25 F466 2010.

Feng:2011:GDA

[FSWF11] Xiutao Feng, Zhenqing Shi, Chuankun Wu, and Dengguo Feng. On guess and determine analysis of Rabbit. *International Journal of Foundations of Computer Science (IJFCS)*, 22 (6):1283–1296, September 2011. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Fujioka:2012:SHI

[FSX12a] Atsushi Fujioka, Taiichi Saito, and Keita Xagawa. Secure hierarchical identity-based identification without random oracles. *Lecture Notes in Computer Science*, 7483: 258–273, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33383-5_16/.

Fujioka:2012:SEI

[FSX12b] Atsushi Fujioka, Taiichi Saito, and Keita Xagawa. Security enhancement of identity-based identification with reversibility. *Lecture Notes in Computer Science*, 7618: 202–213, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34129-8_18/.

Fujioka:2012:SEP

[FSX12c] Atsushi Fujioka, Taiichi Saito, and Keita Xagawa. Security enhancements by OR-proof in identity-based identification. *Lecture Notes in Computer Science*, 7341:135–152, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31284-7_9/.

Fadlullah:2010:DCA

[FTV+10] Zubair M. Fadlullah, Tarik Taleb, Athanasios V. Vasilakos, Mohsen Guizani, and Nei Kato. DTRAB: combating against attacks on encrypted protocols through traffic-feature analysis. *IEEE/ACM Transactions on Networking*, 18(4):1234–1247, August 2010. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Fuchsbauer:2011:CSV

[Fuc11] Georg Fuchsbauer. Commuting signatures and verifiable encryption. *Lecture Notes in Computer Science*, 6632:224–245, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_14.

Fulton:2010:BRB

[Ful10] Ben Fulton. Book review: *Introduction to Modern Cryptography*, by Jonathan Katz and Yehuda Lindell, Publisher: Chapman & Hall-CRC 2008 1-58488-551-3. *ACM SIGACT News*, 41(4):44–47, December 2010. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [KL08].

Fanti:2018:DLC

[FVB+18] Giulia Fanti, Shaileshh Bojja Venkatakrishnan, Surya Bakshi, Bradley Denby, Shruti Bhargava, Andrew Miller, and Pramod Viswanath. Dandelion++: Lightweight cryptocurrency networking with formal anonymity guarantees. *ACM SIGMETRICS Performance Evaluation Review*, 46(1):5–7, June 2018. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Franken:2019:ECP

[FVJ19] G. Franken, T. Van Goethem, and W. Joosen. Exposing cookie policy flaws through an extensive evaluation of browsers and their extensions. *IEEE Security & Privacy*, 17(4):25–34, July/August 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Fathi-Vajargah:2017:IMC

[FVK17] Behrouz Fathi-Vajargah and Mohadeseh Kanafchian. Improved Markov chain Monte Carlo method for cryptanalysis substitution-transposition cipher. *Monte Carlo Methods and Applications*, 23(2):147–??, June 2017. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL https://www.degruyter.com/view/

j/mcma.2017.23.issue-2/mcma-2017-0108/mcma-2017-0108.xml.

Fiore:2017:PGP

[FVS17] Dario Fiore, María Isabel González Vasco, and Claudio Soriente. Partitioned group password-based authenticated key exchange. *The Computer Journal*, 60(12):1912–1922, December 1, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/12/1912/4210211.

Feng:2013:ECE

[FWS13] Jun Feng, Xueming Wang, and Hong Sun. Efficiently computable endomorphism for genus 3 hyperelliptic curve cryptosystems. *Information Processing Letters*, 113(12):405–408, June 30, 2013. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013000914.

Fanyang:2012:SAK

[FXP12] Fanyang, Naixue Xiong, and Jong Hyuk Park. A self-adaptive K selection mechanism for re-authentication load balancing in large-scale systems. *The Journal of Supercomputing*, 61(1):166–188, July 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=1&spage=166.

Fu:2017:DFA

[FXP+17] Shan Fu, Guoai Xu, Juan Pan, Zongyue Wang, and An Wang. Differential fault attack on ITUbee block cipher. *ACM Transactions on Embedded Computing Systems*, 16(2):54:1–54:??, April 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Feng:2011:VBF

[FY11] Keqin Feng and Jing Yang. Vectorial Boolean functions with good cryptographic properties. *International Journal of Foundations of Computer Science (IJFCS)*, 22(6):1271–1282, September 2011. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Feng:2019:SHO

[FYD+19] J. Feng, L. T. Yang, G. Dai, W. Wang, and D. Zou. A secure high-order Lanczos-based orthogonal tensor SVD for big data reduction in cloud environment. *IEEE Transactions on Big Data*, 5(3):

355–367, September 2019. ISSN 2332-7790.

Fan:2015:IRD

[FYMY15] Xinyu Fan, Guomin Yang, Yi Mu, and Yong Yu. On indistinguishability in remote data integrity checking. *The Computer Journal*, 58(4):823–830, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/823.

Fyodorov:2019:SGM

[Fyo19] Yan V. Fyodorov. A spin glass model for reconstructing nonlinearly encrypted signals corrupted by noise. *Journal of Statistical Physics*, 175(5):789–818, June 2019. CODEN JSTPSB. ISSN 0022-4715 (print), 1572-9613 (electronic). URL http://link.springer.com/content/pdf/10.1007/s10955-018-02217-9.pdf.

Fan:2013:KIS

[FZT13] J. Fan, Y. Zheng, and X. Tang. Key-insulated signcryption. *J.UCS: Journal of Universal Computer Science*, 19(10):1351–??, ???? 2013. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL http://www.jucs.org/jucs_19_10/key_insulated_signcryption.

Fan:2014:NCI

[FZT14] Jia Fan, Yuliang Zheng, and Xiaohu Tang. A new construction of identity-based signcryption without random oracles. *International Journal of Foundations of Computer Science (IJFCS)*, 25(1):1–??, January 2014. CODEN IFCSEN. ISSN 0129-0541.

Fu:2012:EHA

[FZZ+12] Anmin Fu, Yuqing Zhang, Zhenchao Zhu, Qi Jing, and Jingyu Feng. An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network. *Computers & Security*, 31(6):741–749, September 2012. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404812001009.

GomezPardo:2013:ICM

[G´13] José Luis Gómez Pardo. *Introduction to Cryptography with Maple*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2013. ISBN 3-642-32165-8, 3-642-32166-6. xxx + 705 pp. LCCN QA76.9.A25 G66 2013. URL http://www.springerlink.com/content/978-3-642-32166-5.

Gross-Amblard:2011:QPW

[GA11] David Gross-Amblard. Query-preserving watermarking of relational databases and XML documents. *ACM Transactions on Database Systems*, 36(1):3:1–3:??, March 2011. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Grondahl:2019:TAA

[GA19] Tommi Gröndahl and N. Asokan. Text analysis in adversarial settings: Does deception leave a stylistic trace? *ACM Computing Surveys*, 52(3):45:1–45:??, July 2019. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3310331`.

Guimaraes:2019:OIQ

[GAB19] Antonio Guimarães, Diego F. Aranha, and Edson Borin. Optimized implementation of QC–MDPC code-based cryptography. *Concurrency and Computation: Practice and Experience*, 31(18):e5089:1–e5089:??, September 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Gregio:2015:TTM

[GAF+15] André Ricardo Abed Grégio, Vitor Monte Afonso, Dario Simões Fernandes Filho, Paulo Lício de Geus, and Mario Jino. Toward a taxonomy of malware behaviors. *The Computer Journal*, 58(10):2758–2777, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/10/2758`.

Gope:2018:LPP

[GAI+18] Prosanta Gope, Ruhul Amin, S. K. Hafizul Islam, Neeraj Kumar, and Vinod Kumar Bhalla. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Generation Computer Systems*, 83(??):629–637, June 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X17313043`.

Galindo:2013:NIC

[Gal13] David Galindo. A note on an IND-CCA2 secure Paillier-based cryptosystem. *Information Processing Letters*, 113(22–24):913–914, November/December 2013. CODEN IFPLAT. ISSN 0020-0190

(print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013002457.

Gasarch:2013:RBC

[Gas13] William Gasarch. Review of *Theoretical Computer Science: Introduction to Automata, Computability, Complexity, Algorithmics, Randomization, Communication, and Cryptography* by Juraj Hromkovic. *ACM SIGACT News*, 44(3):7–8, September 2013. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (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).

Ghoshal:2019:RSC

[GB19] Sucheta Ghoshal and Amy Bruckman. The role of social computing technologies in grassroots movement building. *ACM Transactions on Computer-Human Interaction*, 26(3): 18:1–18:??, June 2019. CODEN ATCIF4. ISSN 1073-0516 (print), 1557-7325 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3318140.

Gupta:2019:DRB

[GBC19] Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. DriverAuth: a risk-based multi-modal biometric-based driver authentication scheme for ride-sharing platforms. *Computers & Security*, 83(??):122–139, June 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818310113.

Gorantla:2011:MKC

[GBNM11] M. C. Gorantla, Colin Boyd, Juan Manuel González Nieto, and Mark Manulis. Modeling key compromise impersonation attacks on group key exchange protocols. *ACM Transactions on Information and System Security*, 14(4):28:1–28:??, December 2011. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Guyeux:2015:ECS

[GCH15] Christophe Guyeux, Raphaël Couturier, and Pierre-Cyrille Héam. Efficient and cryptographically secure generation of chaotic pseudorandom numbers on GPU. *The Journal of Supercomputing*, 71(10): 3877–3903, October 2015. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-015-1479-8.

Gao:2019:LBD

[GCH+19] Wen Gao, Liqun Chen, Yupu Hu, Christopher J. P. Newton, Baocang Wang, and Jiangshan Chen. Lattice-based deniable ring signatures. *International Journal of Information Security*, 18 (3):355–370, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0417-1; http://link.springer.com/content/pdf/10.1007/s10207-018-0417-1.pdf.

Gupta:2012:CDF

[GCK12] Swati Gupta, Seongho Cho, and C.-C. Jay Kuo. Current developments and future trends in audio authentication. *IEEE MultiMedia*, 19(1):50–59, January/March 2012. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Gupta:2013:HPH

[GCS+13] Sourav Sen Gupta, A. Chattopadhyay, K. Sinha, S. Maitra, and B. P. Sinha. High-performance hardware implementation for RC4 stream cipher. *IEEE Transactions on Computers*, 62(4):730–743, April 2013. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Guerra-Casanova:2011:SOT

[GCSÁddP11] J. Guerra-Casanova, C. Sánchez-Ávila, A. de Santos Sierra, and G. Bailador del Pozo. Score optimization and template updating in a biometric technique for authentication in mobiles based on gestures. *The Journal of Systems and Software*, 84 (11):2013–2021, November 2011. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211001427.

Granado-Criado:2017:HCH

[GCVR17] José M. Granado-Criado and Miguel A. Vega-Rodríguez. Hardware coprocessors for high-performance symmetric cryptography. *The Journal of Supercomputing*, 73 (6):2456–2482, June 2017. CODEN JOSUED. ISSN

0920-8542 (print), 1573-0484 (electronic).

Gong:2016:ATI

[GDCC16] Junqing Gong, Xiaolei Dong, Zhenfu Cao, and Jie Chen. Almost-tight identity based encryption against selective opening attack. *The Computer Journal*, 59(11):1669–1688, November 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/59/11/1669`.

Gao:2018:PRR

[GDLL18] Xinwei Gao, Jintai Ding, Lin Li, and Jiqiang Liu. Practical randomized RLWE-based key exchange against signal leakage attack. *IEEE Transactions on Computers*, 67(11):1584–1593, November 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `https://ieeexplore.ieee.org/document/8300634/`.

Guerin:2016:TDU

[GdM16] Nilson Donizete Guerin, Jr., Flavio de Barros Vidal, and Bruno Macchiavello. Text-dependent user verification of handwritten words and signatures on mobile devices. *The Computer Journal*, 59(9):1415–1425, September 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/59/9/1415`.

Giot:2011:UKD

[GEAHR11] Romain Giot, Mohamad El-Abed, Baptiste Hemery, and Christophe Rosenberger. Unconstrained keystroke dynamics authentication with shared secret. *Computers & Security*, 30(6–7):427–445, September/October 2011. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404811000502`.

Geller:2013:MIS

[Gel13] Tom Geller. Making the Internet safe for gadgets. *Communications of the Association for Computing Machinery*, 56(10):18–20, October 2013. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Gentry:2010:CAF

[Gen10] Craig Gentry. Computing arbitrary functions of encrypted data. *Communications of the Association for Computing Machinery*, 53(3):97–105, March 2010. CODEN CACMA2. ISSN

0001-0782 (print), 1557-7317 (electronic).

Gentry:2013:EMH

[Gen13] Craig Gentry. Encrypted messages from the heights of cryptomania. *Lecture Notes in Computer Science*, 7785:120–121, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/accesspage/chapter/10.1007/978-3-642-36594-2_7?coverImageUrl=/static/0.8699/sites/link/images/abstract_cover_placeholder.png`.

Gaspar:2012:SEF

[GFBF12] Lubos Gaspar, Viktor Fischer, Lilian Bossuet, and Robert Fouquet. Secure extension of FPGA general purpose processors for symmetric key cryptography with partial reconfiguration capabilities. *ACM Transactions on Reconfigurable Technology and Systems*, 5(3):16:1–16:??, October 2012. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Gong:2010:PCI

[GG10] Guang Gong and Kishan Chand Gupta, editors. *Progress in cryptology — Indocrypt 2010: 11th international conference on cryptology in India, Hyderabad, India, December 12–15, 2010. Proceedings*, volume 6498 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-17400-0 (softcover). LCCN ????

Grigg:2011:CCN

[GG11] Ian Grigg and Peter Gutmann. The curse of cryptographic numerology. *IEEE Security & Privacy*, 9(3): 70–72, May/June 2011. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Garg:2016:CIO

[GGH+16a] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. *SIAM Journal on Computing*, 45(3):882–929, ???? 2016. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Garg:2016:HSS

[GGH+16b] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Hiding secrets in software: a cryptographic approach to program obfuscation. *Communications of the Association for Computing Machinery*, 59(5):113–120, May 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2016/5/201597/fulltext.

Garg:2014:TRS

[GGHR14] Sanjam Garg, Craig Gentry, Shai Halevi, and Mariana Raykova. Two-round secure MPC from indistinguishability obfuscation. *Lecture Notes in Computer Science*, 8349:74–94, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_4/.

Garg:2017:IDI

[GGHW17] Sanjam Garg, Craig Gentry, Shai Halevi, and Daniel Wichs. On the implausibility of differing-inputs obfuscation and extractable witness encryption with auxiliary input. *Algorithmica*, 79(4):1353–1373, December 2017. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Gunleifsen:2018:TCP

[GGK18] Håkon Gunleifsen, Vasileios Gkioulos, and Thomas Kemmerich. A tiered control plane model for service function chaining isolation. *Future Internet*, 10 (6):46, June 04, 2018. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/10/6/46.

Gentry:2011:FHE

[GH11a] C. Gentry and S. Halevi. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits. In IEEE [IEE11b], pages 107–109. ISBN 1-4577-1843-X. LCCN ????

Gentry:2011:IGF

[GH11b] Craig Gentry and Shai Halevi. Implementing Gentry's fully-homomorphic encryption scheme. *Lecture Notes in Computer Science*, 6632:129–148, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_9.

Guo:2012:EBP

[GH12] Lifeng Guo and Lei Hu. Efficient bidirectional proxy re-encryption with direct chosen-ciphertext security. *Computers and Mathematics with Applications*, 63(1):151–157, January 2012. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122111009680.

Gentry:2013:EIF

[GH13] Craig B. Gentry and Shai Halevi. Efficient implementation of fully homomorphic encryption. US Patent 8,565,435., October 22, 2013. Filed 9 August 2011.

Gope:2015:RLA

[GH15] Prosanta Gope and Tzonelih Hwang. A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system. *Computers & Security*, 55(??):271–280, November 2015. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404815000681.

Gope:2016:EMA

[GH16] Prosanta Gope and Tzonelih Hwang. An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks. *Journal of Network and Computer Applications*, 62(??): 1–8, February 2016. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804515002969.

Genge:2019:ESA

[GHD19] Béla Genge, Piroska Haller, and Adrian-Vasile Duka. Engineering security-aware control applications for data authentication in smart industrial cyber-physical systems. *Future Generation Computer Systems*, 91(??):206–222, February 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X18303431.

Gordon:2011:CFS

[GHKL11] S. Dov Gordon, Carmit Hazay, Jonathan Katz, and Yehuda Lindell. Complete fairness in secure Two-Party computation. *Journal of the ACM*, 58 (6):24:1–24:??, December 2011. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Gentry:2012:RSB

[GHPS12] Craig Gentry, Shai Halevi, Chris Peikert, and Nigel P. Smart. Ring switching in BGV-style homomorphic encryption. *Lecture Notes in Computer Science*, 7485:19–37, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32928-9_2/.

Gentry:2013:FSB

[GHPS13] Craig Gentry, Shai Halevi, Chris Peikert, and Nigel P. Smart. Field switching in BGV-style homomorphic encryption. *Journal of Computer Security*, 21 (5):663–684, ???? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gentry:2012:FHE

[GHS12] Craig Gentry, Shai Halevi, and Nigel P. Smart. Fully homomorphic encryption with polylog overhead. *Lecture Notes in Computer Science*, 7237: 465–482, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_27; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_28/.

Gilad:2014:PHI

[GHS14] Yossi Gilad, Amir Herzberg, and Haya Shulman. Off-path hacking: The illusion of challenge–response authentication. *IEEE Security & Privacy*, 12(5): 68–77, September/October 2014. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://www.computer.org/csdl/mags/sp/2014/05/msp2014050068-abs.html.

Guo:2018:AFH

[GHY18] Qingwen Guo, Qiong Huang, and Guomin Yang. Authorized function homomorphic signature. *The Computer Journal*, 61(12): 1897–1908, December 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/12/1897/5158246.

Godor:2012:HBM

[GI12] Győző Gódor and Sándor Imre. Hash-based mutual authentication protocol for low-cost RFID systems. *Lecture Notes in Computer Science*, 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/.

Georgiev:2012:MDC

[GIJ+12] Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, and Vitaly Shmatikov. The most dangerous code in the world: Validating SSL certificates in non-browser software. In ????, editor, *ACM Conference on Computer and Communications Security*, page ?? ACM Press, New York, NY 10036, USA, 2012. ISBN ???? LCCN ???? URL ????.

Gilbert:2010:ACE

[Gil10] Henri Gilbert, editor. *Advances in cryptology — Eurocrypt 2010: 29th annual international conference on the theory and applications of cryptographic techniques, Monaco, May 30–June 3, 2010. Proceedings*, volume 6110 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-13189-1 (softcover). LCCN ????

Giry:2015:BCK

[Gir15] Damien Giry. Bluekrypt cryptographic key length recommendation. Web site, February 26, 2015. URL http://www.keylength.com/.

Gao:2013:LCA

[GJ13] Guangyong Gao and Guoping Jiang. A lossless copyright authentication scheme based on Bessel–Fourier moment and extreme learning machine in curvature-feature domain. *The Journal of Systems and Software*, 86(1):222–232, January 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212002270.

Guo:2019:NBT

[GJ19] Qian Guo and Thomas Johansson. A new birthday-type algorithm for attacking the fresh re-keying countermeasure. *Information Processing Letters*, 146 (??):30–34, June 2019. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019019300420.

Gu:2015:EIB

[GJJ15] Ke Gu, Weijia Jia, and Chunlin Jiang. Efficient identity-based proxy signature in the standard model. *The Computer Journal*, 58(4):792–807, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/792.

Geetha:2018:OVC

[GJJ18] P. Geetha, V. S. Jayanthi, and A. N. Jayanthi. Optimal visual cryptographic scheme with multiple share creation for multimedia applications. *Computers & Security*, 78(??):301–320, September 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818308241.

Gravier:2015:WOD

[GJMP15] Sylvain Gravier, Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. On weak odd domination and graph-based quantum secret sharing. *Theoretical Computer Science*, 598(??):129–137, September 20, 2015. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397515004806.

Goyal:2013:CZK

[GJO+13] Vipul Goyal, Abhishek Jain, Rafail Ostrovsky, Silas Richelson, and Ivan Visconti. Concurrent zero knowledge in the bounded player model. *Lecture Notes in Computer Science*, 7785:60–79, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_4/.

Gu:2017:IBM

[GJZ17] Ke Gu, Weijia Jia, and Jianming Zhang. Identity-based multi-proxy signature scheme in the standard model. *Fundamenta Informaticae*, 150(2):179–210, ???? 2017. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Geetha:2011:VRN

[GKCK11] S. Geetha, V. Kabilan, S. P. Chockalingam, and N. Kamaraj. Varying radix numeral system based adaptive image steganography. *Information Processing Letters*, 111(16):792–797, August 30, 2011. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019011001414.

Gunleifsen:2019:PCD

[GKG19] Håkon Gunleifsen, Thomas Kemmerich, and Vasileios Gkioulos. A proof-of-concept demonstration of isolated and encrypted service function chains. *Future Internet*, 11(9):183, August 24, 2019. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/11/9/183.

Garay:2016:MPA

[GKM16] Juan A. Garay, Vladimir Kolesnikov, and Rae Mclellan. MAC precomputation with applications to secure memory. *ACM Transactions on Privacy and Security (TOPS)*, 19(2):6:1–6:??, September 2016. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Grigoriev:2017:YMP

[GKS17] Dima Grigoriev, Laszlo B. Kish, and Vladimir Shpilrain. Yao's millionaires' problem and public-key encryption without computational assumptions. *International Journal of Foundations of Computer Science (IJFCS)*, 28(4):379–??, June 2017. CODEN IFCSEN. ISSN 0129-0541.

Gaj:2017:DCR

[GKSB17] Sibaji Gaj, Aditya Kanetkar, Arijit Sur, and Prabin Kumar Bora. Drift-compensated robust watermarking algorithm for H.265/HEVC video stream. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 13(1):11:1–11:??, January 2017. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Guo:2010:HMW

[GL10] Jing-Ming Guo and Yun-Fu Liu. Hiding multitone watermarks in halftone images. *IEEE MultiMedia*, 17 (1):65, January 2010. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Gouvea:2012:HSI

[GL12] Conrado P. L. Gouvêa and Julio López. High speed implementation of authenticated encryption for the MSP430X microcontroller. *Lecture Notes in Computer Science*, 7533: 288–304, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-33481-8_16/`.

Gu:2019:GRM

[GL19] Z. Gu and S. Li. A generalized RNS Mclaughlin modular multiplication with non-coprime moduli sets. *IEEE Transactions on Computers*, 68(11):1689–1696, November 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Glassey:2011:MIM

[Gla11] Olivier Glassey. Metadata for identity management of population registers. *Future Internet*, 3(2): 130–143, April 18, 2011. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/3/2/130`.

Guo:2018:KAA

[GLB+18] Cheng Guo, Ningqi Luo, Md Zakirul Alam Bhuiyan, Yingmo Jie, Yuanfang Chen, Bin Feng, and Muhammad Alam. Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage. *Future Generation Computer Systems*, 84(??):190–199, July 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17307926.

Gorawski:2012:EAS

[GLG12] Marcin Gorawski, Michal Lorek, and Michal Gorawski. Encrypted adaptive storage model — analysis and performance tests. *Lecture Notes in Computer Science*, 7449:118–128, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32287-7_10/.

Gligor:2012:SLT

[Gli12] Virgil Gligor. Street-level trust semantics for attribute authentication (transcript of discussion). *Lecture Notes in Computer Science*, 7622:116–125, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35694-0_13/.

Gollmann:2010:SCR

[GLIC10] Dieter Gollmann, Jean-Louis Lanet, and Julien Iguchi-Cartigny, editors. *Smart card research and advanced application: 9th IFIP WG 8.8/11.2 International Conference, CARDIS 2010, Passau, Germany, April 14–16, 2010: proceedings*, volume 6035 of *Lecture Notes in Computer Science*. Springer, Berlin, Germany, 2010. ISBN 3-642-12509-3 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.S62 C36 2010.

Ge:2016:DSR

[GLL16] Yongyong Ge, Yannan Li, and Zhusong Liu. Delegation of signing rights for emerging 5G networks. *Concurrency and Computation: Practice and Experience*, 28(4):1193–1203, March 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Guo:2018:PSC

[GLL+18] Yuyan Guo, Jiguo Li, Yang Lu, Yichen Zhang, and Futai Zhang. Provably secure certificate-based encryption with leakage resilience. *Theoretical Computer Science*, 711(??):1–10, February 8, 2018. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S030439751730748X`.

Gagne:2012:AVB

[GLLSN12] Martin Gagné, Pascal Lafourcade, Yassine Lakhnech, and Reihaneh Safavi-Naini. Automated verification of block cipher modes of operation, an improved method. *Lecture Notes in Computer Science*, 6888:23–31, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-27901-0_3/`.

Guo:2011:EDA

[GLM+11] Hua Guo, Zhoujun Li, Yi Mu, Fan Zhang, Chuankun Wu, and Jikai Teng. An efficient dynamic authenticated key exchange protocol with selectable identities. *Computers and Mathematics with Applications*, 61(9):2518–2527, May 2011. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122111001404`.

Gong:2016:HES

[GLM+16] Linming Gong, Shundong Li, Qing Mao, Daoshun Wang, and Jiawei Dou. A homomorphic encryption scheme with adaptive chosen ciphertext security but without random oracle. *Theoretical Computer Science*, 609 (part 1)(??):253–261, January 4, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397515008725`.

Gupta:2019:OIT

[GLM+19] Peeyush Gupta, Yin Li, Sharad Mehrotra, Nisha Panwar, Shantanu Sharma, and Sumaya Almanee. Obscure: information-theoretic oblivious and verifiable aggregation queries. *Proceedings of the VLDB Endowment*, 12(9):1030–1043, May 2019. CODEN ???? ISSN 2150-8097.

Gerault:2018:RAR

[GLMS18] David Gérault, Pascal Lafourcade, Marine Minier, and Christine Solnon. Revisiting AES related-key differential attacks with constraint programming. *Information Processing Letters*, 139(??):18–23, November 2018. CODEN

IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S002001901830139X.

Gradwohl:2010:SRC

[GLR10] R. Gradwohl, N. Livne, and A. Rosen. Sequential rationality in cryptographic protocols. In IEEE [IEE10], pages 623–632. ISBN 1-4244-8525-8. LCCN ???? URL http://ieeexplore.ieee.org/servlet/opac?punumber=5669376. IEEE Computer Society Order Number P4244.

Gradwohl:2013:SRC

[GLR13] Ronen Gradwohl, Noam Livne, and Alon Rosen. Sequential rationality in cryptographic protocols. *ACM Transactions on Economics and Computation*, 1(1):2:1–2:??, January 2013. CODEN ???? ISSN 2167-8375 (print), 2167-8383 (electronic).

Guo:2012:ETD

[GLW12] Teng Guo, Feng Liu, and ChuanKun Wu. On the equivalence of two definitions of visual cryptography scheme. *Lecture Notes in Computer Science*, 7232:217–227, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29101-2_15/.

Guo:2013:TVS

[GLW13] Teng Guo, Feng Liu, and ChuanKun Wu. Threshold visual secret sharing by random grids with improved contrast. *The Journal of Systems and Software*, 86(8):2094–2109, August 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121213000745.

Goyal:2011:SCP

[GM11] V. Goyal and H. K. Maji. Stateless cryptographic protocols. In IEEE [IEE11b], pages 678–687. ISBN 1-4577-1843-X. LCCN ????

Garmany:2013:PPR

[GM13a] Behrad Garmany and Tilo Müller. PRIME: Private RSA infrastructure for memory-less encryption. In *Proceedings of the 29th Annual Computer Security Applications Conference*, ACSAC '13, pages 149–158. ACM Press, New York, NY 10036, USA, 2013. ISBN 1-4503-2015-5.

Goglin:2013:KGS

[GM13b] Brice Goglin and Stéphanie Moreaud. KNEM: a generic and scalable kernel-assisted intra-node MPI communication framework. *Journal of Parallel and Distributed Computing*, 73(2):176–188, February 2013. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731512002316.

Gotzfried:2014:MAT

[GM14] Johannes Götzfried and Tilo Müller. Mutual authentication and trust bootstrapping towards secure disk encryption. *ACM Transactions on Information and System Security*, 17(2):6:1–6:??, November 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Gofman:2016:MBE

[GM16a] Mikhail I. Gofman and Sinjini Mitra. Multimodal biometrics for enhanced mobile device security. *Communications of the Association for Computing Machinery*, 59(4): 58–65, April 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2016/4/200169/fulltext.

Gueron:2016:HIA

[GM16b] Shay Gueron and Sanu Mathew. Hardware implementation of AES using area-optimal polynomials for composite-field representation $GF(2^4)^2$ of $GF(2^8)$. In Montuschi et al. [MSH+16], pages 112–117. ISBN 1-5090-1615-5. ISSN 1063-6889. LCCN QA76.9.C62 S95 2016. URL http://ieeexplore.ieee.org/servlet/opac?punumber=7562813.

Gonzalez-Manzano:2017:EHE

[GMdFPLC17] L. González-Manzano, José M. de Fuentes, P. Peris-Lopez, and C. Camara. Encryption by Heart (EbH) — using ECG for time-invariant symmetric key generation. *Future Generation Computer Systems*, 77(??):136–148, December 2017. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16307798.

Gonzalez-Manzano:2019:LUR

[GMDR19] Lorena Gonzalez-Manzano, Jose M. De Fuentes, and Arturo Ribagorda. Leveraging user-related Internet of Things for continuous authentication: a survey. *ACM Computing Surveys*, 52(3):53:1–53:??, July 2019. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://

`dl.acm.org/ft_gateway.cfm?id=3314023`.

Gunson:2011:UPS

[GMMJ11] Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, 30(4):208–220, June 2011. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404810001148`.

Giambruno:2015:GGB

[GMNS15] Laura Giambruno, Sabrina Mantaci, Jean Néraud, and Carla Selmi. A generalization of Girod's bidirectional decoding method to codes with a finite deciphering delay. *International Journal of Foundations of Computer Science (IJFCS)*, 26(6):733–??, September 2015. CODEN IFCSEN. ISSN 0129-0541.

Garcia-Martinez:2015:HEB

[GMOGCCC15] M. García-Martínez, L. J. Ontañón-García, E. Campos-Cantón, and S. Celikovský. Hyperchaotic encryption based on multi-scroll piecewise linear systems. *Applied Mathematics and Computation*, 270(??):413–424, November 1, 2015. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0096300315010929`.

Garcia-Morchon:2015:HCR

[GMRT+15] Oscar García-Morchón, Ronald Rietman, Ludo Tolhuizen, Domingo Gómez, and Jaime Gutiérrez. HIMMO: a collusion-resistant identity-based scheme for symmetric key generation. *ACM Communications in Computer Algebra*, 49(1):19, March 2015. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Guo:2011:ISS

[GMS11] Fuchun Guo, Yi Mu, and Willy Susilo. Improving security of q-SDH based digital signatures. *The Journal of Systems and Software*, 84(10):1783–1790, October 2011. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121211001233`.

Guo:2014:SAS

[GMSV14] Fuchun Guo, Yi Mu, Willy Susilo, and Vijay Varadharajan. Server-aided signature verification for lightweight devices. *The Computer Journal*, 57(4):481–493, April 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/57/4/481.full.pdf+html.

Gao:2014:URA

[GMSW14] Lijun Gao, Maode Ma, Yantai Shu, and Yuhua Wei. An ultralightweight RFID authentication protocol with CRC and permutation. *Journal of Network and Computer Applications*, 41(??):37–46, May 2014. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804513002269.

Good:2012:BTC

[GMT+12] Irving John Good, Donald Michie, G. (Geoffrey) Timms, James A. Reeds, Whitfield Diffie, and Judith Veronica Field, editors. *Breaking teleprinter ciphers at Bletchley Park: general report on Tunny with emphasis on statistical methods (1945)*. John Wiley and Sons, Inc., New York, NY, USA, 2012. ISBN 0-470-46589-1 (hardcover). cxi + 673 pp. LCCN D810.C88 G66 2015.

Groza:2017:LCL

[GMVV17] Bogdan Groza, Stefan Murvay, Anthony Van Herrewege, and Ingrid Verbauwhede. LiBrA–CAN: Lightweight broadcast authentication for controller area networks. *ACM Transactions on Embedded Computing Systems*, 16(3): 90:1–90:??, July 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Gardiner:2016:SML

[GN16] Joseph Gardiner and Shishir Nagaraja. On the security of machine learning in malware C&C detection: a survey. *ACM Computing Surveys*, 49(3):59:1–59:??, December 2016. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Gong:2012:KNF

[GNL12] Zheng Gong, Svetla Nikova, and Yee Wei Law. KLEIN: a new family of lightweight block ciphers. *Lecture Notes in Computer Science*, 7055:1–18, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-25286-0_1/.

Garay:2017:SIA

[GO17] Juan A. Garay and Rafail Ostrovsky. Special issue: Algorithmic tools in cryptography. *Algorithmica*, 79(4):985–986, December 2017. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL http://link.springer.com/content/pdf/10.1007/s00453-017-0368-3.pdf.

Goldreich:2019:PSF

[Gol19] Oded Goldreich, editor. *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*. ACM Press, New York, NY 10036, USA, October 2019. ISBN 1-4503-7266-X (hardcover), 1-4503-7266-X (paperback), 1-4503-7267-8 (e-pub). ISSN 2374-6777. xxxv + 800 pp. LCCN TK5102.94 .P767 2019.

Goodin:2012:CBS

[Goo12] Dan Goodin. Crypto breakthrough shows Flame was designed by world-class scientists: The spy malware achieved an attack unlike any cryptographers have seen before. Web document., June 7, 2012. URL http://arstechnica.com/security/2012/06/flame-crypto-breakthrough/.

Gope:2019:LLA

[Gop19] Prosanta Gope. LAAP: Lightweight anonymous authentication protocol for D2D-aided fog computing paradigm. *Computers & Security*, 86(??):223–237, September 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S016740481831160X.

Garcia:2012:ERP

[GOPB12] Sergio Sanchez Garcia, Ana Gomez Oliva, and Emilia Perez-Belleboni. Is Europe ready for a pan-European identity management system? *IEEE Security & Privacy*, 10(4): 44–49, July/August 2012. ISSN 1540-7993 (print), 1558-4046 (electronic).

Gorski:2010:CDS

[Gor10] Michael Gorski. *Cryptanalysis and design of symmetric primitives*. Ph.D. thesis (??), Bauhausuniversität, Weimar, Germany, 2010. vi + 146 pp.

Groth:2012:NTN

[GOS12] Jens Groth, Rafail Ostrovsky, and Amit Sahai. New techniques for noninteractive zero-knowledge. *Journal of the ACM*, 59(3): 11:1–11:??, June 2012. CODEN JACOAH. ISSN

0004-5411 (print), 1557-735X (electronic).

Glowacz:2017:IDW

[GP17] Andrzej Glowacz and Marcin Pietroń. Implementation of digital watermarking algorithms in parallel hardware accelerators. *International Journal of Parallel Programming*, 45(5):1108–1127, October 2017. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic).

Gong:2013:NOT

[GPLZ13] Longyan Gong, Jingxin Pan, Beibei Liu, and Shengmei Zhao. A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords. *Journal of Computer and System Sciences*, 79(1):122–130, February 2013. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000012001249.

Goodrich:2012:EVW

[GPN+12] Michael T. Goodrich, Charalampos Papamanthou, Duy Nguyen, Roberto Tamassia, Cristina Videira Lopes, Olga Ohrimenko, and Nikos Triandopoulos. Efficient verification of web-content searching through authenticated web crawlers. *Proceedings of the VLDB Endowment*, 5(10): 920–931, June 2012. CODEN ???? ISSN 2150-8097.

Genkin:2016:PKE

[GPP+16] Daniel Genkin, Lev Pachmanov, Itamar Pipman, Adi Shamir, and Eran Tromer. Physical key extraction attacks on PCs. *Communications of the Association for Computing Machinery*, 59(6):70–79, June 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2016/6/202646/fulltext.

Gottel:2019:SPE

[GPR+19] Christian Göttel, Rafael Pires, Isabelly Rocha, Sébastien Vaucher, Pascal Felber, Marcelo Pasin, and Valerio Schiavoni. Security, performance and energy trade-offs of hardware-assisted memory protection mechanisms. *arXiv.org*, ?? (??):1–11, June 26, 2019. URL https://arxiv.org/pdf/1903.04203.pdf.

Grossschadl:2012:EJI

[GPT12] Johann Großschädl, Dan Page, and Stefan Tillich. Efficient Java implementation of elliptic curve cryptography for J2ME-enabled mobile devices.

Lecture Notes in Computer Science, 7322:189–207, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-30955-7_17/`.

Genkin:2014:GYH

[GPT14] Daniel Genkin, Itamar Pipman, and Eran Tromer. Get your hands off my laptop: Physical side-channel key-extraction attacks on PCs. Report, Technion and Tel Aviv University, Tel Aviv, Israel, July 31, 2014. 25 pp. URL `http://www.cs.tau.ac.il/~tromer/handsoff/`.

Gonzalez-Pardo:2012:CID

[GPVCdBRO12] Antonio González-Pardo, Pablo Varona, David Camacho, and Francisco de Borja Rodriguez Ortiz. Communication by identity discrimination in bio-inspired multi-agent systems. *Concurrency and Computation: Practice and Experience*, 24(6):589–603, ???? 2012. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Gai:2017:SCI

[GQH17] Keke Gai, Meikang Qiu, and Houcine Hassan. Secure cyber incident analytics framework using Monte Carlo simulations for financial cybersecurity insurance in cloud computing. *Concurrency and Computation: Practice and Experience*, 29(7):??, April 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Ghatak:2019:IBS

[GR19a] Debolina Ghatak and Bimal K. Roy. An improved bound for security in an identity disclosure problem. *International Journal of Statistics and Probability*, 8(3): 24–??, ???? 2019. CODEN ???? ISSN 1927-7032 (print), 1927-7040 (electronic). URL `http://www.ccsenet.org/journal/index.php/ijsp/article/view/0/39033`.

Ghosal:2019:NPP

[GR19b] Purnata Ghosal and B. V. Raghavendra Rao. A note on parameterized polynomial identity testing using hitting set generators. *Information Processing Letters*, 151(??):Article 105839, November 2019. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S002001901930122X`.

Greengard:2011:MRM

[Gre11] Samuel Greengard. In

memoriam: Robert Morris, 1932–2011. *Communications of the Association for Computing Machinery*, 54(9):17, September 2011. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Green:2017:SSE

[Gre17] Matthew Green. The strange story of "extended random". Web news story, December 19, 2017. URL `https://blog.cryptographyengineering.com/2017/12/19/the-strange-story-of-extended-random/`. Discussion of suspected NSA-supported back door in the 2007 NIST standard for the Dual Elliptic-Curve default random number generator, and the associated RSA cryptographic library BSAFE. There is evidence that the back door exists in some older Canon laser printers.

Green:2019:RMC

[Gre19a] Frederic Green. Review of *Modern Cryptography and Elliptic Curves, A Beginner's Guide* by Thomas R. Shemanske. *ACM SIGACT News*, 50(2):12–14, June 2019. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Green:2019:RNT

[Gre19b] Frederic Green. Review of *Number Theory: an Introduction via the Density of Primes*, second edition. *ACM SIGACT News*, 50 (1):9–13, March 2019. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Grimes:2015:CCT

[Gri15] William Grimes. Cracking codes through the centuries. *New York Times*, ?? (??):??, February 4, 2015. CODEN NYTIAO. ISSN 0362-4331 (print), 1542-667X, 1553-8095.

Gibson-Robinson:2012:AAL

[GRL12] Thomas Gibson-Robinson and Gavin Lowe. Analysing applications layered on unilaterally authenticating protocols. *Lecture Notes in Computer Science*, 7140:164–181, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-29420-4_11/`.

Guo:2018:WBS

[GRRZ18] Jinyi Guo, Wei Ren, Yi Ren, and Tianqing Zhu. A watermark-based in-situ access control model for image big data. *Future Internet*, 10(8):69, July 29, 2018. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/10/8/69.

Gonzalez-Serrano:2018:SML

[GSAMCA18] Francisco-Javier González-Serrano, Adrián Amor-Martín, and Jorge Casamayón-Antón. Supervised machine learning using encrypted training data. *International Journal of Information Security*, 17(4): 365–377, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0381-1.

Gupta:2018:SCA

[GSAV18] Haritabh Gupta, Shamik Sural, Vijayalakshmi Atluri, and Jaideep Vaidya. A side-channel attack on smartphones: Deciphering key taps using built-in microphones. *Journal of Computer Security*, 26 (2):255–281, ???? 2018. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guha:2017:RTS

[GSC17] Krishnendu Guha, Debasri Saha, and Amlan Chakrabarti. Real-time SoC security against passive threats using crypsis behavior of geckos. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 13(3):41:1–41:??, May 2017. CODEN ???? ISSN 1550-4832 (print), 1550-4840 (electronic).

Guin:2016:FCS

[GSFT16] Ujjwal Guin, Qihang Shi, Domenic Forte, and Mark M. Tehranipoor. FORTIS: a comprehensive solution for establishing forward trust for protecting IPs and ICs. *ACM Transactions on Design Automation of Electronic Systems*, 21(4):63:1–63:??, September 2016. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Gutman:2016:EAF

[GSGM16] R. Gutman, C. J. Sammartino, T. C. Green, and B. T. Montague. Error adjustments for file linking methods using encrypted unique client identifier (eUCI) with application to recently released prisoners who are HIV+. *Statistics in Medicine*, 35 (1):115–129, January 15, 2016. CODEN SMEDDA. ISSN 0277-6715 (print), 1097-0258 (electronic).

Gong:2016:FSC

[GSN+16] Wei Gong, Ivan Stojmenovic, Amiya Nayak, Kebin Liu, and Haoxiang Liu. Fast and scalable counterfeits estimation for large-scale RFID systems. *IEEE/ACM Transactions on Networking*, 24(2):1052–1064, April 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Gierlichs:2012:ICD

[GST12] Benedikt Gierlichs, Jörn-Marc Schmidt, and Michael Tunstall. Infective computation and dummy rounds: Fault protection for block ciphers without check-before-output. *Lecture Notes in Computer Science*, 7533:305–321, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-33481-8_17/`.

Genkin:2013:RKE

[GST13] Daniel Genkin, Adi Shamir, and Eran Tromer. RSA key extraction via low-bandwidth acoustic cryptanalysis. Technical and web report, Technion and Tel Aviv University and Weizmann Institute of Science, Haifa and Tel Aviv, Israel, December 18, 2013. URL `http://www.cs.tau.ac.il/~tromer/acoustic/`; `http://www.tau.ac.il/~tromer/papers/acoustic-20131218.pdf`.

Ge:2016:KPA

[GSW+16] Chunpeng Ge, Willy Susilo, Jiandong Wang, Zhiqiu Huang, Liming Fang, and Yongjun Ren. A key-policy attribute-based proxy re-encryption without random oracles. *The Computer Journal*, 59(7):970–982, July 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/59/7/970`.

Gazi:2012:EOS

[GT12] Peter Gaži and Stefano Tessaro. Efficient and optimally secure key-length extension for block ciphers via randomized cascading. *Lecture Notes in Computer Science*, 7237:63–80, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-29011-4_6/`.

Gallin:2019:GFP

[GT19] G. Gallin and A. Tisserand. Generation of finely-pipelined GF(PP) multipliers for flexible curve based cryptography on FPGAs. *IEEE Transactions on Computers*, 68(11):1612–1622, November 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Gupta:2019:LAU

[GTSS19] Ankur Gupta, Meenakshi Tripathi, Tabish Jamil Shaikh, and Aakar Sharma. A lightweight anonymous user authentication and key establishment scheme for wearable devices. *Computer Networks (Amsterdam, Netherlands: 1999)*, 149(??):29–42, February 11, 2019. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128618304389.

Goodrich:2011:EAD

[GTT11] Michael T. Goodrich, Roberto Tamassia, and Nikos Triandopoulos. Efficient authenticated data structures for graph connectivity and geometric search problems. *Algorithmica*, 60(3):505–552, July 2011. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0178-4617&volume=60&issue=3&spage=505.

Grosse:2013:AS

[GU13] Eric Grosse and Mayank Upadhyay. Authentication at scale. *IEEE Security & Privacy*, 11(1): 15–22, January/February 2013. ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://www.computer.org/cms/Computer.org/ComputingNow/pdfs/AuthenticationAtScale.pdf.

Gueron:2016:MEG

[Gue16] Shay Gueron. Memory encryption for general-purpose processors. *IEEE Security & Privacy*, 14(6): 54–62, November/December 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/06/msp2016060054-abs.html.

Gupta:2015:GEM

[Gup15] Vinay Gupta. Guest eof: a machine for keeping secrets? *Linux Journal*, 2015(254):7:1–7:??, June 2015. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://dl.acm.org/ft_gateway.cfm?id=2807685.

Galindo:2014:LCL

[GV14a] David Galindo and Srinivas Vivek. Limits of a conjecture on a leakage-resilient cryptosystem. *Information Processing Letters*, 114(4): 192–196, April 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://

www.sciencedirect.com/science/article/pii/S0020019013002949.

Ghosh:2014:BBB

[GV14b] Santosh Ghosh and Ingrid Verbauwhede. BLAKE-512-based 128-bit CCA2 secure timing attack resistant McEliece cryptoprocessor. *IEEE Transactions on Computers*, 63(5):1124–1133, May 2014. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Gorbunov:2012:FEB

[GVW12] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Functional encryption with bounded collusions via multi-party computation. *Lecture Notes in Computer Science*, 7417: 162–179, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32009-5_11/.

Gorbunov:2015:ABE

[GVW15] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. *Journal of the ACM*, 62 (6):45:1–45:??, December 2015. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Greenberg:2014:GWB

[GW14] Joel Greenberg and Rosamond Welchman. *Gordon Welchman: Bletchley Park's architect of ultra intelligence*. Frontline Books, Barnsley, UK, 2014. ISBN 1-84832-752-8 (hardcover), 1-4738-3463-5 (e-book). xvi + 286 + 16 pp. LCCN TK5102.94 .G744 2014xeb. URL http://lib.myilibrary.com?id=943722.

Gebotys:2016:PCP

[GWM16] Catherine H. Gebotys, Brian A. White, and Edgar Mateos. Preaveraging and carry propagate approaches to side-channel analysis of HMAC-SHA256. *ACM Transactions on Embedded Computing Systems*, 15(1):4:1–4:??, February 2016. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Gao:2019:EUE

[GWP+19] Yang Gao, Wei Wang, Vir V. Phoha, Wei Sun, and Zhanpeng Jin. EarEcho: Using ear canal echo for wearable authentication. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 3(3):1–24, September 2019. CODEN ???? ISSN 2474-9567 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3351239.

Wang:2014:RAW

[gWpNyY+14] Xian gyang Wang, Pan pan Niu, Hong ying Yang, Yan Zhang, and Tian xiao Ma. A robust audio watermarking scheme using higher-order statistics in empirical mode decomposition domain. *Fundamenta Informaticae*, 130(4):467–490, October 2014. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Gao:2015:GCC

[GWWC15] Wei Gao, Guilin Wang, Xueli Wang, and Kefei Chen. Generic construction of certificate-based encryption from certificateless encryption revisited. *The Computer Journal*, 58(10):2747–2757, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2747.

Goh:2013:TOT

[GY13] Weihan Goh and Chai Kiat Yeo. Teaching an old TPM new tricks: Repurposing for identity-based signatures. *IEEE Security & Privacy*, 11(5):28–35, September/October 2013. ISSN 1540-7993 (print), 1558-4046 (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 Distributed Systems*, 30(6):1283–1297, June 2019. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Guo:2012:AKE

[GZ12] Yanfei Guo and Zhenfeng Zhang. Authenticated key exchange with entities from different settings and varied groups. *Lecture Notes in Computer Science*, 7496:276–287, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33272-2_18/.

Guo:2017:EMD

[GZH17] Jianting Guo, Peijia Zheng, and Jiwu Huang. An efficient motion detection and tracking scheme for encrypted surveillance videos. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 13(4):61:1–61:??, October 2017. CO-

DEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Gao:2012:RHC

[GZHD12] Xifeng Gao, Caiming Zhang, Yan Huang, and Zhigang Deng. A robust high-capacity affine-transformation-invariant scheme for watermarking 3D geometric models. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 8(2S):34:1–34:??, September 2012. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Guo:2018:SMK

[GZS+18] Ziqing Guo, Hua Zhang, Caijun Sun, Qiaoyan Wen, and Wenmin Li. Secure multi-keyword ranked search over encrypted cloud data for multiple data owners. *The Journal of Systems and Software*, 137(??):380–395, March 2018. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121217303011.

Gao:2019:VQS

[GZSW19] Pengfei Gao, Jun Zhang, Fu Song, and Chao Wang. Verifying and quantifying side-channel resistance of masked software implementations. *ACM Transactions on Software Engineering and Methodology*, 28(3):16:1–16:??, August 2019. CODEN ATSMER. ISSN 1049-331X (print), 1557-7392 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3330392.

Guo:2019:NTP

[GZXA19] Hui Guo, Zhenfeng Zhang, Jing Xu, and Ningyu An. Non-transferable proxy re-encryption. *The Computer Journal*, 62(4):490–506, April 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/4/490/5146175.

Ge:2013:SAP

[GZZ+13] Aijun Ge, Jiang Zhang, Rui Zhang, Chuangui Ma, and Zhenfeng Zhang. Security analysis of a privacy-preserving decentralized key-policy attribute-based encryption scheme. *IEEE Transactions on Parallel and Distributed Systems*, 24(11):2319–2321, November 2013. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Hernandez-Ardieta:2013:TSA

[HAGTdFR13] Jorge L. Hernandez-Ardieta,

Ana I. Gonzalez-Tablas, Jose M. de Fuentes, and Benjamin Ramos. A taxonomy and survey of attacks on digital signatures. *Computers & Security*, 34(??):67–112, May 2013. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404812001794.

Haigh:2017:HRC

[Hai17] Thomas Haigh. Historical reflections: Colossal genius: Tutte, Flowers, and a bad imitation of Turing. *Communications of the Association for Computing Machinery*, 60(1):29–35, January 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2017/1/211102/fulltext.

Hajiali:2019:PPA

[HAK19] Mahdi Hajiali, Maryam Amirmazlaghani, and Hossain Kordestani. Preventing phishing attacks using text and image watermarking. *Concurrency and Computation: Practice and Experience*, 31(13): e5083:1–e5083:??, July 10, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Hamamreh:2012:RPA

[Ham12] Rushdi Hamamreh. Routing path authentication in link-state routing protocols. *Network Security*, 2012(5):14–20, May 2012. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485812700375.

Hamlin:2017:NMC

[Ham17] Nathan Hamlin. Number in mathematical cryptography. *Open Journal of Discrete Mathematics*, 7(1):13–31, January 2017. ISSN 2161-7635 (print), 2161-7643 (electronic). URL http://www.scirp.org/Journal/PaperInformation.aspx?PaperID=73743.

Hamidi:2019:ADS

[Ham19] Hodjat Hamidi. An approach to develop the smart health using Internet of Things and authentication based on biometric technology. *Future Generation Computer Systems*, 91(??):434–449, February 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X18313517.

Hanyok:2012:EHH

[Han12] Robert J. Hanyok. *Eavesdropping on Hell: historical guide to Western communications intelligence and the Holocaust, 1939–1945*. Dover Publications, Inc., New York, NY, USA, second edition, 2012. ISBN 0-486-48127-1. xxi + 196 pp. LCCN D810.C88 H36 2012. URL `http://catdir.loc.gov/catdir/enhancements/fy1108/2011011467-d.html`; `http://www.loc.gov/catdir/enhancements/fy1318/2011011467-t.html`.

Harn:2013:GA

[Har13] Lein Harn. Group authentication. *IEEE Transactions on Computers*, 62 (9):1893–1898, September 2013. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Harrington:2014:GEF

[Har14] Surya Michael Harrington. *Google Earth forensics: using Google Earth geolocation in digital forensic investigations*. Elsevier, Amsterdam, The Netherlands, 2014. ISBN 0-12-800216-6. vii + 113 pp. LCCN ????

Hardesty:2015:BAC

[Har15] Larry Hardesty. A basis for all cryptography. *R&D Magazine*, ??(??):??, October 28, 2015. URL `http://www.rdmag.com/news/2015/10/basis-all-cryptography`.

Hardesty:2016:SUC

[Har16] Larry Hardesty. Secure, user-controlled cryptographic system developed. *Scientific Computing*, ??(??):??, March 22, 2016. URL `http://www.scientificcomputing.com/news/2016/03/secure-user-controlled-cryptographic-system-developed`.

Hastings:2016:SWS

[Has16] Max Hastings. *The Secret War: Spies, Ciphers, and Guerrillas 1939–1945*. Harper, New York, NY, 2016. ISBN 0-06-225927-X (hardcover), 0-06-225928-8 (paperback), 0-06-244156-6. xxvii + 610 + 32 pp. LCCN D810.S7 H365 2017.

Hayes:2013:NSA

[Hay13] Adrian Hayes. Network service authentication timing attacks. *IEEE Security & Privacy*, 11(2):80–82, March/April 2013. ISSN 1540-7993 (print), 1558-4046 (electronic).

Houmansadr:2013:BCN

[HB13] Amir Houmansadr and Nikita Borisov. BotMosaic: Collaborative network watermark for the detection of IRC-based botnets. *The Journal of Systems and Software*, 86(3):707–715, March 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212003068.

Hurlburt:2014:BBC

[HB14] G. F. Hurlburt and I. Bojanova. Bitcoin: Benefit or curse? *IT Professional*, 16 (3):10–15, May 2014. CODEN IPMAFM. ISSN 1520-9202 (print), 1941-045x (electronic).

Hetzelt:2017:SAE

[HB17] Felicitas Hetzelt and Robert Buhren. Security analysis of encrypted virtual machines. *ACM SIGPLAN Notices*, 52(7):129–142, July 2017. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Hernandez-Becerril:2016:GIS

[HBBRNM+16] Rogelio Adrian Hernandez-Becerril, Ariana Guadalupe Bucio-Ramirez, Mariko Nakano-Miyatake, Hector Perez-Meana, and Marco Pedro Ramirez-Tachiquin. A GPU implementation of secret sharing scheme based on cellular automata. *The Journal of Supercomputing*, 72 (4):1291–1311, April 2016. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-016-1646-6.

Han:2019:ABI

[HBC+19] Jinguang Han, Maoxuan Bei, Liqun Chen, Yang Xiang, Jie Cao, Fuchun Guo, and Weizhi Meng. Attribute-based information flow control. *The Computer Journal*, 62(8):1214–1231, August 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/8/1214/5488733.

He:2013:HEH

[HBCC13] Daojing He, Jiajun Bu, Sammy Chan, and Chun Chen. Handauth: Efficient handover authentication with conditional privacy for wireless networks. *IEEE Transactions on Computers*, 62(3):616–622, March 2013. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

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.

Hao:2012:SAM

[HC12] Feng Hao and Dylan Clarke. Security analysis of a multi-factor authenticated key exchange protocol. *Lecture Notes in Computer Science*, 7341:1–11, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31284-7_1/.

Hu:2017:ATE

[HC17] Jingwei Hu and Ray C. C. Cheung. Area-time efficient computation of Niederreiter encryption on QC-MDPC codes for embedded hardware. *IEEE Transactions on Computers*, 66(8):1313–1325, ???? 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/document/7862221/.

Hwang:2010:RIB

[HCC10] Min-Shiang Hwang, Song-Kong Chong, and Te-Yu Chen. DoS-resistant ID-based password authentication scheme using smart cards. *The Journal of Systems and Software*, 83 (1):163–172, January 2010. CODEN JSSODM. ISSN 0164-1212.

Hsu:2011:NLM

[HCCC11] Ching-Fang Hsu, Guo-Hua Cui, Qi Cheng, and Jing Chen. A novel linear multi-secret sharing scheme for group communication in wireless mesh networks. *Journal of Network and Computer Applications*, 34(2):464–468, March 2011. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S108480451000055X.

Hore:2012:IED

[HCDM12] Bijit Hore, Ee-Chien Chang, Mamadou H. Diallo, and Sharad Mehrotra. Indexing encrypted documents for supporting efficient keyword search. *Lecture Notes in Computer Science*, 7482:93–110, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32873-2_7/.

Hernandez-Castro:2012:MTA

[HCETPL+12] Julio Cesar Hernandez-Castro, Juan Manuel Estevez-Tapiador, Pedro Peris-Lopez, John A. Clark, and El-Ghazali Talbi. Metaheuristic traceability attack against SLMAP, an RFID lightweight authentication protocol.

International Journal of Foundations of Computer Science (IJFCS), 23(2): 543–553, February 2012. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Huang:2014:FOS

[HCL+14] Xinyi Huang, Xiaofeng Chen, Jin Li, Yang Xiang, and Li Xu. Further observations on smart-card-based password-authenticated key agreement in distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, 25(7):1767–1775, July 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Hsu:2011:WLC

[HCM11] Francis Hsu, Hao Chen, and Sridhar Machiraju. WebCallerID: Leveraging cellular networks for Web authentication. *Journal of Computer Security*, 19(5): 869–893, ???? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

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 Computer Science*, 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/`.

Huang:2018:BLD

[HCYZ18] Chenyu Huang, Huangxun Chen, Lin Yang, and Qian Zhang. BreathLive: Liveness detection for heart sound authentication with deep breathing. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2(1): 1–25, March 2018. CODEN ???? ISSN 2474-9567 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3191744`.

Hosny:2019:RCI

[HD19] Khalid M. Hosny and Mohamed M. Darwish. Resilient color image watermarking using accurate quaternion radial substituted Chebyshev moments. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 15(2): 46:1–46:??, June 2019. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3325193`.

Han:2013:RMA

[HDPC13] Song Han, Tharam Dillon, Vidy Potdar, and Elizabeth Chang. RFID mutual authentication protocols for tags and readers with and without a server. *International Journal of Computer Systems Science and Engineering*, 28(2):??, ???? 2013. CODEN CSSEEI. ISSN 0267-6192.

Heninger:2012:MYP

[HDWH12] Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Mining your Ps and Qs: Detection of widespread weak keys in network devices. In ????, editor, *Proceedings of the 21st USENIX Security Symposium, August 2012*, pages 205–220. USENIX, Berkeley, CA, USA, 2012. ISBN ???? LCCN ???? URL https://dl.acm.org/doi/10.5555/2362793.2362828; https://factorable.net/paper.html; https://factorable.net/weakkeys12.conference.pdf; https://factorable.net/weakkeys12.extended.pdf.

Heath:2015:HNS

[Hea15] Nick Heath. Hacking the Nazis: The secret story of the women who broke Hitler's codes. *TechRepublic*, ??(??):??, March 26, 2015. URL http://www.techrepublic.com/article/the-women-who-helped-crack-nazi-codes-at-bletchley-park/.

Hwang:2012:ABA

[HEC+12] Jung Yeon Hwang, Sungwook Eom, Ku-Young Chang, Pil Joong Lee, and DaeHun Nyang. Anonymity-based authenticated key agreement with full binding property. *Lecture Notes in Computer Science*, 7690:177–191, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35416-8_13/.

Hamad:2018:DWU

[HEK18] Safwat Hamad, Ahmed Elhadad, and Amal Khalifa. DNA watermarking using codon postfix technique. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 15(5):1605–1610, September 2018. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Hellegren:2017:HCD

[Hel17a] Z. Isadora Hellegren. A history of crypto-discourse: encryption as a site of struggles to define Internet freedom. *Internet Histories*, 1(4):285–311, 2017.

CODEN ???? ISSN 2470-1483. URL http://www.tandfonline.com/doi/full/10.1080/24701475.2017.1387466.

Hellman:2017:TLC

[Hel17b] Martin E. Hellman. Turing Lecture: Cybersecurity, nuclear security, Alan Turing, and illogical logic. *Communications of the Association for Computing Machinery*, 60(12):52–59, December 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL https://cacm.acm.org/magazines/2017/12/223042-cybersecurity-nuclear-security-alan-turing-and-illogical-logic.

Hanka:2011:DPK

[HEP+11] Oliver Hanka, Michael Eichhorn, Martin Pfannenstein, Jörg Eberspächer, and Eckehard Steinbach. A distributed public key infrastructure based on threshold cryptography for the HiiMap next generation Internet architecture. *Future Internet*, 3(1):14–30, February 01, 2011. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/3/1/14.

Hermelin:2010:MLC

[Her10] Miia Hermelin. *Multidimensional linear cryptanalysis*. Ph.D. thesis, Aalto-yliopiston teknillinen korkeakoulu, Espoo, Finland, 2010. 97 pp.

Herranz:2014:ABS

[Her14] Javier Herranz. Attribute-based signatures from RSA. *Theoretical Computer Science*, 527(??):73–82, March 27, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397514000772.

Herardian:2019:SUC

[Her19] R. Herardian. The soft underbelly of cloud security. *IEEE Security & Privacy*, 17(3):90–93, May/June 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Hess:2012:GJC

[Hes12] Florian Hess. Generalised Jacobians in cryptography and coding theory. *Lecture Notes in Computer Science*, 7369:1–15, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31662-3_1/.

Heys:2017:SCF

[Hey17] Howard M. Heys. Statistical cipher feedback of stream ciphers. *The*

Computer Journal, 60 (12):1839–1851, December 1, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/12/1839/3959607.

Harn:2014:MTS

[HF14a] Lein Harn and Miao Fuyou. Multilevel threshold secret sharing based on the Chinese Remainder Theorem. *Information Processing Letters*, 114(9):504–509, September 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019014000659.

Hoang:2014:IMD

[HF14b] Anh-Tuan Hoang and Takeshi Fujino. Intra-masking dual-rail memory on LUT implementation for SCA-resistant AES on FPGA. *ACM Transactions on Reconfigurable Technology and Systems*, 7(2):10:1–10:??, June 2014. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Hocking:2013:COU

[HFCR13] C. G. Hocking, S. M. Furnell, N. L. Clarke, and P. L. Reynolds. Cooperative user identity verification using an authentication aura. *Computers & Security*, 39 (part B)(??):486–502, November 2013. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404813001417.

Hastings:2016:WKR

[HFH16] Marcella Hastings, Joshua Fried, and Nadia Heninger. Weak keys remain widespread in network devices. In *IMC'16: Proceedings of the 2016 Internet Measurement Conference, November 2016*, pages 49–63. ACM Press, New York, NY 10036, USA, 2016.

Hintze:2019:CUR

[HFS+19] Daniel Hintze, Matthias Füller, Sebastian Scholz, Rainhard D. Findling, Muhammad Muaaz, Philipp Kapfer, Eckhard Koch, and René Mayrhofer. CORMORANT: Ubiquitous risk-aware multi-modal biometric authentication across mobile devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 3(3):1–23, September 2019. CODEN ???? ISSN 2474-9567 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3351243.

Huang:2016:EDP

[HFT16] Shi-Yuan Huang, Chun-I Fan, and Yi-Fan Tseng. Enabled/disabled predicate encryption in clouds. *Future Generation Computer Systems*, 62(??):148–160, September 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X15003921.

Hanocka:2019:APS

[HFW+19] Rana Hanocka, Noa Fish, Zhenhua Wang, Raja Giryes, Shachar Fleishman, and Daniel Cohen-Or. ALIGNet: Partial-shape agnostic alignment via unsupervised learning. *ACM Transactions on Graphics*, 38(1):1:1–1:??, February 2019. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3267347.

Heyse:2012:TOC

[HG12] Stefan Heyse and Tim Güneysu. Towards one cycle per bit asymmetric encryption: Code-based cryptography on reconfigurable hardware. *Lecture Notes in Computer Science*, 7428:340–355, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33027-8_20/.

Hibschman:2019:ISS

[HGOZ19] Joshua Hibschman, Darren Gergle, Eleanor O'Rourke, and Haoqi Zhang. Isopleth: Supporting sensemaking of professional Web applications to create readily available learning experiences. *ACM Transactions on Computer-Human Interaction*, 26(3):16:1–16:??, June 2019. CODEN ATCIF4. ISSN 1073-0516 (print), 1557-7325 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3310274.

Hua:2015:TSE

[HGT15] Guang Hua, J. Goh, and V. L. L. Thing. Time-spread echo-based audio watermarking with optimized imperceptibility and robustness. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 23(2):227–239, February 2015. CODEN ???? ISSN 2329-9290.

Han:2011:PEB

[HGWY11] Yiliang Han, Xiaolin Gui, Xuguang Wu, and Xiaoyuan Yang. Proxy encryption based secure multicast in wireless mesh networks. *Journal of Network and Computer Applications*, 34(2):469–477, March 2011. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804510000974.

Harn:2015:DTS

[HH15] Lein Harn and Ching-Fang Hsu. Dynamic threshold secret reconstruction and its application to the threshold cryptography. *Information Processing Letters*, 115(11):851–857, November 2015. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019015001106.

Hu:2016:EWS

[HH16] Changhui Hu and Lidong Han. Efficient wildcard search over encrypted data. *International Journal of Information Security*, 15(5):539–547, October 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0302-0.

Huber:2019:FCL

[HHAW19] Manuel Huber, Julian Horsch, Junaid Ali, and Sascha Wessel. Freeze and crypt: Linux kernel support for main memory encryption. *Computers & Security*, 86(??):420–436, September 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818310435.

Hammi:2018:BTD

[HHBS18] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, and Ahmed Serhrouchni. Bubbles of trust: a decentralized blockchain-based authentication system for IoT. *Computers & Security*, 78(??):126–142, September 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818300890.

Hayashi:2013:AEI

[HHH+13] Y.-I. Hayashi, Y. Hayashi, N. Homma, T. Mizuki, and T. Aoki. Analysis of electromagnetic information leakage from cryptographic devices with different physical structures. *IEEE Transactions on Electromagnetic Compatibility*, ??(??):1–10, 2013. CODEN IEMCAE. ISSN 0018-9375 (print), 1558-187X (electronic).

Huber:2014:TPW

[HHMK14] Stefan Huber, Martin Held, Peter Meerwald, and Roland Kwitt. Topologypreserving watermarking of vector graphics. *International Journal of Computational Geometry and Applications (IJCGA)*, 24(1): 61–??, March 2014. CODEN IJCAEV. ISSN 0218-1959.

Huang:2017:BBC

[HHP17] Jianye Huang, Qiong Huang, and Chunhua Pan. A black-box construction of strongly unforgeable signature scheme in the leakage setting. *International Journal of Foundations of Computer Science (IJFCS)*, 28(6):761–??, September 2017. CODEN IFCSEN. ISSN 0129-0541.

Haitner:2011:PRI

[HHR11] Iftach Haitner, Danny Harnik, and Omer Reingold. On the power of the randomized iterate. *SIAM Journal on Computing*, 40(6):1486–1528, ???? 2011. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sicomp/resource/1/smjcat/v40/i6/p1486_s1`.

Hong:2015:RSM

[HHS+15] Wien Hong, Gwoboa Horng, Chih-Wei Shiu, Tung-Shou Chen, and Yu-Chi Chen. Reversible steganographic method using complexity control and human visual system. *The Computer Journal*, 58(10):2583–2594, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/10/2583`.

Huang:2018:LRD

[HHS18] Jianye Huang, Qiong Huang, and Willy Susilo. Leakage-resilient dual-form signatures. *The Computer Journal*, 61(8):1216–1227, August 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/61/8/1216/5035762`.

Hinarejos:2015:MES

[HIDFGPC15] M. Francisca Hinarejos, Andreu Pere Isern-Deyà, Josep-Lluís Ferrer-Gomila, and Magdalena Payeras-Capellà. MC-2D: an efficient and scalable multi-coupon scheme. *The Computer Journal*, 58(4):758–778, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/4/758`.

Hao:2019:IDP

[HIJ+19] Y. Hao, T. Isobe, L. Jiao, C. Li, W. Meier, Y. Todo, and Q. Wang. Improved division property based cube attacks exploiting algebraic properties of Superpoly. *IEEE Transactions on Computers*, 68 (10):1470–1486, October 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Hinek:2010:CRV

[Hin10] M. Jason Hinek. *Cryptanalysis of RSA and its variants*. Chapman and Hall/CRC cryptography and network security. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 2010. ISBN 1-4200-7518-7 (hardcover). xviii + 268 pp. LCCN TK5102.94 .H56 2010.

Harb:2019:FIE

[HJ19] Salah Harb and Moath Jarrah. FPGA implementation of the ECC over GF(2^m) for small embedded applications. *ACM Transactions on Embedded Computing Systems*, 18(2):17:1–17:??, April 2019. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3310354`.

Hinkelmann:2011:CPA

[HJM+11] Markus Hinkelmann, Andreas Jakoby, Nina Moebius, Tiark Rompf, and Peer Stechert. A cryptographically t-private auction system. *Concurrency and Computation: Practice and Experience*, 23 (12):1399–1413, August 25, 2011. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Hasan:2014:TFL

[HK14a] O. Hasan and S. A. Khayam. Towards formal linear cryptanalysis using HOL4. *J.UCS: Journal of Universal Computer Science*, 20(2):193–??, ???? 2014. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL `http://www.jucs.org/jucs_20_2/towards_formal_linear_cryptanalysis`.

Hur:2014:SDR

[HK14b] Junbeom Hur and Kyungtae Kang. Secure data retrieval for decentralized disruption-tolerant military networks. *IEEE/ACM Transactions on Networking*, 22(1):16–26, February 2014. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Hasan:2017:UAF

[HK17] Ragib Hasan and Rasib Khan. Unified authentication factors and fuzzy service access using interaction provenance. *Comput-*

ers & Security, 67(??):211–231, June 2017. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404817300408.

Hussain:2018:PPP

[HK18] Siam Umar Hussain and Farinaz Koushanfar. P3: Privacy preserving positioning for smart automotive systems. *ACM Transactions on Design Automation of Electronic Systems*, 23(6):79:1–79:??, December 2018. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Hiemenz:2019:DSS

[HK19] Benedikt Hiemenz and Michel Krämer. Dynamic searchable symmetric encryption for storing geospatial data in the cloud. *International Journal of Information Security*, 18(3):333–354, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0414-4.

Hameed:2018:TFV

[HKA+18] Khizar Hameed, Abid Khan, Mansoor Ahmed, Alavalapati Goutham Reddy, and M. Mazhar Rathore. Towards a formally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks. *Future Generation Computer Systems*, 82(??):274–289, May 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17322756.

Handa:2019:SES

[HKA19] Rohit Handa, C. Rama Krishna, and Naveen Aggarwal. Searchable encryption: a survey on privacy-preserving search schemes on encrypted outsourced data. *Concurrency and Computation: Practice and Experience*, 31(17):e5201:1–e5201:??, September 10, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Houmansadr:2014:NBW

[HKB14] Amir Houmansadr, Negar Kiyavash, and Nikita Borisov. Non-blind watermarking of network flows. *IEEE/ACM Transactions on Networking*, 22(4):1232–1244, August 2014. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Hur:2013:REC

[HKHK13] Junbeom Hur, Dongyoung Koo, Seong Oun Hwang, and Kyungtae Kang. Removing escrow from ciphertext policy attribute-based encryption. *Computers and Mathematics with Applications*, 65(9):1310–1317, May 2013. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122112001198.

Hanzlik:2019:CPC

[HKK19] Lucjan Hanzlik, Kamil Kluczniak, and Mirosław Kutyłowski. CTRL-PACE: Controlled randomness for e-passport password authentication. *Fundamenta Informaticae*, 169(4):295–330, ???? 2019. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Heyse:2012:LEA

[HKL+12] Stefan Heyse, Eike Kiltz, Vadim Lyubashevsky, Christof Paar, and Krzysztof Pietrzak. Lapin: An efficient authentication protocol based on ring-LPN. *Lecture Notes in Computer Science*, 7549:346–365, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34047-5_20/.

Heil:2014:APH

[HKL+14] Timothy Heil, Anil Krishna, Nicholas Lindberg, Farnaz Toussi, and Steven Vanderwiel. Architecture and performance of the hardware accelerators in IBM's PowerEN processor. *ACM Transactions on Parallel Computing (TOPC)*, 1(1):5:1–5:??, September 2014. CODEN ???? ISSN 2329-4949 (print), 2329-4957 (electronic).

Howe:2018:PDG

[HKR+18] James Howe, Ayesha Khalid, Ciara Rafferty, Francesco Regazzoni, and Máire O'Neill. On practical discrete Gaussian samplers for lattice-based cryptography. *IEEE Transactions on Computers*, 67(3):322–334, ???? 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/document/7792671/.

Holenstein:2011:ERO

[HKT11] Thomas Holenstein, Robin Künzler, and Stefano Tessaro. The equivalence of the random oracle model and the ideal cipher model, revisited. In ACM [ACM11], pages 89–98. ISBN ???? LCCN

???? URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Harn:2010:AGK

[HL10a] L. Harn and Changlu Lin. Authenticated group key transfer protocol based on secret sharing. *IEEE Transactions on Computers*, 59(6):842–846, June 2010. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5416683.

Hazay:2010:EST

[HL10b] Carmit Hazay and Yehuda Lindell. *Efficient Secure Two-Party Protocols: Techniques and Constructions*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-14302-4 (hardcover), 3-642-14303-2 (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xiii + 263 + 1 pp. LCCN Z103 .H39 2010. URL http://www.springerlink.com/content/978-3-642-14303-8.

Hsu:2011:NIB

[HL11] Chien-Lung Hsu and Han-Yu Lin. New identity-based key-insulated convertible multi-authenticated encryption scheme. *Journal of Network and Computer Applications*, 34(5):1724–1731, September 2011. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804511001172.

Hsieh:2012:EHF

[HL12] Wen-Bin Hsieh and Jenq-Shiou Leu. Exploiting hash functions to intensify the remote user authentication scheme. *Computers & 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.

Hsieh:2014:AMU

[HL14] Wen-Bin Hsieh and Jenq-Shiou Leu. An anonymous mobile user authentication protocol using self-certified public keys based on multi-server architectures. *The Journal of Supercomputing*, 70(1):133–148, October 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-014-1135-8.

Hejun:2019:OAI

[HL19] Zhu Hejun and Zhu Liehuang.

Online and automatic identification of encryption network behaviors in big data environment. *Concurrency and Computation: Practice and Experience*, 31(12): e4849:1–e4849:??, June 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Hmood:2015:ACA

[HLAZ15] Haider Salim Hmood, Zhitang Li, Hasan Khalaf Abdulwahid, and Yang Zhang. Adaptive caching approach to prevent DNS cache poisoning attack. *The Computer Journal*, 58(4):973–985, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/4/973`.

Hu:2012:VMS

[HLC12] Chunqiang Hu, Xiaofeng Liao, and Xiuzhen Cheng. Verifiable multi-secret sharing based on LFSR sequences. *Theoretical Computer Science*, 445(1):52–62, August 3, 2012. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397512004276`.

Hu:2016:PBR

[HLC16] Yu-Chen Hu, Chun-Chi Lo, and Wu-Lin Chen. Probability-based reversible image authentication scheme for image demosaicking. *Future Generation Computer Systems*, 62(??):92–103, September 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X1630070X`.

Hu:2018:SVA

[HLC+18] C. Hu, W. Li, X. Cheng, J. Yu, S. Wang, and R. Bie. A secure and verifiable access control scheme for big data storage in clouds. *IEEE Transactions on Big Data*, 4(3): 341–355, September 2018. ISSN 2332-7790.

Hu:2019:AAA

[HLC+19] Yupu Hu, Zhizhu Lian, Jiangshan Chen, Baocang Wang, and Shanshan Zhang. Algebraic attacks against several weak variants of GVW 13 ABE. *International Journal of Foundations of Computer Science (IJFCS)*, 30(4): 607–618, June 2019. ISSN 0129-0541. URL `https://www.worldscientific.com/doi/10.1142/S012905411940015X`.

Huang:2011:ISL

[HLCL11] Y.-L. Huang, F.-Y. Leu, C.-H. Chiu, and I.-L. Lin. Improving security levels of IEEE802.16e authentication by involving Diffie–Hellman PKDS. *J.UCS: Journal of Universal Computer Science*, 17(6):891–??, ???? 2011. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL http://www.jucs.org/jucs_17_6/improving_security_levels_of.

Hwang:2019:ELS

[HLH19] Min-Shiang Hwang, Cheng-Chi Lee, and Shih-Ting Hsu. An ElGamal-like secure channel free public key encryption with keyword search scheme. *International Journal of Foundations of Computer Science (IJFCS)*, 30(2):??, February 2019. ISSN 0129-0541.

Huang:2015:MSE

[HLKL15] Chanying Huang, Hwaseong Lee, Hyoseung Kim, and Dong Hoon Lee. mvSERS: a secure emergency response solution for mobile healthcare in vehicular environments. *The Computer Journal*, 58(10):2461–2475, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2461.

Harn:2011:FDM

[HLLC11] Lein Harn, Chia-Yin Lee, Changlu Lin, and Chin-Chen Chang. Fully deniable message authentication protocols preserving confidentiality. *The Computer Journal*, 54 (10):1688–1699, October 2011. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/54/10/1688.full.pdf+html.

Han:2018:TSE

[HLLG18] Shuai Han, Shengli Liu, Lin Lyu, and Dawu Gu. Tightly secure encryption schemes against related-key attacks. *The Computer Journal*, 61(12): 1825–1844, December 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/12/1825/5067538.

Huffmire:2010:SPR

[HLN+10] Ted Huffmire, Timothy Levin, Thuy Nguyen, Cynthia Irvine, Brett Brotherton, Gang Wang, Timothy Sherwood, and Ryan Kastner. Security primitives for reconfigurable hardware-based systems. *ACM Transactions on Reconfigurable Technology and Systems*, 3(2):10:1–10:??, May 2010. CODEN ???? ISSN

1936-7406 (print), 1936-7414 (electronic).

Herranz:2011:RBS

[HLR11] Javier Herranz, Fabien Laguillaumie, and Carla Ràfols. Relations between semantic security and anonymity in identity-based encryption. *Information Processing Letters*, 111(10):453–460, April 30, 2011. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ham:2018:IYP

[HLS18] HyoungMin Ham, JongHyup Lee, and JooSeok Song. Improved yoking proof protocols for preserving anonymity. *International Journal of Information Security*, 17(4): 379–393, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0383-z.

Huang:2015:CEA

[HLT+15] Xinyi Huang, J. K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, and Jianying Zhou. Cost-effective authentic and anonymous data sharing with forward security. *IEEE Transactions on Computers*, 64(4):971–983, April 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Howard:2010:DSS

[HLV10] Michael Howard, David LeBlanc, and John Viega. *24 deadly sins of software security: programming flaws and how to fix them*. McGraw-Hill, New York, NY, USA, 2010. ISBN 0-07-162675-1. xxxvii + 393 pp. LCCN QA76.9.A25 H6977 2010.

Hohenberger:2012:DDQ

[HLW12] Susan Hohenberger, Allison Lewko, and Brent Waters. Detecting dangerous queries: a new approach for chosen ciphertext security. *Lecture Notes in Computer Science*, 7237:663–681, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_38; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_39/.

Huang:2014:SWC

[HLYS14] Yi-Li Huang, Fang-Yie Leu, Ilsun You, and Yao-Kuo Sun. A secure wireless communication system integrating RSA, Diffie–Hellman PKDS, intelligent protection-key chains and a

Data Connection Core in a 4G environment. *The Journal of Supercomputing*, 67 (3):635–652, March 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-013-0958-z.

Hefeeda:2010:ASM

[HM10] Mohamed Hefeeda and Kianoosh Mokhtarian. Authentication schemes for multimedia streams: Quantitative analysis and comparison. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 6(1):6:1–6:??, February 2010. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Herzberg:2012:TJA

[HM12] Amir Herzberg and Ronen Margulies. Training Johnny to authenticate (safely). *IEEE Security & Privacy*, 10(1):37–45, January/February 2012. ISSN 1540-7993 (print), 1558-4046 (electronic).

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).

Hore:2012:SMR

[HMCK12] Bijit Hore, Sharad Mehrotra, Mustafa Canim, and Murat Kantarcioglu. Secure multidimensional range queries over outsourced data. *VLDB Journal: Very Large Data Bases*, 21(3): 333–358, June 2012. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Hajihassani:2019:FAI

[HMKG19] O. Hajihassani, S. K. Monfared, S. H. Khasteh, and S. Gorgin. Fast AES implementation: A high-throughput bitsliced approach. *IEEE Transactions on Parallel and Distributed Systems*, 30(10): 2211–2222, October 2019. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Hoang:2012:ESB

[HMR12] Viet Tung Hoang, Ben Morris, and Phillip Rogaway. An enciphering scheme based on a card shuffle. *Lecture Notes in Computer Science*, 7417:1–13, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32009-5_1/.

Hirt:2014:BA

[HMR14] Martin Hirt, Ueli Maurer, and Pavel Raykov. Broadcast amplification. *Lecture Notes in Computer Science*, 8349:419–439, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_18/`.

Harnik:2010:CIC

[HN10] Danny Harnik and Moni Naor. On the compressibility of $\mathcal{NP}$ instances and cryptographic applications. *SIAM Journal on Computing*, 39(5):1667–1713, ???? 2010. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Hodgson:2019:SSC

[Hod19] Roderick Hodgson. Solving the security challenges of IoT with public key cryptography. *Network Security*, 2019(1):17–19, January 2019. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S135348581930011X`.

Hoffmann:2015:LBQb

[Hof15] Leah Hoffmann. Last byte: Q&A: A passion for pairings. *Communications of the Association for Computing Machinery*, 58(9):128–ff, September 2015. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2015/9/191171/fulltext`.

Hoffmann:2016:LBQb

[Hof16] Leah Hoffmann. Last byte: Q&A: Finding new directions in cryptography: Whitfield Diffie and Martin Hellman on their meeting, their research, and the results that billions use every day. *Communications of the Association for Computing Machinery*, 59(6):112–ff, June 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2016/6/202666/fulltext`.

Hollings:2012:CCE

[Hol12] Christopher Hollings. I, Claudius and the cipher extraordinary. *The Mathematical Gazette*, 96(537):466–470, November 2012. CODEN MAGAAS. ISSN 0025-5572.

Homer:2017:RCS

[Hom17] Steve Homer. Review of *Crypto School* by Joachim von zur Gathen. *ACM SIGACT News*, 48(3):10–13, September 2017. CODEN SIGNDM. ISSN

0163-5700 (print), 1943-5827 (electronic).

Horsman:2019:CPE

[Hor19] G. Horsman. A call for the prohibition of encryption: Panacea or problem? *IEEE Security & Privacy*, 17(2):59–66, March/April 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Hyla:2012:CBE

[HP12] Tomasz Hyla and Jerzy Pejaś. Certificate-based encryption scheme with general access structure. *Lecture Notes in Computer Science*, 7564:41–55, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-33260-9_3/`.

Hazay:2014:OSA

[HP14] Carmit Hazay and Arpita Patra. One-sided adaptively secure two-party computation. *Lecture Notes in Computer Science*, 8349:368–393, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_16/`.

Hyla:2017:HLS

[HP17] Tomasz Hyla and Jerzy Pejaś. A Hess-like signature scheme based on implicit and explicit certificates. *The Computer Journal*, 60(4):457–475, March 23, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `https://academic.oup.com/comjnl/article/60/4/457/2608054`.

Haigh:2018:CP

[HP18] Thomas Haigh and Mark Priestley. Colossus and programmability. *IEEE Annals of the History of Computing*, 40(4):5–27, October/December 2018. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic). URL `https://ieeexplore.ieee.org/document/8509146/`.

Halder:2010:WTR

[HPC10] R. Halder, S. Pal, and A. Cortesi. Watermarking techniques for relational databases: Survey, classification and comparison. *J.UCS: Journal of Universal Computer Science*, 16 (21):3164–??, ???? 2010. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL `http://www.jucs.org/jucs_16_21/watermarking_techniques_for_relational`.

He:2012:ECT

[HPC12] Debiao He, Sahadeo Padhye, and Jianhua Chen. An efficient certificateless two-party authenticated key agreement protocol. *Computers and Mathematics with Applications*, 64(6):1914–1926, September 2012. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122112002490`.

Hadlington:2019:ERW

[HPJ+19] Lee Hadlington, Masa Popovac, Helge Janicke, Iryna Yevseyeva, and Kevin Jones. Exploring the role of work identity and work locus of control in information security awareness. *Computers & Security*, 81(??):41–48, March 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404818308897`.

Hurrah:2019:DWF

[HPL+19] Nasir N. Hurrah, Shabir A. Parah, Nazir A. Loan, Javaid A. Sheikh, Mohammad Elhoseny, and Khan Muhammad. Dual watermarking framework for privacy protection and content authentication of multimedia. *Future Generation Computer Systems*, 94(??):654–673, May 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X18317096`.

Howe:2015:PLB

[HPO+15] James Howe, Thomas Pöppelmann, Máire O'Neill, Elizabeth O'Sullivan, and Tim Güneysu. Practical lattice-based digital signature schemes. *ACM Transactions on Embedded Computing Systems*, 14(3):41:1–41:??, April 2015. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Hoffstein:2008:IMC

[HPS08] Jeffrey Hoffstein, Jill Catherine Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*, volume 666 of *Undergraduate texts in mathematics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 0-387-77993-0 (hardcover). xv + 523 pp. LCCN QA268 .H64 2008.

Hur:2010:CCS

[HPY10] Junbeom Hur, Chanil Park, and Hyunsoo Yoon. Chosen ciphertext secure authenticated group communication using identity-based signcryption. *Computers and Mathematics with Applications*, 60(2): 362–375, July 2010. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122110000167.

Han:2016:GGA

[HQY+16] Jinsong Han, Chen Qian, Panlong Yang, Dan Ma, Zhiping Jiang, Wei Xi, and Jizhong Zhao. GenePrint: generic and accurate physical-layer identification for UHF RFID tags. *IEEE/ACM Transactions on Networking*, 24(2):846–858, April 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Han:2018:BEI

[HQY+18] Jinsong Han, Chen Qian, Yuqin Yang, Ge Wang, Han Ding, Xin Li, and Kui Ren. Butterfly: Environment-independent physical-layer authentication for passive RFID. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2(4):1–21, December 2018. CODEN ???? ISSN 2474-9567 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3287044.

Han:2014:GTK

[HQZH14] Fei Han, Jing Qin, Huawei Zhao, and Jiankun Hu. A general transformation from KP-ABE to searchable encryption. *Future Generation Computer Systems*, 30(??):107–115, January 2014. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X13001921.

He:2013:GME

[HR13] Q. Y. He and M. D. Reid. Genuine multipartite Einstein–Podolsky–Rosen steering. *Physical Review Letters*, 111(25): 250403, December 2013. CODEN PRLTAO. ISSN 0031-9007 (print), 1079-7114 (electronic), 1092-0145. URL http://link.aps.org/doi/10.1103/PhysRevLett.111.250403; http://www.scientificcomputing.com/news/2014/03/einsteins-entanglement-produces-quantum-encryption; http://www.swinburne.edu.au/engineering/caous/news_and_events/mulitipartite%20EPR%20steering%20paper.htm.

Hisil:2019:KLF

[HR19] Huseyin Hisil and Joost Renes. On Kummer lines with full rational 2-torsion and their usage in cryptography. *ACM Transactions on Mathematical Software*, 45(4):39:1–39:17, December 2019. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL https://dl.acm.org/citation.cfm?id=3361680.

Hulsing:2013:OPX

[HRB13] Andreas Hülsing, Lea Rausch, and Johannes Buchman. Optimal parameters for XMSS^{MT}. *Lecture Notes in Computer Science*, 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.

Huang:2014:AFS

[HREJ14] Lin-Shung Huang, Alex Rice, Erling Ellingsen, and Collin Jackson. Analyzing forged SSL certificates in the wild. In ????, editor, *IEEE Symposium on Security and Privacy*, page ?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2014. ISBN ???? LCCN ???? URL ????.

Hussain:2018:SSH

[HRK18] Siam Umar Hussain, M. Sadegh Riazi, and Farinaz Koushanfar. SHAIP: Secure Hamming Distance for Authentication of Intrinsic PUFs. *ACM Transactions on Design Automation of Electronic Systems*, 23(6):75:1–75:??, December 2018. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Herranz:2013:SMS

[HRS13] Javier Herranz, Alexandre Ruiz, and Germán Sáez. Sharing many secrets with computational provable security. *Information Processing Letters*, 113(14–16):572–579, July/August 2013. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013001373.

Hulsing:2016:MMT

[HRS16] Andreas Hülsing, Joost Rijneveld, and Fang Song. Mitigating multi-target attacks in hash-based signatures. *Lecture Notes in Computer Science*, 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.

Haitner:2010:EIC

[HRV10] Iftach Haitner, Omer Reingold, and Salil Vadhan.

Efficiency improvements in constructing pseudorandom generators from one-way functions. In ACM [ACM10], pages 437–446. ISBN 1-60558-817-2. LCCN QA 76.6 .A152 2010. URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Hwang:2011:CDA

[HS11] Shin-Jia Hwang and Yun-Hao Sung. Confidential deniable authentication using promised signcryption. *The Journal of Systems and Software*, 84(10):1652–1659, October 2011. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211000999.

Hubballi:2018:NTC

[HS18] Neminath Hubballi and Mayank Swarnkar. BitCoding: Network traffic classification through encoded bit level signatures. *IEEE/ACM Transactions on Networking*, 26(5):2334–2346, October 2018. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Homma:2014:TFD

[HSA14] N. Homma, K. Saito, and T. Aoki. Toward formal design of practical cryptographic hardware based on Galois field arithmetic. *IEEE Transactions on Computers*, 63 (10):2604–2613, October 2014. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Hall:2019:BIA

[HSC19] Calum C. Hall, Lynsay A. Shepherd, and Natalie Coull. BlackWatch: Increasing attack awareness within Web applications. *Future Internet*, 11(2):44, February 15, 2019. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/11/2/44.

Halevi:2011:TBH

[HSH11] Tzipora Halevi, Nitesh Saxena, and Shai Halevi. Tree-based HB protocols for privacy-preserving authentication of RFID tags. *Journal of Computer Security*, 19(2):343–363, ???? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Han:2013:IBD

[HSM13] Jinguang Han, Willy Susilo, and Yi Mu. Identity-based data storage in cloud computing. *Future Generation Computer Systems*, 29(3): 673–681, March 2013. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X12001719.

Han:2014:IBS

[HSM14] Jinguang Han, Willy Susilo, and Yu Mu. Identity-based secure distributed data storage schemes. *IEEE Transactions on Computers*, 63(4):941–953, April 2014. CODEN ITCOB4. ISSN 0018-9340.

Han:2012:PPD

[HSMY12] Jinguang Han, Willy Susilo, Yi Mu, and Jun Yan. Privacy-preserving decentralized key-policy attribute-based encryption. *IEEE Transactions on Parallel and Distributed Systems*, 23(11):2150–2162, November 2012. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Heather:2014:CPE

[HST14] James Heather, Steve Schneider, and Vanessa Teague. Cryptographic protocols with everyday objects. *Formal Aspects of Computing*, 26(1):37–62, January 2014. CODEN FACME5. ISSN 0934-5043 (print), 1433-299X (electronic). URL http://link.springer.com/article/10.1007/s00165-013-0274-7.

Ho:2011:EIB

[HSUS11] Chen-Han Ho, Garret Staus, Aaron Ulmer, and Karthikeyan Sankaralingam. Exploring the interaction between device lifetime reliability and security vulnerabilities. *IEEE Computer Architecture Letters*, 10(2):37–40, July/December 2011. CODEN ????. ISSN 1556-6056 (print), 1556-6064 (electronic).

Shi:2015:CTS

[hSZZ15] Run hua Shi, Hong Zhong, and Shun Zhang. Comments on two schemes of identity-based user authentication and key agreement for mobile client-server networks. *The Journal of Supercomputing*, 71 (11):4015–4018, November 2015. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-015-1496-7.

Hamdy:2011:HPB

[HT11] Omar Hamdy and Issa Traoré. Homogeneous physio-behavioral visual and mouse-based biometric. *ACM Transactions on Computer-Human Interaction*, 18(3):12:1–12:??, July 2011. CODEN ATCIF4. ISSN 1073-0516.

Henson:2013:MES

[HT13] Michael Henson and Stephen Taylor. Memory encryption: a survey of existing techniques. *ACM Computing Surveys*, 46(4):53:1–53:??, March 2013. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Hu:2010:TTW

[HTC+10] Wen Hu, Hailun Tan, Peter Corke, Wen Chan Shih, and Sanjay Jha. Toward trusted wireless sensor networks. *ACM Transactions on Sensor Networks*, 7(1): 5:1–5:??, August 2010. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Huang:2015:PAP

[HTC+15] Kaibin Huang, Raylin Tso, Yu-Chi Chen, Sk Md Mizanur Rahman, Ahmad Almogren, and Atif Alamri. PKE-AET: Public key encryption with authorized equality test. *The Computer Journal*, 58 (10):2686–2697, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2686.

Huang:2017:SSS

[HTC17] Kaibin Huang, Raylin Tso, and Yu-Chi Chen. Somewhat semantic secure public key encryption with filtered-equality-test in the standard model and its extension to searchable encryption. *Journal of Computer and System Sciences*, 89(??):400–409, November 2017. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000017300831.

Herbert:2012:SMP

[HTZR12] Matthias Herbert, Tobias Thieme, Jan Zibuschka, and Heiko Roßnagel. Secure mashup-providing platforms — implementing encrypted wiring. *Lecture Notes in Computer Science*, 7059:99–108, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27997-3_9/.

Hald:2015:RRA

[HU15] David Hald and Alex Udakis. Rethinking remote authentication: time to kiss tokens goodbye? *Network Security*, 2015(6):15–17, June 2015. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485815300507.

Hulsing:2013:WOS

[Hül13] Andreas Hülsing. W-OTS+ — shorter signatures for hash-based signature scheme. *Lecture Notes in Computer Science*, 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.

Hurlburt:2016:MBO

[Hur16] G. Hurlburt. Might the blockchain outlive Bitcoin? *IT Professional*, 18(2):12–16, March 2016. CODEN IPMAFM. ISSN 1520-9202 (print), 1941-045x (electronic).

Hammerle-Uhl:2011:RWI

[HURU11] Jutta Hämmerle-Uhl, Karl Raab, and Andreas Uhl. Robust watermarking in iris recognition: application scenarios and impact on recognition performance. *ACM SIGAPP Applied Computing Review*, 11(3):6–18, August 2011. CODEN ???? ISSN 1559-6915 (print), 1931-0161 (electronic). URL https://dl.acm.org/doi/abs/10.1145/2034594.2034595.

Harvey:2017:FPM

[HVL17] David Harvey, Joris Van Der Hoeven, and Grégoire Lecerf. Faster polynomial multiplication over finite fields. *Journal of the ACM*, 63(6):52:1–52:??, February 2017. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Hunger:2018:DDC

[HVP+18] Casen Hunger, Lluis Vilanova, Charalampos Papamanthou, Yoav Etsion, and Mohit Tiwari. DATS — data containers for Web applications. *ACM SIGPLAN Notices*, 53(2):722–736, February 2018. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Han:2012:MIA

[HvS12] Fengling Han and Ron van Schyndel. M-identity and its authentication protocol for secure mobile commerce applications. *Lecture Notes in Computer Science*, 7672:1–10, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35362-8_1/.

Hammad:2019:PSF

[HW19] Mohamed Hammad and Kuanquan Wang. Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network. *Computers & Security*, 81(??):107–122, March 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404818308411`.

Hwang:2011:NIB

[Hwa11] Jung Yeon Hwang. A note on an identity-based ring signature scheme with signer verifiability. *Theoretical Computer Science*, 412(8–10):796–804, March 4, 2011. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Holbl:2010:TPI

[HWB10] Marko Hölbl, Tatjana Welzer, and Bostjan Brumen. Two proposed identity-based three-party authenticated key agreement protocols from pairings. *Computers & Security*, 29(2):244–252, March 2010. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S016740480900090X`.

Holbl:2012:ITP

[HWB12] Marko Hölbl, Tatjana Welzer, and Bostjan Brumen. An improved two-party identity-based authenticated key agreement protocol using pairings. *Journal of Computer and System Sciences*, 78(1):142–150, January 2012. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0022000011000031`.

He:2016:STI

[HWDL16] Kai He, Jian Weng, Robert H. Deng, and Joseph K. Liu. On the security of two identity-based conditional proxy re-encryption schemes. *Theoretical Computer Science*, 652(??):18–27, November 1, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397516304443`.

Heng:2010:CNS

[HWG10] Swee-Huay Heng, Rebecca N. Wright, and Bok-Min Goi, editors. *Cryptology and network security: 9th international conference, CANS 2010, Kuala Lumpur, Malaysia, December 12–14, 2010. Proceedings*, volume 6467 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-17618-6 (softcover). LCCN ????

He:2015:SSQ

[HWK+15] Zhian He, Wai Kit Wong, Ben Kao, David Wai Lok Cheung, Rongbin Li, Siu Ming Yiu, and Eric Lo. SDB: a secure query processing system with data interoperability. *Proceedings of the VLDB Endowment*, 8(12): 1876–1879, August 2015. CODEN VLDBFR. ISSN 2150-8097.

Hong:2019:MCP

[HWS+19] Haibo Hong, Licheng Wang, Jun Shao, Jianhua Yan, Haseeb Ahmad, Guiyi Wei, Mande Xie, and Yixian Yang. A miniature CCA public key encryption scheme based on non-abelian factorization problem in finite groups of Lie type. *The Computer Journal*, 62(12):1840–1848, December 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/62/12/1840/5627776`.

Hsu:2014:VWR

[HWYW14] Fu-Hau Hsu, Min-Hao Wu, Cheng-Hsing Yang, and Shiuh-Jeng Wang. Visible watermarking with reversibility of multimedia images for ownership declarations. *The Journal of Supercomputing*, 70(1): 247–268, October 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://link.springer.com/article/10.1007/s11227-014-1258-y`.

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:2019:AIA

[HWZZ19] Anna Huang, Dong Wang, Run Zhao, and Qian Zhang. Au-Id: Automatic user identification and authentication through the motions captured from sequential human activities using RFID. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 3(2): 1–26, June 2019. CODEN ???? ISSN 2474-9567 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3328919`.

Huang:2011:GFT

[HXC+11] Xinyi Huang, Yang Xiang, Ashley Chonka, Jianying Zhou, and Robert H. Deng. A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, 22(8): 1390–1397, August 2011. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

He:2017:APP

[HXHP17] Jingsha He, Qi Xiao, Peng He, and Muhammad Salman Pathan. An adaptive privacy protection method for smart home environments using supervised learning. *Future Internet*, 9(1):7, March 05, 2017. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/9/1/7.

Huang:2018:PIB

[HYF18] Qinlong Huang, Yixian Yang, and Jingyi Fu. PRECISE: Identity-based private data sharing with conditional proxy re-encryption in online social networks. *Future Generation Computer Systems*, 86(??): 1523–1533, September 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17310257.

Hu:2019:CAC

[HYL+19] Chengyu Hu, Rupeng Yang, Pengtao Liu, Tong Li, and Fanyu Kong. A countermeasure against cryptographic key leakage in cloud: public-key encryption with continuous leakage and tampering resilience. *The Journal of Supercomputing*, 75(6):3099–3122, June 2019. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Hao:2011:NTV

[HYS11] Rong Hao, Jia Yu, and Zhiling Song. A note on a threshold verifiable multi-secret sharing scheme. *International Journal of Computer Applications*, 33(4):330–334, 2011. ISSN 1206-212X (print), 1925-7074 (electronic). URL https://www.tandfonline.com/doi/full/10.2316/Journal.202.2011.4.202-3074.

Huang:2018:CT

[HYS18] Qinlong Huang, Yixian Yang, and Mansuo Shen. Corrigendum to "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing" [Future Gener. Comput. Syst. **72** (2017) 239–249]. *Future Generation Computer Systems*, 86(??):1534, September 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X18312238. See [?].

Huang:2011:IBS

[HYWS11] Qiong Huang, Guomin Yang, Duncan S. Wong, and Willy Susilo. Identity-based strong designated verifier signature revisited. *The Journal of Systems and Software*, 84(1):120–129, January 2011. CODEN JSSODM. ISSN 0164-1212.

Heys:2011:PSC

[HZ11] Howard M. Heys and Liang Zhang. Pipelined statistical cipher feedback: a new mode for high-speed self-synchronizing stream encryption. *IEEE Transactions on Computers*, 60 (11):1581–1595, November 2011. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5499465.

Han:2012:ERI

[HZC+12] Qi Han, Yinghui Zhang, Xiaofeng Chen, Hui Li, and Jiaxiang Quan. Efficient and robust identity-based handoff authentication in wireless networks. *Lecture Notes in Computer Science*, 7645:180–191, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34601-9_14/.

Han:2014:ERI

[HZC+14] Qi Han, Yinghui Zhang, Xiaofeng Chen, Hui Li, and Jiaxiang Quan. Efficient and robust identity-based handoff authentication for EAP-based wireless networks. *Concurrency and Computation: Practice and Experience*, 26(8): 1561–1573, June 10, 2014. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Han:2018:ERA

[HZL18] Qi Han, Yinghui Zhang, and Hui Li. Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things. *Future Generation Computer Systems*, 83(??):269–277, June 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X1731868X.

Huang:2019:ILA

[HZS+19] Bo-Yuan Huang, Hongce Zhang, Pramod Subramanyan, Yakir Vizel, Aarti Gupta, and Sharad Malik. Instruction-level abstraction (ILA): a uniform specification for system-on-chip (SoC) verification. *ACM Transactions on Design Automation of Electronic Systems*, 24(1):10:1–10:??, January 2019. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Huang:2005:EMP

[HZSL05] Liusheng Huang, Hong Zhong, Hong Shen, and Yonglong Luo. An efficient multiple-precision division algorithm. In Hong Shen and Koji Nakano, editors, *Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2005. PDCAT 2005: 5–8 December 2005, Dalian, China*, pages 971–974. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2005. ISBN 0-7695-2405-2. LCCN QA76.58 .I5752 2005. The authors present an integer-division algorithm that runs three to five times faster than Knuth's 1981 original. However, there is an error in the renormalization algorithm that is corrected in [MN14], while retaining the speedup.

Han:2014:ATS

[HZW+14] Tao Han, Weiming Zhang, Chao Wang, Nenghai Yu, and Yuefei Zhu. Adaptive ±1 steganography in extended noisy region. *The Computer Journal*, 57(4):557–566, April 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/57/4/557.full.pdf+html`.

Hammad:2019:NTD

[HZW19] Mohamed Hammad, Shanzhuo Zhang, and Kuanquan Wang. A novel two-dimensional ECG feature extraction and classification algorithm based on convolution neural network for human authentication. *Future Generation Computer Systems*, 101(??):180–196, December 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X18329923`.

He:2017:AHA

[HZWW17] Debiao He, Sherali Zeadally, Libing Wu, and Huaqun Wang. Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography. *Computer Networks (Amsterdam, Netherlands: 1999)*, 128(??):154–163, December 9, 2017. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128616304285`.

He:2018:LAB

[HZWZ18] Qian He, Ning Zhang, Yongzhuang Wei, and Yan Zhang. Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems. *Computer Networks (Amsterdam, Netherlands: 1999)*, 140(??):163–173, July 20, 2018. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128618300458`.

He:2015:IEI

[HZX15] Debiao He, Mingwu Zhang, and Baowen Xu. Insecurity of an efficient identity-based proxy signature in the standard model. *The Computer Journal*, 58(10):2507–2508, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/10/2507`.

Hunt:2018:RDS

[HZX+18] Tyler Hunt, Zhiting Zhu, Yuanzhong Xu, Simon Peter, and Emmett Witchel. Ryoan: a distributed sandbox for untrusted computation on secret data. *ACM Transactions on Computer Systems*, 35(4):13:1–13:??, December 2018. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3231594`.

Islam:2015:MBA

[IA15] Md Saiful Islam and Naif Alajlan. Model-based alignment of heartbeat morphology for enhancing human recognition capability. *The Computer Journal*, 58(10):2622–2635, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/10/2622`.

Ibrahim:2019:RAM

[IAA+19] Tahir Musa Ibrahim, Shafi'i Muhammad Abdulhamid, Ala Abdusalam Alarood, Haruna Chiroma, Mohammed Ali Al-garadi, Nadim Rana, Amina Nuhu Muhammad, Adamu Abubakar, Khalid Haruna, and Lubna A. Gabralla. Recent advances in mobile touch screen security authentication methods: a systematic literature review. *Computers & Security*, 85(??):1–24, August 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818305030.

Ismail:2010:EAE

[IAD10] I. A. Ismail, M. Amin, and H. Diab. An efficient adaptive ergodic matrix and chaotic system for image encryption. *International Journal of Computer Applications*, 32(3):381–388, 2010. ISSN 1206-212X (print), 1925-7074 (electronic). URL https://www.tandfonline.com/doi/full/10.2316/Journal.202.2010.3.202-2330.

Islam:2011:MES

[IB11] Sk. Hafizul Islam and G. P. Biswas. A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. *The Journal of Systems and Software*, 84(11):1892–1898, November 2011. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211001646.

IBM:2013:DMP

[IBM13a] IBM. Daunting mathematical puzzle solved, enables unlimited analysis of encrypted data. *Scientific Computing*, December 24, 2013. URL http://www.scientificcomputing.com/news/2013/12/daunting-mathematical-puzzle-solved-enables-unlimited-analysis-encrypted-data. See patent [GH13].

IBM:2013:IPC

[IBM13b] IBM. IBM PCIe Cryptographic Coprocessor. Web document, 2013. URL http://www-03.ibm.com/security/cryptocards/pciecc/overview.shtml.

Irshad:2017:CPP

[IC17] Azeem Irshad and Shehzad Ashraf Chaudhry. Comments on "A privacy preserving three-factor authentication protocol for e-health clouds". *The Journal of Supercomputing*, 73(4):1504–1508, April 2017. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). See [JKL+16].

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:PIS

[IEE13] IEEE, editor. *Proceedings of the 21st IEEE Symposium on Computer Arithmetic, Austin, Texas, USA, 8–10 April 2013*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2013. ISBN 0-7695-4957-8. ISSN 1063-6889. LCCN QA76.9.C62 S95 2013.

IEEE:2015:ISS

[IEE15] IEEE, editor. *2015 IEEE Symposium on Security and Privacy (SP 2015) San Jose, California, USA, 18–20 May 2015*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2015. ISBN 1-4673-6949-7 (print), 1-4673-6950-0 (e-book). ISSN 1081-6011 (print), 2375-1207 (electronic). LCCN QA76.9.A25. URL `http://www.gbv.de/dms/tib-ub-hannover/836112652.pdf`.

Imanimehr:2016:HPR

[IF16] Fatemeh Imanimehr and Mehran S. Fallah. How powerful are run-time monitors with static information? *The Computer Journal*, 59(11):1623–1636, November 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/11/1623.

Islam:2011:MDA

[IG11] Salekul Islam and Jean-Charles Grégoire. Multi-domain authentication for IMS services. *Computer Networks (Amsterdam, Netherlands: 1999)*, 55(12):2689–2704, August 25, 2011. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128611001423.

Iyengar:2016:SPS

[IGR+16] Anirudh Iyengar, Swaroop Ghosh, Kenneth Ramclam, Jae-Won Jang, and Cheng-Wei Lin. Spintronic PUFs for security, trust, and authentication. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 13(1):4:1–4:??, December 2016. CODEN ???? ISSN 1550-4832.

Imai:2015:IRR

[IK15] Shigeyoshi Imai and Kaoru Kurosawa. Improved reconstruction of RSA private-keys from their fraction. *Information Processing Letters*, 115(6–8):630–632, June/August 2015. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019015000368.

Islam:2015:LFP

[IL15] Sk Hafizul Islam and Fagen Li. Leakage-free and provably secure certificateless signcryption scheme using bilinear pairings. *The Computer Journal*, 58(10):2636–2648, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2636.

Ioannou:2014:PKC

[IM14] Lawrence M. Ioannou and Michele Mosca. Public-key cryptography based on bounded quantum reference frames. *Theoretical Computer Science*, 560 (part 1)(??):33–45, December 4, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S030439751400694X.

Ingram:2016:AMB

[IM16] C. Ingram and M. Morisse. Almost an MNC: Bitcoin entrepreneurs' use of collective resources and decoupling to build legitimacy. In *2016 49th Hawaii International Con-*

ference on System Sciences (HICSS), pages 4083–4092. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, January 2016. ISSN 1530-1605.

I:2017:ETB

[IMB17] Indu I., Rubesh Anand P. M., and Vidhyacharan Bhaskar. Encrypted token based authentication with adapted SAML technology for cloud web services. *Journal of Network and Computer Applications*, 99(??):131–145, December 1, 2017. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804517303156.

Intel:2019:IAM

[Int19] Intel. *Intel Architecture Memory Encryption Technologies Specification*. Intel Corporation, ????, 336907-002us (revision 1.2) edition, April 2019. URL https://software.intel.com/sites/default/files/managed/a5/16/Multi-Key-Total-Memory-Encryption-Spec.pdf.

Isobe:2012:SCL

[IOM12] Takanori Isobe, Toshihiro Ohigashi, and Masakatu Morii. Slide cryptanalysis of lightweight stream cipher RAKAPOSHI. *Lecture Notes in Computer Science*, 7631:138–155, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34117-5_9/.

Islam:2018:REP

[IOV+18] SK Hafizul Islam, Mohammad S. Obaidat, Pandi Vijayakumar, Enas Abdulhay, Fagen Li, and M. Krishna Chaitanya Reddy. A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. *Future Generation Computer Systems*, 84(??):216–227, July 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17308439.

Isobe:2012:SAL

[IS12] Takanori Isobe and Kyoji Shibutani. Security analysis of the lightweight block ciphers XTEA, LED and Piccolo. *Lecture Notes in Computer Science*, 7372:71–86, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31448-3_6/.

Irshad:2016:EAM

[ISC+16] Azeem Irshad, Muhammad Sher, Shehzad Ashraf Chaudhary, Husnain Naqvi, and Mohammad Sabzinejad Farash. An efficient and anonymous multi-server authenticated key agreement based on chaotic map without engaging Registration Centre. *The Journal of Supercomputing*, 72 (4):1623–1644, April 2016. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-016-1688-9.

Ishai:2014:PCP

[IW14] Yuval Ishai and Mor Weiss. Probabilistically checkable proofs of proximity with zero-knowledge. *Lecture Notes in Computer Science*, 8349:121–145, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_6/.

Jacobs:2016:STB

[Jac16] Todd A. Jacobs. Secure token-based authentication with YubiKey 4. *Linux Journal*, 2016(265): 1:1–1:??, May 2016. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://dl.acm.org/ft_gateway.cfm?id=2953927.

Jie:2010:AAI

[JAE10] Wei Jie, Junaid Arshad, and Pascal Ekin. Authentication and authorization infrastructure for Grids — issues, technologies, trends and experiences. *The Journal of Supercomputing*, 52 (1):82–96, April 2010. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=52&issue=1&spage=82.

Jie:2011:RGA

[JAS+11] Wei Jie, Junaid Arshad, Richard Sinnott, Paul Townend, and Zhou Lei. A review of grid authentication and authorization technologies and support for federated access control. *ACM Computing Surveys*, 43(2):12:1–12:26, January 2011. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Prins:2011:DCA

[JB11] JR Prins and Business Unit Cybercrime. Diginotar certificate authority breach

"Operation Black Tulip". Unknown, November 2011. Fox-IT.

Jain:2013:MSD

[JC13] Ajay Jain and Kusha Chopra. Malware signing detection system. *ACM SIGSOFT Software Engineering Notes*, 38(5):1–8, September 2013. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

Jho:2016:SSE

[JCHS16] Nam-Su Jho, Ku-Young Chang, Dowon Hong, and Changho Seo. Symmetric searchable encryption with efficient range query using multi-layered linked chains. *The Journal of Supercomputing*, 72(11):4233–4246, November 2016. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Jia:2018:ERH

[JCL+18] Hongyong Jia, Yue Chen, Julong Lan, Kaixiang Huang, and Jun Wang. Efficient revocable hierarchical identity-based encryption using cryptographic accumulators. *International Journal of Information Security*, 17(4):477–490, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0387-8.

Jakobsson:2012:AWD

[JCM12] Markus Jakobsson, Richard Chow, and Jesus Molina. Authentication — are we doing well enough? *IEEE Security & Privacy*, 10(1):19–21, January/February 2012. ISSN 1540-7993 (print), 1558-4046 (electronic).

Chang:2012:TRR

[jCPB+12] S. j. Chang, R. Perlner, W. E. Burr, M. S. Turan, J. M. Kelsey, S. Paul, and L. E. Bassham. Third-round report of the SHA-3 cryptographic hash algorithm competition. Report, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 2012.

Joldzic:2016:TSA

[JDV16] Ognjen Joldzic, Zoran Djuric, and Pavle Vuletic. A transparent and scalable anomaly-based DoS detection method. *Computer Networks (Amsterdam, Netherlands: 1999)*, 104(??):27–42, July 20, 2016. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128616301347.

Jogenfors:2015:HBT

[JEA+15] Jonathan Jogenfors, Ashraf Mohamed Elhassan, Johan Ahrens, Mohamed Bourennane, and Jan-Åke Larsson. Hacking the Bell test using classical light in energy–time entanglement-based quantum key distribution. *Science Advances*, 1(11):e1500793, December 18, 2015. CODEN SACDAF. ISSN 2375-2548. URL `http://advances.sciencemag.org/content/1/11/e1500793`.

Jeong:2013:CBC

[Jeo13] Kitae Jeong. Cryptanalysis of block cipher Piccolo suitable for cloud computing. *The Journal of Supercomputing*, 66(2):829–840, November 2013. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://link.springer.com/article/10.1007/s11227-013-0902-2`.

Jaeger:2018:FAP

[JGP+18] David Jaeger, Hendrik Graupner, Chris Pelchen, Feng Cheng, and Christoph Meinel. Fast automated processing and evaluation of identity leaks. *International Journal of Parallel Programming*, 46(2):441–470, April 2018. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic).

Jo:2014:ODE

[JHCC14] Heeseung Jo, Seung-Tae Hong, Jae-Woo Chang, and Dong Hoon Choi. Offloading data encryption to GPU in database systems. *The Journal of Supercomputing*, 69(1):375–394, July 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://link.springer.com/article/10.1007/s11227-014-1159-0`.

Jing:2012:MVB

[JHHN12] Huiyun Jing, Xin He, Qi Han, and Xiamu Niu. Motion vector based information hiding algorithm for H.264/AVC against motion vector steganalysis. *Lecture Notes in Computer Science*, 7197:91–98, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-28490-8_10/`.

Jiang:2019:SSL

[JHW+19] Yichen Jiang, Jenny Hamer, Chenghong Wang, Xiaoqian Jiang, Miran Kim, Yongsoo Song, Yuhou Xia, Noman Mohammed, Md Nazmus Sadat, and Shuang Wang. SecureLR:

Secure logistic regression model via a hybrid cryptographic protocol. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 16(1): 113–123, January 2019. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Jiang:2014:UIS

[Jia14a] Shaoquan Jiang. On unconditional μ-security of private key encryption. *The Computer Journal*, 57(10):1570–1579, October 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/57/10/1570.

Jiang:2014:TEA

[Jia14b] Shaoquan Jiang. Timed encryption with application to deniable key exchange. *Theoretical Computer Science*, 560 (part 2)(??):172–189, December 4, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S030439751400098X.

Jiang:2016:MAC

[Jia16] Shaoquan Jiang. On message authentication with a correlated setup. *Information Processing Letters*, 116(4):289–293, April 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019015001908.

Jiang:2017:BMA

[Jia17] Shaoquan Jiang. Bounds for message authentication with distortion. *The Computer Journal*, 60(4):497–506, March 23, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/4/497/2608061.

Jin:2010:ADW

[Jin10] C. Jin. Adaptive digital watermark system using soft computation. *International Journal of Computer Applications*, 32(3): 341–346, 2010. ISSN 1206-212X (print), 1925-7074 (electronic). URL https://www.tandfonline.com/doi/full/10.2316/Journal.202.2010.3.202-2846.

Jain:2010:QP

[JJUW10] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. *Communications of the Association for Computing Machinery*, 53(12):102–109, December 2010. CODEN CACMA2.

ISSN 0001-0782 (print), 1557-7317 (electronic).

Jawad:2013:GAD

[JK13] Khurram Jawad and Asifullah Khan. Genetic algorithm and difference expansion based reversible watermarking for relational databases. *The Journal of Systems and Software*, 86(11):2742–2753, November 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121213001428.

Jannati:2019:SOR

[JK19] Hoda Jannati and Ramtin Khosravi. On the security of one-round meeting location determination protocol. *Information Processing Letters*, 146(??):35–38, June 2019. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019019300274.

Jamil:2018:SPU

[JKA+18] Fuzel Jamil, Abid Khan, Adeel Anjum, Mansoor Ahmed, Farhana Jabeen, and Nadeem Javaid. Secure provenance using an authenticated data structure approach. *Computers & Security*, 73(??):34–56, March 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404817302122.

Jan:2019:PBM

[JKAU19] Mian Ahmad Jan, Fazlullah Khan, Muhammad Alam, and Muhammad Usman. A payload-based mutual authentication scheme for Internet of Things. *Future Generation Computer Systems*, 92(??):1028–1039, March 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17303898.

Jun:2012:IIR

[JKHeY12] Jong Yun Jun, Kunho Kim, Jae-Pil Heo, and Sung eui Yoon. IRIW: Image retrieval based image watermarking for large-scale image databases. *Lecture Notes in Computer Science*, 7128:126–141, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32205-1_12/.

Jiang:2016:PPT

[JKL+16] Qi Jiang, Muhammad Khurram Khan, Xiang Lu, Jianfeng Ma, and Debiao He. A privacy preserving three-factor authentication protocol for e-Health clouds. *The Journal of Supercomputing*, 72(10):3826–3849, October 2016. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). See comments [IC17].

Jovanovic:2012:FAL

[JKP12] Philipp Jovanovic, Martin Kreuzer, and Ilia Polian. A fault attack on the LED Block cipher. *Lecture Notes in Computer Science*, 7275:120–134, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29912-4_10/.

Josefsson:2016:ECD

[JL16] Simon Josefsson and Ilari Liusvaara. Edwards-curve Digital Signature Algorithm (EdDSA). Internet Draft report draft-irtf-cfrg-eddsa-05, SJD AB, Stockholm 113 47, Sweden, March 21, 2016. URL https://tools.ietf.org/html/draft-irtf-cfrg-eddsa-05.

Jordan:2018:QCS

[JL18] S. P. Jordan and Y. Liu. Quantum cryptanalysis: Shor, Grover, and beyond. *IEEE Security & Privacy*, 16(5):14–21, September/October 2018. ISSN 1540-7993 (print), 1558-4046 (electronic).

Jiang:2018:AHP

[JLC18] Rong Jiang, Rongxing Lu, and Kim-Kwang Raymond Choo. Achieving high performance and privacy-preserving query over encrypted multidimensional big metering data. *Future Generation Computer Systems*, 78 (part 1)(??):392–401, January 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16301157.

Jeong:2012:IKP

[JLH12] Kyung Chul Jeong, Dong Hoon Lee, and Daewan Han. An improved known plaintext attack on PKZIP encryption algorithm. *Lecture Notes in Computer Science*, 7259:235–247, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31912-9_16/.

Jajodia:2012:RET

[JLS12] Sushil Jajodia, Witold Litwin, and Thomas Schwarz. Recoverable encryption through noised secret over a large cloud. *Lecture Notes in Computer Sci-*

ence, 7450:13–24, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32344-7_2/.

Jia:2012:PKD

[JLT+12] Zhongtian Jia, Xiaodong Lin, Seng-Hua Tan, Lixiang Li, and Yixian Yang. Public key distribution scheme for delay tolerant networks based on two-channel cryptography. *Journal of Network and Computer Applications*, 35(3):905–913, May 2012. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804511000634.

Jiang:2019:PPP

[JLX+19] Wenbo Jiang, Hongwei Li, Guowen Xu, Mi Wen, Guishan Dong, and Xiaodong Lin. PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI. *Future Generation Computer Systems*, 96(??):185–195, July 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18315097.

Ji:2018:DIR

[JLZ18] Wusheng Ji, Li Li, and Weiwei Zhou. Design and implementation of a RFID reader/router in RFID-WSN hybrid system. *Future Internet*, 10(11):106, November 03, 2018. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/10/11/106.

Jiang:2016:OOC

[JMG+16] Peng Jiang, Yi Mu, Fuchun Guo, Xiaofen Wang, and Qiaoyan Wen. Online/offline ciphertext retrieval on resource constrained devices. *The Computer Journal*, 59(7):955–969, July 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/7/955.

Jiang:2016:UTC

[JMW+16] Qi Jiang, Jianfeng Ma, Fushan Wei, Youliang Tian, Jian Shen, and Yuanyuan Yang. An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. *Journal of Network and Computer Applications*, 76(??):37–48, December 2016. CODEN JNCAF3. ISSN 1084-8045

(print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804516302302.

Jain:2012:BAS

[JN12] Anil K. Jain and Karthik Nandakumar. Biometric authentication: System security and user privacy. *Computer*, 45(11):87–92, November 2012. CODEN CPTRB4. ISSN 0018-9162.

Jan:2017:PPB

[JNUH17] Mian Jan, Priyadarsi Nanda, Muhammad Usman, and Xiangjian He. PAWN: a payload-based mutual authentication scheme for wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 29(17), September 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Johnson:2010:BRF

[Joh10] Neil F. Johnson. Book review: Frank Y. Shih, *Digital Watermarking and Steganography: Fundamentals and Techniques.* CRC/ Taylor & Francis (2008). ISBN-13 978-1-4200-4757-8. £46.99. 180 pp. Hardcover. *The Computer Journal*, 53(5):616–617, June 2010. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/reprint/53/5/616.

Johnson:2015:NGA

[Joh15] Kevin Wade Johnson. *The neglected giant: Agnes Meyer Driscoll*, volume 10 of *Center for Cryptologic History special series.* National Security Agency, Center for Cryptologic History, Fort George G. Meade, MD, USA, 2015. 66 pp. LCCN ????

Joux:2013:NIC

[Jou13] Antoine Joux. A new index calculus algorithm with complexity $L(1/4+o(1))$ in very small characteristic. Report 2013/095, CryptoExperts and Université de Versailles Saint-Quentin-en-Yvelines, Laboratoire PRISM, 45 avenue des Etats-Unis, F-78035 Versailles Cedex, France, February 20, 2013. 23 pp. URL http://eprint.iacr.org/2013/095.

Jin:2019:RPP

[JP19] Hongyu Jin and Panos Papadimitratos. Resilient privacy protection for location-based services through decentralization. *ACM Transactions on Privacy and Security (TOPS)*, 22(4):21:1–21:??, December 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3319401.

Jeffs:2013:CCP

[JR13] R. Amzi Jeffs and Mike Rosulek. Characterizing the cryptographic properties of reactive 2-party functionalities. *Lecture Notes in Computer Science*, 7785:263–280, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_15/.

Juels:2014:HEE

[JR14] Ari Juels and Thomas Ristenpart. Honey encryption: Encryption beyond the brute-force barrier. *IEEE Security & Privacy*, 12(4): 59–62, July/August 2014. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://www.computer.org/csdl/mags/sp/2014/04/msp2014040059-abs.html.

Jain:2018:MDN

[JS18a] Ajay Jain and Sachin Soni. Multi-directional navigation method for optimized consumption of user generated content through semantic mapping of features derived from the user generated content. *ACM SIGSOFT Software Engineering Notes*, 43(4):52, October 2018. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

Jaiyeola:2018:IPN

[JS18b] Temitope Gbolahan Jaiyeola and Florentin Smarandache. Inverse properties in neutrosophic triplet loop and their application to cryptography. *Algorithms (Basel)*, 11(3), March 2018. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL https://www.mdpi.com/1999-4893/11/3/32.

Jalili:2017:EAS

[JSA17] Majid Jalili and Hamid Sarbazi-Azad. Endurance-aware security enhancement in non-volatile memories using compression and selective encryption. *IEEE Transactions on Computers*, 66(7):1132–1144, July 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL https://www.computer.org/csdl/trans/tc/2017/07/07792116-abs.html.

Jevdjic:2017:ASC

[JSCM17] Djordje Jevdjic, Karin Strauss, Luis Ceze, and Henrique S. Malvar. Approximate storage of compressed and encrypted videos. *Operating Systems Review*, 51(2):361–

373, June 2017. CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Jain:2016:APQ

[JSK+16] Nitin Jain, Birgit Stiller, Imran Khan, Dominique Elser, Christoph Marquardt, and Gerd Leuchs. Attacks on practical quantum key distribution systems (and how to prevent them). *Contemporary Physics*, 57(3):366–??, 2016. CODEN CTPHAF. ISSN 0010-7514 (print), 1366-5812 (electronic).

Judmayer:2017:BCI

[JSK+17] Aljosha Judmayer, Nicholas Stifter, Katharina Krombholz, Edgar Weippl, Elisa Bertino, and Ravi Sandhu. Blocks and chains: Introduction to Bitcoin, cryptocurrencies, and their consensus mechanisms. *Synthesis Lectures on Information Security, Privacy, and Trust*, 9(1):1–123, June 2017. ISBN 1-62705-713-7. ISSN 1945-9742 (print), 1945-9750 (electronic). URL http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7987472.

Jordan:2018:EPE

[JSM+18] M. Jordan, N. Sardino, M. McGrath, C. Zoellin, T. E. Morris, C. Carranza Lewis, G. Vance, B. Naylor, J. Pickel, M. S. Almeida, D. Wierbowski, C. Meyer, R. Buendgen, M. Zagorski, H. Schoone, and K. Voss. Enabling pervasive encryption through IBM Z stack innovations. *IBM Journal of Research and Development*, 62(2–3): 2:1–2:11, ???? 2018. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL https://ieeexplore.ieee.org/document/8270590/.

Jiang:2018:CPA

[JSMG18a] Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. *Future Generation Computer Systems*, 78 (part 2)(??):720–729, January 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17301322.

Jiang:2018:FCP

[JSMG18b] Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. Flexible ciphertext-policy attribute-based encryption supporting AND-gate and threshold with short ciphertexts. *International Journal of Information Security, 17(4): 463–475, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0376-y.

Jiang:2012:DCA

[JSZS12] Xinghao Jiang, Tanfeng Sun, Yue Zhou, and Yun Q. Shi. A drift compensation algorithm for H.264/AVC video robust watermarking scheme. *Lecture Notes in Computer Science*, 7128:30–41, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32205-1_5/.

Joye:2012:FAC

[JT12a] Marc Joye and Michael Tunstall, editors. *Fault Analysis in Cryptography*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. ISBN 3-642-29655-6, 3-642-29656-4 (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xvi + 354 + 98 pp. LCCN QA76.9.A25 F38 2012; QA76.9.D35. URL http://www.springerlink.com/content/978-3-642-29656-7.

Tong:2012:NBD

[jT12b] Xiao jun Tong. The novel bilateral — Diffusion image encryption algorithm with dynamical compound chaos. *The Journal of Systems and Software*, 85(4):850–858, April 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211002834.

Jiang:2016:CVI

[JTZ+16] Yijing Jiang, Shanyu Tang, Liping Zhang, Muzhou Xiong, and Yau Jim Yip. Covert voice over Internet protocol communications with packet loss based on fractal interpolation. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 12(4):54:1–54:??, August 2016. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Juels:2014:INC

[JW14] Ari Juels and Bonnie Wong. The interplay of neuroscience and cryptography: technical perspective. *Communications of the Association for Computing Machinery*, 57(5): 109, May 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Jiang:2017:SLD

[JWJ+17] Wei Jiang, Liang Wen, Ke Jiang, Xia Zhang, Xiong Pan, and Keran Zhou. System-level design to detect fault injection attacks on embedded real-time applications. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 13(2):22:1–22:??, March 2017. CODEN ???? ISSN 1550-4832.

Jiao:2019:AMC

[JWNS19] Y. Jiao, P. Wang, D. Niyato, and K. Suankaewmanee. Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks. *IEEE Transactions on Parallel and Distributed Systems*, 30(9):1975–1989, September 2019. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Jin:2015:NCD

[JXLZ15] Chunhua Jin, Chunxiang Xu, Fagen Li, and Xiaojun Zhang. A novel certificateless deniable authentication protocol. *International Journal of Computer Applications*, 37(3-4):181–192, 2015. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.1080/1206212X.2016.1188564`.

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.

Jiang:2010:EDI

[JZS+10] Yixin Jiang, Haojin Zhu, Minghui Shi, Xuemin (Sherman) Shen, and Chuang Lin. An efficient dynamic-identity based signature scheme for secure network coding. *Computer Networks (Amsterdam, Netherlands: 1999)*, 54(1):28–40, January 15, 2010. CODEN ???? ISSN 1389-1286.

Jan:2019:SEE

[JZU+19] Mian Ahmad Jan, Wenjing Zhang, Muhammad Usman, Zhiyuan Tan, Fazlullah Khan, and Entao Luo. SmartEdge: an end-to-end encryption framework for an edge-enabled smart city application. *Journal of Network and Computer Applications*, 137(??):1–10, July 1, 2019. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804519300827`.

Khazaei:2017:COA

[KA17] Shahram Khazaei and Siavash Ahmadi. Ciphertext-only attack on $d \times d$ Hill in $O(d13^d)$. *Information Processing Letters*, 118(??):25–29, February 2017. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019016301338`.

Kurkcu:2018:CBE

[KA18] Ömür Kıvanç Kürkçü and Ersin Aslan. A comparison between edge neighbor rupture degree and edge scattering number in graphs. *International Journal of Foundations of Computer Science (IJFCS)*, 29(7):??, November 2018. ISSN 0129-0541. URL `https://www.worldscientific.com/doi/10.1142/S0129054118500247`.

Kornycky:2017:RFT

[KAHKB17] Joe Kornycky, Omar Abdul-Hameed, Ahmet Kondoz, and Brian C. Barber. Radio frequency traffic classification over WLAN. *IEEE/ACM Transactions on Networking*, 25(1):56–68, February 2017. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Koziel:2018:HPS

[KAK18] Brian Koziel, Reza Azarderakhsh, and Mehran Mozaffari Kermani. A high-performance and scalable hardware architecture for isogeny-based cryptography. *IEEE Transactions on Computers*, 67(11):1594–1609, ???? 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `https://ieeexplore.ieee.org/document/8315051/`.

Kamp:2013:MES

[Kam13] Poul-Henning Kamp. More encryption is not the solution. *ACM Queue: Tomorrow's Computing Today*, 11(7):10, July 2013. CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic).

Kamp:2016:MEM

[Kam16] Poul-Henning Kamp. More encryption means less privacy. *Communications of the Association for Computing Machinery*, 59(4):

40–42, April 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2016/4/200167/fulltext.

Kammuller:2019:ATI

[Kam19] Florian Kammüller. Attack trees in Isabelle extended with probabilities for quantum cryptography. *Computers & Security*, 87(??):Article 101572, November 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S016740481930135X.

Kapera:2011:SPD

[Kap11] Zdzisław Jan Kapera. *In the Shadow of Pont du Gard: the Polish Enigma in Vichy France (June 1940 to November 1942)*, volume 7 of *The Enigma Bulletin*. The Enigma Press, Kraków, Poland, 2011. ISBN 83-86110-72-4. ISSN 0867-8693. 111 + 1 + 16 pp. LCCN ????

Kapera:2013:MRM

[Kap13] Zdzisław Jan Kapera. *Marian Rejewski: the man who defeated "Enigma"*, volume 8 of *The Enigma bulletin*. The Enigma Press, Kraków, Poland, 2013. ISBN 83-86110-72-4. 111 pp. LCCN ????

Karafyllidis:2012:QGC

[Kar12] Ioannis G. Karafyllidis. Quantum gate circuit model of signal integration in bacterial quorum sensing. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 9(2):571–579, March 2012. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Kong:2015:CSM

[KAS15] Jia Hao Kong, Li-Minn Ang, and Kah Phooi Seng. A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments. *Journal of Network and Computer Applications*, 49(??):15–50, March 2015. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804514002136.

Katz:2013:RIB

[Kat13] Jon Katz. Review of *Identity-based encryption* by Sanjit Chattarjee and Palash Sarkar. *ACM SIGACT News*, 44(4):29–31, December 2013. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

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).

Karthigaikumar:2010:PPV

[KB10] P. Karthigaikumar and K. Baskaran. Partially pipelined VLSI implementation of Blowfish encryption/decryption algorithm. *International Journal of Image and Graphics (IJIG)*, 10(3):327–341, July 2010. CODEN ???? ISSN 0219-4678.

Kallel:2011:SMM

[KBL11] Mohamed Kallel, Mohamed-Salim Bouhlel, and Jean-Christophe Lapayre. Security of the medical media using a hybrid and multiple watermark technique. *International Journal of Image and Graphics (IJIG)*, 11(1):103–115, January 2011. CODEN ???? ISSN 0219-4678.

Kleinrouweler:2017:SAP

[KCC17] Jan Willem Kleinrouweler, Sergio Cabrero, and Pablo Cesar. An SDN architecture for privacy-friendly network-assisted DASH. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 13(3s):44:1–44:??, August 2017. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (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.

Khan:2018:APS

[KCS+18] Imran Khan, Shehzad Ashraf Chaudhry, Muhammad Sher, Javed I. Khan, and Muhammad Khurram Khan. An anonymous and provably secure biometric-based authentication scheme using chaotic maps for accessing medical drop box data. *The Journal of Supercomputing*, 74(8):3685–3703, August 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Koz:2012:ASE

[KD12a] Alper Koz and Claude Delpha. Adaptive selection of embedding locations for spread spectrum watermarking of compressed audio. *Lecture*

Notes in Computer Science, 7128:97–110, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32205-1_10/.

Kraetzer:2012:PCS

[KD12b] Christian Kraetzer and Jana Dittmann. Plausibility considerations on steganalysis as a security mechanism — discussions on the example of audio steganalysis. *Lecture Notes in Computer Science*, 7228:80–101, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31971-6_5/.

Kieffer:2018:IBC

[KD18] Jean Kieffer and Luca De Feo. Isogeny-based cryptography in Julia/Nemo: a case study. *ACM Communications in Computer Algebra*, 52(4):130–132, December 2018. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Kumar:2019:SSH

[KD19] Chanchal Kumar and Mohammad Najmud Doja. A secure structure for hiding information in a cryptosystem based on machine-learning techniques and content-based optimization using portfolio selection data. *Scalable Computing: Practice and Experience*, 20(1):161–180, ???? 2019. CODEN ???? ISSN 1895-1767. URL https://www.scpe.org/index.php/scpe/article/view/1488.

Karakoc:2013:BCL

[KDH13] F. Karakoç, H. Demirci, and A. E. Harmanci. Biclique cryptanalysis of LBlock and TWINE. *Information Processing Letters*, 113(12):423–429, June 30, 2013. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013000884.

Karakoc:2015:AKA

[KDH15] F. Karakoç, H. Demirci, and A. E. Harmanci. AKF: a key alternating Feistel scheme for lightweight cipher designs. *Information Processing Letters*, 115(2):359–367, February 2015. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019014002257.

Kumari:2017:DSU

[KDW+17] Saru Kumari, Ashok Kumar Das, Mohammad Wazid, Xiong Li, Fan Wu, Kim-Kwang Raymond Choo, and Muhammad Khurram Khan. On the design of a secure user authentication and key agreement scheme for wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 29(23):??, December 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Kara:2019:ALS

[KE19] Orhun Kara and Muhammed F. Esgin. On analysis of lightweight stream ciphers with keyed update. *IEEE Transactions on Computers*, 68(1):99–110, ???? 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `https://ieeexplore.ieee.org/document/8400392/`.

Keblusek:2015:BRK

[Keb15] Marika Keblusek. Book review: Kristie Macrakis, *Prisoners, Lovers, and Spies: The Story of Invisible Ink from Herodotus to Al-Qaeda*. *Isis*, 106(3):692–693, September 2015. CODEN ISISA4. ISSN 0021-1753 (print), 1545-6994 (electronic). URL `http://www.jstor.org/stable/10.1086/683195`.

Kemshall:2011:WMT

[Kem11] Andy Kemshall. Why mobile two-factor authentication makes sense. *Network Security*, 2011(4):9–12, April 2011. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485811700381`.

Kabirirad:2019:HSG

[KFE19] Saeideh Kabirirad, Mahmood Fazlali, and Ziba Eslami. High-speed GPU implementation of a secret sharing scheme based on cellular automata. *The Journal of Supercomputing*, 75(11):7314–7336, November 2019. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Kleinjung:2010:FBR

[KFL+10] Thorsten Kleinjung, Kazumaro Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann. Factorization of a 768-bit RSA modulus. Report 1.4, EPFL IC LACAL [and others], Station 14, CH-1015 Lausanne, Switzerland [and others], February

18, 2010. URL https://eprint.iacr.org/2010/006.pdf.

Kikuchi:2012:SSN

[KFOS12] Ryo Kikuchi, Atsushi Fujioka, Yoshiaki Okamoto, and Taiichi Saito. Strong security notions for timed-release public-key encryption revisited. *Lecture Notes in Computer Science*, 7259:88–108, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31912-9_7/.

Kostic:2019:UNV

[KG19] Dusan Kostic and Shay Gueron. Using the new VPMADD instructions for the new post quantum key encapsulation mechanism SIKE. In Takagi et al. [TBL19], pages 215–218. ISBN 1-72813-366-1. ISSN 1063-6889.

Kramer:2010:FDC

[KGO10] Simon Kramer, Rajeev Goré, and Eiji Okamoto. Formal definitions and complexity results for trust relations and trust domains fit for TTPs, the web of trust, PKIs, and ID-based cryptography. *ACM SIGACT News*, 41(1):75–98, March 2010. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Kim:2012:SLT

[KGP12] Tiffany Hyun-Jin Kim, Virgil Gligor, and Adrian Perrig. Street-level trust semantics for attribute authentication. *Lecture Notes in Computer Science*, 7622:96–115, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35694-0_12/.

K:2019:IAM

[KGP+19] Deepa K., Radhamani G., Vinod P., Mohammad Shojafar, Neeraj Kumar, and Mauro Conti. Identification of Android malware using refined system calls. *Concurrency and Computation: Practice and Experience*, 31 (20):e5311:1–e5311:??, October 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Khedr:2016:SSH

[KGV16] Alhassan Khedr, Glenn Gulak, and Vinod Vaikuntanathan. SHIELD: Scalable homomorphic implementation of encrypted data-classifiers. *IEEE Transactions on Computers*, 65(9):2848–2858, ????

2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Kwon:2010:SEB

[KH10] Taekyoung Kwon and Jin Hong. Secure and efficient broadcast authentication in wireless sensor networks. *IEEE Transactions on Computers*, 59(8):1120–1133, August 2010. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5313804.

Koo:2018:PPD

[KH18] Dongyoung Koo and Junbeom Hur. Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing. *Future Generation Computer Systems*, 78 (part 2)(??):739–752, January 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17301309.

Khazaei:2010:NBS

[Kha10] Shahram Khazaei. *Neutrality-Based Symmetric Cryptanalysis*. Thèse, École polytechnique fédérale de Lausanne (EPFL), Lausanne, Switzerland, 2010. 138 pp.

Kastner:2010:AOT

[KHF10] Ryan Kastner, Anup Hosangadi, and Farzan Fallah. *Arithmetic optimization techniques for hardware and software design*. Cambridge University Press, Cambridge, UK, 2010. ISBN 0-521-88099-8. vii + 187 pp. LCCN QA76.9.C62 K37 2010; QA76.9.C62 KAS 2010. URL http://assets.cambridge.org/97805218/80992/cover/9780521880992.jpg.

Kim:2014:MBM

[KHHH14] Heeseok Kim, Dong-Guk Han, Seokhie Hong, and Jaecheol Ha. Message blinding method requiring no multiplicative inversion for RSA. *ACM Transactions on Embedded Computing Systems*, 13(4):80:1–80:??, February 2014. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Khleborodov:2018:FEC

[Khl18] Denis Khleborodov. Fast elliptic curve point multiplication based on window Non-Adjacent Form method. *Applied Mathematics and Computation*, 334(??):41–59, October 1, 2018. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://

www.sciencedirect.com/science/article/pii/S0096300318302935.

Khalil-Hani:2013:BEB

[KHMB13] Mohamed Khalil-Hani, Muhammad N. Marsono, and Rabia Bakhteri. Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm. *Future Generation Computer Systems*, 29(3): 800–810, March 2013. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X12000350.

Kinkelin:2011:UTS

[KHN+11] Holger Kinkelin, Ralph Holz, Heiko Niedermayer, Simon Mittelberger, and Georg Carle. On using TPM for secure identities in future home networks. *Future Internet*, 3(1):1–13, January 07, 2011. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/3/1/1.

Kim:2016:EPE

[KHPP16] Intae Kim, Seong Oun Hwang, Jong Hwan Park, and Chanil Park. An efficient predicate encryption with constant pairing computations and minimum costs. *IEEE Transactions on Computers*, 65 (10):2947–2958, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Kolsch:2019:SBP

[KHRG19] Johannes Kölsch, Christopher Heinz, Axel Ratzke, and Christoph Grimm. Simulation-based performance validation of homomorphic encryption algorithms in the Internet of Things. *Future Internet*, 11 (10):218, October 22, 2019. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/11/10/218.

Kai:2011:CIS

[KI11] Hiroshi Kai and Shigenobu Inoue. Cheater identification on a secret sharing scheme using GCD. *ACM Communications in Computer Algebra*, 45(2):119–120, June 2011. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Kiayias:2011:TCC

[Kia11] Aggelos Kiayias, editor. *Topics in cryptology — CT-RSA 2011: the cryptographers' track at the RSA conference 2011, San Francisco, CA, USA, February 14–18, 2011. proceedings*, volume 6558 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011. ISBN 3-642-19073-1. LCCN ????

Kompara:2019:REM

[KIH19] Marko Kompara, SK Hafizul Islam, and Marko Hölbl. A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs. *Computer Networks (Amsterdam, Netherlands: 1999)*, 148(??):196–213, January 15, 2019. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128618303955.

Kim:2011:LBA

[Kim11] Hyun Sung Kim. Location-based authentication protocol for first cognitive radio networking standard. *Journal of Network and Computer Applications*, 34(4):1160–1167, July 2011. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804510002286.

Kim:2015:CEH

[Kim15] Y. Kim. Comments on "An Efficient Homomorphic MAC with Small Key Size for Authentication in Network Coding. *IEEE Transactions on Computers*, 64(12):3619–3620, ???? 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). See [CJ13].

Kim:2016:MAS

[Kim16] Soon Seok Kim. Mutual authentication scheme between biosensor device and data manager in healthcare environment. *The Journal of Supercomputing*, 72 (1):177–184, January 2016. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-015-1536-3.

Khan:2016:BSW

[KJN+16] Abid Khan, Farhana Jabeen, Farah Naz, Sabah Suhail, Mansoor Ahmed, and Sarfraz Nawaz. Buyer seller watermarking protocols issues and challenges — a survey. *Journal of Network and Computer Applications*, 75(??):317–334, November 2016. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804516301941.

Konstantinou:2010:RCI

[KK10] Elisavet Konstantinou and Aristides Kontogeorgis. Ramanujan's class invariants and their use in elliptic curve cryptography. *Computers and*

Mathematics with Applications, 59(8):2901–2917, April 2010. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122110001173`.

Kawai:2012:SHS

[KK12] Yutaka Kawai and Noboru Kunihiro. Secret handshake scheme with request-based-revealing. *Lecture Notes in Computer Science*, 7163:1–16, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-29804-2_1/`.

Kawai:2013:SHS

[KK13] Yutaka Kawai and Noboru Kunihiro. Secret handshake scheme with request-based-revealing. *Computers and Mathematics with Applications*, 65(5):786–798, March 2013. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122112004919`.

Khalil:2014:CIM

[KKA14] Issa Khalil, Abdallah Khreishah, and Muhammad Azeem. Consolidated Identity Management System for secure mobile cloud computing. *Computer Networks (Amsterdam, Netherlands: 1999)*, 65 (??):99–110, June 2, 2014. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128614001194`.

Khan:2015:CMB

[KKA15] Abdul Nasir Khan, M. L. Mat Kiah, and Mazhar Ali. A cloud-manager-based re-encryption scheme for mobile users in cloud environment: a hybrid approach. *Journal of Grid Computing*, 13(4):651–675, December 2015. CODEN ???? ISSN 1570-7873 (print), 1572-9184 (electronic). URL `http://link.springer.com/article/10.1007/s10723-015-9352-9`.

Kumari:2018:SAS

[KKD+18] Saru Kumari, Marimuthu Karuppiah, Ashok Kumar Das, Xiong Li, Fan Wu, and Neeraj Kumar. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. *The Journal of Supercomputing*, 74 (12):6428–6453, December 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Khan:2014:MEK

[KKG14] Muhammad Khurram Khan,

Saru Kumari, and Mridul K. Gupta. More efficient key-hash based fingerprint remote authentication scheme using mobile device. *Computing*, 96(9): 793–816, September 2014. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL `http://link.springer.com/article/10.1007/s00607-013-0308-2`.

Karopoulos:2010:FIP

[KKGK10] Giorgos Karopoulos, Georgios Kambourakis, Stefanos Gritzalis, and Elisavet Konstantinou. A framework for identity privacy in SIP. *Journal of Network and Computer Applications*, 33(1):16–28, January 2010. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804509001052`.

Kim:2016:DBM

[KKJ+16] Yonggon Kim, Ohmin Kwon, Jinsoo Jang, Seongwook Jin, Hyeongboo Baek, Brent Byunghoon Kang, and Hyunsoo Yoon. On-demand bootstrapping mechanism for isolated cryptographic operations on commodity accelerators. *Computers & Security*, 62(??):33–48, September 2016. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404816300712`.

Kubota:2016:SAV

[KKK+16] Takahiro Kubota, Yoshihiko Kakutani, Go Kato, Yasuhito Kawano, and Hideki Sakurada. Semi-automated verification of security proofs of quantum cryptographic protocols. *Journal of Symbolic Computation*, 73(??):192–220, March/April 2016. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0747717115000462`.

Kim:2018:EPP

[KKK+18a] Jinsu Kim, Dongyoung Koo, Yuna Kim, Hyunsoo Yoon, Junbum Shin, and Sungwook Kim. Efficient privacy-preserving matrix factorization for recommendation via fully homomorphic encryption. *ACM Transactions on Privacy and Security (TOPS)*, 21(4):17:1–17:??, October 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3212509`.

Kim:2018:ARD

[KKK+18b] Sung Ryoung Kim, Jeong Nyeo Kim, Sung Tae Kim, Sunwoo Shin, and Jeong Hyun

Yi. Anti-reversible dynamic tamper detection scheme using distributed image steganography for IoT applications. *The Journal of Supercomputing*, 74(9):4261–4280, September 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Koblitz:2011:ECC

[KKM11] Ann Hibner Koblitz, Neal Koblitz, and Alfred Menezes. Elliptic curve cryptography: the serpentine course of a paradigm shift. *Journal of Number Theory*, 131(5):781–814, May 2011. CODEN JNUTA9. ISSN 0022-314X (print), 1096-1658 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022314X09000481.

Khan:2013:EDC

[KKM+13] Abdul Nasir Khan, M. L. Mat Kiah, Sajjad A. Madani, Atta ur Rehman Khan, and Mazhar Ali. Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing. *The Journal of Supercomputing*, 66(3):1687–1706, December 2013. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-013-0967-y.

Khan:2014:IPR

[KKM+14] Abdul Nasir Khan, M. L. Mat Kiah, Sajjad A. Madani, Mazhar Ali, Atta ur Rehman Khan, and Shahaboddin Shamshirband. Incremental proxy re-encryption scheme for mobile cloud computing environment. *The Journal of Supercomputing*, 68(2):624–651, May 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-013-1055-z.

Katz:2008:IMC

[KL08] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography: Principles and Protocols*. Chapman and Hall/CRC cryptography and network security. Chapman and Hall/CRC, Boca Raton, FL, USA, 2008. ISBN 1-58488-551-3. xviii + 534 pp. LCCN QA76.9.A25 K36 2008. URL http://www.loc.gov/catdir/enhancements/fy0807/2007017861-d.html; http://www.loc.gov/catdir/toc/ecip0716/2007017861.html.

Kushwah:2011:EIB

[KL11] Prashant Kushwah and Sunder Lal. An efficient identity based generalized signcryption scheme. *Theoretical Computer Science*, 412(45):6382–6389, October 21, 2011. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397511006700.

Khakpour:2013:ITA

[KL13] Amir R. Khakpour and Alex X. Liu. An information-theoretical approach to high-speed flow nature identification. *IEEE/ACM Transactions on Networking*, 21(4):1076–1089, August 2013. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Katz:2015:IMC

[KL15] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. Chapman and hall/CRC cryptography and network security series. Taylor and Francis, Boca Raton, FL, USA, second edition, 2015. ISBN 1-4665-7026-1 (hardcover). 583 pp. LCCN QA76.9.A25 K36 2014.

Klapper:2010:PSS

[Kla10] Andrew Klapper. *Pseudorandom Sequences and Stream Ciphers*, chapter 17, pages 1–23. Volume 2 of Atallah and Blanton [AB10b], second edition, 2010. ISBN 1-58488-820-2. LCCN QA76.9.A43 A433 2010. URL http://www.crcnetbase.com/doi/abs/10.1201/9781584888215-c17.

Ko:2010:MME

[KLC+10] Jeonggil Ko, Jong Hyun Lim, Yin Chen, Rvãzvan Musvaloiu-E, Andreas Terzis, Gerald M. Masson, Tia Gao, Walt Destler, Leo Selavo, and Richard P. Dutton. MEDiSN: Medical emergency detection in sensor networks. *ACM Transactions on Embedded Computing Systems*, 10(1):11:1–11:??, August 2010. CODEN ???? ISSN 1539-9087.

Kim:2019:AAI

[KLK+19] Jihye Kim, Jiwon Lee, Hankyung Ko, Donghwan Oh, Semin Han, Gwonho Jeong, and Hyunok Oh. AuthCropper: Authenticated image cropper for privacy preserving surveillance systems. *ACM Transactions on Embedded Computing Systems*, 18(5s):62:1–62:??, October 2019. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3358195.

Koeberl:2012:EPD

[KLM+12] Patrick Koeberl, Jiangtao

Li, Roel Maes, Anand Rajan, Claire Vishik, and Marcin Wójcik. Evaluation of a PUF device authentication scheme on a discrete 0.13um SRAM. *Lecture Notes in Computer Science*, 7222:271–288, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32298-3_18/.

Kent:2015:AGA

[KLN15] Alexander D. Kent, Lorie M. Liebrock, and Joshua C. Neil. Authentication graphs: Analyzing user behavior within an enterprise network. *Computers & Security*, 48(??):150–166, February 2015. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404814001321.

Kumari:2016:UFM

[KLW+16] Saru Kumari, Xiong Li, Fan Wu, Ashok Kumar Das, Hamed Arshad, and Muhammad Khurram Khan. A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps. *Future Generation Computer Systems*, 63(??):56–75, October 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16300930.

Kumari:2017:DPS

[KLW+17] Saru Kumari, Xiong Li, Fan Wu, Ashok Kumar Das, Kim-Kwang Raymond Choo, and Jian Shen. Design of a provably secure biometrics-based multi-cloud-server authentication scheme. *Future Generation Computer Systems*, 68(??):320–330, March 2017. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16303776.

Kim:2012:INS

[KLY+12] Hwi-Gang Kim, Eun Jung Lee, Gang-Joon Yoon, Sung-Dae Yang, Eui Chul Lee, and Sang Min Yoon. Illumination normalization for SIFT based finger vein authentication. *Lecture Notes in Computer Science*, 7432:21–30, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33191-6_3/.

Keller:2010:DAS

[KM10a] Nathan Keller and Stephen D. Miller. Distinguishing attacks on stream ciphers based on arrays of pseudorandom words. *Information Processing Letters*, 110 (4):129–132, January 16, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Khomejani:2010:PCT

[KM10b] S. Khomejani and A. Movaghar. Privacy consideration for trustworthy vehicular ad hoc networks. In IEEE, editor, *Proceedings of the 2010 International Conference On Electronics and Information Engineering (ICEIE), 1–3, August, 2010, Kyoto, Japan*, pages 437–?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 1-4244-7679-8. LCCN ????

Koblitz:2010:BNW

[KM10c] Neal Koblitz and Alfred Menezes. The brave new world of bodacious assumptions in cryptography. *Notices of the American Mathematical Society*, 57(3):357–365, March 2010. CODEN AMNOAN. ISSN 0002-9920 (print), 1088-9477 (electronic). URL `http://www.ams.org/notices/201003/`.

Kiani:2011:MPD

[KM11] Soheila Kiani and Mohsen Ebrahimi Moghaddam. A multipurpose digital image watermarking using fractal block coding. *The Journal of Systems and Software*, 84(9):1550–1562, September 2011. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121211000707`.

Kifer:2014:PFM

[KM14] Daniel Kifer and Ashwin Machanavajjhala. Pufferfish: a framework for mathematical privacy definitions. *ACM Transactions on Database Systems*, 39 (1):3:1–3:??, January 2014. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Koblitz:2015:RWE

[KM15] Neal Koblitz and Alfred J. Menezes. A riddle wrapped in an enigma. Report, ????, ????, November 1, 2015. 1–20 pp. URL `https://eprint.iacr.org/2015/1018.pdf`.

Koblitz:2016:RWE

[KM16] Neal Koblitz and Alfred Menezes. A riddle wrapped in an enigma. *IEEE Security & Privacy*, 14(6):34–42, November/December 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/06/msp2016060034-abs.html.

Kasamatsu:2012:TSE

[KME+12] Kohei Kasamatsu, Takahiro Matsuda, Keita Emura, Nuttapong Attrapadung, and Goichiro Hanaoka. Time-specific encryption from forward-secure encryption. *Lecture Notes in Computer Science*, 7485: 184–204, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32928-9_11/.

Kandi:2017:ELC

[KMG17] Haribabu Kandi, Deepak Mishra, and Subrahmanyam R. K. Sai Gorthi. Exploring the learning capabilities of convolutional neural networks for robust image watermarking. *Computers & Security*, 65(??):247–268, March 2017. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404816301699.

Kline:2018:CAR

[KMJ18] Donald Kline, Jr., Rami Melhem, and Alex K. Jones. Counter advance for reliable encryption in phase change memory. *IEEE Computer Architecture Letters*, 17(2):209–212, July/December 2018. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Kiyoshima:2014:CRB

[KMO14] Susumu Kiyoshima, Yoshifumi Manabe, and Tatsuaki Okamoto. Constant-round black-box construction of composable multi-party computation protocol. *Lecture Notes in Computer Science*, 8349: 343–367, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_15/.

Karger:2011:LLB

[KMP+11] Paul Karger, Suzanne McIntosh, Elaine Palmer, David Toll, and Samuel Weber. Lessons learned: Building the Caernarvon high-assurance operating system. *IEEE Security & Privacy*, 9(1):22–30, January/February 2011. ISSN 1540-7993 (print), 1558-4046 (electronic).

Kanwal:2015:TTM

[KMSM15] Ayesha Kanwal, Rahat Masood, Muhammad Awais Shibli, and Rafia Mumtaz. Taxonomy for trust models in cloud computing. *The Computer Journal*, 58(4):601–626, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/601.

Katz:2012:TSP

[KMTG12] Jonathan Katz, Philip MacKenzie, Gelareh Taban, and Virgil Gligor. Two-server password-only authenticated key exchange. *Journal of Computer and System Sciences*, 78(2):651–669, March 2012. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000011001048.

Kavun:2018:SAE

[KMY18] Elif Bilge Kavun, Hristina Mihajloska, and Tolga Yalçin. A survey on authenticated encryption–ASIC designer's perspective. *ACM Computing Surveys*, 50(6):88:1–88:??, January 2018. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Kang:2019:NBK

[KMZS19] Burong Kang, Xinyu Meng, Lei Zhang, and Yinxia Sun. Nonce-based key agreement protocol against bad randomness. *International Journal of Foundations of Computer Science (IJFCS)*, 30(4):619–633, June 2019. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054119400161.

Khovratovich:2010:RCA

[KN10] Dmitry Khovratovich and Ivica Nikolić. Rotational cryptanalysis of ARX. Report, University of Luxembourg, Luxembourg, January 2010. 24 pp. URL http://www.skein-hash.info/sites/default/files/axr.pdf.

Knijnenburg:2017:PCE

[Kni17] Bart P. Knijnenburg. Privacy? I can't even! Making a case for user-tailored privacy. *IEEE Security & Privacy*, 15(4):62–67, July/August 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2017/04/msp2017040062-abs.html.

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.

Kobsa:2013:CJV

[KNTU13] Alfred Kobsa, Rishab Nithyanand, Gene Tsudik, and Ersin Uzun. Can Jannie verify? Usability of display-equipped RFID tags for security purposes. *Journal of Computer Security*, 21(3):347–370, ???? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kheiri:2014:CCV

[KÖ14] Ahmed Kheiri and Ender Özcan. Constructing constrained-version of magic squares using selection hyper-heuristics. *The Computer Journal*, 57(3): 469–479, March 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/57/3/469.full.pdf+html. See correction [?].

Kumari:2016:APW

[KO16] Shipra Kumari and Hari Om. Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. *Computer Networks (Amsterdam, Netherlands: 1999)*, 104(??):137–154, July 20, 2016. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128616301384.

Koblitz:2010:BRB

[Kob10] Neal Koblitz. Book review: *Decrypted Secrets: Methods and Maxims of Cryptology*. Fourth Edition. *SIAM Review*, 52 (4):777–779, ???? 2010. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Komargodski:2018:LRO

[Kom18] Ilan Komargodski. Leakage resilient one-way functions: the auxiliary-input setting. *Theoretical Computer Science*, 746(??):6–18, October 25, 2018. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397518304304.

Kasper:2012:SCA

[KOP12] Timo Kasper, David Oswald, and Christof Paar. Side-channel analysis of cryptographic RFIDs with analog demodulation. *Lecture Notes in Computer Science*, 7055:61–77, 2012.

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-25286-0_5/.

Khamsemanan:2016:BBU

[KOS16] Nirattaya Khamsemanan, Rafail Ostrovsky, and William E. Skeith. On the black-box use of somewhat homomorphic encryption in noninteractive two-party protocols. *SIAM Journal on Discrete Mathematics*, 30(1):266–295, ???? 2016. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Kawachi:2017:GCR

[KOTY17] Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka, and Kenji Yasunaga. General constructions of rational secret sharing with expected constant-round reconstruction. *The Computer Journal*, 60(5):711–728, April 1, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/5/711/2715224.

Kollmitzer:2010:AQC

[KP10] Christian Kollmitzer and M. (Mario) Pivk, editors. *Applied Quantum Cryptography*, volume 797 of *Lecture notes in physics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-04829-3 (hardcover), 3-642-04831-5 (e-book). xii + 214 pp. LCCN TK5102.94 .A68 2010.

Kang:2012:AKM

[KP12] Hyun-Sun Kang and Chang-Seop Park. An authentication and key management scheme for the proxy mobile IPv6. *Lecture Notes in Computer Science*, 7690:144–160, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35416-8_11/.

Kolman:2017:SCG

[KP17] Eyal Kolman and Benny Pinkas. Securely computing a ground speed model. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 8(4):54:1–54:??, July 2017. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic).

Koya:2018:AHM

[KP18] Aneesh M. Koya and Deepthi P. P. Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network. *Computer Networks (Amsterdam, Netherlands: 1999)*, 140(??):138–151, July 20, 2018. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128618302044.

Kumar:2017:TAU

[KPB17] Vireshwar Kumar, Jung-Min (Jerry) Park, and Kaigui Bian. Transmitter authentication using hierarchical modulation in dynamic spectrum sharing. *Journal of Network and Computer Applications*, 91(??):52–60, August 1, 2017. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804517301935.

Kobusinska:2018:BDF

[KPB18] Anna Kobusińska, Kamil Pawluczuk, and Jerzy Brzeziński. Big data fingerprinting information analytics for sustainability. *Future Generation Computer Systems*, 86(??):1321–1337, September 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17329965.

Kiltz:2011:EAH

[KPC+11] Eike Kiltz, Krzysztof Pietrzak, David Cash, Abhishek Jain, and Daniele Venturi. Efficient authentication from hard learning problems. *Lecture Notes in Computer Science*, 6632:7–26, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_3.

Khalid:2016:RHL

[KPC+16] Ayesha Khalid, Goutam Paul, Anupam Chattopadhyay, Faezeh Abediostad, Syed Imad Ud Din, Muhammad Hassan, Baishik Biswas, and Prasanna Ravi. RunStream: a high-level rapid prototyping framework for stream ciphers. *ACM Transactions on Embedded Computing Systems*, 15(3): 61:1–61:??, July 2016. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Kocabas:2012:CPB

[KPKS12] Ünal Kocabaş, Andreas Peter, Stefan Katzenbeisser, and Ahmad-Reza Sadeghi. Converse PUF-based authentication. *Lecture Notes in Computer Science*, 7344: 142–158, 2012. CODEN LNCSD9. ISSN

0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-30921-2_9/.

Kang:2016:DSA

[KPP16] Jungho Kang, Geunil Park, and Jong Hyuk Park. Design of secure authentication scheme between devices based on zero-knowledge proofs in home automation service environments. *The Journal of Supercomputing*, 72 (11):4319–4336, November 2016. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Keskinarkaus:2010:IWD

[KPS10] A. Keskinarkaus, A. Pramila, and T. Seppänen. Image watermarking with a directed periodic pattern to embed multibit messages resilient to print-scan and compound attacks. *The Journal of Systems and Software*, 83(10): 1715–1725, October 2010. CODEN JSSODM. ISSN 0164-1212.

Krenn:2013:CCR

[KPW13] Stephan Krenn, Krzysztof Pietrzak, and Akshay Wadia. A counterexample to the chain rule for conditional HILL entropy. *Lecture Notes in Computer Science*, 7785:23–39, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_2/.

Knudsen:2011:BCC

[KR11] Lars R. Knudsen and Matthew J. B. Robshaw. *The Block Cipher Companion*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011. ISBN 3-642-17341-1, 3-642-17342-X (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xiv + 267 pp. LCCN QA76.9.A25 K58 2011; QA76.9.D35.

Krantz:2012:EAM

[Kra12] Steven G. (Steven George) Krantz. *Elements of advanced mathematics*. Chapman and Hall/CRC, Boca Raton, FL, USA, third edition, 2012. ISBN 1-4398-9834-0 (hardcover). xvi + 351 pp. LCCN QA37.3 .K73 2012. URL http://marc.crcnetbase.com/isbn/9781439898345.

Kostinger:2012:SBL

[KRB12] Martin Köstinger, Peter M. Roth, and Horst Bischof. Synergy-based learning of facial identity. *Lecture Notes in Computer Science*, 7476:195–204, 2012.

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32717-9_20/.

Kannan:2013:NQF

[KRDH13] S. R. Kannan, S. Ramthilagam, R. Devi, and Yueh-Min Huang. Novel quadratic fuzzy c-means algorithms for effective data clustering problems. *The Computer Journal*, 56(3): 393–406, March 2013. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/56/3/393.full.pdf+html.

Krenn:2013:AWI

[Kre13] Daniel Krenn. Analysis of the width-w non-adjacent form in conjunction with hyperelliptic curve cryptography and with lattices. *Theoretical Computer Science*, 491(??):47–70, June 17, 2013. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397513002685.

K:2018:AAF

[KRH18] Keerthi K., Chester Rebeiro, and Aritra Hazra. An algorithmic approach to formally verify an ECC library. *ACM Transactions on Design Automation of Electronic Systems*, 23(5): 63:1–63:??, October 2018. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Khan:2010:RCB

[KRM+10] Zeeshan Shafi Khan, Khalid Rashid, Fahad Bin Muhaya, Qutbuddin, and Aneel Rahim. Realization of call-back authentication (CBA) for secure web to cellular phone SMS communication. *Computers and Mathematics with Applications*, 60(2):198–208, July 2010. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122110000118.

King:2011:BBB

[KS11] Valerie King and Jared Saia. Breaking the $O(n^2)$ bit barrier: Scalable Byzantine agreement with an adaptive adversary. *Journal of the ACM*, 58 (4):18:1–18:24, July 2011. CODEN JACOAH. ISSN 0004-5411.

Kolesnikov:2012:LPP

[KS12] Vladimir Kolesnikov and Abdullatif Shikfa. On the limits of privacy provided by order-preserving encryption. *Bell Labs Tech-*

nical Journal, 17(3):135–146, December 2012. CODEN BLTJFD. ISSN 1089-7089 (print), 1538-7305 (electronic).

Kumar:2015:RGB

[KS15] Sachin Kumar and Rajendra Kumar Sharma. Random-grid based region incrementing visual secret sharing. *Fundamenta Informaticae*, 137(3):369–386, July 2015. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Kalayappan:2018:PAH

[KS18a] Rajshekar Kalayappan and Smruti R. Sarangi. Providing accountability in heterogeneous systems-on-chip. *ACM Transactions on Embedded Computing Systems*, 17(5):83:1–83:??, November 2018. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3241048`.

Karthiga:2018:PSA

[KS18b] I Karthiga and Sharmila Sankar. Providing secret authentication in clustered security architecture for cloud-based WBAN. *The Computer Journal*, 61(2):223–232, February 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/61/2/223/3861967`.

Korac:2019:FMU

[KS19] Dragan Korać and Dejan Simić. Fishbone model and universal authentication framework for evaluation of multifactor authentication in mobile environment. *Computers & Security*, 85(??):313–332, August 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404818307375`.

Kocabas:2016:ESM

[KSA16] Ovunc Kocabas, Tolga Soyata, and Mehmet K. Aktas. Emerging security mechanisms for medical cyber physical systems. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 13(3):401–416, May 2016. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Khan:2017:TPK

[KSB+17] Suleman Khan, Muhammad Shiraz, Laleh Boroumand, Abdullah Gani, and Muhammad Khurram Khan. Towards port-knocking authentication methods for mobile cloud computing.

Journal of Network and Computer Applications, 97(??):66–78, November 1, 2017. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804517302813`.

Kiljan:2017:SAC

[KSD+17] Sven Kiljan, Koen Simoens, Danny De Cock, Marko Van Eekelen, and Harald Vranken. A survey of authentication and communications security in online banking. *ACM Computing Surveys*, 49(4):61:1–61:??, February 2017. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Kwon:2018:CEI

[KSH18a] Jihoon Kwon, Seog Chung Seo, and Seokhie Hong. Correction to: An efficient implementation of pairing-based cryptography on MSP430 processor. *The Journal of Supercomputing*, 74(5):2254, May 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://link.springer.com/content/pdf/10.1007/s11227-018-2320-y.pdf`. See [KSH18b].

Kwon:2018:EIP

[KSH18b] Jihoon Kwon, Seog Chung Seo, and Seokhie Hong. An efficient implementation of pairing-based cryptography on MSP430 processor. *The Journal of Supercomputing*, 74(3):1394–1417, March 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Ksiezopolski:2012:QMQ

[Ksi12] Bogdan Ksiezopolski. QoP-ML: Quality of protection modelling language for cryptographic protocols. *Computers & Security*, 31(4):569–596, June 2012. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404812000107`.

Kim:2012:SSS

[KSSY12] Cheonshik Kim, Dongkyoo Shin, Dongil Shin, and Ching-Nung Yang. A $(2, 2)$ secret sharing scheme based on Hamming code and AMBTC. *Lecture Notes in Computer Science*, 7197:129–139, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-28490-8_14/`.

Klingler:2013:UPT

[KSU13] Lee Klingler, Rainer Steinwandt, and Dominique Unruh. On using probabilistic Turing machines to model participants in cryptographic protocols. *Theoretical Computer Science*, 501(??):49–51, August 27, 2013. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397513003666.

Kim:2012:SAH

[KTA12] Hyoungshick Kim, John Tang, and Ross Anderson. Social authentication: Harder than it looks. *Lecture Notes in Computer Science*, 7397:1–15, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32946-3_1/.

Khamis:2018:CCT

[KTM+18] Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. CueAuth: Comparing touch, mid-air gestures, and gaze for cue-based authentication on situated displays. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2(4):1–22, December 2018. CODEN ???? ISSN 2474-9567 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3287052.

Kalita:2019:NSM

[KTM19] Manashee Kalita, Themrichon Tuithung, and Swanirbhar Majumder. A new steganography method using integer wavelet transform and least significant bit substitution. *The Computer Journal*, 62 (11):1639–1655, November 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/11/1639/5369945.

Kawachi:2012:SKE

[KTT12] Akinori Kawachi, Hirotoshi Takebe, and Keisuke Tanaka. Symmetric-key encryption scheme with multi-ciphertext non-malleability. *Lecture Notes in Computer Science*, 7631: 123–137, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34117-5_8/.

Kobayashi:2016:ASC

[KTUI16] Kei Kobayashi, Yosuke Totani, Keisuke Utsu, and Hiroshi Ishii. Achieving secure communication over

MANET using secret sharing schemes. *The Journal of Supercomputing*, 72(3): 1215–1225, March 2016. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-016-1657-3.

Klisowski:2012:CCP

[KU12] Michal Klisowski and Vasyl Ustimenko. On the comparison of cryptographical properties of two different families of graphs with large cycle indicator. *Mathematics in Computer Science*, 6(2):181–198, June 2012. CODEN ???? ISSN 1661-8270 (print), 1661-8289 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=1661-8270&volume=6&issue=2&spage=181.

Kai:2014:FSD

[KU14] Hiroshi Kai and Keita Ueda. Fake shares detection on a visual secret sharing scheme by rational interpolation. *ACM Communications in Computer Algebra*, 48(3/4):124–126, September 2014. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Kumagai:2010:UGS

[Kum10] J. Kumagai. UK gets a space agency of its very own. *IEEE Spectrum*, 47 (2):11, February 2010. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Kupcu:2013:DTT

[Küp13] Alptekin Küpçü. Distributing trusted third parties. *ACM SIGACT News*, 44 (2):92–112, June 2013. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Kupcu:2015:OAS

[Küp15] Alptekin Küpçü. Official arbitration with secure cloud storage application. *The Computer Journal*, 58(4):831–852, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/831.

Kushner:2013:RSS

[Kus13] David Kushner. The real story of Stuxnet. *IEEE Spectrum*, 50(3):48–53, March 2013. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Kuznetsov:2011:APP

[Kuz11] A. Kuznetsov. Analytic proof of Pecherskii–Rogozin identity and Wiener–Hopf factorization. *The-*

ory of Probability and its Applications, 55(3):432–443, ???? 2011. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). URL http://epubs.siam.org/tvp/resource/1/tprbau/v55/i3/p432_s1.

Kshetri:2018:BEV

[KV18] N. Kshetri and J. Voas. Blockchain-enabled e-voting. *IEEE Software*, 35(4):95–99, July/August 2018. CODEN IESOEG. ISSN 0740-7459 (print), 1937-4194 (electronic).

Kilgallin:2019:FRK

[KV19a] Jonathan Kilgallin and Ross Vasko. Factoring RSA keys in the IoT era. In IEEE, editor, *First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA): 12–14 December 2019*, pages 184–189. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2019. URL https://ieeexplore.ieee.org/document/9014350.

Kim:2019:IED

[KV19b] Jungwon Kim and Jeffrey S. Vetter. Implementing efficient data compression and encryption in a persistent key–value store for HPC. *The International Journal of High Performance Computing Applications*, 33(6):1098–1112, November 1, 2019. CODEN IHPCFL. ISSN 1094-3420 (print), 1741-2846 (electronic). URL https://journals.sagepub.com/doi/full/10.1177/1094342019847264.

Kiljan:2018:ETA

[KVvE18] Sven Kiljan, Harald Vranken, and Marko van Eekelen. Evaluation of transaction authentication methods for online banking. *Future Generation Computer Systems*, 80(??):430–447, March 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16301352.

Karpovsky:2014:DSS

[KW14] M. Karpovsky and Zhen Wang. Design of strongly secure communication and computation channels by nonlinear error detecting codes. *IEEE Transactions on Computers*, 63(11):2716–2728, November 2014. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Kuo:2016:SDD

[KWH16] Wen-Chung Kuo, Chun-Cheng Wang, and Hong-

Ching Hou. Signed digit data hiding scheme. *Information Processing Letters*, 116(2):183–191, February 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019015001404`.

Koyama:2012:NTD

[KWS+12] Takuma Koyama, Lei Wang, Yu Sasaki, Kazuo Sakiyama, and Kazuo Ohta. New truncated differential cryptanalysis on 3D block cipher. *Lecture Notes in Computer Science*, 7232:109–125, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-29101-2_8/`.

Kamal:2010:EIN

[KY10] A. A. Kamal and A. M. Youssef. Enhanced implementation of the NTRUEncrypt algorithm using graphics cards. In Chaudhuri et al. [CGB+10], pages 168–174. ISBN 1-4244-7675-5. LCCN ????

Kreutz:2018:KPS

[KYEV+18] D. Kreutz, J. Yu, P. Esteves-Veríssimo, C. Magalhães, and F. M. V. Ramos. The KISS principle in software-defined networking: A framework for secure communications. *IEEE Security & Privacy*, 16(5): 60–70, September/October 2018. ISSN 1540-7993 (print), 1558-4046 (electronic).

Kuo:2018:DRA

[KYH18] Tsung-Min Kuo, Sung-Ming Yen, and Meng-Che Han. Dynamic reversed accumulator. *International Journal of Information Security*, 17 (2):183–191, April 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-017-0360-6`.

Kate:2010:PBO

[KZG10] Aniket Kate, Greg M. Zaverucha, and Ian Goldberg. Pairing-based onion routing with improved forward secrecy. *ACM Transactions on Information and System Security*, 13(4):29:1–29:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Kiayias:2017:EEV

[KZZ17] Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang. An efficient E2E verifiable E-voting system without setup assumptions. *IEEE Security & Privacy*, 15(3):

14–23, May/June 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2017/03/msp2017030014-abs.html.

Lu:2010:MSC

[LA10] H. Karen Lu and Asad M. Ali. Making smart cards truly portable. *IEEE Security & Privacy*, 8(2):28–34, March/April 2010. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Lathey:2015:IEE

[LA15] Ankita Lathey and Pradeep K. Atrey. Image enhancement in encrypted domain over cloud. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 11(3):38:1–38:??, January 2015. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Lackey:2015:UHP

[Lac15] Scott Lackey. Using `hiera` with `puppet`. *Linux Journal*, 2015(251):1:1–1:??, March 2015. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://dl.acm.org/ft_gateway.cfm?id=2754912.

Lallie:2014:PCM

[Lal14] Harjinder Singh Lallie. The problems and challenges of managing crowd sourced audio-visual evidence. *Future Internet*, 6(2):190–202, April 01, 2014. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/6/2/190.

Liang:2015:SEC

[LAL+15] Kaitai Liang, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Yong Yu, and Anjia Yang. A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing. *Future Generation Computer Systems*, 52(??):95–108, November 2015. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X14002507.

Lamonica:2013:LDQ

[Lam13] M. Lamonica. Long-distance quantum cryptography [news]. *IEEE Spectrum*, 50(8):12–13, August 2013. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Landau:2010:SSR

[Lan10] Susan Eva Landau. *Surveillance or security?: The* *risks posed by new wiretapping technologies*. MIT Press, Cambridge, MA, USA, 2010. ISBN 0-262-01530-7 (hardcover),0-262-29558-X (e-book). xvi + 383 pp. LCCN TK5102.85 .L36 2010.

Langsworth:2011:USA

[Lan11] Anthony Langsworth. Using static analysis tools to detect and correct noncompliant cryptography. *ACM SIGSOFT Software Engineering Notes*, 36(6): 1–7, November 2011. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

Langley:2013:EDC

[Lan13] Adam Langley. Enhancing digital certificate security. Web site., 2013. URL `http://googleonlinesecurity.blogspot.com/2013/01/enhancing-digital-certificate-security.html`.

Landau:2017:LCI

[Lan17] Susan Landau. *Listening in: Cybersecurity in an insecure age*. Yale University Press, New Haven, CT, USA, 2017. ISBN 0-300-22744-2 (hardcover). xiv + 221 pp. LCCN K3264.C65 L38 2017?

Lopez-Alt:2017:MFH

[LATV17] Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan. Multikey fully homomorphic encryption and applications. *SIAM Journal on Computing*, 46 (6):1827–1892, ???? 2017. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Launchbury:2012:TBC

[Lau12] John Launchbury. Theorem-based circuit derivation in Cryptol. *ACM SIGPLAN Notices*, 47(3):185–186, March 2012. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Lauter:2017:POL

[Lau17] Kristin Lauter. Postquantum opportunities: Lattices, homomorphic encryption, and supersingular isogeny graphs. *IEEE Security & Privacy*, 15(4): 22–27, July/August 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `https://www.computer.org/csdl/mags/sp/2017/04/msp2017040022-abs.html`.

Lazarus:2015:RE

[Laz15] M. Lazarus. Radar everywhere. *IEEE Spectrum*, 52 (2):52–59, February 2015. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Liu:2013:PAE

[LB13] Bin Liu and Bevan M. Baas. Parallel AES encryption engines for many-core processor arrays. *IEEE Transactions on Computers*, 62(3):536–547, March 2013. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Loreti:2018:PAB

[LBC18] Pierpaolo Loreti, Lorenzo Bracciale, and Alberto Caponi. Push attack: Binding virtual and real identities using mobile push notifications. *Future Internet*, 10(2):13, January 31, 2018. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/10/2/13.

Luo:2012:ESI

[LBOX12] Jianqiang Luo, Kevin D. Bowers, Alina Oprea, and Lihao Xu. Efficient software implementations of large finite fields GF(2^n) for secure storage applications. *ACM Transactions on Storage*, 8(1):2:1–2:??, February 2012. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic).

Lupu:2012:IBK

[LBR12] Radu Lupu, Eugen Borcoci, and Tinku Rasheed. Identity-based key derivation method for low delay inter-domain handover re-authentication service. *Lecture Notes in Computer Science*, 7161: 162–175, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29615-4_12/.

Lu:2013:CSA

[LC13] Linzhen Lu and Shaozhen Chen. A compress slide attack on the full GOST block cipher. *Information Processing Letters*, 113(17):634–639, August 30, 2013. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013001543.

Liu:2015:IAC

[LC15] Qingzhong Liu and Zhongxue Chen. Improved approaches with calibrated neighboring joint density to steganalysis and seam-carved forgery detection in JPEG images. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 5(4):63:1–63:??, January 2015. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic).

Laxmi:2017:GGS

[LC17] B. Prathusha Laxmi and A. Chilambuchelvan. GSR: Geographic Secured Routing using SHA-3 algorithm for node and message authentication in wireless sensor networks. *Future Generation Computer Systems*, 76(??):98–105, November 2017. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X1730986X.

Liu:2013:IAG

[LCCJ13] Yining Liu, Chi Cheng, Jianyu Cao, and Tao Jiang. An improved authenticated group key transfer protocol based on secret sharing. *IEEE Transactions on Computers*, 62(11):2335–2336, November 2013. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Liu:2015:IEP

[LCDP15] H. Liu, L. Chen, Z. Davar, and M. R. Pour. Insecurity of an efficient privacy-preserving public auditing scheme for cloud data storage. *J.UCS: Journal of Universal Computer Science*, 21(3):473–??, ???? 2015. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL http://www.jucs.org/jucs_21_3/insecurity_of_an_efficient.

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 ????

Lavington:2012:ATH

[LCKBJ12] S. H. (Simon Hugh) Lavington, Martin Campbell-Kelly, Christopher P. Burton, and Roger Johnson, editors. *Alan Turing and his contemporaries: building the world's first computers*. British Computer Society, London, UK, 2012. ISBN 1-906124-90-6 (paperback), 1-78017-105-6 (PDF e-book), 1-78017-106-4 (ePub e-book), 1-78017-107-2 (Kindle e-book). xiv + 111 pp. LCCN QA76.17 .A423 2012. UK£11.69.

Li:2015:NAC

[LCL+15] Jin Li, Xiaofeng Chen, Jingwei Li, Chunfu Jia, Jianfeng Ma, and Wenjing Lou. New access control systems based on outsourced attribute-based encryption. *Journal of Computer Security*, 23(6):659–683, ???? 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lee:2017:SUE

[LCL+17a] Kwangsu Lee, Seung Geol Choi, Dong Hoon Lee, Jong Hwan Park, and Moti Yung. Self-updatable encryption: Time constrained access control with hidden attributes and better efficiency. *Theoretical Computer Science*, 667(??):51–92, March 8, 2017. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397516307551.

Liu:2017:GAU

[LCL17b] Can Liu, Gradeigh D. Clark, and Janne Lindqvist. Guessing attacks on user-generated gesture passwords. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 1(1):3:1–3:24, March 2017. CODEN ???? ISSN 2474-9567. URL http://dl.acm.org/citation.cfm?id=3053331.

Li:2015:CEH

[LCLL15] Chen Li, Le Chen, Rongxing Lu, and Hui Li. Comment on "An Efficient Homomorphic MAC with Small Key Size for Authentication in Network Coding". *IEEE Transactions on Computers*, 64(3):882–883, March 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). See [CJ13].

Li:2017:RNF

[LCLW17] Yang Li, Mengting Chen, Zhe Liu, and Jian Wang. Reduction in the number of fault injections for blind fault attack on SPN block ciphers. *ACM Transactions on Embedded Computing Systems*, 16(2):55:1–55:??, April 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Li:2017:CCF

[LCM+17] Jenny S. Li, Li-Chiou Chen, John V. Monaco, Pranjal Singh, and Charles C. Tappert. A comparison of classifiers and features for authorship authentication of social networking messages. *Concurrency and Computation: Practice and Experience*, 29(14), July 25, 2017. CODEN CCPEBO. ISSN 1532-0626

(print), 1532-0634 (electronic).

Liu:2018:VRU

[LCR+18] Rui Liu, Cory Cornelius, Reza Rawassizadeh, Ronald Peterson, and David Kotz. Vocal resonance: Using internal body voice for wearable authentication. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2(1): 1–23, March 2018. CODEN ???? ISSN 2474-9567 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3191751.

Liang:2014:CCS

[LCT+14] Kaitai Liang, Cheng-Kang Chu, Xiao Tan, Duncan S. Wong, Chunming Tang, and Jianying Zhou. Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts. *Theoretical Computer Science*, 539(??):87–105, June 19, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397514003326.

Liu:2016:EQD

[LCW+16] Yang Liu, Zhu Cao, Cheng Wu, Daiji Fukuda, Lixing You, Jiaqiang Zhong, Takayuki Numata, Sijing Chen, Weijun Zhang, Sheng-Cai Shi, Chao-Yang Lu, Zhen Wang, Xiongfeng Ma, Jingyun Fan, Qiang Zhang, and Jian-Wei Pan. Experimental quantum data locking. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 94(2):020301, August 2016. CODEN PLRAAN. ISSN 1050-2947 (print), 1094-1622, 1538-4446, 1538-4519. URL http://link.aps.org/doi/10.1103/PhysRevA.94.020301.

Liu:2016:NOP

[LCY+16] Zheli Liu, Xiaofeng Chen, Jun Yang, Chunfu Jia, and Ilsun You. New order preserving encryption model for outsourced databases in cloud environments. *Journal of Network and Computer Applications*, 59(??):198–207, January 2016. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804514001350.

Louchene:2013:WMR

[LD13] Ahmed Louchene and Ammar Dahmani. Watermarking method resilient to RST and compression based on DWT, LPM and phase correlation. *International Journal of Com-

puter Applications, 35(1): 36–43, 2013. ISSN 1206-212X (print), 1925-7074 (electronic). URL https://www.tandfonline.com/doi/full/10.2316/Journal.202.2013.1.202-3503.

Lotz:2015:SCS

[LDB+15] Volkmar Lotz, Francesco Di Cerbo, Michele Bezzi, Samuel Paul Kaluvuri, Antonino Sabetta, and Slim Trabelsi. Security certification for service-based business ecosystems. *The Computer Journal*, 58(4):709–723, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/709.

Lasc:2013:DDA

[LDC13] Ioana Lasc, Reiner Dojen, and Tom Coffey. On the detection of desynchronisation attacks against security protocols that use dynamic shared secrets. *Computers & Security*, 32(??):115–129, February 2013. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404812001678.

Launchbury:2012:ELT

[LDDAM12] John Launchbury, Iavor S. Diatchki, Thomas DuBuisson, and Andy Adams-Moran. Efficient lookup-table protocol in secure multiparty computation. *ACM SIGPLAN Notices*, 47(9):189–200, September 2012. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Li:2014:PSC

[LDZ+14] Jiguo Li, Haiting Du, Yichen Zhang, Tao Li, and Yuexin Zhang. Provably secure certificate-based key-insulated signature scheme. *Concurrency and Computation: Practice and Experience*, 26(8):1546–1560, June 10, 2014. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Li:2016:CBK

[LDZ16] Jiguo Li, Haiting Du, and Yichen Zhang. Certificate-based key-insulated signature in the standard model. *The Computer Journal*, 59(7):1028–1039, July 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/7/1028.

Liu:2019:TTR

[LDZW19] Zhenhua Liu, Shuhong Duan, Peilin Zhou, and Baocang Wang. Traceablethen-revocable ciphertext-policy attribute-based encryption scheme. *Future Generation Computer Systems*, 93(??):903–913, April 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X17320964`.

Ledin:2016:RME

[Led16] George Ledin, Jr. Review of: *The Mathematics of Encryption: An Elementary Introduction* by Margaret Cozzens and Steven J. Miller. *ACM SIGACT News*, 47(3):19–21, September 2016. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Lewand:2010:PC

[Lew10] Robert Edward Lewand. The perfect cipher. *The Mathematical Gazette*, 94 (531):401–411, November 2010. CODEN MAGAAS. ISSN 0025-5572.

Liu:2019:DVP

[LEW19] Y. Liu, M. F. Ezerman, and H. Wang. Double verification protocol via secret sharing for low-cost RFID tags. *Future Generation Computer Systems*, 90(??):118–128, January 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X17323518`.

Lago-Fernandez:2014:NAA

[LFGCGCRP14] J. Lago-Fernández, F. Gil-Castiñeira, F. J. González-Castaño, and A. Román-Portabales. A new approach to authenticating and encrypting Voice over Internet Protocol communications. *Software—Practice and Experience*, 44(5): 593–619, May 2014. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Leung:2018:TTA

[LFH18] Ho-Man Colman Leung, Chi-Wing Fu, and Pheng-Ann Heng. TwistIn: Tangible authentication of smart devices via motion co-analysis with a smartwatch. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2(2):1–24, July 2018. CODEN ???? ISSN 2474-9567 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3214275`.

Luo:2019:SCT

[LFK19] Chao Luo, Yunsi Fei, and David Kaeli. Side-channel timing attack of RSA on a GPU. *ACM Transactions* *on Architecture and Code Optimization*, 16(3):32:1–32:??, August 2019. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3341729`.

Liu:2016:LCR

[LFW+16] Yu Liu, Kai Fu, Wei Wang, Ling Sun, and Meiqin Wang. Linear cryptanalysis of reduced-round SPECK. *Information Processing Letters*, 116(3):259–266, March 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019015001891`.

Liang:2015:CPA

[LFWS15] Kaitai Liang, Liming Fang, Duncan S. Wong, and Willy Susilo. A ciphertext-policy attribute-based proxy re-encryption scheme for data sharing in public clouds. *Concurrency and Computation: Practice and Experience*, 27(8):2004–2027, June 10, 2015. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Li:2018:CIC

[LFX+18] M. Li, H. Fan, Y. Xiang, Y. Li, and Y. Zhang. Cryptanalysis and improvement of a chaotic image encryption by first-order time-delay system. *IEEE MultiMedia*, 25(3):92–101, July/September 2018. CODEN IEMUE4. ISSN 1070-986x (print), 1941-0166 (electronic).

Li:2017:PCL

[LFZ+17] Cong Li, Yuejian Fang, Xing Zhang, Cancan Jin, Qingni Shen, and Zhonghai Wu. A practical construction for large universe hierarchical attribute-based encryption. *Concurrency and Computation: Practice and Experience*, 29(17), September 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Lekkas:2010:PMT

[LG10] Dimitrios Lekkas and Dimitris Gritzalis. e-Passports as a means towards a Globally Interoperable Public Key Infrastructure. *Journal of Computer Security*, 18(3):379–396, ???? 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lancrenon:2012:IPI

[LG12] Jean Lancrenon and Roland Gillard. Isolating partial information of indistinguishable encryptions. *Lecture Notes in Computer Science*, 7163:34–48, 2012. CODEN LNCSD9. ISSN

0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29804-2_3/.

Liu:2017:ECC

[LGH+17] Z. Liu, J. Großschädl, Z. Hu, K. Järvinen, H. Wang, and I. Verbauwhede. Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the Internet of Things. *IEEE Transactions on Computers*, 66(5):773–785, May 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Lan:2010:RNG

[LGKY10] Jingjing Lan, Wang Ling Goh, Zhi Hui Kong, and Kiat Seng Yeo. A random number generator for low power cryptographic application. In *2010 International SoC Design Conference (ISOCC)*, pages 328–331. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5682906.

Li:2012:FDM

[LGL+12] Wei Li, Dawu Gu, Zhiqiang Liu, Ya Liu, and Xiaohu Huang. Fault detection of the MacGuffin Cipher against differential fault attack. *Lecture Notes in Computer Science*, 7222:102–112, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32298-3_7/.

Lee:2017:FFE

[LGLK17] Junghee Lee, Kalidas Ganesh, Hyuk-Jun Lee, and Youngjae Kim. FESSD: A fast encrypted SSD employing on-chip access-control memory. *IEEE Computer Architecture Letters*, 16(2):115–118, July/December 2017. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Liu:2012:LFA

[LGLL12] Zhiqiang Liu, Dawu Gu, Ya Liu, and Wei Li. Linear fault analysis of block ciphers. *Lecture Notes in Computer Science*, 7341:241–256, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31284-7_15/.

Labati:2016:BRA

[LGM+16] Ruggero Donida Labati, Angelo Genovese, Enrique

Muñoz, Vincenzo Piuri, Fabio Scotti, and Gianluca Sforza. Biometric recognition in automated border control: a survey. *ACM Computing Surveys*, 49(2):24:1–24:??, September 2016. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Lee:2019:TES

[LGP19] Wai-Kong Lee, Bok-Min Goi, and Raphael C.-W. Phan. Terabit encryption in a second: Performance evaluation of block ciphers in GPU with Kepler, Maxwell, and Pascal architectures. *Concurrency and Computation: Practice and Experience*, 31(11): e5048:1–e5048:??, June 10, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Lopez-Garcia:2014:PBB

[LGPRH14] Lourdes López-García, Luis J. Dominguez Perez, and Francisco Rodríguez-Henríquez. A pairing-based blind signature e-voting scheme. *The Computer Journal*, 57(10):1460–1471, October 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/57/10/1460.

Li:2014:SCA

[LGR14] Peng Li, Debin Gao, and Michael K. Reiter. StopWatch: a cloud architecture for timing channel mitigation. *ACM Transactions on Information and System Security*, 17(2):8:1–8:??, November 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Liu:2012:FVC

[LGWY12] Feng Liu, Teng Guo, ChuanKun Wu, and Ching-Nung Yang. Flexible visual cryptography scheme without distortion. *Lecture Notes in Computer Science*, 7128:211–227, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32205-1_18/.

Lee:2010:ISC

[LH10a] Donghoon Lee and Seokhie Hong, editors. *Information, security and cryptology – ICISC 2009: 12th international conference, Seoul, Korea, December 2–4, 2009, revised selected papers*, volume 5984 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN

3-642-14422-5 (softcover). LCCN ????

Lee:2010:CGC

[LH10b] Moon Sung Lee and Sang Geun Hahn. Cryptanalysis of the GGH cryptosystem. *Mathematics in Computer Science*, 3(2): 201–208, April 2010. CODEN ???? ISSN 1661-8270 (print), 1661-8289 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=1661-8270&volume=3&issue=2&spage=201.

Li:2010:EBB

[LH10c] Chun-Ta Li and Min-Shiang Hwang. An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*, 33 (1):1–5, January 2010. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804509001192.

Lee:2011:IMS

[LH11a] Jung-San Lee and Ming-Huang Hsieh. An interactive mobile SMS confirmation method using secret sharing technique. *Computers & Security*, 30(8):830–839, November 2011. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404811000836.

Lee:2011:PSE

[LH11b] Tian-Fu Lee and Tzonelih Hwang. Provably secure and efficient authentication techniques for the global mobility network. *The Journal of Systems and Software*, 84(10):1717–1725, October 2011. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211001099.

Lin:2011:NIB

[LH11c] Han-Yu Lin and Chien-Lung Hsu. A novel identity-based key-insulated convertible authenticated encryption scheme. *International Journal of Foundations of Computer Science (IJFCS)*, 22(3):739–756, April 2011. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Lertvorratham:2012:ISM

[LH12] Supachote Lertvorratham and Pipat Hiranvanichakorn. Integrating secure multipath mobile ad hoc network with self-authentication strategy. *International Journal of Computer Ap-*

plications, 34(3):174–184, 2012. ISSN 1206-212X (print), 1925-7074 (electronic). URL https://www.tandfonline.com/doi/full/10.2316/Journal.202.2012.3.202-3245.

Liao:2013:NMS

[LH13] Yi-Pin Liao and Chih-Ming Hsiao. A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients. *Future Generation Computer Systems*, 29(3):886–900, March 2013. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X12000829.

Li:2014:ARM

[LH14] Cai Li and Jiankun Hu. Attacks via record multiplicity on cancelable biometrics templates. *Concurrency and Computation: Practice and Experience*, 26(8):1593–1605, June 10, 2014. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Lenstra:2012:PK

[LHA+12a] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter. Public keys. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Proceedings of the 32nd Annual Conference on Advances in Cryptology*, volume 7417 of *Lecture Notes in Computer Science*, pages 626–642. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. URL https://dl.acm.org/doi/10.1007/978-3-642-32009-5_37.

Lenstra:2012:RWW

[LHA+12b] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter. Ron was wrong, Whit is right. Report, EPFL IC LACAL, Lausanne, Switzerland, February 14, 2012. 16 pp. URL http://eprint.iacr.org/2012/064.

Lum:2016:QEM

[LHA+16] Daniel J. Lum, John C. Howell, M. S. Allman, Thomas Gerrits, Varun B. Verma, Sae Woo Nam, Cosmo Lupo, and Seth Lloyd. Quantum enigma machine: Experimentally demonstrating quantum data locking. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 94(2):022315, August 2016. CODEN PLRAAN. ISSN 1050-2947 (print), 1094-1622, 1538-4446, 1538-4519. URL http:/

/link.aps.org/doi/10.1103/PhysRevA.94.022315.

Li:2012:BVS

[LHF12] Long-Hai Li, Cheng-Qiang Huang, and Shao-Feng Fu. Boardroom voting scheme with unconditionally secret ballots based on DC-Net. *Lecture Notes in Computer Science*, 7645: 220–232, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34601-9_17/.

Lin:2011:ICA

[LHH11] Han-Yu Lin, Chien-Lung Hsu, and Shih-Kun Huang. Improved convertible authenticated encryption scheme with provable security. *Information Processing Letters*, 111(13):661–666, July 1, 2011. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019011000846.

Lin:2018:BBB

[LHH+18] Chao Lin, Debiao He, Xinyi Huang, Kim-Kwang Raymond Choo, and Athanasios V. Vasilakos. BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *Journal of Network and Computer Applications*, 116(??):42–52, August 15, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518301619.

Li:2010:AIS

[LHKR10] Feifei Li, Marios Hadjieleftheriou, George Kollios, and Leonid Reyzin. Authenticated index structures for aggregation queries. *ACM Transactions on Information and System Security*, 13(4):32:1–32:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Li:2014:SOA

[LHL+14] Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang. Securely outsourcing attribute-based encryption with checkability. *IEEE Transactions on Parallel and Distributed Systems*, 25(8):2201–2210, August 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Liu:2015:SSP

[LHL15] Jianghua Liu, Xinyi Huang, and Joseph K. Liu. Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption. *Future Generation Computer Systems*, 52(??):67–76, November 2015. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X14002076`.

Li:2018:OPP

[LHL+18] Tong Li, Zhengan Huang, Ping Li, Zheli Liu, and Chunfu Jia. Outsourced privacy-preserving classification service over encrypted data. *Journal of Network and Computer Applications*, 106(??):100–110, March 15, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804517304356`.

Li:2010:CCB

[LHM+10] Jiguo Li, Xinyi Huang, Yi Mu, Willy Susilo, and Qianhong Wu. Constructions of certificate-based signature secure against key replacement attacks. *Journal of Computer Security*, 18(3):421–449, ???? 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lerch-Hostalot:2013:LMS

[LHM13] Daniel Lerch-Hostalot and David Megías. LSB matching steganalysis based on patterns of pixel differences and random embedding. *Computers & Security*, 32(??):192–206, February 2013. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404812001745`.

Lian:2014:SSA

[LHM14] Yanling Lian, Xinyi Huang, and Yi Mu. SA^3: Self-adaptive anonymous authentication for dynamic authentication policies. *Future Generation Computer Systems*, 30(??):133–139, January 2014. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X13001210`.

Lin:2015:CND

[LHM+15] Hui Lin, Jia Hu, Jianfeng Ma, Li Xu, and Li Yang. CRM: a new dynamic cross-layer reputation computation model in wireless networks. *The Computer Journal*, 58(4):656–667, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/4/656`.

Liu:2018:HMS

[LHW18] Jianqiang Liu, Shuai Huo, and Yi Wang. A hierarchical mapping system for flat identifier to locator resolution based on active degree. *Future Internet*, 10(8):75, August 08, 2018. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/10/8/75.

Liu:2012:ESS

[LHYZ12] Yan-Xiao Liu, Lein Harn, Ching-Nung Yang, and Yu-Qing Zhang. Efficient (n, t, n) secret sharing schemes. *The Journal of Systems and Software*, 85(6):1325–1332, June 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212000234.

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:2017:AMA

[LIK+17] Xiong Li, Maged Hamada Ibrahim, Saru Kumari, Arun Kumar Sangaiah, Vidushi Gupta, and Kim-Kwang Raymond Choo. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 129 (part 2)(??):429–443, December 24, 2017. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128617301044.

Lim:2011:NAN

[Lim11] Chae Hoon Lim. A note on the average number of RSA fixed points. *Theoretical Computer Science*, 412(35):4729–4737, August 12, 2011. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Lin:2014:IVW

[Lin14a] Pei-Yu Lin. Imperceptible visible watermarking based on postcamera histogram operation. *The Journal of Systems and Software*, 95(??):194–208, September 2014. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121214001071.

Lindell:2014:TCT

[Lin14b] Yehuda Lindell, editor. *Theory of cryptography: 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24–26, 2014 proceedings*, volume 8349 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2014. ISBN 3-642-54241-7 (paperback), 3-642-54242-5 (ebk.). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T473 2014. URL http://www.springerlink.com/content/978-3-642-54242-8.

Lin:2015:DVS

[Lin15] Pei-Yu Lin. Double verification secret sharing mechanism based on adaptive pixel pair matching. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 11(3):36:1–36:??, January 2015. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Lindell:2017:TFC

[Lin17] Yehuda Lindell, editor. *Tutorials on the Foundations of Cryptography: Dedicated to Oded Goldreich*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2017. ISBN 3-319-57047-1, 3-319-57048-X (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xv + 450 pp. LCCN QA76.9.A25 T84 2017. URL http://www.springerlink.com/content/978-3-319-57048-8.

Litton:2014:TFA

[Lit14] James Litton. Two-factor authentication system for Apache and SSH. *Linux Journal*, 2014(239):4:1–4:??, March 2014. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Liu:2015:LBD

[LJ15] Huacui Liu and Chenhui Jin. Lower bounds of differential and linear active *S*-boxes for 3D-like structure. *The Computer Journal*, 58(4):904–921, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/904.

Liu:2016:LCP

[LJ16] Guo-Qiang Liu and Chen-Hui Jin. Linear cryptanalysis of PRESENT-like ciphers with secret permutation. *The Com-*

puter Journal, 59(4):549–558, April 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/59/4/549`.

Li:2017:MMA

[LJ17] Rongjia Li and Chenhui Jin. Meet-in-the-middle attack on 11-round 3D block cipher. *International Journal of Foundations of Computer Science (IJFCS)*, 28 (1), January 2017. CODEN IFCSEN. ISSN 0129-0541.

Li:2018:MMA

[LJ18] Rongjia Li and Chenhui Jin. Meet-in-the-middle attacks on reduced-round QARMA-64/128. *The Computer Journal*, 61(8):1158–1165, August 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/61/8/1158/4993053`.

Liu:2019:ICA

[LJ19] Hanqiu Liu and Chenhui Jin. An improvement of the CS attack to DSC cipher. *The Computer Journal*, 62(8):1158–1165, August 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/62/8/1158/5476715`.

Li:2016:IRI

[LJF16] Xinran Li, Chen-Hui Jin, and Fang-Wei Fu. Improved results of impossible differential cryptanalysis on reduced FOX. *The Computer Journal*, 59(4):541–548, April 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/59/4/541`.

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`.

Li:2017:SQS

[LJK17] Songbin Li, Yizhen Jia, and C.-C. Jay Kuo. Steganalysis of QIM steganography in low-bit-rate speech signals. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 25(5):1011–1022, ???? 2017. CODEN ????. ISSN 2329-9290. URL `http://ieeexplore.ieee.org/document/7867798/`.

Li:2012:OEA

[LJLC12] Jingwei Li, Chunfu Jia, Jin Li, and Xiaofeng Chen. Outsourcing encryption of attribute-based encryption with MapReduce. *Lecture Notes in Computer Science*, 7618:191–201, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34129-8_17/.

Lesi:2017:SAS

[LJP17] Vuk Lesi, Ilija Jovanov, and Miroslav Pajic. Security-aware scheduling of embedded control tasks. *ACM Transactions on Embedded Computing Systems*, 16 (5s):188:1–188:??, October 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Laszka:2014:STC

[LJS+14] Aron Laszka, Benjamin Johnson, Pascal Schöttle, Jens Grossklags, and Rainer Böhme. Secure team composition to thwart insider threats and cyber-espionage. *ACM Transactions on Internet Technology (TOIT)*, 14(2–3):19:1–19:??, October 2014. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Liu:2017:OOA

[LJW+17] Zechao Liu, Zoe L. Jiang, Xuan Wang, Xinyi Huang, S. M. Yiu, and Kunihiko Sadakane. Offline/online attribute-based encryption with verifiable outsourced decryption. *Concurrency and Computation: Practice and Experience*, 29(7):??, April 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Liu:2018:PAB

[LJWY18] Zechao Liu, Zoe L. Jiang, Xuan Wang, and S. M. Yiu. Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating. *Journal of Network and Computer Applications*, 108(??):112–123, April 15, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518300304.

Libert:2016:BRD

[LJY16] Benoît Libert, Marc Joye, and Moti Yung. Born and raised distributively: Fully distributed non-interactive adaptively-secure threshold signatures with short shares. *Theoretical Computer Science*, 645(??):1–24, September 13, 2016. CODEN TCSCDI. ISSN

0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397516001626.

Liu:2010:SVE

[LK10] Fuwen Liu and Hartmut Koenig. A survey of video encryption algorithms. *Computers & Security*, 29(1):3–15, February 2010. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404809000698.

Li:2012:BIB

[LK12] Fagen Li and Muhammad Khurram Khan. A biometric identity-based signcryption scheme. *Future Generation Computer Systems*, 28(1):306–310, January 2012. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X10002141.

Lee:2014:SPB

[LK14] Jooyoung Lee and Daesung Kwon. Security of permutation-based compression function lp231. *Information Processing Letters*, 114(7):372–381, July 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019014000325.

Lee:2018:NIC

[LK18] Eunsung Lee and Sang Woo Kim. Non-interactive conditional proxy re-signature in the standard model. *The Computer Journal*, 61 (12):1772–1782, December 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/12/1772/4965847.

Li:2012:IBO

[LKAT12] Fagen Li, Muhammad Khurram Khan, Khaled Alghathbar, and Tsuyoshi Takagi. Identity-based online/offline signcryption for low power devices. *Journal of Network and Computer Applications*, 35(1):340–347, January 2012. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S108480451100155X.

Lee:2019:VCS

[LKBK19] Kyuin Lee, Neil Klingensmith, Suman Banerjee, and Younghyun Kim. VoltKey: Continuous secret key generation based on power line noise for zero-involvement pairing and authentication. *Pro-*

ceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 3(3):1–26, September 2019. CODEN ???? ISSN 2474-9567 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3351251.

Leva:2013:ABN

[LKKL13] Tapio Levä, Miika Komu, Ari Keränen, and Sakari Luukkainen. Adoption barriers of network layer protocols: the case of host identity protocol. *Computer Networks (Amsterdam, Netherlands: 1999)*, 57(10):2218–2232, July 5, 2013. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128613000480.

Le:2011:RMA

[LL11] Duc-Phong Le and Chao-Liang Liu. Refinements of Miller's algorithm over Weierstrass curves revisited. *The Computer Journal*, 54(10):1582–1591, October 2011. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/54/10/1582.full.pdf+html.

Lee:2015:TSS

[LL15] Cheng-Chi Lee and Yan-Ming Lai. Toward a secure single sign-on mechanism for distributed computer networks. *The Computer Journal*, 58(4):934–943, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/934.

Lu:2016:PFC

[LL16a] Yang Lu and Jiguo Li. A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds. *Future Generation Computer Systems*, 62(??):140–147, September 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X1500360X.

Lu:2016:PSC

[LL16b] Yang Lu and Jiguo Li. Provably secure certificateless proxy signature scheme in the standard model. *Theoretical Computer Science*, 639(??):42–59, August 1, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397516301554.

Lee:2010:PMB

[LLC10] Hui-Lung Lee, Chia-Feng

Lee, and Ling-Hwei Chen. A perfect maze based steganographic method. *The Journal of Systems and Software*, 83(12):2528–2535, December 2010. CODEN JSSODM. ISSN 0164-1212.

Lee:2011:TAT

[LLC11] Cheng-Chi Lee, Chun-Ta Li, and Shun-Der Chen. Two attacks on a two-factor user authentication in wireless sensor networks. *Parallel Processing Letters*, 21(1):21–26, March 2011. CODEN PPLTEE. ISSN 0129-6264.

Li:2015:IBE

[LLC+15] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou. Identity-based encryption with outsourced revocation in cloud computing. *IEEE Transactions on Computers*, 64 (2):??, February 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Liu:2019:EEA

[LLD19] Peng Liu, Shunbin Li, and Qingyuan Ding. An energy-efficient accelerator based on hybrid CPU–FPGA devices for password recovery. *IEEE Transactions on Computers*, 68(2):170–181, February 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `https://ieeexplore.ieee.org/document/8453825/`.

Li:2015:ANA

[LLG15] Jie Li, Huang Lu, and Mohsen Guizani. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. *IEEE Transactions on Parallel and Distributed Systems*, 26 (4):938–948, April 2015. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL `http://csdl.computer.org/csdl/trans/td/2015/04/06748095-abs.html`.

Lyu:2019:SPP

[LLG19] Lin Lyu, Shengli Liu, and Dawu Gu. Structure-preserving public-key encryption with leakage-resilient CCA security. *Theoretical Computer Science*, 795(??):57–80, November 26, 2019. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S030439751930386X`.

Lin:2016:SCU

[LLGJ16] Jingqiang Lin, Bo Luo, Le Guan, and Jiwu Jing. Secure computing using registers and caches: The problem, challenges, and solutions. *IEEE Security & Privacy*, 14(6):63–70, November/December 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `https://www.computer.org/csdl/mags/sp/2016/06/msp2016060063-abs.html`.

Li:2017:ESD

[LLH17] Fagen Li, Bo Liu, and Jiaojiao Hong. An efficient signcryption for data access control in cloud computing. *Computing*, 99(5): 465–479, May 2017. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Lyu:2018:PKE

[LLH18] Lin Lyu, Shengli Liu, and Shuai Han. Public-key encryption with tight simulation-based selective-opening security. *The Computer Journal*, 61 (2):288–318, February 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/61/2/288/4259796`.

Li:2012:RIB

[LLHS12] Jian Li, Hongmei Liu, Jiwu Huang, and Yun Q. Shi. Reference index-based H.264 video watermarking scheme. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 8(2S):33:1–33:??, September 2012. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Liu:2018:GEI

[LLK18] Zhe Liu, Patrick Longa, and Çetin Kaya Koç. Guest Editors' introduction to the special issue on cryptographic engineering in a post-quantum world: State of the art advances. *IEEE Transactions on Computers*, 67(11):1532–1534, ???? 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `https://ieeexplore.ieee.org/document/8485531/`.

Liu:2019:SBC

[LLKA19] Jian Liu, Wenting Li, Ghassan O. Karame, and N. Asokan. Scalable Byzantine consensus via hardware-assisted secret sharing. *IEEE Transactions on Computers*, 68(1): 139–151, ???? 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `https://ieeexplore.ieee.org/document/8419336/`.

Li:2017:CIS

[LLL17a] Chengqing Li, Dongdong Lin, and Jinhu Lu. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE MultiMedia*, 24(3):64–71, July/September 2017. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL https://www.computer.org/csdl/mags/mu/2017/03/mmu2017030064-abs.html.

Li:2017:CCD

[LLL+17b] Tong Li, Zheli Liu, Jin Li, Chunfu Jia, and Kuan-Ching Li. CDPS: A cryptographic data publishing system. *Journal of Computer and System Sciences*, 89(??):80–91, November 2017. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000016301313.

Liu:2018:VSE

[LLL+18] Zheli Liu, Tong Li, Ping Li, Chunfu Jia, and Jin Li. Verifiable searchable encryption with aggregate keys for data sharing system. *Future Generation Computer Systems*, 78 (part 2)(??):778–788, January 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17302340.

Li:2018:CIE

[LLLH18] C. Li, D. Lin, J. Lü, and F. Hao. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. *IEEE MultiMedia*, 25(4):46–56, October/December 2018. CODEN IEMUE4. ISSN 1070-986x (print), 1941-0166 (electronic).

Li:2010:DCY

[LLLK10] Chengqing Li, Shujun Li, Kwok-Tung Lo, and Kyandoghere Kyamakya. A differential cryptanalysis of Yen–Chen–Wu multimedia cryptography system. *The Journal of Systems and Software*, 83(8):1443–1452, August 2010. CODEN JSSODM. ISSN 0164-1212.

Lai:2013:SAS

[LLLS13] Chengzhe Lai, Hui Li, Rongxing Lu, and Xuemin (Sherman) Shen. SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 57(17):3492–3510, December 9, 2013. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128613002570.

Libert:2019:ZKA

[LLM+19] Benoît Libert, San Ling, Fabrice Mouhartem, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for matrix-vector relations and lattice-based group encryption. *Theoretical Computer Science*, 759(??):72–97, February 8, 2019. CODEN TCSDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397519300167`.

Lu:2012:IEC

[LLML12] Xianhui Lu, Bao Li, Qixiang Mei, and Yamin Liu. Improved efficiency of chosen ciphertext secure encryption from factoring. *Lecture Notes in Computer Science*, 7232:34–45, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-29101-2_3/`.

Lai:2018:EQK

[LLP+18] Hong Lai, Mingxing Luo, Josef Pieprzyk, Zhiguo Qu, and Mehmet A. Orgun. Efficient quantum key distribution using Fibonacci-number coding with a biased basis choice. *Information Processing Letters*, 134 (??):24–30, June 2018. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019018300267`.

Lee:2019:CSS

[LLPY19] Kwangsu Lee, Dong Hoon Lee, Jong Hwan Park, and Moti Yung. CCA security for self-updatable encryption: Protecting cloud data when clients read/write ciphertexts. *The Computer Journal*, 62(4):545–562, April 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/62/4/545/5239643`.

Liao:2019:ESO

[LLSL19] W. Liao, C. Luo, S. Salinas, and P. Li. Efficient secure outsourcing of large-scale convex separable programming for big data. *IEEE Transactions on Big Data*, 5(3):368–378, September 2019. ISSN 2332-7790.

Lee:2016:CAM

[LLSW16] Hyung Tae Lee, San Ling, Jae Hong Seo, and Huaxiong Wang. CCA2 attack and modification of Huang et al.'s public key encryption with authorized equality test. *The Computer Journal*, 59(11):1689–1694, November 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/11/1689.

Lee:2016:AGA

[LLW16] Hyung Tae Lee, San Ling, and Huaxiong Wang. Analysis of Gong et al.'s CCA2-secure homomorphic encryption. *Theoretical Computer Science*, 640(??):104–114, August 9, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S030439751630250X.

Lee:2006:DCK

[LLY06] Patrick P. C. Lee, John C. S. Lui, and David K. Y. Yau. Distributed collaborative key agreement and authentication protocols for dynamic peer groups. *IEEE/ACM Transactions on Networking*, 14(2):263–276, April 2006. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Ling:2012:NCC

[LLY+12a] Zhen Ling, Junzhou Luo, Wei Yu, Xinwen Fu, Dong Xuan, and Weijia Jia. A new cell-counting-based attack against Tor. *IEEE/ACM Transactions on Networking*, 20(4):1245–1261, August 2012. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Luo:2012:FSI

[LLY+12b] Xiangyang Luo, Fenlin Liu, Chunfang Yang, Shiguo Lian, and Daoshun Wang. On F5 steganography in images. *The Computer Journal*, 55(4):447–456, April 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/55/4/447.full.pdf+html.

Lee:2015:SAS

[LLY15] Kwangsu Lee, Dong Hoon Lee, and Moti Yung. Sequential aggregate signatures with short public keys without random oracles. *Theoretical Computer Science*, 579(??):100–125, May 10, 2015. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397515001164.

Li:2018:WMH

[LLY+18] L. Li, H. Li, W. Yuan, J. Lu, X. Feng, and C. Chang. A watermarking mechanism with high capacity for three-dimensional mesh objects using integer planning. *IEEE MultiMedia*, 25(3):49–64, July/September

2018. CODEN IEMUE4. ISSN 1070-986x (print), 1941-0166 (electronic).

Lu:2012:BBE

[LLZ+12] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, and Xuemin (Sherman) Shen. BECAN: a Bandwidth-Efficient Cooperative Authentication Scheme for filtering injected false data in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 23(1):32–43, January 2012. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Lai:2016:GGB

[LLZ+16] Chengzhe Lai, Rongxing Lu, Dong Zheng, Hui Li, and Xuemin (Sherman) Shen. GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications. *Computer Networks (Amsterdam, Netherlands: 1999)*, 99 (??):66–81, April 22, 2016. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128616300238`.

Li:2017:CBS

[LLZ+17] Qi Li, Patrick P. C. Lee, Peng Zhang, Purui Su, Liang He, Kui Ren, Qi Li, Patrick P. C. Lee, Peng Zhang, Purui Su, Liang He, and Kui Ren. Capability-based security enforcement in named data networking. *IEEE/ACM Transactions on Networking*, 25(5): 2719–2730, October 2017. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Lucamarini:2014:QKD

[LM14] Marco Lucamarini and Stefano Mancini. Quantum key distribution using a two-way quantum channel. *Theoretical Computer Science*, 560 (part 1)(??):46–61, December 4, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397514006951`.

Lambert-Mogiliansky:2012:EII

[LMB12] Ariane Lambert-Mogiliansky and Jerome R. Busemeyer. Emergence and instability of individual identity. *Lecture Notes in Computer Science*, 7620: 102–113, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-35659-9_10/`.

Le:2016:ADS

[LMD16] Anh Le, Athina Markopoulou, and Alexandros G. Dimakis. Auditing for distributed storage systems. *IEEE/ACM Transactions on Networking*, 24(4): 2182–2195, August 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Lai:2018:IBB

[LMG+18] Jianchang Lai, Yi Mu, Fuchun Guo, Peng Jiang, and Sha Ma. Identity-based broadcast encryption for inner products. *The Computer Journal*, 61(8):1240–1251, August 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/8/1240/5035766.

Lai:2017:FPP

[LMGC17] Jianchang Lai, Yi Mu, Fuchun Guo, and Rongmao Chen. Fully privacy-preserving ID-based broadcast encryption with authorization. *The Computer Journal*, 60(12):1809–1821, December 1, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/12/1809/3861972.

Liu:2014:SCS

[LMHH14] Bin Liu, Ralph R. Martin, Ji-Wu Huang, and Shi-Min Hu. Shapes and cryptography: Structure aware visual cryptography. *Computer Graphics Forum*, 33 (7):141–150, October 2014. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Li:2011:NRA

[LMJC11] Guangsong Li, Jianfeng Ma, Qi Jiang, and Xi Chen. A novel re-authentication scheme based on tickets in wireless local area networks. *Journal of Parallel and Distributed Computing*, 71(7):906–914, July 2011. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731511000554.

Lv:2013:NTP

[LML+13] Chao Lv, Maode Ma, Hui Li, Jianfeng Ma, and Yaoyu Zhang. An novel three-party authenticated key exchange protocol using one-time key. *Journal of Network and Computer Applications*, 36(1):498–503, January 2013. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804512000999.

Lubacz:2010:VI

[LMS10] J. Lubacz, W. Mazurczyk, and K. Szczypiorski. Vice over IP. *IEEE Spectrum*, 47(2):42–47, February 2010. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Lukasiewycz:2016:SAO

[LMS16] Martin Lukasiewycz, Philipp Mundhenk, and Sebastian Steinhorst. Security-aware obfuscated priority assignment for automotive CAN platforms. *ACM Transactions on Design Automation of Electronic Systems*, 21(2):32:1–32:??, January 2016. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

LoIacono:2019:NGR

[LNG19] Luigi Lo Iacono, Hoai Viet Nguyen, and Peter Leo Gorski. On the need for a general REST-security framework. *Future Internet*, 11(3):56, February 27, 2019. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/11/3/56.

Li:2018:RBB

[LNK+18a] Xiong Li, Jianwei Niu, Saru Kumari, Fan Wu, and Kim-Kwang Raymond Choo. A robust biometrics based three-factor authentication scheme for Global Mobility Networks in smart city. *Future Generation Computer Systems*, 83(??):607–618, June 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X1730585X.

Li:2018:TFA

[LNK+18b] Xiong Li, Jianwei Niu, Saru Kumari, Fan Wu, Arun Kumar Sangaiah, and Kim-Kwang Raymond Choo. A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments. *Journal of Network and Computer Applications*, 103(??):194–204, February 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804517302254.

Li:2013:ESC

[LNKL13] Xiong Li, Jianwei Niu, Muhammad Khurram Khan, and Junguo Liao. An enhanced smart card based remote user password authentication scheme. *Journal of Network and Computer Applications*, 36 (5):1365–1371, September 2013. CODEN JNCAF3. ISSN 1084-8045

(print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804513000726.

Liu:2019:OMM

[LNL+19] W. Liu, J. Ni, Z. Liu, C. Liu, and M. O. Neill. Optimized modular multiplication for supersingular isogeny Diffie–Hellman. *IEEE Transactions on Computers*, 68(8):1249–1255, August 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Li:2011:CIB

[LNM+11] Xiong Li, Jian-Wei Niu, Jian Ma, Wen-Dong Wang, and Cheng-Lian Liu. Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*, 34(1):73–79, January 2011. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804510001657.

Li:2013:EAF

[LNNH13] Celia Li, Uyen Trang Nguyen, Hoang Lan Nguyen, and Nurul Huda. Efficient authentication for fast handover in wireless mesh networks. *Computers & Security*, 37(??):124–142, September 2013. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404813000916.

Ling:2019:SAR

[LNWZ19] San Ling, Khoa Nguyen, Huaxiong Wang, and Juanyang Zhang. Server-aided revocable predicate encryption: Formalization and lattice-based instantiation. *The Computer Journal*, 62(12):1849–1862, December 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/12/1849/5628022.

Liu:2015:SAB

[LNXY15] Hong Liu, Huansheng Ning, Qingxu Xiong, and Laurence T. Yang. Shared authority based privacy-preserving authentication protocol in cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, 26(1):241–251, January 2015. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL http://www.computer.org/csdl/trans/td/2015/01/06748054-abs.html.

Liu:2013:GPB

[LNZ+13] Hong Liu, Huansheng

Ning, Yan Zhang, Daojing He, Qingxu Xiong, and Laurence T. Yang. Grouping-proofs-based authentication protocol for distributed RFID systems. *IEEE Transactions on Parallel and Distributed Systems*, 24(7):1321–1330, July 2013. CODEN ITDSEO. ISSN 1045-9219.

Loeb:2015:MGM

[Loe15] Larry Loeb. Microsoft, Google, Mozilla abandon RC4 cryptographic standard. *Information Week*, ??(??):??, September 2, 2015. CODEN INFWE4. ISSN 8750-6874. URL http://www.informationweek.com/software/enterprise-applications/microsoft-google-mozilla-abandon-rc4-cryptographic-standard/a/d-id/1322032.

Lopriore:2012:EPP

[Lop12] Lanfranco Lopriore. Encrypted pointers in protection system design. *The Computer Journal*, 55(4):497–507, April 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/55/4/497.full.pdf+html.

Lopriore:2015:PCR

[Lop15a] Lanfranco Lopriore. Password capabilities revisited. *The Computer Journal*, 58(4):782–791, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/782.

Lopriore:2015:PMD

[Lop15b] Lanfranco Lopriore. Password management: Distribution, review and revocation. *The Computer Journal*, 58(10):2557–2566, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2557.

Low:2012:BRB

[Low12] Robert J. Low. Book review: *Codes: an Introduction to Information Communication and Cryptography*, by Norman L. Biggs. *ACM SIGACT News*, 43(1):27–29, March 2012. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [Big08].

Lin:2011:CRN

[LP11] Huijia Lin and Rafael Pass. Constant-round nonmalleable commitments from any one-way function. In ACM [ACM11], pages 705–714. ISBN ???? LCCN ???? URL http://

www.gbv.de/dms/tib-ub-hannover/63314455x..

Ling:2012:SHS

[LP12] Huo-Chong Ling and Raphael C.-W. Phan. On the security of a hybrid SVD–DCT watermarking method based on LPSNR. *Lecture Notes in Computer Science*, 7087: 257–266, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-25367-6_23.

Lima:2010:PKE

[LPdS10] J. B. Lima, D. Panario, and R. M. Campello de Souza. Public-key encryption based on Chebyshev polynomials over GF(q). *Information Processing Letters*, 111(2):51–56, December 31, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lian:2015:GRG

[LPL15] Chunfeng Lian, Liaojun Pang, and Jimin Liang. Generalized random grid-based visual secret sharing for general access structures. *The Computer Journal*, 58(10):2426–2442, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2426.

Liu:2017:HPI

[LPO+17] Zhe Liu, Thomas Pöppelmann, Tobias Oder, Hwajeong Seo, Sujoy Sinha Roy, Tim Güneysu, Johann Großschädl, Howon Kim, and Ingrid Verbauwhede. High-performance ideal lattice-based cryptography on 8-bit AVR microcontrollers. *ACM Transactions on Embedded Computing Systems*, 16(4): 117:1–117:??, August 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Lampe:2012:ATS

[LPS12] Rodolphe Lampe, Jacques Patarin, and Yannick Seurin. An asymptotically tight security analysis of the iterated even-Mansour cipher. *Lecture Notes in Computer Science*, 7658:278–295, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34961-4_18/.

Liu:2015:GTB

[LPZJ15] Shaohui Liu, Anand Paul, Guochao Zhang, and Gwanggil Jeon. A game theory-based block image compression method in encryption domain. *The Journal of Supercomputing*, 71(9):3353–3372, September 2015. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-015-1413-0.

Liu:2016:PPO

[LQD+16] Ximeng Liu, Baodong Qin, Robert H. Deng, Rongxing Lu, and Jianfeng Ma. A privacy-preserving outsourced functional computation framework across large-scale multiple encrypted domains. *IEEE Transactions on Computers*, 65(12):3567–3579, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Libert:2010:KES

[LQY10] Benoît Libert, Jean-Jacques Quisquater, and Moti Yung. Key evolution systems in untrusted update environments. *ACM Transactions on Information and System Security*, 13(4):37:1–37:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lubicz:2015:GMA

[LR15] David Lubicz and Damien Robert. A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties. *Journal of Symbolic Computation*, 67(??):68–92, March/April 2015. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic). URL http://www.sciencedirect.com/science/article/pii/S0747717114000510.

Lukowiak:2014:CEB

[LRVW14] Marcin Lukowiak, Stanislaw Radziszowski, James Vallino, and Christopher Wood. Cybersecurity education: Bridging the gap between hardware and software domains. *ACM Transactions on Computing Education*, 14(1):2:1–2:??, March 2014. CODEN ???? ISSN 1946-6226.

Liskiewicz:2013:GBS

[LRW13] Maciej Liśkiewicz, Rüdiger Reischuk, and Ulrich Wölfel. Grey-box steganography. *Theoretical Computer Science*, 505(??):27–41, September 23, 2013. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S030439751200309X.

Liskiewicz:2017:SLS

[LRW17] Maciej Liśkiewicz, Rüdiger Reischuk, and Ulrich Wölfel. Security levels in steganography — insecurity does not imply detectability. *Theoretical Computer Science*, 692(??):25–45, September 5, 2017. CODEN TCSDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397517305194`.

Lane:2014:PBD

[LSBN14] Julia I. Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum, editors. *Privacy, big data, and the public good: frameworks for engagement*. Cambridge University Press, Cambridge, UK, 2014. ISBN 1-107-06735-9 (hardcover), 1-107-63768-6 (paperback). xix + 322 pp. LCCN JC596 .P747 2015.

Luo:2012:FSU

[LSC12] Song Luo, Qingni Shen, and Zhong Chen. Fully secure unidirectional identity-based proxy re-encryption. *Lecture Notes in Computer Science*, 7259:109–126, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31912-9_8/`.

Lin:2015:SSE

[LSC+15] Chung-Hsiang Lin, De-Yu Shen, Yi-Jung Chen, Chia-Lin Yang, and Cheng-Yuan Michael Wang. SECRET: a selective error correction framework for refresh energy reduction in DRAMs. *ACM Transactions on Architecture and Code Optimization*, 12(2): 19:1–19:??, July 2015. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic).

Lychev:2016:RSI

[LSG16] Robert Lychev, Michael Schapira, and Sharon Goldberg. Rethinking security for Internet routing. *Communications of the Association for Computing Machinery*, 59(10):48–57, October 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2016/10/207763/fulltext`.

Liu:2019:IMM

[LSG+19] Ya Liu, Yifan Shi, Dawu Gu, Zhiqiang Zeng, Fengyu Zhao, Wei Li, Zhiqiang Liu, and Yang Bao. Improved meet-in-the-middle attacks on reduced-round Kiasu-BC and Joltik-BC. *The Computer Journal*, 62(12):1761–1776, December 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/62/12/1761/5525447`.

Lee:2012:IBS

[LSL12a] Woomyo Lee, Jae Woo Seo, and Pil Joong Lee. Identity-based signcryption from identity-based cryptography. *Lecture Notes in Computer Science*, 7115:70–83, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27890-7_6/.

Lei:2012:RAW

[LSL12b] Baiying Lei, Ing Yann Soon, and Zhen Li. A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition. *Lecture Notes in Computer Science*, 7128:86–96, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32205-1_9/.

Liang:2015:EFC

[LSLW15] Kaitai Liang, Willy Susilo, Joseph K. Liu, and Duncan S. Wong. Efficient and fully CCA secure conditional proxy re-encryption from hierarchical identity-based encryption. *The Computer Journal*, 58(10):2778–2792, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2778.

Liu:2011:DBA

[LSQ11a] Qingzhong Liu, Andrew H. Sung, and Mengyu Qiao. Derivative-based audio steganalysis. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 7(3): 18:1–18:??, August 2011. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Liu:2011:NJD

[LSQ11b] Qingzhong Liu, Andrew H. Sung, and Mengyu Qiao. Neighboring joint density-based JPEG steganalysis. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 2(2):16:1–16:??, February 2011. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic).

Lin:2015:IAA

[LSQ15] Xi-Jun Lin, Lin Sun, and Haipeng Qu. Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications. *Computers & Security*, 48(??):142–149, February 2015. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://

www.sciencedirect.com/science/article/pii/S0167404814001229.

Lin:2018:CPF

[LSQL18a] Xi-Jun Lin, Lin Sun, Haipeng Qu, and Dongxiao Liu. Cryptanalysis of a pairing-free certificateless signcryption scheme. *The Computer Journal*, 61(4):539–544, April 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/4/539/4608880.

Lin:2018:SSS

[LSQL18b] Xi-Jun Lin, Lin Sun, Haipeng Qu, and Dongxiao Liu. On the security of secure server-designation public key encryption with keyword search. *The Computer Journal*, 61(12): 1791–1793, December 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/12/1791/5055854.

Lin:2019:CCA

[LSQX19] Xi-Jun Lin, Lin Sun, Haipeng Qu, and He-Qun Xian. Cryptanalysis of a compact anonymous HIBE with constant size private keys. *The Computer Journal*, 62(8):1087–1091, August 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/8/1087/5253748.

Lin:2017:ESF

[LSQZ17] Xi-Jun Lin, Lin Sun, Haipeng Qu, and Xiaoshuai Zhang. Editorial: On the security of the first leakage-free certificateless signcryption scheme. *The Computer Journal*, 60(4): 491–496, March 23, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/4/491/2608059.

Lei:2013:RSW

[LSR13] Baiying Lei, Insu Song, and Shah Atiqur Rahman. Robust and secure watermarking scheme for breath sound. *The Journal of Systems and Software*, 86(6):1638–1649, June 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121213000332.

Landecker:2012:TBB

[LST12] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable blockciphers with beyond birthday-bound security. *Lecture Notes in Computer*

Science, 7417:14–30, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32009-5_2/.

Liu:2016:EPP

[LSY+16] Joseph K. Liu, Willy Susilo, Tsz Hon Yuen, Man Ho Au, Junbin Fang, Zoe L. Jiang, and Jianying Zhou. Efficient privacy-preserving charging station reservation system for electric vehicles. *The Computer Journal*, 59(7):1040–1053, July 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/7/1040.

Lee:2013:CCM

[LT13] Che-Wei Lee and Wen-Hsiang Tsai. A covert communication method via spreadsheets by secret sharing with a self-authentication capability. *The Journal of Systems and Software*, 86(2):324–334, February 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212002464.

Le:2014:IMX

[LT14a] Duc-Phong Le and Chik How Tan. Improved Miller's algorithm for computing pairings on Edwards curves. *IEEE Transactions on Computers*, 63(10):2626–2632, October 2014. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Lee:2014:NDH

[LT14b] Ya-Lin Lee and Wen-Hsiang Tsai. A new data hiding method via revision history records on collaborative writing platforms. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 10(2):20:1–20:??, February 2014. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Liu:2015:IMB

[LTC+15a] Chao-Liang Liu, Cheng-Jung Tsai, Ting-Yi Chang, Wang-Jui Tsai, and Po-Kai Zhong. Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on a smart phone. *Journal of Network and Computer Applications*, 53(??):128–139, July 2015. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://

www.sciencedirect.com/science/article/pii/S1084804515000612.

Liu:2015:MSG

[LTC+15b] Chao-Liang Liu, Wang-Jui Tsai, Ting-Yi Chang, Chun-Cheng Peng, and Peng-Shiang Wong. Meaningful share generation for (2, 2)-multiple visual secret sharing scheme without pixel expansion. *The Computer Journal*, 58(7):1598–1606, July 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/7/1598.

Li:2015:FSC

[LTH+15] Jiguo Li, Huiyun Teng, Xinyi Huang, Yichen Zhang, and Jianying Zhou. A forward-secure certificate-based signature scheme. *The Computer Journal*, 58 (4):853–866, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/853.

Lao:2016:BFD

[LTKP16] Yingjie Lao, Qianying Tang, Chris H. Kim, and Keshab K. Parhi. Beat frequency detector-based high-speed true random number generators: Statistical modeling and analysis. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 13(1):9:1–9:??, December 2016. CODEN ???? ISSN 1550-4832.

Lysyanskaya:2010:AEC

[LTT10] Anna Lysyanskaya, Roberto Tamassia, and Nikos Triandopoulos. Authenticated error-correcting codes with applications to multicast authentication. *ACM Transactions on Information and System Security*, 13(2):17:1–17:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Lin:2011:CNS

[LTW11] Dongdai Lin, Gene Tsudik, and Xiaoyun Wang, editors. *Cryptology and Network Security: 10th International Conference, CANS 2011, Sanya, China, December 10–12. Proceedings*, volume 7092 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011. CODEN LNCSD9. ISBN 3-642-25512-4. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/978-3-642-25512-0.

Li:2016:LRC

[LTZY16] Jiguo Li, Meilin Teng, Yichen Zhang, and Qihong Yu. A leakage-resilient CCA-secure identity-based encryption scheme. *The Computer Journal*, 59(7): 1066–1075, July 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/7/1066.

Ludge:2012:NLD

[Lüd12] Kathy Lüdge, editor. *Nonlinear laser dynamics: from quantum dots to cryptography*. References in nonlinear dynamics and complexity. Wiley-VCH, Weinheim, 2012. ISBN 3-527-41100-3 (hardcover), 3-527-63984-5 (ePDF), 3-527-63982-9 (oBook), 3-527-63983-7 (ePub), 3-527-63985-3 (Mobi). xx + 387 pp. LCCN QC688 .N66 2012; QC689.55.S45 N665 2012. URL http://www.loc.gov/catdir/enhancements/fy1403/2012360633-b.html; http://www.loc.gov/catdir/enhancements/fy1403/2012360633-d.html; http://www.loc.gov/catdir/enhancements/fy1403/2012360633-t.html.

Lucchese:2010:RPT

[LVRY10] Claudio Lucchese, Michail Vlachos, Deepak Rajan, and Philip S. Yu. Rights protection of trajectory datasets with nearest-neighbor preservation. *VLDB Journal: Very Large Data Bases*, 19(4):531–556, August 2010. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Lafitte:2011:CBF

[LVV11] Frédéric Lafitte, Dirk Van Heule, and Julien Van hamme. Cryptographic Boolean functions with R. *The R Journal*, 3(1):44–47, June 2011. CODEN ???? ISSN 2073-4859. URL http://journal.r-project.org/archive/2011-1/RJournal_2011-1_Lafitte~et~al.pdf.

Liu:2010:CIE

[LW10] Hongjun Liu and Xingyuan Wang. Color image encryption based on one-time keys and robust chaotic maps. *Computers and Mathematics with Applications*, 59(10):3320–3327, May 2010. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122110001938.

Lee:2011:ACA

[LW11a] Dong Hoon Lee and Xiaoyun Wang, editors. *Advances in Cryptology — ASIACRYPT 2011: 17th*

International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4–8. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011. CODEN LNCSD9. ISBN 3-642-25384-9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/978-3-642-25384-3.

Lewko:2011:DAB

[LW11b] Allison Lewko and Brent Waters. Decentralizing attribute-based encryption. *Lecture Notes in Computer Science*, 6632: 568–588, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_31.

Lewko:2011:UHA

[LW11c] Allison Lewko and Brent Waters. Unbounded HIBE and attribute-based encryption. *Lecture Notes in Computer Science*, 6632: 547–567, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_30.

Lewko:2012:NPM

[LW12] Allison Lewko and Brent Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. *Lecture Notes in Computer Science*, 7417:180–198, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32009-5_12/.

Liu:2013:SIP

[LW13a] Dongxi Liu and Shenlu Wang. Special issue papers: Nonlinear order preserving index for encrypted database query in service cloud environments. *Concurrency and Computation: Practice and Experience*, 25(13):1967–1984, September 10, 2013. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Liu:2013:TIE

[LW13b] Hongjun Liu and Xingyuan Wang. Triple-image encryption scheme based on one-time key stream generated by chaos and plain images. *The Journal of Systems and Software*, 86

(3):826–834, March 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212003196.

Lui:2013:CBS

[LW13c] Oi-Yan Lui and Kwok-Wo Wong. Chaos-based selective encryption for H.264/AVC. *The Journal of Systems and Software*, 86(12):3183–3192, December 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121213001994.

Liu:2016:PAB

[LW16] Zhen Liu and Duncan S. Wong. Practical attribute-based encryption: Traitor tracing, revocation and large universe. *The Computer Journal*, 59(7):983–1004, July 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/7/983.

Li:2019:TFA

[LW19] Wenting Li and Ping Wang. Two-factor authentication in industrial Internet-of-Things: Attacks, evaluation and new construction. *Future Generation Computer Systems*, 101(??):694–708, December 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19307642.

Liu:2014:DAF

[LWCJ14] Hongbo Liu, Hui Wang, Yingying Chen, and Dayong Jia. Defending against frequency-based attacks on distributed data storage in wireless networks. *ACM Transactions on Sensor Networks*, 10(3):49:1–49:??, April 2014. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Liu:2017:EEC

[LWHS17] Zhe Liu, Jian Weng, Zhi Hu, and Hwajeong Seo. Efficient elliptic curve cryptography for embedded devices. *ACM Transactions on Embedded Computing Systems*, 16(2):53:1–53:??, April 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Liu:2011:SBA

[LWK11] Yu Liu, Kaijie Wu, and Ramesh Karri. Scan-based attacks on linear feedback shift register based stream ciphers. *ACM Transactions on Design Automation of Electronic Systems*, 16(2):20:1–20:??, March 2011.

CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Li:2018:SCM

[LWK+18] Xiong Li, Fan Wu, Muhammad Khurram Khan, Lili Xu, Jian Shen, and Minho Jo. A secure chaotic map-based remote authentication scheme for telecare medicine information systems. *Future Generation Computer Systems*, 84(??):149–159, July 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X1730688X`.

Li:2019:PSA

[LWK+19] Xiong Li, Fan Wu, Saru Kumari, Lili Xu, Arun Kumar Sangaiah, and Kim-Kwang Raymond Choo. A provably secure and anonymous message authentication scheme for smart grids. *Journal of Parallel and Distributed Computing*, 132(??):242–249, October 2019. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731517303064`.

Lu:2012:HOM

[LWKP12] Jiqiang Lu, Yongzhuang Wei, Jongsung Kim, and Enes Pasalic. The higher-order meet-in-the-middle attack and its application to the Camellia block cipher. *Lecture Notes in Computer Science*, 7668: 244–264, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-34931-7_15/`.

Lu:2014:HOM

[LWKP14] Jiqiang Lu, Yongzhuang Wei, Jongsung Kim, and Enes Pasalic. The higher-order meet-in-the-middle attack and its application to the Camellia block cipher. *Theoretical Computer Science*, 527(??):102–122, March 27, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397514000802`.

Liu:2010:NDC

[LWL10a] Feng Liu, ChuanKun Wu, and XiJun Lin. A new definition of the contrast of visual cryptography scheme. *Information Processing Letters*, 110(7): 241–246, March 1, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Liu:2010:SET

[LWL10b] Feng Liu, ChuanKun Wu, and XiJun Lin. Some extensions on threshold visual cryptography schemes. *The Computer Journal*, 53(1):107–119, January 2010. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/53/1/107; http://comjnl.oxfordjournals.org/cgi/reprint/53/1/107.

Liu:2017:SRG

[LWL+17] Jing Liu, Yunyun Wu, Xuezheng Liu, Yunchun Zhang, Gang Xue, Wei Zhou, and Shaowen Yao. On the (in)security of recent group key distribution protocols. *The Computer Journal*, 60(4):507–526, March 23, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/4/507/2608062.

Liu:2011:PIA

[LWLW11] Guangjie Liu, Junwen Wang, Shiguo Lian, and Zhiquan Wang. A passive image authentication scheme for detecting region-duplication forgery with rotation. *Journal of Network and Computer Applications*, 34(5):1557–1565, September 2011. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804510001621.

Liu:2016:NSC

[LWML16] Fangfei Liu, Hao Wu, Kenneth Mai, and Ruby B. Lee. Newcache: Secure cache architecture thwarting cache side-channel attacks. *IEEE Micro*, 36(5):8–16, September/October 2016. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL https://www.computer.org/csdl/mags/mi/2016/05/mmi2016050008-abs.html.

Lu:2012:MMA

[LWPF12] Jiqiang Lu, Yongzhuang Wei, Enes Pasalic, and Pierre-Alain Fouque. Meet-in-the-middle attack on reduced versions of the Camellia block cipher. *Lecture Notes in Computer Science*, 7631:197–215, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34117-5_13/.

Li:2010:GCP

[LWS10] Hui Li, Chuan-Kun Wu,

and Jun Sun. A general compiler for password-authenticated group key exchange protocol. *Information Processing Letters*, 110(4):160–167, January 16, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Lou:2010:NAS

[LWW+10] Der-Chyuan Lou, Nan-I Wu, Chung-Ming Wang, Zong-Han Lin, and Chwei-Shyong Tsai. A novel adaptive steganography based on local complexity and human vision sensitivity. *The Journal of Systems and Software*, 83(7):1236–1248, July 2010. CODEN JSSODM. ISSN 0164-1212.

Li:2019:VCM

[LWW+19] Jing Li, Licheng Wang, Lihua Wang, Xianmin Wang, Zhengan Huang, and Jin Li. Verifiable Chebyshev maps-based chaotic encryption schemes with outsourcing computations in the cloud/fog scenarios. *Concurrency and Computation: Practice and Experience*, 31(22):e4523:1–e4523:??, November 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Luo:2012:ICB

[LWY12] Junzhou Luo, Xiaogang Wang, and Ming Yang. An interval centroid based spread spectrum watermarking scheme for multi-flow traceback. *Journal of Network and Computer Applications*, 35(1):60–71, January 2012. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804511000579.

Li:2016:DDA

[LWYM16] Xinghua Li, Ermeng Wang, Weidong Yang, and Jianfeng Ma. DALP: a demand-aware location privacy protection scheme in continuous location-based services. *Concurrency and Computation: Practice and Experience*, 28(4):1219–1236, March 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Li:2012:IIA

[LWZ12] Yanjun Li, Wenling Wu, and Lei Zhang. Improved integral attacks on reduced-round CLEFIA block cipher. *Lecture Notes in Computer Science*, 7115:28–39, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27890-7_3/.

Lin:2010:DSM

[LWZG10] Dai-Rui Lin, Chih-I Wang, Zhi-Kai Zhang, and D. J. Guan. A digital signature with multiple subliminal channels and its applications. *Computers and Mathematics with Applications*, 60(2):276–284, July 2010. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S089812211000012X.

Li:2011:NIW

[LXCM11] Li Li, He-Huan Xu, Chin-Chen Chang, and Ying-Ying Ma. A novel image watermarking in redistributed invariant wavelet domain. *The Journal of Systems and Software*, 84(6):923–929, June 2011. CODEN JSSODM. ISSN 0164-1212.

Li:2014:IBD

[LXJ14] Fagen Li, Pan Xiong, and Chunhua Jin. Identity-based deniable authentication for ad hoc networks. *Computing*, 96(9):843–853, September 2014. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL http://link.springer.com/article/10.1007/s00607-013-0321-5.

Li:2014:EMK

[LXK+14] Ruixuan Li, Zhiyong Xu, Wanshang Kang, Kin Choong Yow, and Cheng-Zhong Xu. Efficient multi-keyword ranked query over encrypted data in cloud computing. *Future Generation Computer Systems*, 30(??):179–190, January 2014. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X1300143X.

Lai:2012:RHB

[LXLY12] Hong Lai, Jinghua Xiao, Lixiang Li, and Yixian Yang. Recursive hiding of biometrics-based secret sharing scheme using adversary structure. *Information Processing Letters*, 112(17–18):683–687, September 30, 2012. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019012001573.

Li:2012:ESD

[LXMW12] Xiong Li, Yongping Xiong, Jian Ma, and Wendong Wang. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. *Journal of Network and Computer Ap-

plications, 35(2):763–769, March 2012. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804511002244.

Luo:2014:ARP

[LY14] Jia Ning Luo and Ming Hour Yang. An anonymous e-rental protocol based on ID-based cryptography and NFC. *The Journal of Supercomputing*, 70(1):31–53, October 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-013-1051-3.

Liu:2015:SDS

[LY15] Chen Liu and Chengmo Yang. Secure and durable (SEDURA): an integrated encryption and wear-leveling framework for PCM-based main memory. *ACM SIGPLAN Notices*, 50(5):12:1–12:??, May 2015. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Lim:2016:AKE

[LY16] Hoon Wei Lim and Guomin Yang. Authenticated key exchange protocols for parallel network file systems. *IEEE Transactions on Parallel and Distributed Systems*, 27(1):92–105, January 2016. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL http://www.computer.org/csdl/trans/td/2016/01/07004049-abs.html.

Li:2010:AFF

[LYC+10] Peng Li, Xin Yang, Kai Cao, Xunqiang Tao, Ruifang Wang, and Jie Tian. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. *Journal of Network and Computer Applications*, 33(3):207–220, May 2010. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804509001398.

Liu:2018:IMM

[LYD+18] Ya Liu, Anren Yang, Bo Dai, Wei Li, Zhiqiang Liu, Dawu Gu, and Zhiqiang Zeng. Improved meet-in-the middle attacks on reduced-round TWINE-128. *The Computer Journal*, 61(8):1252–1258, August 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/8/1252/5040794.

Lu:2014:DAN

[LYHH14] Jiqiang Lu, Wun-She Yap, Matt Henricksen, and

Swee-Huay Heng. Differential attack on nine rounds of the SEED block cipher. *Information Processing Letters*, 114(3):116–123, March 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S002001901300272X.

Le:2019:ADF

[LYK19] D. Le, S. L. Yeo, and K. Khoo. Algebraic differential fault analysis on SIMON block cipher. *IEEE Transactions on Computers*, 68(11):1561–1572, November 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Liu:2015:SAA

[LYL15] Zhusong Liu, Hongyang Yan, and Zhike Li. Server-aided anonymous attribute-based authentication in cloud computing. *Future Generation Computer Systems*, 52(??):61–66, November 2015. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X14002544.

Lin:2018:SEI

[LYL+18] Tingting Lin, Hailun Yan, Xuejia Lai, Yixin Zhong, and Yin Jia. Security evaluation and improvement of a white-box SMS4 implementation based on affine equivalence algorithm. *The Computer Journal*, 61(12):1783–1790, December 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/12/1783/5055352.

Li:2010:ESS

[LYW+10] Chung Ki Li, Guomin Yang, Duncan S. Wong, Xiaotie Deng, and Sherman S. M. Chow. An efficient signcryption scheme with key privacy and its extension to ring signcryption. *Journal of Computer Security*, 18(3):451–473, ???? 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Liao:2012:NSM

[LyWlZZ12] Xin Liao, Qiao yan Wen, Ze li Zhao, and Jie Zhang. A novel steganographic method with four-pixel differencing and modulus function. *Fundamenta Informaticae*, 118(3):281–289, August 2012. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Liao:2010:MPC

[LyWSZ10] Xin Liao, Qiao yan Wen, Ying Sun, and Jie Zhang.

Multi-party covert communication with steganography and quantum secret sharing. *The Journal of Systems and Software*, 83(10):1801–1804, October 2010. CODEN JSSODM. ISSN 0164-1212.

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 (IJFCS)*, 30(4):589–606, June 2019. ISSN 0129-0541. URL `https://www.worldscientific.com/doi/10.1142/S0129054119400148`.

Liu:2016:FIT

[LYY+16] Joseph K. Liu, Sze Ling Yeo, Wun-She Yap, Sherman S. M. Chow, Duncan S. Wong, and Willy Susilo. Faulty instantiations of threshold ring signature from threshold proof-of-knowledge protocol. *The Computer Journal*, 59(7):945–954, July 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/59/7/945`.

Lai:2018:NSH

[LYY+18a] 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`.

Liu:2018:SKR

[LYY+18b] Jinhui Liu, Yong Yu, Bo Yang, Jianwei Jia, Shijia Wang, and Houzhen Wang. Structural key recovery of simple matrix encryption scheme family. *The Computer Journal*, 61 (12):1880–1896, December 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/61/12/1880/5110544`.

Li:2013:SSS

[LYZ+13] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Transactions on Parallel and Distributed Systems*, 24(1):131–143, January 2013. CODEN ITDSEO. ISSN 1045-9219.

Leng:2011:DKB

[LZ11] Lu Leng and Jiashu Zhang. Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security. *Journal of Network and Computer Applications*, 34(6):1979–1989, November 2011. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804511001287.

Liu:2012:SOCa

[LZC12a] Shengli Liu, Fangguo Zhang, and Kefei Chen. Selective opening chosen ciphertext security directly from the DDH assumption. *Lecture Notes in Computer Science*, 7645: 100–112, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34601-9_8/.

Luo:2012:LVT

[LZC+12b] Yong Luo, Yan Zhao, Lei Cheng, Jianxin Wang, and Xuchong Liu. Lossless visible three-dimensional watermark of digital elevation model data. *Lecture Notes in Computer Science*, 7220:138–147, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31439-1_13/.

Liu:2014:PKE

[LZC14] Shengli Liu, Fangguo Zhang, and Kefei Chen. Public-key encryption scheme with selective opening chosen-ciphertext security based on the Decisional Diffie–Hellman assumption. *Concurrency and Computation: Practice and Experience*, 26(8):1506–1519, June 10, 2014. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Liu:2017:ESS

[LZC17] Chang Liu, Liehuang Zhu, and Jinjun Chen. Efficient searchable symmetric encryption for storing multiple source dynamic social data on cloud. *Journal of Network and Computer Applications*, 86(??):3–14, May 15, 2017. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S108480451630217X.

Liu:2014:CRA

[LZCK14] Jingwei Liu, Zonghua Zhang, Xiaofeng Chen, and Kyung Sup Kwak. Certificateless remote anonymous authentication schemes for wireless body area networks. *IEEE Transactions on Parallel and Distributed Systems*, 25(2): 332–342, February 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Li:2019:APA

[LZD+19] JiLiang Li, WeiGuo Zhang, Vivek Dabra, Kim-Kwang Raymond Choo, Saru Kumari, and Dieter Hogrefe. AEP-PPA: an anonymous, efficient and provably-secure privacy-preserving authentication protocol for mobile services in smart cities. *Journal of Network and Computer Applications*, 134(??):52–61, May 15, 2019. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804519300475`.

Li:2010:PES

[LZJX10] C. H. Li, X. F. Zhang, H. Jin, and W. Xiang. E-passport EAC scheme based on Identity-Based Cryptography. *Information Processing Letters*, 111(1): 26–30, December 15, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Liu:2019:IEU

[LZKX19] Hongjun Liu, Yingqian Zhang, Abdurahman Kadir, and Yanqiu Xu. Image encryption using complex hyper chaotic system by injecting impulse into parameters. *Applied Mathematics and Computation*, 360(??):83–93, November 1, 2019. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0096300319303807`.

Li:2012:ESS

[LZT12] Fagen Li, Mingwu Zhang, and Tsuyoshi Takagi. Efficient signcryption in the standard model. *Concurrency and Computation: Practice and Experience*, 24(17):1977–1989, December 10, 2012. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Li:2019:ESM

[LZWZ19] Xingxin Li, Youwen Zhu, Jian Wang, and Ji Zhang. Efficient and secure multi-dimensional geometric range query over encrypted data in cloud. *Journal of Parallel and Distributed Computing*, 131(??):44–54, September 2019. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731518306294`.

Li:2016:BMA

[LZY+16] Fuxiang Li, Fucai Zhou, Heqing Yuan, Zifeng Xu, and Qiang Wang. Bilinear-map accumulator-based verifiable intersection operations on encrypted data in cloud. *Concurrency and Computation: Practice and Experience*, 28(11):3238–3253, August 10, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Liu:2019:XBL

[LZZ+19a] Weiqiang Liu, Lei Zhang, Zhengran Zhang, Chongyan Gu, Chenghua Wang, Maire O'neill, and Fabrizio Lombardi. XOR-based low-cost reconfigurable PUFs for IoT security. *ACM Transactions on Embedded Computing Systems*, 18(3):25:1–25:??, June 2019. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3274666.

Liu:2019:RAS

[LZZ19b] Xin Liu, Ruisheng Zhang, and Mingqi Zhao. A robust authentication scheme with dynamic password for wireless body area networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 161(??):220–234, October 9, 2019. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128618309885.

Ma:2017:AEJ

[Ma17a] Sha Ma. Authorized equi-join for multiple data contributors in the PKC-based setting. *The Computer Journal*, 60(12):1822–1838, December 1, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/12/1822/3861973.

Masdari:2017:STA

[MA17b] Mohammad Masdari and Safiyyeh Ahmadzadeh. A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems. *Journal of Network and Computer Applications*, 87(??):1–19, June 1, 2017. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804517300978.

MacCormick:2012:NAC

[Mac12] John MacCormick. *Nine algorithms that changed the future: the ingenious ideas that drive today's computers.* Princeton University Press, Princeton, NJ, USA,

2012. ISBN 0-691-14714-0 (hardcover), 0-691-15819-3 (paperback). x + 2 + 219 pp. LCCN QA76 .M21453 2012. URL `http://press.princeton.edu/chapters/s9528.pdf; http://www.jstor.org/stable/10.2307/j.ctt7t71s`. With a foreword by Christopher M. Bishop.

Macrakis:2014:PLS

[Mac14] Kristie Macrakis. *Prisoners, lovers, and spies: the story of invisible ink from Herodotus to al-Qaeda*. Yale University Press, New Haven, CT, USA, 2014. ISBN 0-300-17925-1 (hardcover). xiv + 377 pp. LCCN Z104.5 .M33 2014.

Maffeo:2016:UNC

[Maf16] Steven E. Maffeo. *U.S. Navy codebreakers, linguists, and intelligence officers against Japan, 1910–1941: a biographical dictionary*. Rowan and Littlefield, Lanham, MD, USA, 2016. ISBN 1-4422-5563-3, 1-4422-5564-1 (e-book). LCCN D810.S7 M2535 2015eb.

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).

Moskowitz:2010:ITE

[MAL10] I. S. Moskowitz, F. Ahmed, and P. A. Lafferty. Information theoretic effects of JPEG compression on image steganography. *International Journal of Computer Applications*, 32(3): 318–327, 2010. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.2316/Journal.202.2010.3.202-2736`.

Malkin:2013:SCB

[Mal13] Tal Malkin. Secure computation for big data. *Lecture Notes in Computer Science*, 7785:355, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/accesspage/chapter/10.1007/978-3-642-36594-2_20?coverImageUrl=/static/0.8699/sites/link/images/abstract_cover_placeholder.png`.

Mangard:2013:KSL

[Man13] Stefan Mangard. Keeping secrets on low-cost chips. *IEEE Security & Privacy*, 11(4):75–77, 2013. ISSN 1540-7993 (print), 1558-4046 (electronic).

Martin:2010:FWL

[Mar10a] Douglas Martin. Frank W. Lewis, master of the cryptic crossword, dies at 98. *New York Times*, ?? (??):??, December 3, 2010. CODEN NYTIAO. ISSN 0362-4331 (print), 1542-667X, 1553-8095.

Martin:2010:PCC

[Mar10b] Luther Martin. Protecting credit card information: encryption vs tokenisation. *Network Security*, 2010(6): 17–19, June 2010. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485810700842`.

Martin:2010:XMA

[Mar10c] Luther Martin. XTS: a mode of AES for encrypting hard disks. *IEEE Security & Privacy*, 8(3):68–69, May/June 2010. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Markoff:2012:FFO

[Mar12] John Markoff. Flaw found in an online encryption method. *New York Times*, January 14, 2012.

Mazumdar:2016:CIS

[MAS16] Bodhisatwa Mazumdar, Sk. Subidh Ali, and Ozgur Sinanoglu. A compact implementation of Salsa20 and its power analysis vulnerabilities. *ACM Transactions on Design Automation of Electronic Systems*, 22(1):11:1–11:??, December 2016. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Mashhadi:2017:NMS

[Mas17] Samaneh Mashhadi. New multi-stage secret sharing in the standard model. *Information Processing Letters*, 127(??):43–48, November 2017. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019017301242`.

Matsuda:2014:IBP

[Mat14] Takahiro Matsuda. On the impossibility of basing public-coin one-way permutations on trapdoor permutations. *Lecture Notes in Computer Science*, 8349:265–290, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_12/`.

Matthiessen:2019:RCM

[Mat19] Dana Matthiessen. The rise of cryptographic metaphors in Boyle and their use for the mechanical philosophy. *Studies in History and Philosophy of Science Part A*, 73(??):8–21, February 2019. CODEN SHPSB5. ISSN 0039-3681 (print), 1879-2510 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0039368117302522`.

Maurer:2012:CCN

[Mau12] Ueli Maurer. Constructive cryptography — a new paradigm for security definitions and proofs. *Lecture Notes in Computer Science*, 6993:33–56, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-27375-9_3/`.

Mayron:2015:BAM

[May15] Liam M. Mayron. Biometric authentication on mobile devices. *IEEE Security & Privacy*, 13(3):70–73, May/June 2015. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `http://www.computer.org/csdl/mags/sp/2015/03/msp2015030070-abs.html`.

Mazurczyk:2013:VSD

[Maz13] Wojciech Mazurczyk. VoIP steganography and its detection — a survey. *ACM Computing Surveys*, 46 (2):20:1–20:??, November 2013. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Milo:2011:FGB

[MBB11] Fabrizio Milo, Massimo Bernaschi, and Mauro Bisson. A fast, GPU based, dictionary attack to OpenPGP secret keyrings. *The Journal of Systems and Software*, 84(12):2088–2096, December 2011. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121211001270`.

Mao:2015:PUA

[MBC15] Qian Mao, K. Bharanitharan, and Chin-Chen Chang. A proxy user authentication protocol using source-based image morphing. *The Computer Journal*, 58(7):1573–1584, July 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/7/1573`.

Matias:2018:NNZ

[MBC+18] P. Matias, P. Barbosa,

T. N. C. Cardoso, D. M. Campos, and D. F. Aranha. NIZKCTF: A noninteractive zero-knowledge capture-the-flag platform. *IEEE Security & Privacy*, 16(6): 42–51, November/December 2018. ISSN 1540-7993 (print), 1558-4046 (electronic).

Malone:2013:MOD

[MBF+13] C. V. Malone, E. J. Barkie, B. L. Fletcher, N. Wei, A. Keren, and A. Wyskida. Mobile Optimized Digital Identity (MODI): A framework for easier digital certificate use. *IBM Journal of Research and Development*, 57(6):9:1–9:11, November–December 2013. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Migliore:2018:PPF

[MBF18] Vincent Migliore, Guillaume Bonnoron, and Caroline Fontaine. Practical parameters for somewhat homomorphic encryption schemes on binary circuits. *IEEE Transactions on Computers*, 67(11): 1550–1560, ???? 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `https://ieeexplore.ieee.org/document/8302942/`.

Mainardi:2019:PRA

[MBP19] Nicholas Mainardi, Alessandro Barenghi, and Gerardo Pelosi. Plaintext recovery attacks against linearly decryptable fully homomorphic encryption schemes. *Computers & Security*, 87(??):Article 101587, November 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404819301403`.

Massolino:2015:OSC

[MBR15] Pedro Maat C. Massolino, Paulo S. L. M. Barreto, and Wilson V. Ruggiero. Optimized and scalable co-processor for McEliece with binary Goppa codes. *ACM Transactions on Embedded Computing Systems*, 14 (3):45:1–45:??, April 2015. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Mukhopadhyay:2011:PEA

[MC11] Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. A parallel efficient architecture for large cryptographically robust $n \times k(k \geq n/2)$ mappings. *IEEE Transactions on Computers*, 60(3):375–385, March 2011. CODEN ITCOB4. ISSN 0018-9340

(print), 1557-9956 (electronic).

Matula:2019:PCG

[MC19] David W. Matula and Zizhen Chen. Precise and concise graphical representation of the natural numbers. In Takagi et al. [TBL19], pages 100–103. ISBN 1-72813-366-1. ISSN 1063-6889.

Madanayake:2012:BPS

[MCDB12] H. L. P. Arjuna Madanayake, R. J. Cintra, V. S. Dimitrov, and L. T. Bruton. Block-parallel systolic-array architecture for 2-D NTT-based fragile watermark embedding. *Parallel Processing Letters*, 22(3): 1250009, September 2012. CODEN PPLTEE. ISSN 0129-6264 (print), 1793-642X (electronic).

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`.

McGrayne:2011:TWH

[McG11] Sharon Bertsch McGrayne. *The theory that would not die: how Bayes' rule cracked the Enigma code, hunted down Russian submarines, and emerged triumphant from two centuries of controversy.* Yale University Press, New Haven, CT, USA, 2011. ISBN 0-300-16969-8. xiii + 320 pp. LCCN QA279.5 2011. URL `http://yalepress.yale.edu/yupbooks/book.asp?isbn=9780300169690`.

McGraw:2016:SBTd

[McG16] Gary McGraw. Silver Bullet talks with Martin Hellman. *IEEE Security & Privacy*, 14(4): 7–11, July/August 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `https://www.computer.org/csdl/mags/sp/2016/04/msp2016040007.html`.

McKay:2010:SLB

[McK10] Sinclair McKay. *The secret life of Bletchley Park: the history of the wartime codebreaking centre by the men and women who were there.* Aurum, London, UK, 2010. ISBN 1-84513-539-3 (hardcover). vi + 336 + 8 pp. LCCN D810.C88 M35 2010x.

McKay:2011:SLB

[McK11] Sinclair McKay. *The secret life of Bletchley Park: the history of the wartime codebreaking centre by the men and women who were* *there*. Gardners Books, 2011. ISBN 1-84513-633-0. ???? pp. LCCN ????

McKay:2012:SLC

[McK12] Sinclair McKay. *The secret lives of codebreakers: the men and women who cracked the Enigma code at Bletchley Park*. Plume, New York, NY, USA, 2012. ISBN 0-452-29871-7. vi + 338 pp. LCCN D810.C88 M39 2012.

Ma:2019:TOP

[MCL+19] Ziqiang Ma, Quanwei Cai, Jingqiang Lin, Bo Luo, and Jiwu Jing. Towards the optimal performance of integrating Warm and Delay against remote cache timing side channels on block ciphers. *Journal of Computer Security*, 27(5):547–580, ???? 2019. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Mahmood:2018:ECC

[MCN+18] Khalid Mahmood, Shehzad Ashraf Chaudhry, Husnain Naqvi, Saru Kumari, Xiong Li, and Arun Kumar Sangaiah. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Generation Computer Systems*, 81(??):557–565, April 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17309263.

Marquez-Corbella:2015:ECP

[MCP15] Irene Márquez-Corbella and Ruud Pellikaan. Error-correcting pairs: a new approach to code-based cryptography. *ACM Communications in Computer Algebra*, 49(1):21, March 2015. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Mhenni:2019:DSA

[MCRB19] Abir Mhenni, Estelle Cherrier, Christophe Rosenberger, and Najoua Essoukri Ben Amara. Double serial adaptation mechanism for keystroke dynamics authentication based on a single password. *Computers & Security*, 83(??):151–166, June 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818306059.

Mathew:2015:NMB

[MCS+15] Jimson Mathew, Rajat Subhra Chakraborty, Durga Prasad Sahoo, Yuanfan Yang, and Dhiraj K. Pradhan. A novel memristor-based hardware security primitive. *ACM Transactions on Embedded Computing*

Systems, 14(3):60:1–60:??, April 2015. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Majzoub:2012:MRH

[MD12a] Sohaib Majzoub and Hassan Diab. MorphoSys reconfigurable hardware for cryptography: the Twofish case. *The Journal of Supercomputing*, 59(1):22–41, January 2012. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-010-0413-3.

Mansouri:2012:ACA

[MD12b] Shohreh Sharif Mansouri and Elena Dubrova. An architectural countermeasure against power analysis attacks for FSR-based stream ciphers. *Lecture Notes in Computer Science*, 7275:54–68, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29912-4_5/.

Mansfield-Devine:2015:MIC

[MD15] Steve Mansfield-Devine. Managing identity for a competitive edge. *Network Security*, 2015(1):14–18, January 2015. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485815700103.

Murdoch:2010:CPB

[MDAB10] Steven J. Murdoch, Saar Drimer, Ross Anderson, and Mike Bond. Chip and PIN is broken. In IEEE, editor, *2010 IEEE Symposium on Security and Privacy, 16–19 May 2010, Oakland, CA, USA*, pages 433–446. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 1-4244-6894-9. ISSN 1081-6011. LCCN ???? URL http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf.

Malina:2018:SET

[MDHM18] Lukas Malina, Petr Dzurenda, Jan Hajny, and Zdenek Martinasek. Secure and efficient two-factor zero-knowledge authentication solution for access control systems. *Computers & Security*, 77(??):500–513, August 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818304942.

Mosenia:2017:PTS

[MDMJ17] Arsalan Mosenia, Xiao-liang Dai, Prateek Mittal, and Niraj Jha. PinMe: Tracking a smartphone user around the world. *IEEE Transactions on Multi-Scale Computing Systems*, ??(??):1–17, ???? 2017. ISSN 2332-7766.

Maachaoui:2012:MLA

[MEFO12] M. Maachaoui, A. Abou El Kalam, C. Fraboul, and A. Ait Ouahman. Multi-level authentication based single sign-on for IMS services. *Lecture Notes in Computer Science*, 7394:174–187, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32805-3_14/.

Meiklejohn:2010:BRB

[Mei10] Sarah Meiklejohn. Book review: *An Introduction to Mathematical Cryptography*, by Jeffrey Hoffstein, Jill Pipher, and Joseph Silverman Springer-Verlag, 2008. *ACM SIGACT News*, 41(4):47–50, December 2010. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [HPS08].

Menezes:2013:IPB

[Men13a] Alfred Menezes. An introduction to pairing-based cryptography. Report, Department of Mathematics, University of Waterloo, Waterloo, ON, Canada, October 27, 2013. 19 pp. URL https://www.math.uwaterloo.ca/~ajmeneze/publications/pairings.pdf.

Menn:2013:ESC

[Men13b] Joseph Menn. Exclusive: Secret contract tied NSA and security industry pioneer. Reuters, December 13, 2013.

Meshram:2015:EIB

[Mes15] Chandrashekhar Meshram. An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem. *Information Processing Letters*, 115(2):351–358, February 2015. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019014002221.

Mandal:2016:DIW

[MFG16] Kalikinkar Mandal, Xinxin Fan, and Guang Gong. Design and implementation of Warbler family of lightweight pseudorandom number generators for smart devices. *ACM Transactions on Embedded Computing Systems*, 15(1):1:1–1:??, February 2016. CODEN ???? ISSN 1539-

9087 (print), 1558-3465 (electronic).

Moreno:2013:NIP

[MFH13] Carlos Moreno, Sebastian Fischmeister, and M. Anwar Hasan. Nonintrusive program tracing and debugging of deployed embedded systems through side-channel analysis. *ACM SIGPLAN Notices*, 48(5):77–88, May 2013. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Moufek:2015:MCB

[MG15] Hamza Moufek and Kenza Guenda. McEliece cryptosystem based on punctured convolutional codes and the pseudo-random generators. *ACM Communications in Computer Algebra*, 49(1):21, March 2015. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Mukherjee:2019:EBV

[MGB19] Sankar Mukherjee, Daya Sagar Gupta, and G. P. Biswas. An efficient and batch verifiable conditional privacy-preserving authentication scheme for VANETs using lattice. *Computing*, 101 (12):1763–1788, December 2019. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Misoczki:2019:TPS

[MGG+19] R. Misoczki, S. Gulley, V. Gopal, M. G. Dixon, H. Vrsalovic, and W. K. Feghali. Toward postquantum security for embedded cores. *IEEE Micro*, 39(4): 17–26, July/August 2019. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Meng:2019:SDD

[MGJ19] Wenjuan Meng, Jianhua Ge, and Tao Jiang. Secure data deduplication with reliable data deletion in cloud. *International Journal of Foundations of Computer Science (IJFCS)*, 30(4):551–570, June 2019. ISSN 0129-0541. URL `https://www.worldscientific.com/doi/10.1142/S0129054119400124`.

Marmol:2010:TPA

[MGP10] Félix Gómez Mármol, Joao Girao, and Gregorio Martínez Pérez. TRIMS, a privacy-aware trust and reputation model for identity management systems. *Computer Networks (Amsterdam, Netherlands: 1999)*, 54(16):2899–2912, November 15, 2010. CODEN ???? ISSN 1389-1286.

Matsuda:2014:CCS

[MH14] Takahiro Matsuda and Goichiro Hanaoka. Chosen ciphertext security via point obfuscation. *Lecture Notes in Computer Science*, 8349:95–120, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_5/.

Meloni:2016:RDR

[MH16] Nicolas Méloni and M. Anwar Hasan. Random digit representation of integers. In Montuschi et al. [MSH+16], pages 118–125. ISBN 1-5090-1615-5. ISSN 1063-6889. LCCN QA76.9.C62 S95 2016. URL http://ieeexplore.ieee.org/servlet/opac?punumber=7562813.

Meziani:2012:IPS

[MHC12] Mohammed Meziani, Gerhard Hoffmann, and Pierre-Louis Cayrel. Improving the performance of the SYND stream cipher. *Lecture Notes in Computer Science*, 7374:99–116, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31410-0_7/.

Miller:2014:ADS

[MHKS14] Andrew Miller, Michael Hicks, Jonathan Katz, and Elaine Shi. Authenticated data structures, generically. *ACM SIGPLAN Notices*, 49(1):411–423, January 2014. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). POPL '14 conference proceedings.

Mo:2018:RUA

[MHL18] Jiaqing Mo, Zhongwang Hu, and Yuhua Lin. Remote user authentication and key agreement for mobile client-server environments on elliptic curve cryptography. *The Journal of Supercomputing*, 74(11):5927–5943, November 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Munoz-Hernandez:2016:EES

[MHMSGH16] Mario Diego Munoz-Hernandez, Miguel Morales-Sandoval, and Jose Juan Garcia-Hernandez. An end-to-end security approach for digital document management. *The Computer Journal*, 59(7):1076–1090, July 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/7/1076.

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).

Mohd:2015:SLB

[MHV15] Bassam J. Mohd, Thaier Hayajneh, and Athanasios V. Vasilakos. A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. *Journal of Network and Computer Applications*, 58(??):73–93, December 2015. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804515002076.

Ma:2019:PFC

[MHW+19] Ruijun Ma, Haifeng Hu, Weixuan Wang, Jia Xu, and Zhengming Li. Photorealistic face completion with semantic parsing and face identity-preserving features. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 15(1):28:1–28:??, February 2019. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3300940.

Mohd:2018:HDM

[MHY+18] Bassam Jamil Mohd, Thaier Hayajneh, Khalil M. Ahmad Yousef, Zaid Abu Khalaf, and Md Zakirul Alam Bhuiyan. Hardware design and modeling of lightweight block ciphers for secure communications. *Future Generation Computer Systems*, 83(??):510–521, June 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17304661.

Micciancio:2010:FGC

[Mic10a] Daniele Micciancio. A first glimpse of cryptography's Holy Grail. *Communications of the Association for Computing Machinery*, 53 (3):96, March 2010. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Michiels:2010:OWB

[Mic10b] Wil Michiels. Opportunities in white-box cryptography. *IEEE Security & Privacy*, 8(1):64–67, January/February 2010. ISSN

1540-7993 (print), 1558-4046 (electronic).

Michael:2016:RNI

[Mic16] K. Michael. RFID/NFC implants for Bitcoin transactions. *IEEE Consumer Electronics Magazine*, 5(3): 103–106, July 2016. ISSN 2162-2248 (print), 2162-2256 (electronic).

Midgley:2010:SEE

[Mid10] Stephen Midgley. The state of encryption in Europe: some cultural comparisons. *Network Security*, 2010(8): 18–19, August 2010. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485810701070`.

Martinez-Julia:2012:NIB

[MJGS12] P. Martinez-Julia and A. F. Gómez-Skarmeta. A novel identity-based network architecture for next generation Internet. *J.UCS: Journal of Universal Computer Science*, 18(12): 1643–??, ???? 2012. CODEN ???? ISSN 0948-6968. URL `http://www.jucs.org/jucs_18_12/a_novel_identity_based`.

Martinez-Julia:2013:BSI

[MJS13] Pedro Martinez-Julia and Antonio F. Skarmeta. Beyond the separation of identifier and locator: Building an identity-based overlay network architecture for the Future Internet. *Computer Networks (Amsterdam, Netherlands: 1999)*, 57(10):2280–2300, July 5, 2013. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128613000066`.

Miao:2019:PPT

[MJS+19] Chenglin Miao, Wenjun Jiang, Lu Su, Yaliang Li, Suxin Guo, Zhan Qin, Houping Xiao, Jing Gao, and Kui Ren. Privacy-preserving truth discovery in crowd sensing systems. *ACM Transactions on Sensor Networks*, 15(1):9:1–9:??, February 2019. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3277505`.

Memon:2018:TFS

[MJW+18] Shiraz Memon, Jensen Jens, Elbers Willem, Helmut Neukirchen, Matthias Book, and Morris Riedel. Towards federated service discovery and identity management in collaborative data and compute cloud infrastructures. *Journal of Grid Computing*, 16(4):663–681, December 2018. CODEN ???? ISSN

1570-7873 (print), 1572-9184 (electronic). URL https://link.springer.com/article/10.1007/s10723-018-9445-3.

Mohanty:2011:RTP

[MK11] Saraju P. Mohanty and Elias Kougianos. Real-time perceptual watermarking architectures for video broadcasting. *The Journal of Systems and Software*, 84(5):724–738, May 2011. CODEN JSSODM. ISSN 0164-1212.

Moessner:2012:SAS

[MK12a] M. Moessner and Gul N. Khan. Secure authentication scheme for passive C1G2 RFID tags. *Computer Networks (Amsterdam, Netherlands: 1999)*, 56(1):273–286, January 12, 2012. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128611003422.

Muller:2012:HPC

[MK12b] Sascha Müller and Stefan Katzenbeisser. Hiding the policy in cryptographic access control. *Lecture Notes in Computer Science*, 7170:90–105, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29963-6_8/.

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 Computer Science*, 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.

Malik:2012:AIC

[MKH+12] Sana Ambreen Malik, Asifullah Khan, Mutawarra Hussain, Khurram Jawad, Rafiullah Chamlawi, and Abdul Jalil. Authentication of images for 3D cameras: Reversibly embedding information using intelligent approaches. *The Journal of Systems and Software*, 85(11):2665–2673, November 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212001719.

Menesidou:2017:CKM

[MKK17] Sofia Anna Menesidou, Vasilios Katos, and Georgios Kambourakis. Cryptographic key management in delay tolerant networks: a survey. *Future Internet*, 9(3):26, June 27, 2017. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/9/3/26.

Marconato:2013:VLC

[MKN13] G. Vache Marconato, M. Kaâniche, and V. Nicomette. A vulnerability life cycle-based security modeling and evaluation approach. *The Computer Journal*, 56(4):422–439, April 2013. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/56/4/422.full.pdf+html.

Mozaffari-Kermani:2010:CSI

[MKRM10] M. Mozaffari-Kermani and A. Reyhani-Masoleh. Concurrent structure-independent fault detection schemes for the Advanced Encryption Standard. *IEEE Transactions on Computers*, 59(5):608–622, May 2010. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5406504.

Montecchi:2012:QSE

[MLBL12] Leonardo Montecchi, Paolo Lollini, Andrea Bondavalli, and Ernesto La Mattina. Quantitative security evaluation of a multi-biometric authentication system. *Lecture Notes in Computer Science*, 7613:209–221, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.

com/chapter/10.1007/978-3-642-33675-1_19/.

Mancillas-Lopez:2010:RHI

[MLCH10] C. Mancillas-Lopez, D. Chakraborty, and F. Rodriguez Henriquez. Reconfigurable hardware implementations of tweakable enciphering schemes. *IEEE Transactions on Computers*, 59 (11):1547–1561, November 2010. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5432161.

Mendez:2016:PES

[MLM16] Alejandro Pérez Méndez, Rafael Marín López, and Gabriel López Millán. Providing efficient SSO to cloud service access in AAA-based identity federations. *Future Generation Computer Systems*, 58(??):13–28, May 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X15003854.

Manzanares-Lopez:2012:ICU

[MLMSMG12] Pilar Manzanares-Lopez, Josemaria Malgosa-Sanahuja, and Juan Pedro Muñoz-Gea. The importance of considering unauthentic transactions in trust management systems. *Journal of Parallel and Distributed Computing*, 72(6):809–818, June 2012. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731512000718.

Ma:2017:LBI

[MLO17] Chunguang Ma, Juyan Li, and Weiping Ouyang. Lattice-based identity-based homomorphic conditional proxy re-encryption for secure big data computing in cloud environment. *International Journal of Foundations of Computer Science (IJFCS)*, 28(6):645–??, September 2017. CODEN IFCSEN. ISSN 0129-0541.

Madhusudhan:2012:DIB

[MM12] R. Madhusudhan and R. C. Mittal. Dynamic ID-based remote user password authentication schemes using smart cards: a review. *Journal of Network and Computer Applications*, 35(4):1235–1248, July 2012. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804512000215.

Meshram:2013:IBC

[MM13] Chandrashekhar Meshram and Suchitra A. Meshram.

An identity-based cryptographic model for discrete logarithm and integer factoring based cryptosystem. *Information Processing Letters*, 113 (10–11):375–380, May/ June 2013. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013000550.

Maity:2014:FIR

[MM14a] Hirak Kumar Maity and Santi P. Maity. FPGA implementation of reversible watermarking in digital images using reversible contrast mapping. *The Journal of Systems and Software*, 96(??):93–104, October 2014. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121214001393.

Mondal:2014:DSM

[MM14b] Subijit Mondal and Subhashis Maitra. Data security-modified AES algorithm and its applications. *ACM SIGARCH Computer Architecture News*, 42(2):1–8, May 2014. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Maity:2017:ODC

[MM17a] Santi P. Maity and Hirak Kumar Maity. Optimality in distortion control in reversible watermarking using genetic algorithms. *International Journal of Image and Graphics (IJIG)*, 17(3):1750013, July 2017. CODEN ???? ISSN 0219-4678.

Mazumdar:2017:CRS

[MM17b] Bodhisatwa Mazumdar and Debdeep Mukhopadhyay. Construction of rotation symmetric S-boxes with high nonlinearity and improved DPA resistivity. *IEEE Transactions on Computers*, 66(1):59–72, January 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Mulholland:2017:DCD

[MMB17] John Mulholland, Michele Mosca, and Johannes Braun. The day the cryptography dies. *IEEE Security & Privacy*, 15(4): 14–21, July/August 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2017/04/msp2017040014-abs.html.

Martins:2019:HHR

[MMBS19] Paulo Martins, Jeremy

Marrez, Jean-Claude Bajard, and Leonel Sousa. HyPoRes: An hybrid representation system for ECC. In Takagi et al. [TBL19], pages 207–214. ISBN 1-72813-366-1. ISSN 1063-6889.

Merlo:2015:MEP

[MMF15] Alessio Merlo, Mauro Migliardi, and Paolo Fontanelli. Measuring and estimating power consumption in Android to support energy-based intrusion detection. *Journal of Computer Security*, 23(5):611–637, ???? 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Mailloux:2016:PSS

[MMKP16] Logan O. Mailloux, Michael A. McEvilley, Stephen Khou, and John M. Pecarina. Putting the 'Systems' in security engineering: An examination of NIST Special Publication 800-160. *IEEE Security & Privacy*, 14(4):76–80, July/August 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/04/msp2016040076-abs.html.

Miao:2016:RAS

[MML16] Yinbin Miao, Jianfeng Ma, and Zhiquan Liu. Revocable and anonymous searchable encryption in multi-user setting. *Concurrency and Computation: Practice and Experience*, 28 (4):1204–1218, March 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Maeng:2015:TAU

[MMLN15] YoungJae Maeng, Aziz Mohaisen, Mun-Kyu Lee, and DaeHun Nyang. Transaction authentication using complementary colors. *Computers & Security*, 48(??):167–181, February 2015. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404814001473.

Moldovyan:2012:BBD

[MMN12] Alexandr Moldovyan, Nikolay Moldovyan, and Evgenia Novikova. Blind 384-bit digital signature scheme. *Lecture Notes in Computer Science*, 7531:77–83, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33704-8_7/.

Mahmoody:2014:PPK

[MMP14] Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. On the power of public-key encryption in secure computation. *Lecture Notes in Computer Science*, 8349: 240–264, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_11/.

Marino:2019:ACN

[MMP19] Francesco Marino, Corrado Moiso, and Matteo Petracca. Automatic contract negotiation, service discovery and mutual authentication solutions: a survey on the enabling technologies of the forthcoming IoT ecosystems. *Computer Networks (Amsterdam, Netherlands: 1999)*, 148(??):176–195, January 15, 2019. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128618312167.

Macedo:2017:SSP

[MMS+17a] Ricardo Macedo, Leonardo Melniski, Aldri Santos, Yacine Ghamri-Doudane, and Michele Nogueira. SPARTA: a survival performance degradation framework for identity federations. *Computer Networks (Amsterdam, Netherlands: 1999)*, 121(??):37–52, July 5, 2017. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128617301524.

Mazumder:2017:PSK

[MMS17b] Rashed Mazumder, Atsuko Miyaji, and Chunhua Su. Probably secure keyed-function based authenticated encryption schemes for big data. *International Journal of Foundations of Computer Science (IJFCS)*, 28(6):661–??, September 2017. CODEN IFCSEN. ISSN 0129-0541.

Mazumder:2017:SAE

[MMS17c] Rashed Mazumder, Atsuko Miyaji, and Chunhua Su. A simple authentication encryption scheme. *Concurrency and Computation: Practice and Experience*, 29(16), August 25, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Maity:2013:CRS

[MMSD13] Santi P. Maity, Seba Maity, Jaya Sil, and Claude Delpha. Collusion resilient spread spectrum watermarking in M-band wavelets using GA-fuzzy hybridization. *The Journal of Systems and Software*, 86(1):47–59, January 2013. CODEN JSSODM. ISSN 0164-1212

(print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212001938.

Matsuo:2012:MAK

[MMY12] Shin'ichiro Matsuo, Daisuke Moriyama, and Moti Yung. Multifactor authenticated key renewal. *Lecture Notes in Computer Science*, 7222:204–220, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32298-3_14/.

Meshram:2012:IBC

[MMZ12] Chandrashekhar Meshram, Suchitra A. Meshram, and Mingwu Zhang. An ID-based cryptographic mechanisms based on GDLP and IFP. *Information Processing Letters*, 112(19):753–758, October 15, 2012. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S002001901200169X.

Moran:2010:BCP

[MN10] Tal Moran and Moni Naor. Basing cryptographic protocols on tamper-evident seals. *Theoretical Computer Science*, 411(10):1283–1310, March 4, 2010. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Mukhopadhyay:2014:EMP

[MN14] Debapriyay Mukhopadhyay and Subhas C. Nandy. Efficient multiple-precision integer division algorithm. *Information Processing Letters*, 114(3):152–157, March 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013002627. This paper provides a correction to the algorithm presented in [HZSL05], and also supplies a complicated correctness proof.

Monz:2016:RSS

[MNM+16] Thomas Monz, Daniel Nigg, Esteban A. Martinez, Matthias F. Brandl, Philipp Schindler, Richard Rines, Shannon X. Wang, Isaac L. Chuang, and Rainer Blatt. Realization of a scalable Shor algorithm. *Science*, 351 (6277):1068–1070, March 4, 2016. ISSN 0036-8075. URL http://science.sciencemag.org/content/351/6277/1068.

McKusick:2015:DIF

[MNNW15] Marshall Kirk McKusick, George V. Neville-Neil, and Robert N. M. Watson. *The design and implementation* of the FreeBSD operating system. Addison-Wesley, Reading, MA, USA, second edition, 2015. ISBN 0-321-96897-2 (hardcover). xxx + 886 pp. LCCN QA76.774.F74 M35 2015. URL http://proquest.safaribooksonline.com/9780133761825.

Minier:2012:RKI

[MNP12] Marine Minier and María Naya-Plasencia. A related key impossible differential attack against 22 rounds of the lightweight block cipher LBlock. *Information Processing Letters*, 112(16):624–629, August 31, 2012. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019012001238.

Mizuki:2011:ASN

[MNS11] Takaaki Mizuki, Satoru Nakayama, and Hideaki Sone. An application of ST-numbering to secret key agreement. *International Journal of Foundations of Computer Science (IJFCS)*, 22(5):1211–1227, August 2011. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Maimut:2012:LCR

[MO12] Diana Maimut and Khaled Ouafi. Lightweight cryptography for RFID tags. *IEEE Security & Privacy*, 10(2):76–79, March/April 2012. ISSN 1540-7993 (print), 1558-4046 (electronic).

Minamoto:2014:BDI

[MO14] Teruya Minamoto and Ryuji Ohura. A blind digital image watermarking method based on the dyadic wavelet transform and interval arithmetic. *Applied Mathematics and Computation*, 226(??):306–319, January 1, 2014. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300313010850.

Mone:2013:FPE

[Mon13] Gregory Mone. Future-proof encryption. *Communications of the Association for Computing Machinery*, 56(11):12–14, November 2013. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Moore:2012:RFF

[Moo12] Samuel K. Moore. RSA flaw found. *IEEE Spectrum*, ??(??):??, February 14, 2012. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic). URL http://spectrum.ieee.org/tech-talk/computing/it/rsa-flaw-found.

Moody:2014:DMW

[Moo14] Oliver Moody. Death of man who cracked Hitler's code. *The Times [London]*, March 27, 2014. URL http://www.thetimes.co.uk/tto/news/uk/defence/article4046291.ece.

Morad:2012:OEA

[Mor12] Ameer H. Morad. Office employees authentication based on E-exam techniques. *Lecture Notes in Computer Science*, 7666:60–65, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34478-7_8/.

Morawiecki:2019:MS

[Mor19a] Paweł Morawiecki. Malicious SHA-3. *Fundamenta Informaticae*, 169(4):331–343, ???? 2019. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Moriai:2019:PPD

[Mor19b] Shiho Moriai. Privacy-preserving deep learning via additively homomorphic encryption. In Takagi et al. [TBL19], page 198. ISBN 1-72813-366-1. ISSN 1063-6889.

Mosca:2018:CEQ

[Mos18] M. Mosca. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5):38–41, September/October 2018. ISSN 1540-7993 (print), 1558-4046 (electronic).

Moulick:2015:RDS

[Mou15] Subhayan Roy Moulick. Review of: *Digital Signatures* by Jonathan Katz. *ACM SIGACT News*, 46(1):10–12, March 2015. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Minier:2012:EEC

[MP12] Marine Minier and Raphael C.-W. Phan. Energy-efficient cryptographic engineering paradigm. *Lecture Notes in Computer Science*, 7039:78–88, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27585-2_7/.

Min:2018:AAB

[MPA+18] Donghyun Min, Donggyu Park, Jinwoo Ahn, Ryan Walker, Junghee Lee, Sungyong Park, and Youngjae Kim. Amoeba: An autonomous backup and recovery SSD for ransomware attack defense. *IEEE Computer Architecture Letters*, 17(2):243–246, July/December 2018. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Meiklejohn:2016:FBC

[MPJ+16] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. A fistful of Bitcoins: characterizing payments among men with no names. *Communications of the Association for Computing Machinery*, 59(4): 86–93, April 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2016/4/200174/fulltext`.

Mundhenk:2017:SAN

[MPM+17] Philipp Mundhenk, Andrew Paverd, Artur Mrowca, Sebastian Steinhorst, Martin Lukasiewycz, Suhaib A. Fahmy, and Samarjit Chakraborty. Security in automotive networks: Lightweight authentication and authorization. *ACM Transactions on Design Automation of Electronic Systems*, 22(2):25:1–25:??, March 2017. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Mironov:2012:IDP

[MPRS12] Ilya Mironov, Omkant Pandey, Omer Reingold, and Gil Segev. Incremental deterministic public-key encryption. *Lecture Notes in Computer Science*, 7237:628–644, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_36; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_37/`.

Mukhamedov:2010:IEP

[MR10] Aybek Mukhamedov and Mark D. Ryan. Identity escrow protocol and anonymity analysis in the applied pi-calculus. *ACM Transactions on Information and System Security*, 13(4):41:1–41:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Maimut:2014:AET

[MR14a] Diana Maimut and Reza Reyhanitabar. Authenticated encryption: Toward next-generation algorithms. *IEEE Security & Privacy*, 12(2):70–72, March/April 2014. ISSN 1540-7993.

Marasco:2014:SAS

[MR14b] Emanuela Marasco and Arun Ross. A survey on antispoofing schemes for fingerprint recognition systems. *ACM Computing Surveys*, 47(2):28:1–28:??, November 2014. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Micali:2014:CMS

[MR14c] Silvio Micali and Michael O. Rabin. Cryptography miracles, secure auctions, matching problem verification. *Communications of the Association for Computing Machinery*, 57(2): 85–93, February 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Manimehalai:2016:NRR

[MR16] P. Manimehalai and P. Arockia Jansi Rani. A new robust reversible blind watermarking in wavelet-domain for color images. *International Journal of Image and Graphics (IJIG)*, 16 (2):1650006, April 2016. CODEN ???? ISSN 0219-4678.

Migliore:2018:HSC

[MRL+18] Vincent Migliore, Maria Méndez Real, Vianney Lapotre, Arnaud Tisserand, Caroline Fontaine, and Guy Gogniat. Hardware/software co-design of an accelerator for FV homomorphic encryption scheme using Karatsuba algorithm. *IEEE Transactions on Computers*, 67(3):335–347, March 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/document/7797469/`.

Moataz:2018:SSE

[MRR+18] Tarik Moataz, Indrajit Ray, Indrakshi Ray, Abdullatif Shikfa, Frédéric Cuppens, and Nora Cuppens. Substring search over encrypted data. *Journal of Computer Security*, 26(1): 1–30, ???? 2018. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Martinovic:2017:AUP

[MRRT17] Ivan Martinovic, Kasper Rasmussen, Marc Roeschlin, and Gene Tsudik. Authentication using pulse-response biometrics. *Communications of the Association for Computing Machinery*, 60(2):108–115, February 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2017/2/212440/fulltext`.

Matsumoto:2017:ACG

[MRS+17] Stephanos Matsumoto, Raphael M. Reischuk, Pawel Szalachowski, Tiffany Hyun-Jin Kim, and Adrian Perrig. Authentication challenges in a global environment. *ACM Transactions on Privacy and Security (TOPS)*, 20(1):1:1–1:??, February 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Moghadam:2010:DRN

[MRT10] I. Zarei Moghadam, A. S. Rostami, and M. R. Tanhatalab. Designing a random number generator with novel parallel LFSR substructure for key stream ciphers. In *2010 International Conference on Computer Design and Applications (ICCDA)*, volume 5, pages V5–598–V5–601. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5541188.

Mendel:2012:DAL

[MRTV12] Florian Mendel, Vincent Rijmen, Deniz Toz, and Kerem Varıcı. Differential analysis of the LED block cipher. *Lecture Notes in Computer Science*, 7658:190–207, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34961-4_13/.

Maitra:2012:NAC

[MS12a] Subhashis Maitra and Amitabha Sinha. A new algorithm for computing triple-base number system. *ACM SIGARCH Computer Architecture News*, 40(4):3–9, September 2012. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Mroczkowski:2012:CAS

[MS12b] Piotr Mroczkowski and Janusz Szmidt. The cube attack on stream cipher Trivium and quadraticity tests. *Fundamenta Informaticae*, 114(3–4):309–318, August 2012. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Maitra:2013:DSM

[MS13a] Subhashis Maitra and Amitabha Sinha. Design and simulation of MAC unit using combinational circuit and adder. *ACM SIGARCH Computer Architecture News*, 41(5):25–33, December 2013. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Maitra:2013:HEM

[MS13b] Subhashis Maitra and Amitabha Sinha. High efficiency MAC unit used in digital signal processing and elliptic curve cryptography. *ACM SIGARCH Computer Architecture News*, 41(4):1–7, September 2013. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Maitra:2013:HPM

[MS13c] Subhashis Maitra and Amitabha Sinha. High performance MAC unit for DSP and cryptographic applications. *ACM SIGARCH Computer Architecture News*, 41(2):47–55, May 2013. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Miller:2016:RPS

[MS16] Carl A. Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *Journal of the ACM*, 63(4):33:1–33:??, November 2016. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Mukherjee:2017:EPP

[MS17] Srilekha Mukherjee and Goutam Sanyal. Enhanced position power first mapping (PPFM) based image steganography. *International Journal of Computer Applications*, 39(2):59–68, 2017. CODEN IJCAFW. ISSN 1206-212X (print), 1925-7074 (electronic). URL https://www.tandfonline.com/doi/full/10.1080/1206212X.2016.1273624.

Myers:2012:BCM

[MSas12] Steven Myers, Mona Sergi, and abhi shelat. Black-box construction of a more than non-malleable CCA 1 encryption scheme from plaintext awareness. *Lecture Notes in Computer Science*, 7485:149–165, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32928-9_9/.

Myers:2013:BBC

[MSas13] Steven Myers, Mona Sergi, and abhi shelat. Black-box construction of a more than non-malleable CCA1 encryption scheme from plaintext awareness. *Journal of Computer Security*, 21(5):721–748, ???? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Morales-Sandoval:2018:PBC

[MSGCDPSS18] Miguel Morales-Sandoval, Jose Luis Gonzalez-Compean, Arturo Diaz-Perez, and Victor J. Sosa-Sosa. A pairing-based cryptographic approach for data security in the cloud. *International Journal of Information Security*, 17(4): 441–461, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0375-z.

Montuschi:2016:ISC

[MSH+16] Paolo Montuschi, Michael Schulte, Javier Hormigo, Stuart Oberman, and Nathalie Revol, editors. *2016 IEEE 23nd Symposium on Computer Arithmetic (ARITH 2016), Santa Clara, California, USA, 10–13 July 2016*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2016. ISBN 1-5090-1615-5. ISSN 1063-6889. LCCN QA76.9.C62 S95 2016. URL http://ieeexplore.ieee.org/servlet/opac?punumber=7562813.

Marton:2010:RDC

[MSI10] Kinga Marton, Alin Suciu, and Iosif Ignat. Randomness in digital cryptography: a survey. *Romanian Journal of Information Science and Technology*, 13(3):219–240, ???? 2010. CODEN ???? ISSN 1453-8245. URL http:www.imt.ro/romjist/Volum13/Number13_3/pdf/KMarton.pdf.

Mashimo:2018:VMS

[MSI18] Susumu Mashimo, Ryota Shioya, and Koji Inoue. VMOR: Microarchitectural support for operand access in an interpreter. *IEEE Computer Architecture Letters*, 17(2):217–220, July/December 2018. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Mosenia:2017:CCA

[MSKRJ17] A. Mosenia, S. Sur-Kolay, A. Raghunathan, and N. K. Jha. CABA: Continuous authentication based on BioAura. *IEEE Transactions on Computers*, 66 (5):759–772, May 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Mazurczyk:2013:FWS

[MSL13] W. Mazurczyk, K. Szczypiorski, and J. Lubacz. Four ways to smuggle messages through Internet services. *IEEE Spectrum*, 50(11):42–45, November 2013. CO-

DEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Martins:2018:SFH

[MSM18a] Paulo Martins, Leonel Sousa, and Artur Mariano. A survey on fully homomorphic encryption: an engineering perspective. *ACM Computing Surveys*, 50(6):83:1–83:??, January 2018. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Muhammad:2018:ISU

[MSM+18b] Khan Muhammad, Muhammad Sajjad, Irfan Mehmood, Seungmin Rho, and Sung Wook Baik. Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems*, 86(??):951–960, September 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X16306768.

Migliore:2017:HSA

[MSR+17] Vincent Migliore, Cédric Seguin, Maria Méndez Real, Vianney Lapotre, Arnaud Tisserand, Caroline Fontaine, Guy Gogniat, and Russell Tessier. A high-speed accelerator for homomorphic encryption using the Karatsuba algorithm. *ACM Transactions on Embedded Computing Systems*, 16 (5s):138:1–138:??, October 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Maitra:2017:DFA

[MSS17] Subhamoy Maitra, Akhilesh Siddhanti, and Santanu Sarkar. A differential fault attack on Plantlet. *IEEE Transactions on Computers*, 66(10):1804–1808, October 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/document/7917296/.

Maitra:2018:TAA

[MSS+18] Subhamoy Maitra, Nishant Sinha, Akhilesh Siddhanti, Ravi Anand, and Sugata Gangopadhyay. A TMDTO attack against Lizard. *IEEE Transactions on Computers*, 67(5): 733–739, May 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL https://ieeexplore.ieee.org/document/8107499/.

Miret:2018:PBC

[MST18] Josep M. Miret, Daniel Sadornil, and Juan G. Tena. Pairing-based cryptography on elliptic curves.

Mathematics in Computer Science, 12(3):309–318, September 2018. CODEN ???? ISSN 1661-8270 (print), 1661-8289 (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.

Mosca:2013:QKD

[MSU13] Michele Mosca, Douglas Stebila, and Berkant Ustaoğlu. Quantum key distribution in the classical authenticated key exchange framework. *Lecture Notes in Computer Science*, 7932:136–154, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-38616-9_9/.

Morozov:2012:ZKP

[MT12] Kirill Morozov and Tsuyoshi Takagi. Zero-knowledge protocols for the McEliece encryption. *Lecture Notes in Computer Science*, 7372: 180–193, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31448-3_14/.

Mamais:2017:BVP

[MT17] Stylianos S. Mamais and George Theodorakopoulos. Behavioural verification: Preventing report fraud in decentralized advert distribution systems. *Future Internet*, 9(4):88, November 20, 2017. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/9/4/88.

Mouris:2018:TSB

[MTM18] Dimitris Mouris, Nektarios Georgios Tsoutsos, and Michail Maniatakos. Terminator suite: Benchmarking privacy-preserving architectures. *IEEE Computer Architecture Letters*, 17(2):122–125, July/December 2018. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Malkin:2011:ECS

[MTY11] Tal Malkin, Isamu Teranishi, and Moti Yung. Efficient circuit-size independent public key encryption with KDM security. *Lecture Notes in Computer Science*, 6632:

507–526, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_28.

Meerwald:2012:ERW

[MU12] Peter Meerwald and Andreas Uhl. An efficient robust watermarking method integrated in H.264/SVC. *Lecture Notes in Computer Science*, 7110:1–14, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28693-3_1/.

Muftic:2016:BCC

[Muf16] Sead Muftic. BIX certificates: Cryptographic tokens for anonymous transactions based on certificates public ledger. *Ledger*, 1(??):19–37, ???? 2016. ISSN 2379-5980. URL http://www.ledgerjournal.org/ojs/index.php/ledger/article/view/27.

Mundy:2017:CGU

[Mun17] Liza Mundy. *Code girls: the untold story of the American women code breakers of World War II.* Hachette Books, New York, NY, USA, 2017. ISBN 0-316-35253-5 (hardcover), 0-316-43989-4 (large print), 1-4789-2270-2 (audio book), 1-4789-2271-0 (audio download), 0-316-35255-1 (e-book). xiv + 416 pp. LCCN D810.C88 M86 2017.

Murphy:2010:BRB

[Mur10] Cillian Murphy. Book review: *Introduction to Cryptography*, by Hans Delfs and Helmut Knebl, Publisher: Springer, 2007, ISBN 978-3-540-49243-6. *ACM SIGACT News*, 41 (4):42–44, December 2010. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [DK02, DK07].

Murdoch:2016:IDP

[Mur16] Steven J. Murdoch. Insecure by design: Protocols for encrypted phone calls. *Computer*, 49(3):25–33, March 2016. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://www.computer.org/csdl/mags/co/2016/03/mco2016030025-abs.html.

Miri:2012:SAC

[MV12] Ali Miri and Serge Vaudenay, editors. *Selected Areas in Cryptography: 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11–12, Revised Selected Papers*, volume 7118 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. CODEN LNCSD9. ISBN 3-642-28495-7. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/978-3-642-28495-3`.

Min:2016:RSC

[MV16a] Byungho Min and Vijay Varadharajan. Rethinking software component security: Software component level integrity and cross verification. *The Computer Journal*, 59(11):1735–1748, November 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/59/11/1735`.

Mishra:2016:AFP

[MV16b] Abhishek Mishra and Parv Venkitasubramaniam. Anonymity and fairness in packet scheduling: a quantitative tradeoff. *IEEE/ACM Transactions on Networking*, 24(2):688–702, April 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Modersheim:2018:ABP

[MV18] Sebastian Mödersheim and Luca Viganò. Alpha–beta privacy. *ACM Transactions on Privacy and Security (TOPS)*, 22(1):7:1–7:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3289255`.

Mefenza:2019:CSA

[MV19] Thierry Mefenza and Damien Vergnaud. Cryptanalysis of server-aided RSA protocols with private-key splitting. *The Computer Journal*, 62(8):1194–1213, August 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/62/8/1194/5488732`.

Mannan:2011:LPD

[MvO11] Mohammad Mannan and P. C. van Oorschot. Leveraging personal devices for stronger password authentication from untrusted computers. *Journal of Computer Security*, 19(4):703–750, ???? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Maes:2012:PFF

[MVV12] Roel Maes, Anthony Van Herrewege, and Ingrid Verbauwhede. PUFKY: a fully functional PUF-based cryptographic key generator. *Lecture Notes in Computer Science*, 7428:

302–319, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33027-8_18/.

Mathew:2012:EIC

[MVVR12] K. Preetha Mathew, Sachin Vasant, Sridhar Venkatesan, and C. Pandu Rangan. An efficient IND-CCA2 secure variant of the Niederreiter encryption scheme in the standard model. *Lecture Notes in Computer Science*, 7372:166–179, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31448-3_13/.

Moghimi:2019:MFD

[MWES19] Ahmad Moghimi, Jan Wichelmann, Thomas Eisenbarth, and Berk Sunar. MemJam: a false dependency attack against constant-time crypto implementations. *International Journal of Parallel Programming*, 47(4):538–570, August 2019. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic).

Meng:2018:TTB

[MWW+18] Weizhi Meng, Yu Wang, Duncan S. Wong, Sheng Wen, and Yang Xiang. TouchWB: Touch behavioral user authentication based on web browsing on smartphones. *Journal of Network and Computer Applications*, 117(??):1–9, September 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518301723.

Ma:2012:CIS

[MWZ12] Chun-Guang Ma, Ding Wang, and Qi-Ming Zhang. Cryptanalysis and improvement of Sood et al.'s dynamic ID-based authentication scheme. *Lecture Notes in Computer Science*, 7154:141–152, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28073-3_13/.

Mahmoody:2013:LEZ

[MX13] Mohammad Mahmoody and David Xiao. Languages with efficient zero-knowledge PCPs are in SZK. *Lecture Notes in Computer Science*, 7785:297–314, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_17/.

Ma:2013:PVP

[MYYR13] Chris Y. T. Ma, David K. Y. Yau, Nung Kwan Yip, and Nageswara S. V. Rao. Privacy vulnerability of published anonymous mobility traces. *IEEE/ACM Transactions on Networking*, 21(3):720–733, June 2013. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Meng:2015:CRS

[MZ15] Xianmeng Meng and Xuexin Zheng. Cryptanalysis of RSA with a small parameter revisited. *Information Processing Letters*, 115(11):858–862, November 2015. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S002001901500109X.

Marko:2017:MDI

[MZ17a] Frantisek Marko and Alexandr N. Zubkov. Minimal degrees of invariants of (super)groups — a connection to cryptology. *Linear Multilinear Algebra*, 65(11): 2340–2355, 2017. CODEN LNMLAZ. ISSN 0308-1087 (print), 1563-5139 (electronic).

Mastroeni:2017:APS

[MZ17b] Isabella Mastroeni and Damiano Zanardini. Abstract program slicing: an abstract interpretation-based approach to program slicing. *ACM Transactions on Computational Logic*, 18(1):7:1–7:??, April 2017. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic).

Manshaei:2013:GTM

[MZA+13] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Bacsar, and Jean-Pierre Hubaux. Game theory meets network security and privacy. *ACM Computing Surveys*, 45(3): 25:1–25:??, June 2013. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Ma:2015:PKE

[MZHY15] Sha Ma, Mingwu Zhang, Qiong Huang, and Bo Yang. Public key encryption with delegated equality test in a multi-user setting. *The Computer Journal*, 58(4):986–1002, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/986.

Meng:2019:ESF

[MZL+19] Weizhi Meng, Liqiu Zhu, Wenjuan Li, Jinguang Han, and Yan Li. Enhancing the security of FinTech applications with map-based graphical password authentication. *Future Generation Computer Systems*, 101(??):1018–1027, December 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X19302882`.

Mofrad:2018:CSI

[MZLS18] Saeid Mofrad, Fengwei Zhang, Shiyong Lu, and Weidong (Larry) Shi. A comparison study of Intel SGX and AMD memory encryption technology. Web lecture slides., May 30, 2018. URL `https://caslab.csl.yale.edu/workshops/hasp2018/HASP18_a9-mofrad_slides.pdf`.

Nagy:2010:OTP

[NA10a] Naya Nagy and Selim G. Akl. One-time pads without prior encounter. *Parallel Processing Letters*, 20(3):263–273, September 2010. CODEN PPLTEE. ISSN 0129-6264.

Nagy:2010:QCS

[NA10b] Naya Nagy and Selim G. Akl. A quantum cryptographic solution to the problem of access control in a hierarchy. *Parallel Processing Letters*, 20(3):251–261, September 2010. CODEN PPLTEE. ISSN 0129-6264.

Nikiforakis:2014:BYO

[NA14] N. Nikiforakis and G. Acar. Browse at your own risk. *IEEE Spectrum*, 51(8):30–35, August 2014. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Naccache:2012:CST

[Nac12] David Naccache, editor. *Cryptography and Security: From Theory to Applications: Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday*, volume 6805 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. CODEN LNCSD9. ISBN 3-642-28367-5. ISSN 0302-9743 (print), 1611-3349 (electronic). ???? pp. URL `http://www.springerlink.com/content/978-3-642-28367-3`.

Naccache:2016:FHE

[Nac16] David Naccache. Fully homomorphic encryption: Computations with a blindfold. *IEEE Security & Privacy*, 14(1):63–67, January/February 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Naranjo:2012:SAK

[NACLR12] J. A. M. Naranjo, N. Antequera, L. G. Casado, and J. A. López-Ramos. A suite of algorithms for key distribution and authentication in centralized secure multicast environments. *Journal of Computational and Applied Mathematics*, 236(12):3042–3051, June 2012. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042711000914.

Nagaraj:2019:RCC

[Nag19] S. V. Nagaraj. Review of *Codes, Cryptology and Curves with Computer Algebra*. *ACM SIGACT News*, 50(1):14–16, March 2019. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Nunez:2017:PRE

[NAL17] David Nuñez, Isaac Agudo, and Javier Lopez. Proxy re-encryption: Analysis of constructions and its application to secure access delegation. *Journal of Network and Computer Applications*, 87(??):193–209, June 1, 2017. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804517301078.

Namasudra:2019:IAB

[Nam19] Suyel Namasudra. An improved attribute-based encryption technique towards the data security in cloud computing. *Concurrency and Computation: Practice and Experience*, 31(3):e4364:1–e4364:??, February 10, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Noureddine:2013:AMT

[NB13] M. Noureddine and R. Bashroush. An authentication model towards cloud federation in the enterprise. *The Journal of Systems and Software*, 86(9):2269–2275, September 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212003408.

Nain:2017:SPE

[NBZP17] Ajay Kumar Nain, Jagadish Bandaru, Mohammed Abdullah Zubair, and Rajalakshmi Pachamuthu. A secure phase-encrypted IEEE 802.15.4 transceiver design. *IEEE Transactions on Computers*, 66(8):1421–1427, ???? 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/document/7862216/.

Naskar:2012:FIR

[NC12] Ruchira Naskar and Rajat Subhra Chakraborty. Fuzzy inference rule based reversible watermarking for digital images. *Lecture Notes in Computer Science*, 7671:149–163, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35130-3_11/.

Naskar:2013:GTL

[NC13] Ruchira Naskar and Rajat Subhra Chakraborty. A generalized tamper localization approach for reversible watermarking algorithms. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 9(3):19:1–19:??, June 2013. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Naranjo:2013:FDA

[NCCG13] J. A. M. Naranjo, F. Cores, L. G. Casado, and F. Guirado. Fully distributed authentication with locality exploitation for the CoDiP2P peer-to-peer computing platform. *The Journal of Supercomputing*, 65(3):1037–1049, September 2013. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-012-0842-2.

Ni:2013:EIB

[NCL13] Liang Ni, Gongliang Chen, and Jianhua Li. Escrowable identity-based authenticated key agreement protocol with strong security. *Computers and Mathematics with Applications*, 65(9):1339–1349, May 2013. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S089812211200051X.

Narasimhan:2013:HTD

[NDC+13] Seetharam Narasimhan, Dongdong Du, Rajat Subhra Chakraborty, Somnath Paul, Francis G. Wolff, Christos A. Papachristou, Kaushik Roy, and Swarup Bhunia. Hardware Trojan detection by multiple-parameter side-channel analysis. *IEEE Transactions on Computers*, 62(11):2183–2195, November 2013. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Ngo:2017:CSS

[NDG+17] Xuan Thuy Ngo, Jean-Luc Danger, Sylvain Guilley, Tarik Graba, Yves Mathieu, Zakaria Najm, and

Shivam Bhasin. Cryptographically secure shield for security IPs protection. *IEEE Transactions on Computers*, 66(2):354–360, ???? 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Nedjah:2016:PYP

[NdMMW16] Nadia Nedjah, Luiza de Macedo Mourelle, and Chao Wang. A parallel yet pipelined architecture for efficient implementation of the Advanced Encryption Standard algorithm on reconfigurable hardware. *International Journal of Parallel Programming*, 44(6):1102–1117, December 2016. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic). URL http://link.springer.com/article/10.1007/s10766-016-0408-7.

Newell:2013:PCD

[NDNR13] Andrew Newell, Jing Dong, and Cristina Nita-Rotaru. On the practicality of cryptographic defences against pollution attacks in wireless network coding. *ACM Computing Surveys*, 45(3):39:1–39:??, June 2013. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Nejatollahi:2019:PQL

[NDR+19] Hamid Nejatollahi, Nikil Dutt, Sandip Ray, Francesco Regazzoni, Indranil Banerjee, and Rosario Cammarota. Post-quantum lattice-based cryptography implementations: a survey. *ACM Computing Surveys*, 51(6):129:1–129:??, February 2019. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3292548.

Nacer:2017:DAM

[NDSA17] Hassina Nacer, Nabil Djebari, Hachem Slimani, and Djamil Aissani. A distributed authentication model for composite Web services. *Computers & Security*, 70(??):144–178, September 2017. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404817301153.

Naeem:2014:EIC

[NES+14] Ensherah A. Naeem, Mustafa M. Abd Elnaby, Naglaa F. Soliman, Alaa M. Abbas, Osama S. Faragallah, Noura Semary, Mohiy M. Hadhoud, Saleh A. Alshebeili, and Fathi E. Abd El-Samie. Efficient implementation of chaotic image encryption in transform domains. *The Journal of Systems and Software*, 97(??):118–127, November 2014. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121214001575.

Nafea:2016:HMB

[NGAuHQ16] Ohoud Nafea, Sanaa Ghouzali, Wadood Abdul, and Emad ul Haq Qazi. Hybrid multi-biometric template protection using watermarking. *The Computer Journal*, 59(9):1392–1407, September 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/9/1392.

Nievergelt:2002:FLM

[Nie02] Yves Nievergelt. *Foundations of Logic and Mathematics: Applications to Computer Science and Cryptography*. Birkhäuser Verlag, Basel, Switzerland, 2002. ISBN 0-8176-4249-8 , 3-7643-4249-8. xvi + 415 pp. LCCN QA9 .N53 2002. URL http://www.loc.gov/catdir/enhancements/fy0812/2001052551-d.html; http://www.loc.gov/catdir/enhancements/fy0812/2001052551-t.html.

NIST:2012:RRN

[NIS12] NIST. Recommendation for random number generation using deterministic random bit generators. Special Publication 800-90, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 2012. URL http://csrc.nist.gov/publications/PubsSPs.html#800-90A.

NIST:2013:CSS

[NIS13] NIST. Cryptographic standards statement. National Institute of Standards and Technology, September 2013.

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.

Najafi:2019:VRS

[NJB19] Aniseh Najafi, Hamid Haj Seyyed Javadi, and Majid Bayat. Verifiable ranked search over encrypted data with forward and backward privacy. *Future Generation Computer Systems*, 101(??):410–419, December 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18323318.

Nguyen:2014:DDI

[NKWF14] Thanhvu Nguyen, Deepak Kapur, Westley Weimer, and Stephanie Forrest. DIG: a dynamic invariant generator for polynomial and array invariants. *ACM Transactions on Software Engineering and Methodology*, 23(4): 30:1–30:??, August 2014. CODEN ATSMER. ISSN 1049-331X (print), 1557-7392 (electronic).

Ning:2012:DPB

[NLLJ12] H. Ning, H. Liu, Q. Liu, and G. Ji. Directed path based authentication scheme for the Internet of Things. *J.UCS: Journal of Universal Computer Science*, 18(9):1112–??, ???? 2012. CODEN ???? ISSN 0948-6968. URL `http://www.jucs.org/jucs_18_9/directed_path_based_authentication`.

Ning:2015:APB

[NLY15] Huansheng Ning, Hong Liu, and Laurence T. Yang. Aggregated-proof based hierarchical authentication scheme for the Internet of Things. *IEEE Transactions on Parallel and Distributed Systems*, 26(3): 657–667, March 2015. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL `http://www.computer.org/csdl/trans/td/2015/03/06767153-abs.html`.

Ning:2012:DCA

[NLYZ12] Huansheng Ning, Hong Liu, Laurence T. Yang, and Yan Zhang. Dual cryptography authentication protocol and its security analysis for radio frequency identification systems. *Concurrency and Computation: Practice and Experience*, 24(17):2040–2054, December 10, 2012. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Nguyen:2018:TBU

[NM18] Toan Nguyen and Nasir Memon. Tap-based user authentication for smartwatches. *Computers & Security*, 78(??):174–186, September 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404818303778`.

Norta:2019:SFB

[NML19] Alex Norta, Raimundas Matulevicius, and Benjamin Leiding. Safeguarding a formalized blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns. *Computers & Security*, 86(??): 253–269, September 2019.

CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818302670.

Nieto:2013:PVC

[NMP+13] Juan González Nieto, Mark Manulis, Bertram Poettering, Jothi Rangasamy, and Douglas Stebila. Publicly verifiable ciphertexts. *Journal of Computer Security*, 21(5):749–778, ???? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Nieto:2014:FSH

[NMS14] Juan Manuel González Nieto, Mark Manulis, and Dongdong Sun. Forward-secure hierarchical predicate encryption. *The Computer Journal*, 57(4):510–536, April 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/57/4/510.full.pdf+html.

Ntantogian:2015:GTF

[NMX15] Christoforos Ntantogian, Stefanos Malliaros, and Christos Xenakis. Gaithashing: a two-factor authentication scheme based on gait features. *Computers & Security*, 52(??):17–32, July 2015. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404815000413.

Nguyen:2012:DQB

[NN12] Anh P. Nguyen and Thuc D. Nguyen. Determining quality of S-boxes using pseudo random sequences generated from stream ciphers. *Lecture Notes in Computer Science*, 7440:72–79, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33065-0_8/.

Neville-Neil:2015:KVH

[NN15] George V. Neville-Neil. Kode vicious: Hickory dickory doc. *Communications of the Association for Computing Machinery*, 58(8):27–28, August 2015. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2015/8/189849/fulltext.

Nagy:2010:KDV

[NNA10] Naya Nagy, Marius Nagy, and Selim G. Akl. Key distribution versus key enhancement in quantum cryptography. *Parallel Processing Letters*, 20(3):

239–250, September 2010. CODEN PPLTEE. ISSN 0129-6264.

Navin:2010:ETU

[NNAM10] A. H. Navin, Z. Navadad, B. Aasadi, and M. Mirnia. Encrypted tag by using data-oriented random number generator to increase security in wireless sensor network. In *2010 International Conference on Computational Intelligence and Communication Networks (CICN)*, pages 335–338. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5701989.

Nordrum:2017:GBD

[Nor17] A. Nordrum. Govern by blockchain: Dubai wants one platform to rule them all, while Illinois will try anything. *IEEE Spectrum*, 54(10):54–55, October 2017. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Nose:2011:SWA

[Nos11] Peter Nose. Security weaknesses of authenticated key agreement protocols. *Information Processing Letters*, 111(14):687–696, July 31, 2011. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019011001074.

Nose:2014:SWS

[Nos14] Peter Nose. Security weaknesses of a signature scheme and authenticated key agreement protocols. *Information Processing Letters*, 114(3):107–115, March 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013002731.

Novotny:2010:TAE

[Nov10] Martin Novotny. *Time-area efficient hardware architectures for cryptography and cryptanalysis*, volume 12 of *IT-Security*. Europäischer Universitätsverlag, Bochum, Germany, 2010. ISBN 3-89966-351-9. xxvi + 194 pp. LCCN ????

Nichols:2014:CSS

[NPH+14] Tyler Nichols, Joe Pletcher, Braden Hollembaek, Adam Bates, Dave Tian, Abdulrahman Alkhelaifi, and Kevin Butler. CertShim: Securing SSL certificate verification through dynamic linking. In ????, editor, *ACM Conference on*

Computer and Communications Security, page ?? ACM Press, New York, NY 10036, USA, 2014. ISBN ???? LCCN ???? URL ????.

Nguyen:2011:APB

[NR11] L. H. Nguyen and A. W. Roscoe. Authentication protocols based on low-bandwidth unspoofable channels: A comparative survey. *Journal of Computer Security*, 19(1):139–201, ???? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (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 Computer Science*, 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/.

Negre:2015:NPA

[NR15] C. Negre and J.-M. Robert. New parallel approaches for scalar multiplication in elliptic curve over fields of small characteristic. *IEEE Transactions on Computers*, 64(10):2875–2890, October 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Namasudra:2017:NSA

[NR17] Suyel Namasudra and Pinki Roy. A new secure authentication scheme for cloud computing environment. *Concurrency and Computation: Practice and Experience*, 29(20):??, October 25, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Niu:2015:CRS

[NRZQ15] Danmei Niu, Lanlan Rui, Cheng Zhong, and Xuesong Qiu. A composition and recovery strategy for mobile social network service in disaster. *The Computer Journal*, 58(4):700–708, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/700.

Naccache:2010:THI

[NS10] David Naccache and Ahmad-Reza Sadeghi. *Towards hardware-intrinsic security: foundations and practice*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc.,

2010. ISBN 3-642-14451-9, 3-642-14452-7. xvi + 407 pp. LCCN ????

Nojoumian:2012:SRS

[NS12] Mehrdad Nojoumian and Douglas R. Stinson. Socio-rational secret sharing as a new direction in rational cryptography. *Lecture Notes in Computer Science*, 7638:18–37, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34266-0_2/.

Natarajan:2015:MAD

[NSA15] V. Natarajan, Shina Sheen, and R. Anitha. Multilevel analysis to detect covert social botnet in multimedia social networks. *The Computer Journal*, 58(4):679–687, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/679.

Nguyen:2017:DPA

[NSBM17] Toan Van Nguyen, Napa Sae-Bae, and Nasir Memon. DRAW-a-PIN: Authentication using finger-drawn PIN on touch devices. *Computers & Security*, 66 (??):115–128, May 2017. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404817300123.

Niksefat:2014:ZPP

[NSMS14] Salman Niksefat, Babak Sadeghiyan, Payman Mohassel, and Saeed Sadeghian. ZIDS: a privacy-preserving intrusion detection system using secure two-party computation protocols. *The Computer Journal*, 57(4):494–509, April 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/57/4/494.full.pdf+html.

Neustaedter:2018:BTW

[NSP+18] Carman Neustaedter, Samarth Singhal, Rui Pan, Yasamin Heshmat, Azadeh Forghani, and John Tang. From being there to watching: Shared and dedicated telepresence robot usage at academic conferences. *ACM Transactions on Computer-Human Interaction*, 25(6):33:1–33:??, December 2018. CODEN ATCIF4. ISSN 1073-0516 (print), 1557-7325 (electronic).

Nagano:2018:PRT

[NSX+18] Koki Nagano, Jaewoo Seo, Jun Xing, Lingyu Wei, Zimo Li, Shunsuke Saito, Aviral Agarwal, Jens Fursund, and Hao Li. paGAN: real-time avatars using dynamic textures. *ACM Transactions on Graphics*, 37(6):258:1–258:??, November 2018. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Nandakumar:2017:CAI

[NTKG17] Rajalakshmi Nandakumar, Alex Takakuwa, Tadayoshi Kohno, and Shyamnath Gollakota. CovertBand: Activity information leakage using music. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 1(3): 87:1–87:24, ???? 2017. CODEN ???? ISSN ???? URL `http://musicattacks.cs.washington.edu/activity-information-leakage.pdf`.

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 Computer Science*, 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/`.

Nguyen:2010:LAS

[NV10] Phong Quang Nguyen and Brigitte Vallée, editors. *The LLL Algorithm: Survey and Applications*, Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-02294-4 (hardcover), 3-642-02295-2 (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). LCCN QA9.58 .L55 2010; QA76. Conference in honour of the 25th birthday of the Lenstra–Lenstra–Lovasz Lattice Reduction Algorithm, LLL, Caen, France.

Noorman:2017:SLC

[NVM+17] Job Noorman, Jo Van Bulck, Jan Tobias Mühlberg, Frank Piessens, Pieter Maene, Bart Preneel, Ingrid Verbauwhede, Johannes Götzfried, Tilo Müller, and Felix Freiling. Sancus 2.0: a low-cost security architecture for IoT devices. *ACM Transactions on Privacy and Security (TOPS)*, 20(3):7:1–7:??, August 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (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 Computer Science*, 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/.

Natgunanathan:2017:PBM

[NXH+17] Iynkaran Natgunanathan, Yong Xiang, Guang Hua, Gleb Beliakov, and John Yearwood. Patchwork-based multilayer audio watermarking. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 25(11): 2176–2187, ???? 2017. CODEN ???? ISSN 2329-9290. URL http://ieeexplore.ieee.org/document/8025572/.

Ntantogian:2010:GME

[NXS10] Christoforos Ntantogian, Christos Xenakis, and Ioannis Stavrakakis. A generic mechanism for efficient authentication in b3g networks. *Computers & Security*, 29(4):460–475, June 2010. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404809001242.

Newell:2014:NCR

[NYR+14] Andrew Newell, Hongyi Yao, Alex Ryker, Tracey Ho, and Cristina Nita-Rotaru. Node-capture resilient key establishment in sensor networks: Design space and new protocols. *ACM Computing Surveys*, 47(2):24:1–24:??, November 2014. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Niu:2015:NAS

[NZL+15] Ben Niu, Xiaoyan Zhu, Qinghua Li, Jie Chen, and Hui Li. A novel attack to spatial cloaking schemes in location-based services. *Future Generation Computer Systems*, 49(??):125–132, August 2015. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X14002209.

Nikooghadam:2010:EUE

[NZM10] Morteza Nikooghadam, Ali Zakerolhosseini, and Mohsen Ebrahimi Moghaddam. Efficient utilization of elliptic curve cryptosystem for hierarchical access control. *The Journal of Systems and Software*, 83(10):

1917–1929, October 2010. CODEN JSSODM. ISSN 0164-1212.

Obana:2011:AOC

[Oba11] Satoshi Obana. Almost optimum t-cheater identifiable secret sharing schemes. *Lecture Notes in Computer Science*, 6632:284–302, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_17.

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).

Obrenovic:2012:IUC

[OdH12] Željko Obrenovic and Bart den Haak. Integrating user customization and authentication: The identity crisis. *IEEE Security & Privacy*, 10(5):82–85, September/October 2012. ISSN 1540-7993 (print), 1558-4046 (electronic).

Odelu:2017:PSA

[ODK+17] Vanga Odelu, Ashok Kumar Das, Saru Kumari, Xinyi Huang, and Mohammad Wazid. Provably secure authenticated key agreement scheme for distributed mobile cloud computing services. *Future Generation Computer Systems*, 68(??):74–88, March 2017. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16303065.

Ozturk:2017:CAH

[ÖDSS17] Erdinç Öztürk, Yarkın Doröz, Erkay Savaş, and Berk Sunar. A custom accelerator for homomorphic encryption applications. *IEEE Transactions on Computers*, 66(1):3–16, January 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Oggier:2011:ACA

[OF11] Frédérique Oggier and Hanane Fathi. An authentication code against pollution attacks in network coding. *IEEE/ACM Transactions on Networking*, 19(6):1587–1596, December 2011. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Obrien:2012:EPM

[OF12] James F. O'brien and Hany Farid. Exposing photo manipulation with inconsistent reflections. *ACM Transactions on Graphics*, 31(1):4:1–4:??, January 2012. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Onica:2016:CPP

[OFMR16] Emanuel Onica, Pascal Felber, Hugues Mercier, and Etienne Rivière. Confidentiality-preserving publish/subscribe: a survey. *ACM Computing Surveys*, 49(2):27:1–27:??, September 2016. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Oliynykov:2015:NES

[OGK+15] Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev, Oleksandr Kuznetsov, Yurii Gorbenko, Oleksandr Dyrda, Viktor Dolgov, Andrii Pushkaryov, Ruslan Mordvinov, and Dmytro Kaidalov. A new encryption standard of Ukraine: The Kalyna block cipher. Cryptology ePrint Archive, Report 2015/650, 2015. URL `http://eprint.iacr.org/2015/650`.

Ou:2010:CPA

[OHJ10] Hsia-Hung Ou, Min-Shiang Hwang, and Jinn-Ke Jan. A cocktail protocol with the Authentication and Key Agreement on the UMTS. *The Journal of Systems and Software*, 83(2):316–325, February 2010. CODEN JSSODM. ISSN 0164-1212.

Ogiela:2018:EBI

[OK18] Marek R. Ogiela and Hoon Ko. Editorial: Bio-inspired and cognitive approaches in cryptography and security applications. *Concurrency and Computation: Practice and Experience*, 30(2):??, January 25, 2018. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Oliveira:2012:STA

[OKG+12] Leonardo B. Oliveira, Aman Kansal, Conrado P. L. Gouvêa, Diego F. Aranha, Julio López, Bodhi Priyantha, Michel Goraczko, and Feng Zhao. Secure-TWS: Authenticating node to multi-user communication in shared sensor networks. *The Computer Journal*, 55(4):384–396, April 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.`

org/content/55/4/384.full.pdf+html.

Or-Meir:2019:DMA

[OMNER19] Ori Or-Meir, Nir Nissim, Yuval Elovici, and Lior Rokach. Dynamic malware analysis in the modern era — a state of the art survey. *ACM Computing Surveys*, 52(5):88:1–88:??, October 2019. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3329786.

Ortiz-Martin:2019:FAI

[OMPSPL+19] Lara Ortiz-Martin, Pablo Picazo-Sanchez, Pedro Peris-Lopez, Juan Tapiador, and Gerardo Schneider. Feasibility analysis of inter-pulse intervals based solutions for cryptographic token generation by two electrocardiogram sensors. *Future Generation Computer Systems*, 96(??):283–296, July 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18330784.

Ogiela:2010:UML

[OO10] Marek R. Ogiela and Urszula Ogiela. The use of mathematical linguistic methods in creating secret sharing threshold algorithms. *Computers and Mathematics with Applications*, 60(2):267–271, July 2010. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122110001379.

Ohtake:2012:AAH

[OO12] Go Ohtake and Kazuto Ogawa. Application authentication for hybrid services of broadcasting and communications networks. *Lecture Notes in Computer Science*, 7115: 171–186, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27890-7_15/.

Ogiela:2018:LTC

[OO18] Urszula Ogiela and Lidia Ogiela. Linguistic techniques for cryptographic data sharing algorithms. *Concurrency and Computation: Practice and Experience*, 30(3), February 10, 2018. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic). URL https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.4275.

Orlandi:2014:SCN

[OOR+14] Claudio Orlandi, Rafail Ostrovsky, Vanishree Rao, Amit Sahai, and Ivan Visconti. Statistical concurrent non-malleable zero knowledge. *Lecture Notes in Computer Science*, 8349: 167–191, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-54242-8_8/`.

Obert:2016:PAE

[OPHC16] James Obert, Inna Pivkina, Hong Huang, and Huiping Cao. Proactively applied encryption in multipath networks. *Computers & Security*, 58(??):106–124, May 2016. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404815001960`.

Oppliger:2011:CC

[Opp11] Rolf Oppliger. *Contemporary cryptography*. Artech House Inc., Norwood, MA, USA, second edition, 2011. ISBN 1-60807-145-6. 612 (est.) pp. LCCN ???? URL `http://www.artechhouse.com/Detail.aspx?strIsbn=978-1-60807-145-6`.

Orumiehchiha:2014:PAN

[OPS14] Mohammad Ali Orumiehchiha, Josef Pieprzyk, and Ron Steinfeld. Practical attack on NLM–MAC scheme. *Information Processing Letters*, 114(10):547–550, October 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019014000696`.

Orejel:2014:E

[Ore14] Jorge Luis Orejel. ENIGMA. Web posting adapted from chapter of unpublished textbook, *Applied Algorithms and Data Structures.*, October 20, 2014. URL `http://www.codeproject.com/Articles/831015/ENIGMA`.

Ormond:2016:CPR

[Orm16] Jim Ormond. Cryptography pioneers receive ACM A. M. Turing Award: Diffie and Hellman's invention of public-key cryptography and digital signatures revolutionized computer security and made Internet commerce possible. Web document, March 1, 2016. URL `http://www.acm.org/media-center/2016/march/turing-award-2015`.

Ozen:2011:MIS

[ÖŞ11] Mehmet Özen and Vedat Şiap. The MacWilliams identity for m-spotty weight enumerators of linear codes over finite fields. *Computers and Mathematics with Applications*, 61(4):1000–1004, February 2011. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122110009533.

Owczarek:2012:LPL

[OŚ12] Agnieszka Owczarek and Krzysztof Ślot. Lipreading procedure for liveness verification in video authentication systems. *Lecture Notes in Computer Science*, 7208:115–124, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28942-2_11/.

Osborn:2016:SSR

[OS16] Emma Osborn and Andrew Simpson. On safety and security requirements in emerging ubiquitous computing models. *The Computer Journal*, 59(4):570–591, April 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/4/570.

Ostad-Sharif:2019:TPS

[OSANAM19] Arezou Ostad-Sharif, Hamed Arshad, Morteza Nikooghadam, and Dariush Abbasinezhad-Mood. Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme. *Future Generation Computer Systems*, 100(??):882–892, November 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18309452.

Olson:2016:SIT

[OSH16] Lena E. Olson, Simha Sethumadhavan, and Mark D. Hill. Security implications of third-party accelerators. *IEEE Computer Architecture Letters*, 15(1):50–53, January/June 2016. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Ohtake:2019:OSA

[OSNZ19] Go Ohtake, Reihaneh Safavi-Naini, and Liang Feng Zhang. Outsourcing scheme of ABE encryption secure against malicious adversary. *Computers & Security*, 86(??):437–452, September 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404819300525.

Odelu:2019:EPP

[OSP+19] Vanga Odelu, Sourav Saha, Rajendra Prasath, Lakshminarayana Sadineni, Mauro Conti, and Minho Jo. Efficient privacy preserving device authentication in WBANs for industrial e-health applications. *Computers & Security*, 83(??):300–312, June 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818308204.

Orencik:2016:MKS

[OSSK16] Cengiz Orencik, Ayse Selcuk, Erkay Savas, and Murat Kantarcioğlu. Multi-keyword search over encrypted data with scoring and search pattern obfuscation. *International Journal of Information Security*, 15(3):251–269, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-015-0294-9.

Okamoto:2012:AAH

[OT12] Tatsuaki Okamoto and Katsuyuki Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. *Lecture Notes in Computer Science*, 7237:591–608, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_34; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_35/.

Otmani:2010:CTM

[OTD10] Ayoub Otmani, Jean-Pierre Tillich, and Léonard Dallot. Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes. *Mathematics in Computer Science*, 3(2): 129–140, April 2010. CODEN ???? ISSN 1661-8270 (print), 1661-8289 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=1661-8270&volume=3&issue=2&spage=129.

Ogiela:2018:VCA

[OTO18] Urszula Ogiela, Makoto Takizawa, and Lidia Ogiela. Visual CAPTCHA application in linguistic cryptography. *Concurrency and Computation: Practice and Experience*, 30(2):??, January 25, 2018. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Ohzeki:2012:NWM

[OWHS12] Kazuo Ohzeki, YuanYu Wei, Yutaka Hirakawa, and Kiyotsugu Sato. A new watermarking method with obfuscated quasi-chirp transform. *Lecture Notes in Computer Science*, 7128:57–71, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32205-1_7/.

Ortiz-Yepes:2014:BSA

[OYHSB14] D. A. Ortiz-Yepes, R. J. Hermann, H. Steinauer, and P. Buhler. Bringing strong authentication and transaction security to the realm of mobile devices. *IBM Journal of Research and Development*, 58(1):4:1–4:11, January–February 2014. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Praba:2010:MAC

[PA10] V. Lakshmi Praba and G. Arumugam. Message authentication code algorithm for IP-SEC. *International Journal of Computer Systems Science and Engineering*, 25(5):??, September 2010. CODEN CSSEEI. ISSN 0267-6192.

Parrilla:2019:ECC

[PÁBC+19] Luis Parrilla, José A. Álvarez-Bermejo, Encarnación Castillo, Juan A. López-Ramos, Diego P. Morales-Santos, and Antonio García. Elliptic curve cryptography hardware accelerator for high-performance secure servers. *The Journal of Supercomputing*, 75(3):1107–1122, March 2019. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Parveen:2018:IEE

[PAF18] Farhana Parveen, Shaahin Angizi, and Deliang Fan. IMFlexCom: Energy efficient in-memory flexible computing using dual-mode SOT-MRAM. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 14(3):35:1–35:??, October 2018. CODEN ???? ISSN 1550-4832.

Pal:2015:SDC

[Pal15] Jiban K. Pal. Scientometric dimensions of cryptographic research. *Scientometrics*, 105(1):179–202, October 2015. CODEN SCNTDX. ISSN 0138-9130 (print), 1588-2861 (electronic). URL http://link.springer.com/article/10.1007/s11192-015-1661-z.

Pal:2016:ACC

[Pal16] Jiban K. Pal. Administering a cryptology centre by means of scientometric indicators. *Collnet Journal of Scientometrics and Information Management*, 10(1):97–123, 2016. CODEN ???? ISSN 0973-7766 (print), 2168-930X (electronic).

Pandey:2014:ACR

[Pan14] Omkant Pandey. Achieving constant round leakage-resilient zero-knowledge. *Lecture Notes in Computer Science*, 8349:146–166, 2014. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-54242-8_7/.

Parent:2012:WAI

[Par12a] Xavier Parent. Why be afraid of identity? *Lecture Notes in Computer Science*, 7360:295–307, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29414-3_16/.

Park:2012:APO

[Par12b] Jong Hyuk Park. An authentication protocol offering service anonymity of mobile device in ubiquitous environment. *The Journal of Supercomputing*, 62(1):105–117, October 2012. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=62&issue=1&spage=105.

Park:2018:OTP

[Par18] Chang-Seop Park. One-time password based on hash chain without shared secret and re-registration. *Computers & Security*, 75 (??):138–146, June 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818301391.

Pass:2013:USP

[Pas13a] Rafael Pass. Unprovable security of perfect NIZK and non-interactive non-malleable commitments. *Lecture Notes in Computer Science*, 7785:334–354, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_19/.

Pranata:2013:MDR

[PAS13b] Ilung Pranata, Rukshan Athauda, and Geoff Skinner. Modeling decentralized reputation-based trust for initial transactions in digital environments. *ACM Transactions on Internet*

Technology (TOIT), 12(3): 8:1–8:??, May 2013. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Paulson:2010:SDO

[Pau10] Linda Dailey Paulson. Steganography development offers promise. *Computer*, 43(6):18–21, June 2010. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Paul:2019:RCS

[Pau19] J. D. Paul. Re-creating the Sigsaly quantizer: This 1943 analog-to-digital converter gave the Allies an unbreakable scrambler — [resources]. *IEEE Spectrum*, 56(2):16–17, February 2019. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Pandit:2012:EFS

[PB12] Tapas Pandit and Rana Barua. Efficient fully secure attribute-based encryption schemes for general access structures. *Lecture Notes in Computer Science*, 7496:193–214, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33272-2_13/.

Poh:2017:SDV

[PBC+17] Geong Sen Poh, Vishnu Monn Baskaran, Ji-Jian Chin, Moesfa Soeheila Mohamad, Kay Win Lee, Dharmadharshni Maniam, and Muhammad Reza Z'aba. Searchable data vault: Encrypted queries in secure distributed cloud storage. *Algorithms (Basel)*, 10 (2), June 2017. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL https://www.mdpi.com/1999-4893/10/2/52.

Park:2014:FRI

[PBCC14] Jeong Soo Park, Ki Seok Bae, Yong Je Choi, and Doo Ho Choi. A fault-resistant implementation of AES using differential bytes between input and output. *The Journal of Supercomputing*, 67(3):615–634, March 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-013-0950-7.

Poddar:2019:AED

[PBP19] Rishabh Poddar, Tobias Boelter, and Raluca Ada Popa. Arx: an encrypted database using semantically secure encryption. *Proceedings of the VLDB Endowment*, 12(11): 1664–1678, July 2019. CO-

DEN ???? ISSN 2150-8097.

Pun:2014:GIT

[PC14] Chi-Man Pun and Ka-Cheng Choi. Generalized integer transform based reversible watermarking algorithm using efficient location map encoding and adaptive thresholding. *Computing*, 96(10): 951–973, October 2014. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL http://link.springer.com/article/10.1007/s00607-013-0357-6.

Paul:2016:TSO

[PC16] G. Paul and A. Chattopadhyay. Three snakes in one hole: The first systematic hardware accelerator design for SOSEMANUK with optional serpent and SNOW 2.0 modes. *IEEE Transactions on Computers*, 65(2):640–653, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Papadopoulos:2014:LQA

[PCDG14] Stavros Papadopoulos, Graham Cormode, Antonios Deligiannakis, and Minos Garofalakis. Lightweight query authentication on streams. *ACM Transactions on Database Systems*, 39(4):30:1–30:??, December 2014. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Perkovic:2019:LVL

[PCK19] Toni Perković, Mario Cagalj, and Tonko Kovacević. LISA: Visible light based initialization and SMS based authentication of constrained IoT devices. *Future Generation Computer Systems*, 97(??):105–118, August 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18321083.

Premnath:2014:EHR

[PCPK14] Sriram Nandha Premnath, Jessica Croft, Neal Patwari, and Sneha Kumar Kasera. Efficient high-rate secret key extraction in wireless sensor networks using collaboration. *ACM Transactions on Sensor Networks*, 11(1):2:1–2:??, August 2014. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Poh:2017:SSE

[PCY+17] Geong Sen Poh, Ji-Jian Chin, Wei-Chuen Yau, Kim-Kwang Raymond Choo, and Moesfa Soeheila Mohamad. Searchable symmetric encryption: Designs and challenges. *ACM Computing Surveys*, 50(3):40:1–

40:??, October 2017. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Pang:2014:PPA

[PD14] Hweehwa Pang and Xuhua Ding. Privacy-preserving ad-hoc equi-join on outsourced data. *ACM Transactions on Database Systems*, 39(3):23:1–23:??, September 2014. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Patranabis:2019:SCS

[PDJ+19] S. Patranabis, N. Datta, D. Jap, J. Breier, S. Bhasin, and D. Mukhopadhyay. SCADFA: Combined SCA + DFA attacks on block ciphers with practical validations. *IEEE Transactions on Computers*, 68 (10):1498–1510, October 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Paul:2012:KSS

[PDMR12] Goutam Paul, Ian Davidson, Imon Mukherjee, and S. S. Ravi. Keyless steganography in spatial domain using energetic pixels. *Lecture Notes in Computer Science*, 7671: 134–148, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35130-3_10/.

Pereira:2015:PKE

[PDNH15] Mayana Pereira, Rafael Dowsley, Anderson C. A. Nascimento, and Goichiro Hanaoka. Public-key encryption schemes with bounded CCA security and optimal ciphertext length based on the CDH and HDH assumptions. *The Computer Journal*, 58(10):2738–2746, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2738.

Pippal:2012:SVU

[PDT12] Ravi Singh Pippal, Jaidhar C. D., and Shashikala Tapaswi. Security vulnerabilities of user authentication scheme using smart card. *Lecture Notes in Computer Science*, 7371:106–113, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31540-4_8/.

Pearson:2011:NWC

[Pea11] Joss Pearson, editor. *Neil Webster's cribs for victory: the untold story* *of Bletchley Park's secret room*. Polperro Heritage, Clifton-upon-Teme, UK, 2011. ISBN 0-9559541-8-5 (paperback). ???? pp. LCCN ????

Peck:2012:CAC

[Pec12] Morgan E. Peck. The cryptoanarchists' answer to cash. *IEEE Spectrum*, 49 (6):50–56, June 2012. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Peck:2017:BWD

[Pec17] Morgan E. Peck. Blockchain world — do you need a blockchain? This chart will tell you if the technology can solve your problem. *IEEE Spectrum*, 54(10):38–60, October 2017. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Persichetti:2013:SAH

[Per13] Edoardo Persichetti. Secure and anonymous hybrid encryption from coding theory. *Lecture Notes in Computer Science*, 7932: 174–187, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_12/`.

Peterson:2011:SWS

[Pet11] Heather R. Peterson. The shape of the world: the story of Spanish expansion and the secret science of cosmography. *Studies in History and Philosophy of Science Part A*, 42(1):223–226, March 2011. CODEN SHPSB5. ISSN 0039-3681 (print), 1879-2510 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0039368110000919`.

Petrlic:2012:PRE

[Pet12] Ronald Petrlic. Proxy re-encryption in a privacy-preserving cloud computing DRM scheme. *Lecture Notes in Computer Science*, 7672:194–211, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-35362-8_16/`.

Pfleeger:2010:CJD

[Pfl10] Charles P. Pfleeger. Crypto: Not just for the defensive team. *IEEE Security & Privacy*, 8(2):63–66, March/April 2010. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Peinado:2012:CAT

[PFS12] Alberto Peinado and Amparo Fúster-Sabater. Cryptographic analysis of a type of sequence generators. *Lecture Notes in Computer Science*, 7671: 265–276, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35130-3_19/.

Poppelmann:2012:TEA

[PG12] Thomas Pöppelmann and Tim Güneysu. Towards efficient arithmetic for lattice-based cryptography on reconfigurable hardware. *Lecture Notes in Computer Science*, 7533: 139–158, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33481-8_8/.

Pendleton:2017:SSS

[PGLCX17] Marcus Pendleton, Richard Garcia-Lebron, Jin-Hee Cho, and Shouhuai Xu. A survey on systems security metrics. *ACM Computing Surveys*, 49(4):62:1–62:??, February 2017. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Peng:2010:SFW

[PGLL10] Fei Peng, Re-Si Guo, Chang-Tsun Li, and Min Long. A semi-fragile watermarking algorithm for authenticating 2D CAD engineering graphics based on log-polar transformation. *Computer-Aided Design*, 42(12):1207–1216, 2010. CODEN CAIDA5. ISSN 0010-4485 (print), 1879-2685 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010448510001491.

Park:2012:IDF

[PH12a] JeaHoon Park and JaeCheol Ha. Improved differential fault analysis on block cipher ARIA. *Lecture Notes in Computer Science*, 7690:82–95, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35416-8_7/.

Pohls:2012:RDI

[PH12b] Henrich C. Pöhls and Focke Höhne. The role of data integrity in EU digital signature legislation — achieving statutory trust for sanitizable signature schemes. *Lecture Notes in Computer Science*, 7170:175–192, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29963-6_13/.

Premnath:2016:SPC

[PH16] Sriram Nandha Premnath and Zygmunt J. Haas. Supporting privacy of computations in mobile big data systems. *Future Internet*, 8 (2):17, May 10, 2016. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/8/2/17.

Parno:2016:PNP

[PHGR16] Bryan Parno, Jon Howell, Craig Gentry, and Mariana Raykova. Pinocchio: nearly practical verifiable computation. *Communications of the Association for Computing Machinery*, 59(2):103–112, February 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2016/2/197429/fulltext.

Papas:2012:MLR

[PHN+12] Marios Papas, Thomas Houit, Derek Nowrouzezahrai, Markus Gross, and Wojciech Jarosz. The magic lens: refractive steganography. *ACM Transactions on Graphics*, 31(6):186:1–186:??, November 2012. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Park:2010:SIC

[PHWM10] Jong Hyuk Park, Sajid Hussain, Guilin Wang, and Yi Mu. Special issue of computers and mathematics with applications on "Advances in cryptography, security and applications for future computer science". *Computers and Mathematics with Applications*, 60(2):175, July 2010. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122110002695.

Pieprzyk:2010:TCC

[Pie10] Josef Pieprzyk, editor. *Topics in cryptology — CT-RSA 2010: the 10th cryptographers' track at the RSA conference 2010, San Francisco, CA, USA, March 1–5, 2010. Proceedings*, volume 5985 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-11924-7 (softcover). LCCN ????

Pointcheval:2012:ACE

[PJ12] David Pointcheval and Thomas Johansson, editors. *Advances in Cryptology — EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge,* UK, April 15–19. Proceedings, volume 7237 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. CODEN LNCSD9. ISBN 3-642-29010-8. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/978-3-642-29010-7.

Patel:2018:LLA

[PJ18] Hasmukh Patel and Devesh C. Jinwala. LPM: A lightweight authenticated packet marking approach for IP traceback. *Computer Networks (Amsterdam, Netherlands: 1999)*, 140 (??):41–50, July 20, 2018. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128618301786.

Premarathne:2015:LDD

[PKA15] Uthpala Subodhani Premarathne, Ibrahim Khalil, and Mohammed Atiquzzaman. Location-dependent disclosure risk based decision support framework for persistent authentication in pervasive computing applications. *Computer Networks (Amsterdam, Netherlands: 1999)*, 88(??):161–177, September 9, 2015. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128615001954.

Pramila:2018:ICA

[PKS18] Anu Pramila, Anja Keskinarkaus, and Tapio Seppänen. Increasing the capturing angle in print-cam robust watermarking. *The Journal of Systems and Software*, 135(??):205–215, January 2018. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121217302522.

Peter:2012:AHE

[PKTK12] Andreas Peter, Max Kronberg, Wilke Trei, and Stefan Katzenbeisser. Additively homomorphic encryption with a double decryption mechanism, revisited. *Lecture Notes in Computer Science*, 7483: 242–257, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33383-5_15/.

Phuc:2016:SAS

[PL16] Tran Song Dat Phuc and Changhoon Lee. Security analysis of SDDObased block cipher for wireless sensor network. *The Journal of Supercomputing*, 72(9):3619–3628, September 2016. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://link.springer.com/article/10.1007/s11227-015-1589-3`.

Perez:2011:FDS

[PLCGS11] Alejandro Pérez, Gabriel López, Óscar Cánovas, and Antonio F. Gómez-Skarmeta. Formal description of the SWIFT identity management framework. *Future Generation Computer Systems*, 27(8): 1113–1123, October 2011. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Peris-Lopez:2018:EAC

[PLGMCdF18] Pedro Peris-Lopez, Lorena González-Manzano, Carmen Camara, and José María de Fuentes. Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things. *Future Generation Computer Systems*, 81(??):67–77, April 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X17300407`.

Pang:2013:IMA

[PLPW13] Liaojun Pang, Huixian Li, Qingqi Pei, and Yumin Wang. Improvement on Meshram et al.'s ID-based cryptographic mechanism. *Information Processing Letters*, 113(19–21):789–792, September/October 2013. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019013002081`.

Peris-Lopez:2010:CSP

[PLSvdLE10] Pedro Peris-Lopez, Enrique San Millán, Jan C. A. van der Lubbe, and Luis A. Entrena. Cryptographically secure pseudo-random bit generator for RFID tags. In *2010 International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5678035`.

Perumal:2019:SDE

[PMG19a] Kaliram Perumal, Suganthi Muthusamy, and Gowrison Gengavel. Sparse data encoder and decoder to improve security in video steganography. *Concurrency and Computation: Practice and Experience*, 31(14):e4971:1–e4971:??, July 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Pisani:2019:ABS

[PMG+19b] Paulo Henrique Pisani, Abir Mhenni, Romain Giot, Estelle Cherrier, Norman Poh, André Carlos Ponce de Leon Ferreira de Carvalho, Christophe Rosenberger, and Najoua Essoukri Ben Amara. Adaptive biometric systems: Review and perspectives. *ACM Computing Surveys*, 52(5):102:1–102:??, October 2019. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3344255.

Poh:2012:SEC

[PMZ12] Geong Sen Poh, Moesfa Soeheila Mohamad, and Muhammad Reza Z'aba. Structured encryption for conceptual graphs. *Lecture Notes in Computer Science*, 7631:105–122, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34117-5_7/.

Pande:2013:SMC

[PMZ13] Amit Pande, Prasant Mohapatra, and Joseph Zambreno. Securing multimedia content using joint compression and encryption. *IEEE MultiMedia*, 20(4):50–61, October/December 2013. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Poursakidis:2010:TPC

[PN10] V. Poursakidis and C. Nikolaou. Towards a person-centric Identity Management Infrastructure (IMI). *International Journal of Computer Systems Science and Engineering*, 25(1):??, January 2010. CODEN CSSEEI. ISSN 0267-6192.

Puthal:2017:DDK

[PNRC17] Deepak Puthal, Surya Nepal, Rajiv Ranjan, and Jinjun Chen. DLSeF: a dynamic key-length-based efficient real-time security verification model for big data stream. *ACM Transactions on Embedded Computing Systems*, 16 (2):51:1–51:??, April 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Niu:2014:RDW

[pNyWyY+14] Pan pan Niu, Xiang yang Wang, Hong ying Yang, Pei Wang, and Ai long

Wang. A robust digital watermarking based on local complex angular radial transform. *Fundamenta Informaticae*, 135(3):243–268, July 2014. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Powers:2014:OSCa

[Pow14] Shawn Powers. The open-source classroom: encrypting your cat photos. *Linux Journal*, 2014(237):8:1–8:??, January 2014. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Paar:2010:UCT

[PP10a] Christof Paar and Jan Pelzl. *Understanding Cryptography: a Textbook for Students and Practitioners*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-04100-0 (hardcover), 3-642-04101-9 (ebk.). xviii + 372 pp. LCCN Z104 .P33 2010.

Papadopoulos:2010:TRM

[PP10b] Konstantinos Papadopoulos and Ioannis Papaefstathiou. Titan-R: a multigigabit reconfigurable combined compression/decompression unit. *ACM Transactions on Reconfigurable Technology and Systems*, 3(2):7:1–7:??, May 2010. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Park:2011:ACC

[PP11] Ki-Woong Park and Kyu Ho Park. ACCENT: Cognitive cryptography plugged compression for SSL/TLS-based cloud computing services. *ACM Transactions on Internet Technology (TOIT)*, 11(2):7:1–7:??, December 2011. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

P:2018:ABE

[PPA18] Praveen Kumar P, Syam Kumar P, and Alphonse P. J. A. Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. *Journal of Network and Computer Applications*, 108(??):37–52, April 15, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804518300547`.

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 JS-

SODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121215001466.

Pennino:2019:PIS

[PPG19] Diego Pennino, Maurizio Pizzonia, and Federico Griscioli. Pipeline-integrity: Scaling the use of authenticated data structures up to the cloud. *Future Generation Computer Systems*, 100(??):618–647, November 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18328048.

Pendl:2012:ECC

[PPH12] Christian Pendl, Markus Pelnar, and Michael Hutter. Elliptic curve cryptography on the WISP UHF RFID tag. *Lecture Notes in Computer Science*, 7055:32–47, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-25286-0_3/.

Pyun:2012:IBF

[PPR+12] Young June Pyun, Younghee Park, Douglas S. Reeves, Xinyuan Wang, and Peng Ning. Interval-based flow watermarking for tracing interactive traffic. *Computer Networks (Amsterdam, Netherlands: 1999)*, 56(5):1646–1665, March 30, 2012. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128612000412.

Pathak:2012:PPS

[PPRT12] Manas Pathak, Jose Portelo, Bhiksha Raj, and Isabel Trancoso. Privacy-preserving speaker authentication. *Lecture Notes in Computer Science*, 7483:1–22, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33383-5_1/.

Phan:2012:DDB

[PPS12a] Duong Hieu Phan, David Pointcheval, and Mario Strefler. Decentralized dynamic broadcast encryption. *Lecture Notes in Computer Science*, 7485:166–183, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32928-9_10/.

Phan:2012:MBT

[PPS12b] Duong Hieu Phan, David Pointcheval, and Mario

Strefler. Message-based traitor tracing with optimal ciphertext rate. *Lecture Notes in Computer Science*, 7533:56–77, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33481-8_4/.

Papadopoulos:2015:PAP

[PPTT15] Dimitrios Papadopoulos, Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Practical authenticated pattern matching with optimal proof size. *Proceedings of the VLDB Endowment*, 8(7):750–761, February 2015. CODEN ???? ISSN 2150-8097.

Pandey:2012:PPS

[PR12] Omkant Pandey and Yannis Rouselakis. Property preserving symmetric encryption. *Lecture Notes in Computer Science*, 7237:375–391, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_22; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_23/.

Piret:2012:PBC

[PRC12] Gilles Piret, Thomas Roche, and Claude Carlet. PICARO — a block cipher allowing efficient higher-order side-channel resistance. *Lecture Notes in Computer Science*, 7341:311–328, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31284-7_19/.

Perez-Resa:2019:SSE

[PRGBSAC19] A. Pérez-Resa, M. Garcia-Bosque, C. Sánchez-Azqueta, and S. Celma. Self-synchronized encryption for physical layer in 10Gbps optical links. *IEEE Transactions on Computers*, 68(6):899–911, June 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Puthal:2019:SAL

[PRN+19] Deepak Puthal, Rajiv Ranjan, Ashish Nanda, Priyadarsi Nanda, Prem Prakash Jayaraman, and Albert Y. Zomaya. Secure authentication and load balancing of distributed edge datacenters. *Journal of Parallel and Distributed Computing*, 124(??):60–69, February 2019. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://

www.sciencedirect.com/science/article/pii/S074373151830741X.

Proudfoot:2015:WTH

[Pro15] D. Proudfoot. What Turing himself said about the imitation game. *IEEE Spectrum*, 52(7):42–47, July 2015. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Polyakov:2017:FPR

[PRSV17] Yuriy Polyakov, Kurt Rohloff, Gyana Sahu, and Vinod Vaikuntanathan. Fast proxy re-encryption for publish/subscribe systems. *ACM Transactions on Privacy and Security (TOPS)*, 20(4):14:1–14:??, October 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Popa:2012:CPQ

[PRZB12] Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan. CryptDB: processing queries on an encrypted database. *Communications of the Association for Computing Machinery*, 55(9):103–111, September 2012. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Priemuth-Schmid:2012:ASV

[PS12] Deike Priemuth-Schmid. Attacks on simplified versions of K2. *Lecture Notes in Computer Science*, 7053:117–127, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-25261-7_9/.

Permpoontanalarp:2014:FTG

[PS14] Yongyuth Permpoontanalarp and Panupong Sornkhom. On-the-fly trace generation approach to the security analysis of cryptographic protocols: Coloured Petri nets-based method. *Fundamenta Informaticae*, 130 (4):423–466, October 2014. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Perazzo:2015:DRL

[PSD15] Pericle Perazzo, Pavel Skvortsov, and Gianluca Dini. On designing resilient location-privacy obfuscators. *The Computer Journal*, 58(10):2649–2664, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2649.

Pereira:2013:SLC

[PSdO+13] Geovandro C. C. F. Pereira,

Mateus A. S. Santos, Bruno T. de Oliveira, Marcos A. Simplicio, Jr., Paulo S. L. M. Barreto, Cíntia B. Margi, and Wilson V. Ruggiero. SMSCrypto: a lightweight cryptographic framework for secure SMS transmission. *The Journal of Systems and Software*, 86(3): 698–706, March 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212003056.

Phatak:2013:SIN

[PSJ+13] Dhananjay Phatak, Alan T. Sherman, Nikhil Joshi, Bhushan Sonawane, Vivek G. Relan, and Amol Dawalbhakta. Spread identity: A new dynamic address remapping mechanism for anonymity and DDoS defense. *Journal of Computer Security*, 21(2):233–281, ???? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Patranabis:2017:PSK

[PSM17] S. Patranabis, Y. Shrivastava, and D. Mukhopadhyay. Provably secure key-aggregate cryptosystems with broadcast aggregate keys for online data sharing on the cloud. *IEEE Transactions on Computers*, 66(5):891–904, May 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Pizzi:2018:ETM

[PSM+18] Sara Pizzi, Chiara Suraci, Leonardo Militano, Antonino Orsino, Antonella Molinaro, Antonio Iera, and Giuseppe Araniti. Enabling trustworthy multicast wireless services through D2D communications in 5G networks. *Future Internet*, 10(7):66, July 11, 2018. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/10/7/66.

Picazo-Sanchez:2013:CRS

[PSOMPL13] Pablo Picazo-Sanchez, Lara Ortiz-Martin, and Pedro Peris-Lopez. Cryptanalysis of the RNTS system. *The Journal of Supercomputing*, 65(2):949–960, August 2013. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-013-0873-3.

Park:2013:PPM

[PSS+13] Y. Park, C. Sur, S. Shin, K.-H. Rhee, and C. Seo. A privacy preserving message delivery protocol using identity-hidden index in VDTNs. *J.UCS: Journal of Universal Computer*

Science, 19(16):2385–??, ???? 2013. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL http://www.jucs.org/jucs_19_16/a_privacy_preserving_message.

Pankhuri:2019:PBM

[PSSK19] Pankhuri, Akash Sinha, Gulshan Shrivastava, and Prabhat Kumar. A pattern-based multi-factor authentication system. *Scalable Computing: Practice and Experience*, 20 (1):101–112, ???? 2019. CODEN ???? ISSN 1895-1767. URL https://www.scpe.org/index.php/scpe/article/view/1460.

Papamanthou:2013:SCC

[PST13] Charalampos Papamanthou, Elaine Shi, and Roberto Tamassia. Signatures of correct computation. *Lecture Notes in Computer Science*, 7785: 222–242, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-36594-2_13/.

Peng:2019:GCS

[PT19] Liqiang Peng and Atsushi Takayasu. Generalized cryptanalysis of small CRT-exponent RSA. *Theoretical Computer Science*, 795(??):432–458, November 26, 2019. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397519304669.

Papakostas:2014:MBL

[PTK14] G. A. Papakostas, E. D. Tsougenis, and D. E. Koulouriotis. Moment-based local image watermarking via genetic optimization. *Applied Mathematics and Computation*, 227(??):222–236, January 15, 2014. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300313012046.

Paletov:2018:ICA

[PTRV18] Rumen Paletov, Petar Tsankov, Veselin Raychev, and Martin Vechev. Inferring crypto API rules from code changes. *ACM SIGPLAN Notices*, 53(4):450–464, April 2018. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Papamanthou:2016:AHT

[PTT16] Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Authenticated hash tables based on cryptographic accumulators. *Al-*

gorithmica, 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.

Pudovkina:2012:RKA

[Pud12] Marina Pudovkina. A related-key attack on block ciphers with weak recurrent key schedules. *Lecture Notes in Computer Science*, 6888:90–101, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27901-0_8/.

Padget:2017:FGA

[PV17] Julian A. Padget and Wamberto W. Vasconcelos. Fine-grained access control via policy-carrying data. *ACM Transactions on Internet Technology (TOIT)*, 18(3):31:1–31:??, May 2017. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Pellikaan:2017:CCC

[PWBJ17] Ruud Pellikaan, Xin-Wen Wu, Stanislav Bulygin, and Relinde Jurrius. *Codes, Cryptology and Curves with Computer Algebra*. Cambridge University Press, Cambridge, UK, 2017. ISBN 0-521-52036-3 (paperback), 0-521-81711-0 (hardcover), 0-511-98217-8 (e-book). xii + 597 pp. LCCN QA268 .P45 2017.

Pei:2013:ARW

[PWLL13] Qingqi Pei, Xiang Wang, Yuan Li, and Hui Li. Adaptive reversible watermarking with improved embedding capacity. *The Journal of Systems and Software*, 86(11):2841–2848, November 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121213001623.

Pham:2019:SSS

[PWS19a] Hoang Pham, Jason Woodworth, and Mohsen Amini Salehi. Survey on secure search over encrypted data on the cloud. *Concurrency and Computation: Practice and Experience*, 31(17): e5284:1–e5284:??, September 10, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Puthal:2019:SSE

[PWS+19b] D. Puthal, X. Wu, N. Surya, R. Ranjan, and J. Chen. SEEN: A selective encryption method to ensure confidentiality for big sensing data streams. *IEEE Transactions on Big Data*, 5(3):

379–392, September 2019. ISSN 2332-7790.

Poller:2012:EIC

[PWVT12] Andreas Poller, Ulrich Waldmann, Sven Vowe, and Sven Turpe. Electronic identity cards for user authentication — promise and practice. *IEEE Security & Privacy*, 10(1): 46–54, January/February 2012. ISSN 1540-7993 (print), 1558-4046 (electronic).

Peng:2010:IWM

[PWW10] Hong Peng, Jun Wang, and Weixing Wang. Image watermarking method in multiwavelet domain based on support vector machines. *The Journal of Systems and Software*, 83(8):1470–1477, August 2010. CODEN JSSODM. ISSN 0164-1212.

Pongaliur:2013:SNS

[PX13] Kanthakumar Pongaliur and Li Xiao. Sensor node source privacy and packet recovery under eavesdropping and node compromise attacks. *ACM Transactions on Sensor Networks*, 9(4):50:1–50:??, July 2013. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Pja:2019:SSG

[PY19] Alphonse Pja and Venkatramana Reddy Y. Scalable and secure group key agreement for wireless adhoc networks by extending RSA scheme. *Concurrency and Computation: Practice and Experience*, 31(14): e4969:1–e4969:??, July 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Pagnin:2018:HDB

[PYH+18] Elena Pagnin, Anjia Yang, Qiao Hu, Gerhard Hancke, and Aikaterini Mitrokotsa. HB^+DB: Distance bounding meets human based authentication. *Future Generation Computer Systems*, 80(??):627–639, March 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X16301492`.

Philippaerts:2013:CMC

[PYM+13] Pieter Philippaerts, Yves Younan, Stijn Muylle, Frank Piessens, Sven Lachmund, and Thomas Walter. CPM: Masking code pointers to prevent code injection attacks. *ACM Transactions on Information and System Security*, 16(1):1:1–1:??, June 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Pei:2015:SWT

[PYM+15] Qingqi Pei, Dingyu Yan, Lichuan Ma, Zi Li, and Yang Liao. A strong and weak ties feedback-based trust model in multimedia social networks. *The Computer Journal*, 58(4):627–643, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/4/627`.

Papadopoulos:2010:CAR

[PYP10] Stavros Papadopoulos, Yin Yang, and Dimitris Papadias. Continuous authentication on relational streams. *VLDB Journal: Very Large Data Bases*, 19(2):161–180, April 2010. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Phuong:2018:CBE

[PYS18] Tran Viet Xuan Phuong, Guomin Yang, and Willy Susilo. Criteria-based encryption. *The Computer Journal*, 61(4):512–525, April 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/61/4/512/4430306`.

Popa:2015:HCD

[PZ15] R. A. Popa and N. Zeldovich. How to compute with data you can't see. *IEEE Spectrum*, 52(8):42–47, August 2015. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Pournaghi:2018:NNE

[PZBF18] Seyed Morteza Pournaghi, Behnam Zahednejad, Majid Bayat, and Yaghoub Farjami. NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. *Computer Networks (Amsterdam, Netherlands: 1999)*, 134(??):78–92, April 7, 2018. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128618300227`.

Peng:2019:EDI

[PZL+19] Su Peng, Fucai Zhou, Jin Li, Qiang Wang, and Zifeng Xu. Efficient, dynamic and identity-based Remote Data Integrity Checking for multiple replicas. *Journal of Network and Computer Applications*, 134(??):72–88, May 15, 2019. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804519300657`.

Patsakis:2015:PSM

[PZPS15] Constantinos Patsakis, Athanasios Zigomitros, Achilleas Papageorgiou, and Agusti Solanas. Privacy and security for multimedia content shared on OSNs: Issues and countermeasures. *The Computer Journal*, 58(4):518–535, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/4/518`.

Qiu:2018:QDS

[QCX18] Lirong Qiu, Feng Cai, and Guixian Xu. Quantum digital signature for the access control of sensitive data in the big data era. *Future Generation Computer Systems*, 86(??):372–379, September 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X18301250`.

Qin:2016:VTQ

[QD16] Huawang Qin and Yuewei Dai. Verifiable (t, n) threshold quantum secret sharing using d-dimensional Bell state. *Information Processing Letters*, 116(5):351–355, May 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019016000077`.

Queiroz:2019:WBF

[QF19] Jordan S. Queiroz and Eduardo L. Feitosa. A Web browser fingerprinting method based on the Web audio API. *The Computer Journal*, 62(8):1106–1120, August 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/62/8/1106/5298776`.

Qu:2013:DPA

[QGGL13] Bo Qu, Dawu Gu, Zheng Guo, and Junrong Liu. Differential power analysis of stream ciphers with LFSRs. *Computers and Mathematics with Applications*, 65(9):1291–1299, May 2013. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122112001381`.

Qin:2018:NUW

[QJC+18] C. Qin, P. Ji, C. Chang, J. Dong, and X. Sun. Non-uniform watermark sharing based on optimal iterative BTC for image tampering recovery. *IEEE MultiMedia*, 25(3):36–48, July/September 2018. CODEN

IEMUE4. ISSN 1070-986x (print), 1941-0166 (electronic).

Qin:2017:DIR

[QLL17] Chuan Qin, Jingwei Li, and Patrick P. C. Lee. The design and implementation of a rekeying-aware encrypted deduplication storage system. *ACM Transactions on Storage*, 13(1): 9:1–9:??, March 2017. CODEN ???? ISSN 1553-3077 (print), 1553-3093 (electronic).

Qiu:2019:CPT

[QLZ19] Jian Qiu, Hengjian Li, and Chuan Zhao. Cancelable palmprint templates based on random measurement and noise data for security and privacy-preserving authentication. *Computers & Security*, 82(??):1–14, May 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404818306618`.

Qiu:2017:AAS

[QMC17] Yue Qiu, Maode Ma, and Shuo Chen. An anonymous authentication scheme for multi-domain machine-to-machine communication in cyber-physical systems. *Computer Networks (Amsterdam, Netherlands: 1999)*, 129 (part 1)(??): 306–318, December 24, 2017. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S138912861730381X`.

Qiu:2017:PSB

[QMW17] Yue Qiu, Maode Ma, and Xilei Wang. A proxy signature-based handover authentication scheme for LTE wireless networks. *Journal of Network and Computer Applications*, 83(??):63–71, April 1, 2017. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804517300449`.

Qiao:2018:CTC

[QRW+18] Huidong Qiao, Jiangchun Ren, Zhiying Wang, Haihe Ba, and Huaizhe Zhou. Compulsory traceable ciphertext-policy attribute-based encryption against privilege abuse in fog computing. *Future Generation Computer Systems*, 88(??):107–116, November 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X17328820`.

Quaglia:2018:SVA

[QS18] Elizabeth A. Quaglia and Ben Smyth. Secret, verifiable auctions from elections. *Theoretical Computer Science*, 730(??):44–92, June 19, 2018. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S030439751830183X`.

Qin:2016:STI

[QYWX16] Zhen Qin, Chen Yuan, Yilei Wang, and Hu Xiong. On the security of two identity-based signature schemes based on pairings. *Information Processing Letters*, 116(6):416–418, June 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019016300096`.

Qian:2014:IAF

[QZ14] Zhenxing Qian and Xinpeng Zhang. Improved anti-forensics of JPEG compression. *The Journal of Systems and Software*, 91(??):100–108, May 2014. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121214000168`.

Qiang:2016:SCF

[QZDJ16] Weizhong Qiang, Kang Zhang, Weiqi Dai, and Hai Jin. Secure cryptographic functions via virtualization-based outsourced computing. *Concurrency and Computation: Practice and Experience*, 28(11):3149–3163, August 10, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Qi:2016:SID

[QZL+16a] Saiyu Qi, Yuanqing Zheng, Mo Li, Yunhao Liu, and Jinli Qiu. Scalable industry data access control in RFID-enabled supply chain. *IEEE/ACM Transactions on Networking*, 24(6):3551–3564, December 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Qi:2016:SPR

[QZL+16b] Saiyu Qi, Yuanqing Zheng, Mo Li, Li Lu, and Yunhao Liu. Secure and private RFID-enabled third-party supply chain systems. *IEEE Transactions on Computers*, 65 (11):3413–3426, November 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Qin:2018:BRO

[QZZ18] Baodong Qin, Qinglan Zhao, and Dong Zheng. Bounded revocable and outsourceable ABE for secure data sharing. *The Computer Journal*, 61 (8):1259–1268, August 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/8/1259/5045945.

Rabin:2010:ACC

[Rab10] Tal Rabin, editor. *Advances in cryptology — Crypto 2010: 30th annual cryptology conference, Santa Barbara, CA, USA, August 15–19, 2010. Proceedings*, volume 6223 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-14622-8 (softcover). LCCN ????

Rankin:2010:HLH

[Ran10] Kyle Rankin. Hack and /: lightning hacks—SSH strikes back. *Linux Journal*, 2010(195):10:1–10:??, July 2010. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Rankin:2014:HEY

[Ran14] Kyle Rankin. Hack and / : encrypt your dog (Mutt and GPG). *Linux Journal*, 2014(242):7:1–7:??, June 2014. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Rankin:2016:HSP

[Ran16] Kyle Rankin. Hack and / : Preseeding full disk encryption. *Linux Journal*, 2016(261):5:1–5:??, January 2016. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://dl.acm.org/ft_gateway.cfm?id=2903198.

Rao:2010:PAA

[Rao10] Rajesh P. N. Rao. Probabilistic analysis of an ancient undeciphered script. *Computer*, 43(4):76–80, April 2010. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Rao:2017:SEC

[Rao17] Y. Sreenivasa Rao. A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing. *Future Generation Computer Systems*, 67(??):133–151, February 2017. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16302746.

Rauscher:2015:FMT

[Rau15] Karl Frederick Rauscher. Forum: A matter of trust. *Scientific American*, 312

(3):8, March 2015. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.nature.com/scientificamerican/journal/v312/n3/full/scientificamerican0315-8.html; http://www.nature.com/scientificamerican/journal/v312/n3/pdf/scientificamerican0315-8.pdf.

Raz:2019:FLR

[Raz19] Ran Raz. Fast learning requires good memory: a time-space lower bound for parity learning. *Journal of the ACM*, 66(1):3:1–3:??, January 2019. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Ruoti:2015:WJS

[RAZS15] Scott Ruoti, Jeff Andersen, Daniel Zappala, and Kent Seamons. Why Johnny still, still can't encrypt: Evaluating the usability of a modern PGP client. *arxiv.org*, ??(??):1–5, October 29, 2015. URL http://arxiv.org/pdf/1510.08555.pdf.

Radke:2017:SPP

[RB17] Kenneth Radke and Colin Boyd. Security proofs for protocols involving humans. *The Computer Journal*, 60(4):527–540, March 23, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/4/527/2354604.

Rupp:2015:CTM

[RBHP15] Andy Rupp, Foteini Baldimtsi, Gesine Hinterwälder, and Christof Paar. Cryptographic theory meets practice: Efficient and privacy-preserving payments for public transport. *ACM Transactions on Information and System Security*, 17(3):10:1–10:??, March 2015. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Radke:2015:CFA

[RBNB15] Kenneth Radke, Colin Boyd, Juan Gonzalez Nieto, and Harry Bartlett. CHURNs: Freshness assurance for humans. *The Computer Journal*, 58(10):2404–2425, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2404.

Reaves:2017:MBM

[RBS+17] Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bhartiya, Patrick Traynor, and Kevin R. B. Butler. Mo(bile) money, mo(bile) problems: Analysis of branchless banking applications. *ACM Transactions on Privacy and Security (TOPS)*, 20(3):11:1–11:??, August 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

R:2018:SDM

[RC18] Jithin R and Priya Chandran. Secure and dynamic memory management architecture for virtualization technologies in IoT devices. *Future Internet*, 10(12):119, November 30, 2018. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/10/12/119.

Rao:2019:HPR

[RCBK19] Fang-Yu Rao, Jianneng Cao, Elisa Bertino, and Murat Kantarcioglu. Hybrid private record linkage: Separating differentially private synopses from matching records. *ACM Transactions on Privacy and Security (TOPS)*, 22 (3):15:1–15:??, July 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3318462.

Reinicke:2017:RDS

[RCK17] Bryan Reinicke, Jeffrey Cummings, and Howard Kleinberg. The right to digital self-defense. *IEEE Security & Privacy*, 15(4): 68–71, July/August 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2017/04/msp2017040068-abs.html.

Raisaro:2018:PPS

[RCP+18] Jean Louis Raisaro, Gwangbae Choi, Sylvain Pradervand, Raphael Colsenet, Nathalie Jacquemont, Nicolas Rosat, Vincent Mooser, and Jean-Pierre Hubaux. Protecting privacy and security of genomic data in i2b2 with homomorphic encryption and differential privacy. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 15(5):1413–1426, September 2018. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Rabbachin:2015:WNI

[RCW15] Alberto Rabbachin, Andrea Conti, and Moe Z. Win. Wireless network intrinsic secrecy. *IEEE/ACM Transactions on Networking*, 23(1):56–69, February 2015. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Rao:2017:CFA

[RD17] Y. Sreenivasa Rao and Ratna Dutta. Computational friendly attribute-based encryptions with short ciphertext. *Theoretical Computer Science*, 668(??):1–26, March 15, 2017. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397516307587.

Riazi:2019:DLP

[RDK19] M. S. Riazi, B. Darvish Rouani, and F. Koushanfar. Deep learning on private data. *IEEE Security & Privacy*, 17(6):54–63, November 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Ren:2016:IBE

[RDZ+16] Yanli Ren, Ning Ding, Xinpeng Zhang, Haining Lu, and Dawu Gu. Identity-based encryption with verifiable outsourced revocation. *The Computer Journal*, 59(11):1659–1668, November 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/11/1659.

Reardon:2016:SDD

[Rea16] Joel Reardon. *Secure Data Deletion*. Information security and cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2016. ISBN 3-319-28778-8 (e-book), 3-319-28777-X. ISSN 1619-7100 (print), 2197-845X (electronic). xvii + 203 + 32 pp. LCCN QA76.9.D3 R4223 2016. URL http://www.springerlink.com/content/978-3-319-28778-2.

Reeve:2015:ARC

[Ree15] Tom Reeve. Aged RC4 cipher to be shunned by security conscious browsers. *SC Magazine*, ??(??):??, September 2, 2015. URL http://www.scmagazine.com/aged-rc4-cipher-to-be-shunned-by-security-conscious-browsers/article/436521/.

Ren:2010:CSH

[RG10] Yanli Ren and Dawu Gu. CCA2 secure (hierarchical) identity-based parallel key-insulated encryption without random oracles. *The Journal of Systems and Software*, 83(1):153–162, January 2010. CODEN JSSODM. ISSN 0164-1212.

Roh:2010:BSW

[RH10] Dongyoung Roh and Sang Geun Hahn. On the bit security of the weak Diffie–Hellman problem. *Information Processing Letters*, 110(18–19):799–802, September 15, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Rouhani:2018:RRT

[RHLK18] Bita Darvish Rouhani, Siam Umar Hussain, Kristin Lauter, and Farinaz Koushanfar. ReDCrypt: Real-time privacy-preserving deep learning inference in clouds using FPGAs. *ACM Transactions on Reconfigurable Technology and Systems*, 11(3):21:1–21:??, December 2018. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Robert-Inacio:2011:SAP

[RITF+11] Frédérique Robert-Inacio, Alain Trémeau, Mike Fournigault, Yannick Teglia, and Pierre-Yvan Liardet. Shape analysis for power signal cryptanalysis on secure components. *The Journal of Systems and Software*, 84(5):753–762, May 2011. CODEN JSSODM. ISSN 0164-1212.

Rjasko:2012:BBP

[Rja12] Michal Rjaško. Black-box property of cryptographic hash functions. *Lecture Notes in Computer Science*, 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/.

Roy:2018:HFB

[RJV+18] Sujoy Sinha Roy, Kimmo Järvinen, Jo Vliegen, Frederik Vercauteren, and Ingrid Verbauwhede. HEPCloud: An FPGA-based multicore processor for FV somewhat homomorphic function evaluation. *IEEE Transactions on Computers*, 67(11):1637–1650, November 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL https://ieeexplore.ieee.org/document/8318681/.

Regev:2011:QOW

[RK11] Oded Regev and Bo'az Klartag. Quantum one-way communication can be exponentially stronger than classical communication. In ACM [ACM11], pages 31–40. ISBN ???? LCCN ???? URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Rakshit:2018:LLO

[RM18] Joydeep Rakshit and Kartik Mohanram. LEO: Low overhead encryption ORAM for non-volatile memories. *IEEE Computer Architecture Letters*, 17(2):100–104, July/December 2018. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Rezaeibagha:2019:EMC

[RM19] Fatemeh Rezaeibagha and Yi Mu. Efficient micropayment of cryptocurrency from blockchains. *The Computer Journal*, 62(4):507–517, April 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/62/4/507/5155318`.

Reyhani-Masoleh:2019:NMI

[RMERM19] A. Reyhani-Masoleh, H. El-Razouk, and A. Monfared. New multiplicative inverse architectures using Gaussian normal basis. *IEEE Transactions on Computers*, 68(7):991–1006, July 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Roy:2018:HIR

[RMG18] Aniket Roy, Arpan Kumar Maiti, and Kuntal Ghosh. An HVS inspired robust non-blind watermarking scheme in YCbCr color space. *International Journal of Image and Graphics (IJIG)*, 18(3):??, July 2018. ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S0219467818500158`.

Rahaman:2010:STB

[RMP10] H. Rahaman, J. Mathew, and D. K. Pradhan. Secure testable S-box architecture for cryptographic hardware implementation. *The Computer Journal*, 53(5):581–591, June 2010. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/cgi/content/abstract/53/5/581`; `http://comjnl.oxfordjournals.org/cgi/reprint/53/5/581`.

Reyhani-Masoleh:2018:NAR

[RMTA18] Arash Reyhani-Masoleh, Mostafa Taha, and Doaa Ashmawy. New area record for the AES combined S-box/inverse S-box. In Tenca and Takagi [TT18], pages 145–152. ISBN 1-5386-2612-8 (USB), 1-5386-2665-9. ISSN 2576-2265. LCCN QA76.9.C62. IEEE catalog number CFP18121-USB.

Rezaeibagha:2019:PSB

[RMZW19] Fatemeh Rezaeibagha, Yi Mu, Shiwei Zhang, and Xiaofen Wang. Provably secure (broadcast) homomorphic signcryption. *International Journal of Foundations of Computer Science (IJFCS)*, 30(4):511–529, June 2019. ISSN 0129-0541. URL `https://www.worldscientific.com/doi/10.1142/S0129054119400100`.

Ryan:2016:NCE

[RNQ16] Peter Y. A. Ryan, David

Naccache, and Jean-Jacques Quisquater, editors. *The New Codebreakers: essays dedicated to David Kahn on the occasion of his 85th birthday*, volume 9100 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2016. ISBN 3-662-49300-4 (paperback); 3-662-49301-2 (e-book). xiv + 551 pp. LCCN QA76.9.A25. URL http://link.springer.com/book/10.1007/978-3-662-49301-4.

Rogaway:2016:POP

[Rog16] Phillip Rogaway. Practice-oriented provable security and the social construction of cryptography. *IEEE Security & Privacy*, 14(6):10–17, November/December 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/06/msp2016060010-abs.html.

Rohloff:2019:CAR

[Roh19] Kurt Rohloff. Computer arithmetic research to accelerate privacy-protecting encrypted computing such as homomorphic encryption. In Takagi et al. [TBL19], page 197. ISBN 1-72813-366-1. ISSN 1063-6889.

Romero:2011:FSW

[Rom11] J. J. Romero. Fast start for world's biggest biometrics ID project. *IEEE Spectrum*, 48(5):11–12, May 2011. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Romero:2012:IBB

[Rom12] J. J. Romero. India's big bet on identity. *IEEE Spectrum*, 49(3):48–56, March 2012. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Rose:2011:KBT

[Ros11] Greg Rose. KISS: a bit too simple. Report ??, Qualcomm Inc., San Diego, CA, USA, April 18, 2011. URL http://eprint.iacr.org/2011/007.pdf.

Rao:2012:SSA

[RP12] Burepalli V. S. Rao and Munaga V. N. K. Prasad. Subset selection approach for watermarking relational databases. *Lecture Notes in Computer Science*, 6411:181–188, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-27872-3_27.

Rifa-Pous:2012:AHD

[RPG12] Helena Rifà-Pous and Carles Garrigues. Authenticating hard decision sensing reports in cognitive radio networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 56(2): 566–576, February 2, 2012. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128611003720`.

Rifa-Pous:2011:CEC

[RPHJ11] Helena Rifà-Pous and Jordi Herrera-Joancomartí. Computational and energy costs of cryptographic algorithms on handheld devices. *Future Internet*, 3(1):31–48, February 14, 2011. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/3/1/31`.

Rhee:2010:TSS

[RPSL10] Hyun Sook Rhee, Jong Hwan Park, Willy Susilo, and Dong Hoon Lee. Trapdoor security in a searchable public-key encryption scheme with a designated tester. *The Journal of Systems and Software*, 83(5): 763–771, May 2010. CODEN JSSODM. ISSN 0164-1212.

Ren:2015:ASE

[RQD+15] Jianbao Ren, Yong Qi, Yuehua Dai, Xiaoguang Wang, and Yi Shi. AppSec: a safe execution environment for security sensitive applications. *ACM SIGPLAN Notices*, 50(7):187–199, July 2015. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Rawat:2011:CBR

[RR11] Sanjay Rawat and Balasubramanian Raman. A chaos-based robust watermarking algorithm for rightful ownership protection. *International Journal of Image and Graphics (IJIG)*, 11(4):471–493, October 2011. CODEN ???? ISSN 0219-4678.

Razaque:2016:TDP

[RR16] Abdul Razaque and Syed S. Rizvi. Triangular data privacy-preserving model for authenticating all key stakeholders in a cloud environment. *Computers & Security*, 62(??):328–347, September 2016. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404816300979`.

Razaque:2017:SDA

[RR17] Abdul Razaque and Syed S. Rizvi. Secure data aggregation using access control and authentication for wireless sensor networks. *Computers & Security*, 70(??):532–545, September 2017. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404817301402`.

Rosen:2010:CCS

[RS10] Alon Rosen and Gil Segev. Chosen-ciphertext security via correlated products. *SIAM Journal on Computing*, 39(7):3058–3088, ???? 2010. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Reeder:2011:WPD

[RS11] Robert W. Reeder and Stuart Schechter. When the password doesn't work: Secondary authentication for websites. *IEEE Security & Privacy*, 9(2):43–49, March/April 2011. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

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`.

Rossi:2015:IBS

[RS15] Francesco Rossi and Giovanni Schmid. Identity-based secure group communications using pairings. *Computer Networks (Amsterdam, Netherlands: 1999)*, 89(??):32–43, 2015. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128615002303`.

Rana:2016:DBV

[RS16] Shuvendu Rana and Arijit Sur. Depth-based view-invariant blind 3D image watermarking. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 12(4):48:1–48:??, August 2016. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Rawat:2017:VIS

[RS17a] Hemendra Rawat and Patrick Schaumont. Vector instruction set extensions for efficient computation of Keccak. *IEEE Transactions on Computers*, 66(10):1778–1789, October 2017. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http:/`

/ieeexplore.ieee.org/document/7918507/.

Rivest:2017:WEV

[RS17b] Ronald L. Rivest and Philip B. Stark. When is an election verifiable? *IEEE Security & Privacy*, 15 (3):48–50, May/June 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2017/03/msp2017030048-abs.html.

Roy:2017:LOS

[RS17c] Dipanjan Roy and Anirban Sengupta. Low overhead symmetrical protection of reusable IP core using robust fingerprinting and watermarking during high level synthesis. *Future Generation Computer Systems*, 71(??):89–101, June 2017. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16305556.

Roetteler:2018:QCC

[RS18] M. Roetteler and K. M. Svore. Quantum computing: Codebreaking and beyond. *IEEE Security & Privacy*, 16(5):22–36, September/October 2018. ISSN 1540-7993 (print), 1558-4046 (electronic).

Ruoti:2019:JJT

[RS19] S. Ruoti and K. Seamons. Johnny's journey toward usable secure email. *IEEE Security & Privacy*, 17 (6):72–76, November 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Rangasamy:2012:ERP

[RSBGN12] Jothi Rangasamy, Douglas Stebila, Colin Boyd, and Juan Manuel González-Nieto. Effort-release public-key encryption from cryptographic puzzles. *Lecture Notes in Computer Science*, 7372:194–207, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31448-3_15/.

Ren:2018:IAS

[RSCX18] Shuai Ren, Yan Shi, Maolin Cai, and Weiqing Xu. Influence of airway secretion on airflow dynamics of mechanical ventilated respiratory system. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 15 (5):1660–1668, September 2018. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Rastegari:2019:ECS

[RSD19] Parvin Rastegari, Willy Susilo, and Mohammad

Dakhlalian. Efficient certificateless signcryption in the standard model: Revisiting Luo and Wan's scheme from wireless personal communications (2018). *The Computer Journal*, 62 (8):1178–1193, August 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/8/1178/5485598.

Roy:2015:SCP

[RSGG15] Arpan Roy, Santonu Sarkar, Rajeshwari Ganesan, and Geetika Goel. Secure the cloud: From the perspective of a service-oriented organization. *ACM Computing Surveys*, 47(3):41:1–41:??, April 2015. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Ribeiro:2015:QBS

[RSM15] J. Ribeiro, A. Souto, and P. Mateus. Quantum blind signature with an offline repository. *International Journal of Quantum Information*, 13(2):1550016, ???? 2015. URL www.worldscientific.com/doi/pdf/10.1142/S0219749915500161. See also news story [Ano15a].

Resende:2019:BMI

[RSMA19] João S. Resende, Patrícia R. Sousa, Rolando Martins, and Luís Antunes. Breaking MPC implementations through compression. *International Journal of Information Security*, 18(4): 505–518, August 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-018-0424-2.

Ruj:2014:DAC

[RSN14] Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak. Decentralized access control with anonymous authentication of data stored in clouds. *IEEE Transactions on Parallel and Distributed Systems*, 25(2):384–394, February 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Rahulamathavan:2019:PPI

[RSR+19] Y. Rahulamathavan, K. R. Sutharsini, I. G. Ray, R. Lu, and M. Rajarajan. Privacy-preserving iVector-based speaker verification. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 27 (3):496–506, March 2019. ISSN 2329-9290.

Ryan:2015:EEVa

[RST15a] Peter Y. A. Ryan, Steve Schneider, and Vanessa

Teague. End-to-end verifiability in voting systems, from theory to practice. *IEEE Security & Privacy*, 13(3):59–62, May/June 2015. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `http://www.computer.org/csdl/mags/sp/2015/03/msp2015030059-abs.html`.

Ryan:2015:EEVb

[RST15b] Peter Y. A. Ryan, Steve Schneider, and Vanessa Teague. End-to-end verifiability in voting systems, from theory to practice. *ComputingEdge*, 1(10):9–11, October 2015. ISSN 2376-113X. URL `http://www.computer.org/cms/Computer.org/computing-edge/ce-oct15-final.pdf`.

Rexha:2018:ITF

[RSX18] Blerim Rexha, Gresa Shala, and Valon Xhafa. Increasing trustworthiness of face authentication in mobile devices by modeling gesture behavior and location using neural networks. *Future Internet*, 10 (2):17, February 05, 2018. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/10/2/17`.

Russo:2015:FPT

[Rus15] Alejandro Russo. Functional pearl: two can keep a secret, if one of them uses Haskell. *ACM SIGPLAN Notices*, 50(9):280–288, September 2015. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Rahulamathavan:2016:UCA

[RVH+16] Yogachandran Rahulamathavan, Suresh Veluru, Jinguang Han, Fei Li, Muttukrishnan Rajarajan, and Rongxing Lu. User collusion avoidance scheme for privacy-preserving decentralized key-policy attribute-based encryption. *IEEE Transactions on Computers*, 65(9):2939–2946, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Rodriguez-Vazquez:2012:SCB

[RVRSCM12] Juan José Rodríguez-Vázquez, Sixto Romero-Sánchez, and Miguel Cárdenas-Montes. Speeding up a chaos-based image encryption algorithm using GPGPU. *Lecture Notes in Computer Science*, 6927: 592–599, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-27549-4_76`.

Reaves:2018:CSS

[RVS+18] Bradley Reaves, Luis Vargas, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin R. B. Butler. Characterizing the security of the SMS ecosystem with public gateways. *ACM Transactions on Privacy and Security (TOPS)*, 22(1):2:1–2:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3268932.

Roettger:2012:PKC

[RW12] Eric Roettger and Hugh C. Williams. Public-key cryptography based on a cubic extension of the Lucas functions. *Fundamenta Informaticae*, 114(3–4):325–344, August 2012. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Ren:2014:HHM

[RWLL14] Jian Ren, Jie Wu, Yun Li, and Jian Li. Hop-by-hop message authentication and source privacy in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 25(5):1223–1232, May 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Rogaway:2012:SCS

[RWZ12] Phillip Rogaway, Mark Wooding, and Haibin Zhang. The security of ciphertext stealing. *Lecture Notes in Computer Science*, 7549:180–195, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34047-5_11/.

Ren:2013:PPK

[RWZ13] Yanli Ren, Shuozhong Wang, and Xinpeng Zhang. Practical parallel key-insulated encryption with multiple helper keys. *Computers and Mathematics with Applications*, 65(9):1403–1412, May 2013. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122112000429.

Ristenpart:2010:WGR

[RY10] Thomas Ristenpart and Scott Yilek. When good randomness goes bad: Virtual machine reset vulnerabilities and hedging deployed cryptography. In Anonymous [Ano10a], page ?? ISBN 1-891562-29-0, 1-891562-30-4. LCCN ???? URL http://www.isoc.org/isoc/conferences/

ndss/10/pdf/15.pdf; http://www.isoc.org/isoc/conferences/ndss/10/proceedings.shtml.

Ren:2013:DSE

[RYF+13] Ling Ren, Xiangyao Yu, Christopher W. Fletcher, Marten van Dijk, and Srinivas Devadas. Design space exploration and optimization of path oblivious RAM in secure processors. *ACM SIGARCH Computer Architecture News*, 41(3): 571–582, June 2013. ICSA '13 conference proceedings.

Romashchenko:2019:OCM

[RZ19] Andrei Romashchenko and Marius Zimand. An operational characterization of mutual information in algorithmic information theory. *Journal of the ACM*, 66(5):38:1–38:??, September 2019. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3356867.

Rajendran:2015:FAB

[RZZ+15] J. Rajendran, Huan Zhang, Chi Zhang, G. S. Rose, Youngok Pino, O. Sinanoglu, and R. Karri. Fault analysis-based logic encryption. *IEEE Transactions on Computers*, 64(2): ??, February 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Sang:2012:SSF

[SA12] Lifeng Sang and Anish Arora. A shared-secret free security infrastructure for wireless networks. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 7(2): 23:1–23:??, July 2012. CODEN ???? ISSN 1556-4665 (print), 1556-4703 (electronic).

Sakalli:2014:ACC

[SA14] Muharrem Tolga Sakalli and Bora Aslan. On the algebraic construction of cryptographically good 32×32 binary linear transformations. *Journal of Computational and Applied Mathematics*, 259 (part B)(??):485–494, March 15, 2014. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042713002719.

Somanatha:2015:RAK

[SA15] Revathi Bangalore Somanatha and J. William Atwood. Router authentication, key management, and adjacency management for securing inter-router control messages. *Computer Networks (Amsterdam, Netherlands:*

1999), 79(??):68–90, March 14, 2015. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128614004691.

Shivani:2016:PVC

[SA16a] Shivendra Shivani and Suneeta Agarwal. Progressive visual cryptography with unexpanded meaningful shares. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 12(4): 50:1–50:??, August 2016. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Siad:2016:NFI

[SA16b] A. Siad and M. Amara. A new framework for implementing identity-based cryptosystems. *The Journal of Systems and Software*, 118(??):36–48, August 2016. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121216300346.

Subramanian:2019:SAF

[SA19] Nalini Subramanian and J. Andrews. Strong authentication framework using statistical approach for cloud environments. *Concurrency and Computation: Practice and Experience*, 31(12):e4870:1–e4870:??, June 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Saarinen:2012:PPK

[Saa12a] Markku-Juhani O. Saarinen. The PASSERINE public key encryption and authentication mechanism. *Lecture Notes in Computer Science*, 7127: 283–288, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27937-9_20/.

Suoranta:2012:SAM

[SAA12b] Sanna Suoranta, André Andrade, and Tuomas Aura. Strong authentication with mobile phone. *Lecture Notes in Computer Science*, 7483:70–85, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33383-5_5/.

Sarreshtedari:2015:WMD

[SAA15] S. Sarreshtedari, M. A. Akhaee, and A. Abbasfar. A watermarking method for digital speech self-recovery. *IEEE/ACM Transactions on Audio,* *Speech, and Language Processing*, 23(11):1917–1925, November 2015. CODEN ???? ISSN 2329-9290.

Schutz:2010:DIN

[SAAB10] Simon Schütz, Henrik Abrahamsson, Bengt Ahlgren, and Marcus Brunner. Design and implementation of the Node Identity Internetworking Architecture. *Computer Networks (Amsterdam, Netherlands: 1999)*, 54(7):1142–1154, May 17, 2010. CODEN ???? ISSN 1389-1286.

Sacco:2014:MC

[Sac14] Luigi Sacco. *Manuale di crittografia. (Italian) [Manual of cryptography]*. Apogeo, Milano, Italia, fourth edition, 2014. ???? pp.

Sahai:2013:TCT

[Sah13] Amit Sahai, editor. *Theory of cryptography: 10th Theory of Cryptography Conference, TCC 2013, Tokyo, Japan, March 3–6, 2013: proceedings*, volume 7785 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2013. ISBN 3-642-36594-9 (paperback), 3-642-36593-0 (e-book). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 T473 2013. URL `http://www.loc.gov/catdir/enhancements/fy1310/2013931230-d.html; http://www.loc.gov/catdir/enhancements/fy1310/2013931230-t.html; http://www.springerlink.com/content/978-3-642-36594-2`.

Saeed:2016:IID

[SAJL16] Ahmed Saeed, Ali Ahmadinia, Abbas Javed, and Hadi Larijani. Intelligent intrusion detection in low-power IoTs. *ACM Transactions on Internet Technology (TOIT)*, 16(4):27:1–27:??, December 2016. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Saleh:2016:PED

[SAKM16] Eyad Saleh, Ahmad Alsa'deh, Ahmad Kayed, and Christoph Meinel. Processing over encrypted data: Between theory and practice. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 45(3):5–16, September 2016. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Suomalainen:2018:SAS

[SAM+18] Jani Suomalainen, Kimmo Ahola, Mikko Majanen, Olli Mämmelä, and Pekka Ruuska. Security awareness in software-defined multi-domain 5G networks.

Future Internet, 10(3):27, March 08, 2018. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/10/3/27`.

Sadat:2019:SSG

[SAM+19a] Md Nazmus Sadat, Md Momin Al Aziz, Noman Mohammed, Feng Chen, Xiaoqian Jiang, and Shuang Wang. SAFETY: Secure gwAs in Federated Environment through a hYbrid Solution. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 16(1):93–102, January 2019. CODEN ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).

Saracevic:2019:NAS

[SAM+19b] Muzafer Saracević, Sasa Adamović, Vladislav Miskovic, Nemanja Macek, and Marko Sarac. A novel approach to steganography based on the properties of Catalan numbers and Dyck words. *Future Generation Computer Systems*, 100(??):186–197, November 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X19300184`.

Sarier:2010:IAS

[Sar10a] Neyire Deniz Sarier. Improving the accuracy and storage cost in biometric remote authentication schemes. *Journal of Network and Computer Applications*, 33(3):268–274, May 2010. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804510000068`.

Sarkar:2010:SGC

[Sar10b] 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:TES

[Sar11] Palash Sarkar. Tweakable enciphering schemes using only the encryption function of a block cipher. *Information Processing Letters*, 111(19):945–955, October 15, 2011. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019011001852`.

Sarier:2012:SNB

[Sar12] Neyire Deniz Sarier. Security notions of biometric remote authentication revisited. *Lecture Notes in Computer Science*, 7170:72–89, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29963-6_7/.

Sarkar:2014:PEK

[Sar14] Santanu Sarkar. Proving empirical key-correlations in RC4. *Information Processing Letters*, 114(5): 234–238, May 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019014000039.

Sarier:2018:MBI

[Sar18a] Neyire Deniz Sarier. Multimodal biometric Identity Based Encryption. *Future Generation Computer Systems*, 80(??):112–125, March 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17302613.

Singh:2018:SDD

[SAR18b] Priyanka Singh, Nishant Agarwal, and Balasubramanian Raman. Secure data deduplication using secret sharing schemes over cloud. *Future Generation Computer Systems*, 88(??):156–167, November 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17327474.

Sasaki:2012:DSW

[Sas12] Yu Sasaki. Double-SP is weaker than single-SP: Rebound attacks on Feistel ciphers with several rounds. *Lecture Notes in Computer Science*, 7668: 265–282, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34931-7_16/.

Sasaki:2018:QKD

[Sas18] M. Sasaki. Quantum key distribution and its applications. *IEEE Security & Privacy*, 16(5):42–48, September/October 2018. ISSN 1540-7993 (print), 1558-4046 (electronic).

Savage:2013:NSL

[Sav13a] Neil Savage. News: Stopping the leaks. *Communications of the Association for Computing Machinery*, 56(1):19–21, January 2013. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Savage:2013:PP

[Sav13b] Neil Savage. Proofs probable. *Communications of the Association for Computing Machinery*, 56(6): 22–24, June 2013. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Savage:2015:NVS

[Sav15] Neil Savage. News: Visualizing sound. *Communications of the Association for Computing Machinery*, 58(2):15–17, February 2015. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2015/2/182639/fulltext.

Savage:2016:NKP

[Sav16] Neil Savage. News: The key to privacy. *Communications of the Association for Computing Machinery*, 59(6):12–14, June 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2016/6/202654/fulltext.

Safkhani:2017:PSD

[SB17] Masoumeh Safkhani and Nasour Bagheri. Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things. *The Journal of Supercomputing*, 73(8): 3579–3585, August 2017. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Shwartz:2018:DMI

[SB18] Ofir Shwartz and Yitzhak Birk. Distributed memory integrity trees. *IEEE Computer Architecture Letters*, 17(2):159–162, July/December 2018. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

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.

Sarkar:2015:DFA

[SBM15] S. Sarkar, S. Banik, and S. Maitra. Differential fault attack against grain family with very few faults and minimal assumptions. *IEEE Transactions on Computers*, 64 (6):1647–1657, June 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Safkhani:2012:SMA

[SBS+12] Masoumeh Safkhani, Nasour Bagheri, Somitra Kumar Sanadhya, Majid Naderi, and Hamid Behnam. On the security of mutual authentication protocols for RFID systems: The case of Wei et al. 's protocol. *Lecture Notes in Computer Science*, 7122:90–103, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28879-1_7/.

Safkhani:2018:SRO

[SBS18] Masoumeh Safkhani, Nasour Bagheri, and Mahyar Shariat. On the security of rotation operation based ultra-lightweight authentication protocols for RFID systems. *Future Internet*, 10(9):82, August 21, 2018. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/10/9/82.

Santos:2014:ACD

[SBV14] Ricardo Jorge Santos, Jorge Bernardino, and Marco Vieira. Approaches and challenges in database intrusion detection. *SIGMOD Record (ACM Special Interest Group on Management of Data)*, 43(3): 36–47, September 2014. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

Shyu:2010:VMS

[SC10] Shyong Jian Shyu and Kun Chen. Visual multiple-secret sharing by circle random grids. *SIAM Journal on Imaging Sciences*, 3(4):926–953, ???? 2010. CODEN SJISBI. ISSN 1936-4954. URL http://epubs.siam.org/siims/resource/1/sjisbi/v3/i4/p926_s1.

Srinivasan:2012:RAP

[SC12] Avinash Srinivasan and Lashidhar Chennupati. Robust authentication of public access points using digital certificates — a novel approach. *Lecture Notes in Computer Science*, 7672:153–164, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35362-8_13/.

Singh:2019:SID

[SC19a] J. Singh and J. Cobbe. The security implications of data subject rights. *IEEE Security & Privacy*, 17 (6):21–30, November 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Sujitha:2019:HSP

[SC19b] V. Sujitha and D. Chitra. Highly secure palmprint based biometric template using fuzzy vault. *Concurrency and Computation: Practice and Experience*, 31(12):e4513:1–e4513:??, June 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Sun:2016:TCA

[SCBL16] Yanming Sun, Min Chen, Abel Bacchus, and Xiaodong Lin. Towards collusion-attack-resilient group key management using one-way function tree. *Computer Networks (Amsterdam, Netherlands: 1999)*, 104(??):16–26, July 20, 2016. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128616301128.

Saevanee:2015:CUA

[SCFB15] Hataichanok Saevanee, Nathan Clarke, Steven Furnell, and Valerio Biscione. Continuous user authentication using multi-modal biometrics. *Computers & Security*, 53(??):234–246, September 2015. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404815000875.

Syta:2014:SAA

[SCGW+14] Ewa Syta, Henry Corrigan-Gibbs, Shu-Chun Weng, David Wolinsky, Bryan Ford, and Aaron Johnson. Security analysis of accountable anonymity in Dissent. *ACM Transactions on Information and System Security*, 17(1):4:1–4:??, August 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Schoenmakers:2010:VS

[Sch10] Berry Schoenmakers. *Voting Schemes*, chapter 15, pages 1–21. Volume 2 of Atallah and Blanton [AB10b], second edition, 2010. ISBN 1-58488-820-2. LCCN QA76.9.A43 A433 2010. URL http://www.crcnetbase.com/doi/abs/10.1201/9781584888215-c15.

Schwartz:2011:IMP

[Sch11] Ari Schwartz. Identity management and privacy: a rare opportunity to get it right. *Communications of the Association for Computing Machinery*, 54(6):22–24, June 2011. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Schaathun:2012:MLI

[Sch12a] Hans Georg Schaathun. *Machine learning in image steganalysis*. John Wiley and Sons, Inc., New York, NY, USA, 2012. ISBN 0-470-66305-7, 1-118-43795-0, 1-283-60392-6, 1-118-43796-9, 1-118-43798-5, 1-118-43800-0. xi + 284 pp. LCCN Q325.5 .S285 2012. URL http://onlinelibrary.wiley.com/book/10.1002/9781118437957.

Schneier:2012:LOE

[Sch12b] Bruce Schneier. *Liars and outliers: enabling the trust that society needs to thrive*. John Wiley and Sons, Inc., New York, NY, USA, 2012. ISBN 1-118-14330-2 (paperback). 384 (est.) pp. LCCN ???? URL http://spectrum.ieee.org/at-work/innovation/review-liars-outliers.

Schnoor:2012:DES

[Sch12c] Henning Schnoor. Deciding epistemic and strategic properties of cryptographic protocols. *Lecture Notes in Computer Science*, 7459:91–108, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33167-1_6/.

Schneier:2013:HDD

[Sch13] Bruce Schneier. How to design — and defend against — the perfect security backdoor. Web site., 2013. URL https://www.schneier.com/essays/archives/2013/10/how_to_design_and_de.html.

Schaefer:2015:BRB

[Sch15a] Edward F. Schaefer. Book review: *The Mathematics of Encryption: An Elementary Introduction*, Reviewed work(s): The Mathematics of Encryption: An Elementary Introduction. By Margaret Cozzens and Steven J. Miller. American Mathematical Society, Providence, RI, 2013, xviii + 332 pp., ISBN 978-0-8218-8321-1, $49.00. *American Mathematical Monthly*, 122(1):83–88, January 2015. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic). URL http://www.jstor.org/stable/10.4169/amer.math.monthly.122.01.83.

Schaffer:2015:ECA

[Sch15b] Kim B. Schaffer. Expanding continuous authentication with mobile devices. *Computer*, 48(11):92–95, November 2015. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://www.computer.org/csdl/mags/co/2015/11/mco2015110092-abs.html.

Schneier:2015:DGH

[Sch15c] Bruce Schneier. *Data and Goliath: the hidden battles to collect your data and control your world*. W. W. Norton & Co., New York, NY, USA, 2015. ISBN 0-393-24481-4 (hardcover). 383 pp. LCCN HM846 .S362 2015. URL http://www.democracynow.org/2015/3/13/data_and_goliath_bruce_schneier_on; http://www.democracynow.org/blog/2015/3/13/part_2_bruce_schneier_on_the.

Schneider:2016:MSI

[Sch16a] D. Schneider. $100 million SETI initiative starts listening for E.T. *IEEE Spectrum*, 53(1):41–42, January 2016. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Schneider:2016:DEE

[Sch16b] D. Schneider. Don't expect encrypted e-mail in 2016. *IEEE Spectrum*, 53(1):42–43, January 2016. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Schneier:2016:CHT

[Sch16c] Bruce Schneier. Cryptography is harder than it looks. *IEEE Security & Privacy*, 14(1):87–88, January/February 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Schneier:2018:CAA

[Sch18] B. Schneier. Cryptography after the aliens land. *IEEE Security & Privacy*, 16(5): 86–88, September/October 2018. ISSN 1540-7993 (print), 1558-4046 (electronic).

Schneier:2019:CPI

[Sch19a] B. Schneier. Cybersecurity for the public interest. *IEEE Security & Privacy*, 17(1):84–83, January/February 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Scholl:2019:SIE

[Sch19b] Travis Scholl. Super-isolated elliptic curves and Abelian surfaces in cryptography. *Experimental Mathematics*, 28(4): 385–397, 2019. CODEN ???? ISSN 1058-6458 (print), 1944-950X (electronic). URL http://www.tandfonline.com/doi/full/10.1080/10586458.2017.1412371.

Shrestha:2010:KBA

[SCKH10] Anish Prasad Shrestha, Dong-You Choi, Goo Rak Kwon, and Seung-Jo Han.

Kerberos based authentication for inter-domain roaming in wireless heterogeneous network. *Computers and Mathematics with Applications*, 60(2):245–255, July 2010. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122110000416.

Stobert:2018:TAL

[SCMS18] E. Stobert, E. Cavar, L. Malisa, and D. Sommer. Teaching authentication as a life skill. *IEEE Security & Privacy*, 16(5):82–85, September/October 2018. ISSN 1540-7993 (print), 1558-4046 (electronic).

Seberry:2010:CTAa

[SCPSN10a] Jennifer Seberry, Chris Charnes, Josef Pieprzyk, and Rei Safavi-Naini. *Crypto Topics and Applications I*, chapter 12, pages 1–31. Volume 2 of Atallah and Blanton [AB10b], second edition, 2010. ISBN 1-58488-820-2. LCCN QA76.9.A43 A433 2010. URL http://www.crcnetbase.com/doi/abs/10.1201/9781584888215-c12.

Seberry:2010:CTAb

[SCPSN10b] Jennifer Seberry, Chris Charnes, Josef Pieprzyk, and Rei Safavi-Naini. *Crypto Topics and Applications II*, chapter 13, pages 1–32. Volume 2 of Atallah and Blanton [AB10b], second edition, 2010. ISBN 1-58488-820-2. LCCN QA76.9.A43 A433 2010. URL http://www.crcnetbase.com/doi/abs/10.1201/9781584888215-c13.

Scriber:2018:FDB

[Scr18] B. A. Scriber. A framework for determining blockchain applicability. *IEEE Software*, 35(4):70–77, July/August 2018. CODEN IESOEG. ISSN 0740-7459 (print), 1937-4194 (electronic).

shree:2019:ERC

[sCR19a] S. Raja shree, A. Chilambu Chelvan, and M. Rajesh. An efficient RSA cryptosystem by applying cuckoo search optimization algorithm. *Concurrency and Computation: Practice and Experience*, 31(12):e4845:1–e4845:??, June 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Smith-Creasey:2019:NWI

[SCR19b] Max Smith-Creasey and Muttukrishnan Rajarajan. A novel word-independent gesture-typing continuous authentication scheme for mobile devices. *Computers & Security*, 83(??):140–150, June 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818306552.

Shu:2015:PML

[SCY15] Tao Shu, Yingying Chen, and Jie Yang. Protecting multi-lateral localization privacy in pervasive environments. *IEEE/ACM Transactions on Networking*, 23(5):1688–1701, October 2015. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Saleh:2010:GTF

[SD10] Mohamed Saleh and Mourad Debbabi. A game-theoretic framework for specification and verification of cryptographic protocols. *Formal Aspects of Computing*, 22(5):585–609, September 2010. CODEN FACME5. ISSN 0934-5043 (print), 1433-299X (electronic). URL http://link.springer.com/article/10.1007/s00165-009-0129-4.

Shen:2012:PAS

[SD12] Jing Shen and Yusong Du. A password authentication scheme against Smart Card security breach. *Lecture Notes in Computer Science*, 7473:37–44, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34062-8_5/.

Sengupta:2017:USB

[SD17] Binanda Sengupta and Abhijit Das. Use of SIMD-based data parallelism to speed up sieving in integer-factoring algorithms. *Applied Mathematics and Computation*, 293(??):204–217, January 15, 2017. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300316305148.

Streit:2018:PQK

[SD18] Silvan Streit and Fabrizio De Santis. Post-quantum key exchange on ARMv8-A: a new hope for NEON made simple. *IEEE Transactions on Computers*, 67(11):1651–1662, November 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL https://ieeexplore.ieee.org/document/8107588/.

Sherman:2017:ICC

[SDC+17] Alan Sherman, Melissa Dark, Agnes Chan, Rylan Chong, Thomas Morris, Linda Oliva, John Springer, Bhavani Thuraisingham, Christopher Vatcher, Rakesh Verma, and Susanne Wetzel. INSuRE: Collaborating centers of academic excellence engage students in cybersecurity research. *IEEE Security & Privacy*, 15(4): 72–78, July/August 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2017/04/msp2017040072-abs.html.

Shakiba:2010:IID

[SDM10] Mohsen Shakiba, Mohammad Dakhilalian, and Hamid Mala. An improved impossible differential cryptanalysis of Zodiac. *The Journal of Systems and Software*, 83(4): 702–709, April 2010. CODEN JSSODM. ISSN 0164-1212.

Souissi:2012:OCP

[SDM+12] Youssef Souissi, Nicolas Debande, Sami Mekki, Sylvain Guilley, and Ali Maalaoui. On the optimality of correlation power attack on embedded cryptographic systems. *Lecture Notes in Computer Science*, 7322:169–178, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-30955-7_15/.

Shakiba:2014:CCI

[SDM14] Mohsen Shakiba, Mohammad Dakhilalian, and Hamid Mala. On computational complexity of impossible differential cryptanalysis. *Information Processing Letters*, 114(5):252–255, May 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013003116.

Seo:2014:RHI

[SE14] Jae Hong Seo and Keita Emura. Revocable hierarchical identity-based encryption. *Theoretical Computer Science*, 542(??):44–62, July 3, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397514003363.

Seo:2016:RHI

[SE16] Jae Hong Seo and Keita Emura. Revocable hierarchical identity-based encryption via history-free approach. *Theoretical Computer Science*, 615(??):45–60, February 15, 2016. CODEN TCSCDI. ISSN 0304-3975

(print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397515011354.

Salman:2018:BMM

[SE18] S. M. Salman and A. A. Elsadany. On the bifurcation of Marotto's map and its application in image encryption. *Journal of Computational and Applied Mathematics*, 328(??):177–196, January 15, 2018. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042717303515.

Sasaki:2012:IKK

[SEHK12] Yu Sasaki, Sareh Emami, Deukjo Hong, and Ashish Kumar. Improved known-key distinguishers on Feistel–SP ciphers and application to Camellia. *Lecture Notes in Computer Science*, 7372:87–100, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31448-3_7/.

Staples:2019:SAB

[SEK+19] J. Staples, C. Endicott, L. Krause, P. Pal, P. Samouelian, R. Schantz, and A. Wellman. A semi-autonomic bytecode repair framework. *IEEE Software*, 36(2):97–102, March/April 2019. CODEN IESOEG. ISSN 0740-7459 (print), 1937-4194 (electronic).

Sendrier:2010:PQC

[Sen10] Nicolas Sendrier, editor. *Post-Quantum Cryptography: Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25–28, 2010. Proceedings*, volume 6061 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-12928-5. LCCN QA76.9.A25 2010.

Sendrier:2017:CBC

[Sen17] Nicolas Sendrier. Code-based cryptography: State of the art and perspectives. *IEEE Security & Privacy*, 15(4):44–50, July/August 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2017/04/msp2017040044-abs.html.

Seo:2018:CSI

[Seo18] Hwajeong Seo. Compact software implementation of public-key cryptography on MSP430X. *ACM Transactions on Embedded Computing Systems*, 17(3):

66:1–66:??, June 2018. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Serrato:2012:IAN

[Ser12] Christy Serrato. Identity assurance and network security. *Network Security*, 2012(4):19–20, April 2012. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485812700284.

Sallam:2012:EBM

[SERF12] Ahmed I. Sallam, El-Sayed El-Rabaie, and Osama S. Faragallah. Encryption-based multilevel model for DBMS. *Computers & Security*, 31(4):437–446, June 2012. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404812000417.

Sakai:2016:CDN

[SES+16] Yusuke Sakai, Keita Emura, Jacob C. N. Schuldt, Goichiro Hanaoka, and Kazuo Ohta. Constructions of dynamic and non-dynamic threshold public-key encryption schemes with decryption consistency. *Theoretical Computer Science*, 630(??):95–116, May 30, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397516300317.

Sethumadhavan:2016:HEP

[Set16] Simha Sethumadhavan. Hardware-enforced privacy. *Computer*, 49(10):10, October 2016. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL https://www.computer.org/csdl/mags/co/2016/10/mco2016100010.html.

Severance:2016:BSB

[Sev16] Charles Severance. Bruce Schneier: Building cryptographic systems. *Computer*, 49(4):13–15, April 2016. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://www.computer.org/csdl/mags/co/2016/04/mco2016040013.html.

Seo:2018:AOF

[SEXY18] Jae Hong Seo, Keita Emura, Keita Xagawa, and Kazuki Yoneyama. Accumulable optimistic fair exchange from verifiably encrypted homomorphic signatures. *International Journal of Information Security*, 17(2):193–220, April 2018. CODEN ???? ISSN

1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0367-z.

Savas:2014:SMQ

[SEY14] Erkay Savas, Serdar Suer Erdem, and Kazim Yumbul. On selection of modulus of quadratic codes for the protection of cryptographic operations against fault attacks. *IEEE Transactions on Computers*, 63 (5):1182–1196, May 2014. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Su:2012:IIN

[SF12] Chen Su and Haining Fan. Impact of Intel's new instruction sets on software implementation of GF(2)[x] multiplication. *Information Processing Letters*, 112(12):497–502, June 30, 2012. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019012000804.

Shabtai:2010:SAP

[SFE10] Asaf Shabtai, Yuval Fledel, and Yuval Elovici. Securing Android-powered mobile devices using SELinux. *IEEE Security & Privacy*, 8(3):36–44, May/June 2010. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Schneier:2015:SWC

[SFKR15] Bruce Schneier, Matthew Fredrikson, Tadayoshi Kohno, and Thomas Ristenpart. Surreptitiously weakening cryptographic systems. Report, Co3 Systems; University of Wisconsin; University of Washington, ????; Madison, WI, USA; Seattle, WA, USA, February 9, 2015. URL http://eprint.iacr.org/2015/097.

Sarma:2012:STP

[SG12] Amardeo Sarma and Joao Girao. Supporting trust and privacy with an identity-enabled architecture. *Future Internet*, 4 (4):1016–1025, November 19, 2012. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/4/4/1016.

Sasdrich:2015:ICS

[SG15] Pascal Sasdrich and Tim Güneysu. Implementing Curve25519 for side-channel–protected elliptic curve cryptography. *ACM Transactions on Reconfigurable Technology and Systems*, 9(1):3:1–3:??, November 2015. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Sakellariou:2019:HEK

[SG19a] Georgios Sakellariou and Anastasios Gounaris. Homomorphically encrypted k-means on cloud-hosted servers with low client-side load. *Computing*, 101 (12):1813–1836, December 2019. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Sgantzos:2019:AII

[SG19b] Konstantinos Sgantzos and Ian Grigg. Artificial intelligence implementations on the blockchain. Use cases and future applications. *Future Internet*, 11(8):170, August 02, 2019. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/11/8/170`.

Shu:2014:DAS

[SGC14] Yuanchao Shu, Yu Jason Gu, and Jiming Chen. Dynamic authentication with sensory information for the access control systems. *IEEE Transactions on Parallel and Distributed Systems*, 25(2):427–436, February 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Saxena:2016:API

[SGC16] Neetesh Saxena, Santiago Grijalva, and Narendra S. Chaudhari. Authentication protocol for an IoT-enabled LTE network. *ACM Transactions on Internet Technology (TOIT)*, 16(4):25:1–25:??, December 2016. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Silva-Garcia:2018:SBG

[SGFCRM+18] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, and M. Aldape-Pérez. Substitution box generation using Chaos: An image encryption application. *Applied Mathematics and Computation*, 332(??):123–135, September 1, 2018. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S009630031830184X`.

S:2018:EDS

[SGG18] Prabu S, Gpinath Ganapathy, and Ranjan Goyal. Enhanced data security for public cloud environment with secured hybrid encryption authentication mechanisms. *Scalable Computing: Practice and Experience*, 19 (4):351–360, ???? 2018. CODEN ???? ISSN 1895-1767. URL `https://www.scpe.org/index.`

php/scpe/article/view/1422.

Sanchez-Garcia:2016:SSA

[SGGCR+16] J. Sánchez-García, J. M. García-Campos, D. G. Reina, S. L. Toral, and F. Barrero. On-siteDriverID: a secure authentication scheme based on Spanish eID cards for vehicular ad hoc networks. *Future Generation Computer Systems*, 64(??):50–60, November 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16301121.

Sun:2015:FSW

[SGH15] Shi-Feng Sun, Dawu Gu, and Zhengan Huang. Fully secure wicked identity-based encryption against key leakage attacks. *The Computer Journal*, 58(10):2520–2536, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2520.

Shen:2018:CAL

[SGJ+18] Jian Shen, Ziyuan Gui, Sai Ji, Jun Shen, Haowen Tan, and Yi Tang. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *Journal of Network and Computer Applications*, 106(??):117–123, March 15, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518300031.

Susilo:2016:EDT

[SGM16] Willy Susilo, Fuchun Guo, and Yi Mu. Efficient dynamic threshold identity-based encryption with constant-size ciphertext. *Theoretical Computer Science*, 609 (part 1)(??):49–59, January 4, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397515008087.

Shankar:2012:BDF

[SGP+12] Deepa D. Shankar, T. Gireeshkumar, K. Praveen, R. Jithin, and Ashji S. Raj. Block dependency feature based classification scheme for uncalibrated image steganalysis. *Lecture Notes in Computer Science*, 6411: 189–195, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-27872-3_28.

Sun:2017:PKE

[SGP+17] Shi-Feng Sun, Dawu Gu, Udaya Parampalli, Yu Yu, and Baodong Qin. Public key encryption resilient to leakage and tampering attacks. *Journal of Computer and System Sciences*, 89(??):142–156, November 2017. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0022000017300326`.

Sipiran:2014:SCA

[SGS14] Ivan Sipiran, Robert Gregor, and Tobias Schreck. Shapes and cryptography: Approximate symmetry detection in partial 3D meshes. *Computer Graphics Forum*, 33(7):131–140, October 2014. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (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`.

Seyedzadeh:2011:IEA

[SH11] Seyed Mohammad Seyedzadeh and Yasaman Hashemi. Image encryption algorithm based on Choquet Fuzzy Integral with self-adaptive pseudo-random number generator. In *2011 11th International Conference on Intelligent Systems Design and Applications (ISDA)*, pages 642–647. 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=6121728`.

Song:2015:ADT

[SH15] WeiTao Song and Bin Hu. Approach to detecting type-flaw attacks based on extended strand spaces. *The Computer Journal*, 58(4):572–587, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/4/572`.

Shallit:2010:BRB

[Sha10] Jeffrey Shallit. Book review: *Cryptographic Applications of Analytic Number Theory: Lower Bounds and Pseudorandomness*, by Igor Shparlinski, Birkäuser, 2003. *ACM*

SIGACT News, 41(3):44–45, September 2010. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [Shp03].

Shaw:2013:DE

[Sha13] John Shaw. Dealing with encryption. *Network Security*, 2013(11):8–11, November 2013. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348581370120X.

Syed:2019:TGB

[SHBC19] Zahid Syed, Jordan Helmick, Sean Banerjee, and Bojan Cukic. Touch gesture-based authentication on mobile devices: the effects of user posture, device size, configuration, and inter-session variability. *The Journal of Systems and Software*, 149(??):158–173, March 2019. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121218302516.

Sodsong:2016:DPB

[SHC+16] Wasuwee Sodsong, Jingun Hong, Seongwook Chung, Yeongkyu Lim, Shin-Dug Kim, and Bernd Burgstaller. Dynamic partitioning-based JPEG decompression on heterogeneous multicore architectures. *Concurrency and Computation: Practice and Experience*, 28(2):517–536, February 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Shen:2014:LES

[She14] Xuemin Shen. A lightweight encryption scheme for network-coded mobile ad hoc networks. *IEEE Transactions on Parallel and Distributed Systems*, 25(9):2211–2221, September 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL http://www.computer.org/csdl/trans/td/2014/09/06559980-abs.html.

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.

Shim:2011:SAT

[Shi11] K.-A. Shim. Security analysis of three password authentication schemes. *J.UCS: Journal of Universal Computer Science*, 17 (11):1623–??, ???? 2011. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL `http://www.jucs.org/jucs_17_11/security_analysis_of_three`.

Shparlinski:2003:CAA

[Shp03] Igor E. Shparlinski. *Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness*, volume 22 of *Progress in computer science and applied logic*. Birkhäuser Verlag, Basel, Switzerland, 2003. ISBN 3-7643-6654-0 , 0-8176-6654-0. viii + 411 pp. LCCN QA267.7 .S55 2003.

Shparlinski:2010:NWP

[Shp10] Igor E. Shparlinski. Numbers at work and play. *Notices of the American Mathematical Society*, 57(3):334–342, March 2010. CODEN AMNOAN. ISSN 0002-9920 (print), 1088-9477 (electronic). URL `http://www.ams.org/notices/201003/`.

Suoranta:2012:ASM

[SHS12] Sanna Suoranta, Jani Heikkinen, and Pekka Silvekoski. Authentication session migration. *Lecture Notes in Computer Science*, 7127:17–32, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-27937-9_2/`.

Shyu:2015:VCR

[Shy15] Shyong Jian Shyu. Visual cryptograms of random grids for threshold access structures. *Theoretical Computer Science*, 565(??):30–49, February 2, 2015. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397514008408`.

Satir:2012:CBT

[SI12] Esra Satir and Hakan Isik. A compression-based text steganography method. *The Journal of Systems and Software*, 85(10):2385–2394, October 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121212001379`.

Siad:2012:NAP

[Sia12] Amar Siad. A new approach for private searches on public-key encrypted data. *Lecture Notes in Computer Science*, 7394: 160–173, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32805-3_13/.

Simpson:2010:ESB

[Sim10] Edward Simpson. Edward Simpson: Bayes at Bletchley Park. *Significance (Oxford, England)*, 7 (2):76–80, June 2010. CODEN ???? ISSN 1740-9705 (print), 1740-9713 (electronic).

Simion:2015:RST

[Sim15a] Emil Simion. The relevance of statistical tests in cryptography. *IEEE Security & Privacy*, 13(1):66–70, January/February 2015. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://www.computer.org/csdl/mags/sp/2015/01/msp2015010066-abs.html.

Simmonds:2015:DII

[Sim15b] Paul Simmonds. The digital identity issue. *Network Security*, 2015(8):8–13, August 2015. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485815300696.

Sirer:2016:TPS

[Sir16] Emin Gün Sirer. Technical perspective: The state (and security) of the Bitcoin economy. *Communications of the Association for Computing Machinery*, 59(4):85, April 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2016/4/200172/fulltext.

Shakeri:2012:RZW

[SJ12] Mahsa Shakeri and Mansour Jamzad. A robust zero-watermark copyright protection scheme based on DWT and image normalization. *Lecture Notes in Computer Science*, 7088:359–370, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-25346-1_32.

Sartakhti:2019:CPL

[SJ19] Javad Salimi Sartakhti and Saeed Jalili. On the computational power of the light: a plan for breaking Data Encryption Standard. *Theoretical Com-*

puter Science, 773(??):71–78, June 14, 2019. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397518305310.

Seo:2018:CIA

[SJLK18] Hwajeong Seo, Ilwoong Jeong, Jungkeun Lee, and Woo-Hwan Kim. Compact implementations of ARX-based block ciphers on IoT processors. *ACM Transactions on Embedded Computing Systems*, 17(3):60:1–60:??, June 2018. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Shin:2017:CGI

[SJWH+17] Kyuyong Shin, Carlee Joe-Wong, Sangtae Ha, Yung Yi, Injong Rhee, and Douglas S. Reeves. T-Chain: a general incentive scheme for cooperative computing. *IEEE/ACM Transactions on Networking*, 25(4):2122–2137, August 2017. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Sherman:2019:OVB

[SJZG19] A. T. Sherman, F. Javani, H. Zhang, and E. Golaszewski. On the origins and variations of blockchain technologies. *IEEE Security & Privacy*, 17(1):72–77, January/February 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Sabri:2011:AFS

[SK11] Khair Eddin Sabri and Ridha Khedri. Algebraic framework for the specification and analysis of cryptographic-key distribution. *Fundamenta Informaticae*, 112(4):305–335, December 2011. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Sachnev:2012:IME

[SK12a] Vasily Sachnev and Hyoung Joong Kim. An improved matrix encoding scheme for JPEG steganography. *Lecture Notes in Computer Science*, 7128:3–15, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32205-1_3/.

Seo:2012:MPM

[SK12b] Hwajeong Seo and Howon Kim. Multi-precision multiplication for public-key cryptography on embedded microprocessors. *Lecture Notes in Computer Science*, 7690:55–67, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-

3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35416-8_5/.

Scarani:2014:BPQ

[SK14] Valerio Scarani and Christian Kurtsiefer. The black paper of quantum cryptography: Real implementation problems. *Theoretical Computer Science*, 560 (part 1)(??):27–32, December 4, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397514006938.

Sepczuk:2018:NRB

[SK18] Mariusz Sepczuk and Zbigniew Kotulski. A new risk-based authentication management model oriented on user's experience. *Computers & Security*, 73(??):17–33, March 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404817302079.

Son:2017:NOC

[SKB+17] Junggab Son, Donghyun Kim, Md Zakirul Alam Bhuiyan, Rasheed Hussain, and Heekuck Oh. A new outsourcing conditional proxy re-encryption suitable for mobile cloud environment. *Concurrency and Computation: Practice and Experience*, 29(14), July 25, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Saha:2018:ASS

[SKE+18] Seemanta Saha, Ismet Burak Kadron, William Eiers, Lucas Bang, and Tevfik Bultan. Attack synthesis for strings using metaheuristics. *ACM SIGSOFT Software Engineering Notes*, 43(4):56, October 2018. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

Soupionis:2014:GTA

[SKEG14] Yannis Soupionis, Remous-Aris Koutsiamanis, Pavlos Efraimidis, and Dimitris Gritzalis. A game-theoretic analysis of preventing spam over Internet Telephony via audio CAPTCHA-based authentication. *Journal of Computer Security*, 22(3):383–413, ???? 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sirivianos:2014:LSF

[SKGY14] Michael Sirivianos, Kyungbaek Kim, Jian Wei Gan, and Xiaowei Yang. Leveraging social feedback to verify online identity claims. *ACM Transactions on the Web (TWEB)*, 8(2): 9:1–9:??, March 2014. CODEN ???? ISSN 1559-1131 (print), 1559-114X (electronic).

Seo:2015:AEC

[SKH15] Seog Chung Seo, Taehong Kim, and Seokhie Hong. Accelerating elliptic curve scalar multiplication over GF(2^m) on graphic hardwares. *Journal of Parallel and Distributed Computing*, 75(??):152–167, January 2015. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731514001646`.

Shin:2017:SSD

[SKH17] Youngjoo Shin, Dongyoung Koo, and Junbeom Hur. A survey of secure data deduplication schemes for cloud storage systems. *ACM Computing Surveys*, 49(4): 74:1–74:??, February 2017. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Szalachowski:2010:CCG

[SKK10] P. Szalachowski, B. Ksiezopolski, and Z. Kotulski. CMAC, CCM and GCM/GMAC: Advanced modes of operation of symmetric block ciphers in wireless sensor networks. *Information Processing Letters*, 110(7): 247–251, March 1, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

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`.

Singh:2018:MWT

[SKS+18] Amit Kumar Singh, Basant Kumar, Sanjay Kumar Singh, S. P. Ghrera, and Anand Mohan. Multiple watermarking technique for securing online social network contents using back propagation neural network. *Future Generation Computer Systems*, 86(??):926–939, September 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X16306628`.

Scheidat:2012:STT

[SKV12] Tobias Scheidat, Karl Kümmel, and Claus Vielhauer. Short term template aging effects on biometric dynamic handwriting authentication performance. *Lecture Notes in*

Computer Science, 7394: 107–116, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32805-3_9/.

Schmitz:2012:NAC

[SLGZ12] Roland Schmitz, Shujun Li, Christos Grecos, and Xinpeng Zhang. A new approach to commutative watermarking-encryption. *Lecture Notes in Computer Science*, 7394: 117–130, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32805-3_10/.

Srivatsa:2011:ESA

[SLI11] Mudhakar Srivatsa, Ling Liu, and Arun Iyengar. EventGuard: a system architecture for securing publish–subscribe networks. *ACM Transactions on Computer Systems*, 29 (4):10:1–10:??, December 2011. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

Schultz:2010:MMP

[SLL10] David Schultz, Barbara Liskov, and Moses Liskov. MPSS: Mobile Proactive Secret Sharing. *ACM Transactions on Information and System Security*, 13(4):34:1–34:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Sandor:2019:EDM

[SLL+19] Voundi Koe Arthur Sandor, Yaping Lin, Xiehua Li, Feng Lin, and Shiwen Zhang. Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage. *Journal of Network and Computer Applications*, 129(??):25–36, March 1, 2019. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804519300037.

Somani:2010:IDS

[SLM10] U. Somani, K. Lakhani, and M. Mundra. Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing. In Chaudhuri et al. [CGB+10], pages 211–216. ISBN 1-4244-7675-5. LCCN ????

Su:2016:SSP

[SLXX16] Shenghui Su, Shuwang Lü, Maozhi Xu, and Tao Xie. A semantically secure public key cryptoscheme using bit-pair shadows. *Theoretical Computer Science*, 654(??):113–127, November 22, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397516300561.

Sun:2016:RSP

[SLY+16] Shi-Feng Sun, Joseph K. Liu, Yu Yu, Baodong Qin, and Dawu Gu. RKA-secure public key encryptions against efficiently invertible functions. *The Computer Journal*, 59 (11):1637–1658, November 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/11/1637.

Shao:2012:AKP

[SLZ12] Jun Shao, Peng Liu, and Yuan Zhou. Achieving key privacy without losing CCA security in proxy re-encryption. *The Journal of Systems and Software*, 85(3):655–665, March 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211002421.

Sarkar:2010:CRM

[SM10a] Santanu Sarkar and Subhamoy Maitra. Cryptanalysis of RSA with more than one decryption exponent. *Information Processing Letters*, 110(8–9):336–340, April 1, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Sarkar:2010:CRT

[SM10b] Santanu Sarkar and Subhamoy Maitra. Cryptanalysis of RSA with two decryption exponents. *Information Processing Letters*, 110(5):178–181, February 1, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Sorniotti:2010:PSS

[SM10c] Alessandro Sorniotti and Refik Molva. A provably secure secret handshake with dynamic controlled matching. *Computers & Security*, 29(5):619–627, July 2010. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404809001370.

Seyedzadeh:2011:IES

[SM11] S. M. Seyedzadeh and S. Mirzakuchaki. Image encryption scheme based on Choquet fuzzy integral with pseudo-random keystream generator. In

2011 International Symposium on Artificial Intelligence and Signal Processing (AISP), pages 101–106. 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=5960982.

Sengupta:2012:SAI

[SM12] Madhumita Sengupta and J. K. Mandal. Self authentication of image through Daubechies transform technique (SADT). *arXiv.org*, ??(??):1–4, December 9, 2012. CODEN ???? ISSN 2331-8422. URL https://arxiv.org/abs/1212.1863.

Sencar:2013:DIF

[SM13] Husrev T. Sencar and Nasir D. Memon, editors. *Digital image forensics: there is more to a picture than meets the eye*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2013. ISBN 1-4614-0757-5 (ebook). viii + 370 pp. LCCN TA1637 .D54 2013. URL http://site.ebrary.com/id/10589376.

Swami:2018:AAS

[SM18] Shivam Swami and Kartik Mohanram. ARSENAL: Architecture for secure non-volatile memories. *IEEE Computer Architecture Letters*, 17(2): 192–196, July/December 2018. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Shibu:2019:ARR

[SM19a] N. V. Shibu and P. Malathi. Accurate and reliable reversible data hiding using sequential encoding techniques. *Concurrency and Computation: Practice and Experience*, 31(14): e4979:1–e4979:??, July 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Shokri:2019:ESS

[SM19b] Madeh Shokri and Meghdad Mirabi. An efficient stream structure for broadcasting the encrypted XML data in mobile wireless broadcast channels. *The Journal of Supercomputing*, 75(11):7147–7173, November 2019. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Smart:2016:CMS

[Sma16] Nigel P. (Nigel Paul) Smart. *Cryptography Made Simple*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK /

etc., 2016. ISBN 3-319-21935-9 (hardcover), 3-319-21936-7 (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xii + 481 + 119 pp. LCCN QA76.9.A25; QA76.9.D35 S63 2016. URL http://link.springer.com/10.1007/978-3-319-21936-3.

Stanton:2010:FAD

[SMBA10] Paul T. Stanton, Benjamin McKeown, Randal Burns, and Giuseppe Ateniese. FastAD: an authenticated directory for billions of objects. *Operating Systems Review*, 44(1):45–49, January 2010. CODEN OSRED8. ISSN 0163-5980.

Salmon:2011:PRN

[SMDS11] John K. Salmon, Mark A. Moraes, Ron O. Dror, and David E. Shaw. Parallel random numbers: as easy as $1, 2, 3$. In Lathrop et al. [LCK11], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ????

Smith:2011:SSX

[Smi11a] Michael Smith. *The secrets of Station X: how the Bletchley Park codebreakers helped win the war*. Biteback Pub., London, UK, 2011. ISBN 1-84954-095-0 (paperback). 328 + 16 pp. LCCN D810.C88 S659 2011.

Smith:2011:RBA

[Smi11b] Sean W. Smith. Room at the bottom: Authenticated encryption on slow legacy networks. *IEEE Security & Privacy*, 9(4):60–63, July/August 2011. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Smith:2015:HHB

[Smi15a] Christopher Smith. *The hidden history of Bletchley Park: a social and organisational history, 1939–1945*. Palgrave Macmillan, New York, NY, USA, 2015. ISBN 1-137-48492-6. vii + 238 pp. LCCN D810.C88 C653 2015. URL http://www.loc.gov/catdir/enhancements/fy1608/2015015176-d.html; http://www.loc.gov/catdir/enhancements/fy1608/2015015176-t.html.

Smith:2015:DBP

[Smi15b] Michael Smith. *The Debs of Bletchley Park and other stories*. Aurum Press, London, UK, 2015. ISBN 1-78131-387-3 (hardcover), 1-78131-388-1. 298 + 8 pp. LCCN D810.S7 S65 2015.

Swierczynski:2015:PSE

[SMOP15] Pawel Swierczynski, Amir Moradi, David Oswald, and Christof Paar. Physical security evaluation of the bitstream encryption mechanism of Altera

Stratix II and Stratix III FPGAs. *ACM Transactions on Reconfigurable Technology and Systems*, 7 (4):7:1–7:??, January 2015. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Stankovski:2014:CFE

[SMS14] Tomislav Stankovski, Peter V. E. McClintock, and Aneta Stefanovska. Coupling functions enable secure communications. *Physical Review X*, 4 (1):011026, February 2014. CODEN PRXHAE. ISSN 2160-3308. URL `http://link.aps.org/doi/10.1103/PhysRevX.4.011026; http://www.rdmag.com/news/2014/04/unbreakable-security-codes-inspired-nature`.

Sucasas:2016:APP

[SMS+16] Victor Sucasas, Georgios Mantas, Firooz B. Saghezchi, Ayman Radwan, and Jonathan Rodriguez. An autonomous privacy-preserving authentication scheme for intelligent transportation systems. *Computers & Security*, 60(??):193–205, July 2016. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404816300463`.

Sharma:2018:CSS

[SMSK18] Himani Sharma, D. C. Mishra, R. K. Sharma, and Naveen Kumar. Crypto-stego system for securing text and image data. *International Journal of Image and Graphics (IJIG)*, 18 (4):??, October 2018. ISSN 0219-4678. URL `https://www.worldscientific.com/doi/10.1142/S0219467818500201`.

Sadeghi:2010:THI

[SN10] Ahmad-Reza. Sadeghi and David Naccache, editors. *Towards Hardware-Intrinsic Security: Foundations and Practice*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-14451-9 (hardcover), 3-642-14452-7 (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xvi + 407 pp. LCCN TK7887.5 .T69 2010eb. URL `http://www.springerlink.com/content/978-3-642-14452-3`. Foreword by Pim Tuyls.

Son:2018:GFD

[SNCK18] Yunmok Son, Juhwan Noh, Jaeyeong Choi, and Yongdae Kim. GyrosFinger: Fingerprinting drones for location tracking based on the outputs of MEMS gyroscopes. *ACM Transactions on Privacy and Security*

(TOPS), 21(2):10:1–10:??, February 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3177751`.

Siadati:2017:MYS

[SNG+17] Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson, and Nasir Memon. Mind your SMSes: Mitigating social engineering in second factor authentication. *Computers & Security*, 65(??):14–28, March 2017. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S016740481630116X`.

Safavi-Naini:2011:USC

[SNJ11] Reihaneh Safavi-Naini and Shaoquan Jiang. Unconditionally secure conference key distribution: Security notions, bounds and constructions. *International Journal of Foundations of Computer Science (IJFCS)*, 22(6):1369–1393, September 2011. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Seyedzadeh:2014:RCI

[SNM14] Seyed Mohammad Seyedzadeh, Benyamin Norouzi, and Sattar Mirzakuchaki. RGB color image encryption based on Choquet fuzzy integral. *The Journal of Systems and Software*, 97(??):128–139, November 2014. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121214001563`.

Soderstrom:2013:DDY

[Söd13] Sylvia Söderström. Digital differentiation in young people's Internet use — eliminating or reproducing disability stereotypes. *Future Internet*, 5(2):190–204, May 07, 2013. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/5/2/190`.

Suriadi:2012:PCV

[SOF12] Suriadi Suriadi, Chun Ouyang, and Ernest Foo. Privacy compliance verification in cryptographic protocols. *Lecture Notes in Computer Science*, 7400: 251–276, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-35179-2_11/`.

Schaumont:2015:IEP

[SOG15] Patrick Schaumont, Maire O'Neill, and Tim Güneysu.

Introduction for embedded platforms for cryptography in the coming decade. *ACM Transactions on Embedded Computing Systems*, 14(3):40:1–40:??, April 2015. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Strizhov:2016:SPS

[SOR16] Mikhail Strizhov, Zachary Osman, and Indrajit Ray. Substring position search over encrypted cloud data supporting efficient multi-user setup. *Future Internet*, 8(3):28, July 04, 2016. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/8/3/28`.

Suresh:2015:AGU

[SOS15] Chandra K. H. Suresh, Sule Ozev, and Ozgur Sinanoglu. Adaptive generation of unique IDs for digital chips through analog excitation. *ACM Transactions on Design Automation of Electronic Systems*, 20(3):46:1–46:??, June 2015. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Serwadda:2013:ELK

[SP13] Abdul Serwadda and Vir V. Phoha. Examining a large keystroke biometrics dataset for statistical-attack openings. *ACM Transactions on Information and System Security*, 16(2):8:1–8:??, September 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Shiaeles:2015:FII

[SP15a] Stavros N. Shiaeles and Maria Papadaki. FHSD: an improved IP spoof detection method for Web DDoS attacks. *The Computer Journal*, 58(4):892–903, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/4/892`.

Shim:2015:SDA

[SP15b] Kyung-Ah Shim and Cheol-Min Park. A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 26(8):2128–2139, August 2015. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL `http://www.computer.org/csdl/trans/td/2015/08/06875932-abs.html`.

Spafford:2016:SE

[Spa16] Eugene H. Spafford. The strength of encryption.

Communications of the Association for Computing Machinery, 59(3):5, March 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2016/3/198867/fulltext`.

Salvail:2010:STR

[SPD+10] Louis Salvail, Momtchil Peev, Eleni Diamanti, Romain Alléaume, Norbert Lütkenhaus, and Thomas Länger. Security of trusted repeater quantum key distribution networks. *Journal of Computer Security*, 18(1):61–87, ???? 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sherman:2019:PBL

[SPG+19] A. T. Sherman, P. A. H. Peterson, E. Golaszewski, E. LaFemina, E. Goldschen, M. Khan, L. Mundy, M. Rather, B. Solis, W. Tete, E. Valdez, B. Weber, D. Doyle, C. O'Brien, L. Oliva, J. Roundy, and J. Suess. Project-based learning inspires cybersecurity students: A scholarship-for-service research study. *IEEE Security & Privacy*, 17(3):82–88, May/June 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Skracic:2017:AAU

[SPK17] Kristian Skracić, Predrag Pale, and Zvonko Kostanjcar. Authentication approach using one-time challenge generation based on user behavior patterns captured in transactional data sets. *Computers & Security*, 67(??):107–121, June 2017. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S016740481730055X`.

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].

Sun:2013:IUP

[SPM+13] San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov.

Investigating users' perspectives of Web single sign-on: Conceptual gaps and acceptance model. *ACM Transactions on Internet Technology (TOIT)*, 13(1):2:1–2:??, November 2013. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Serwadda:2016:TRR

[SPW+16] Abdul Serwadda, Vir V. Phoha, Zibo Wang, Rajesh Kumar, and Diksha Shukla. Toward robotic robbery on the touch screen. *ACM Transactions on Information and System Security*, 18(4):14:1–14:??, May 2016. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Shaikh:2010:CTO

[SR10] Siraj A. Shaikh and Joseph R. Rabaiotti. Characteristic trade-offs in designing large-scale biometric-based identity management systems. *Journal of Network and Computer Applications*, 33(3):342–351, May 2010. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804510000032.

Schilling:2012:ATU

[SR12a] Thorsten Ernst Schilling and Håvard Raddum. Analysis of Trivium using compressed right hand side equations. *Lecture Notes in Computer Science*, 7259:18–32, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31912-9_2/.

Sur:2012:SSU

[SR12b] Arijit Sur and Vignesh Ramanathan. Secure steganography using randomized cropping. *Lecture Notes in Computer Science*, 7110:82–95, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28693-3_6/.

Stanton:2014:BRB

[SR14] Jeffrey M. Stanton and Ben Rothke. Book reviews: *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents* — by Jean-François Blanchette. *Journal of the Association for Information Science and Technology*, 65(7):1509–1510, July 2014. CODEN ???? ISSN 2330-1643 (print), 2330-1643 (electronic).

Singh:2017:SCB

[SRAA17] Priyanka Singh, Balasubramanian Raman, Nishant Agarwal, and Pradeep K. Atrey. Secure cloud-based image tampering detection and localization using POB number system. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 13(3):23:1–23:??, August 2017. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Stefan:2012:ACT

[SRB+12] Deian Stefan, Alejandro Russo, Pablo Buiras, Amit Levy, John C. Mitchell, and David Maziéres. Addressing covert termination and timing channels in concurrent information flow systems. *ACM SIGPLAN Notices*, 47(9):201–214, September 2012. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Sutar:2017:DPI

[SRK+17] Soubhagya Sutar, Arnab Raha, Devadatta Kulkarni, Rajeev Shorey, Jeffrey Tew, and Vijay Raghunathan. D-PUF: An intrinsically reconfigurable DRAM PUF for device authentication and random number generation. *ACM Transactions on Embedded Computing Systems*, 17 (1):1–31, December 2017. ISSN 1539-9087 (print), 1558-3465 (electronic).

Sutar:2018:DPI

[SRK+18] Soubhagya Sutar, Arnab Raha, Devadatta Kulkarni, Rajeev Shorey, Jeffrey Tew, and Vijay Raghunathan. D-PUF: an intrinsically reconfigurable DRAM PUF for device authentication and random number generation. *ACM Transactions on Embedded Computing Systems*, 17(1):17:1–17:??, January 2018. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Sluganovic:2018:ARE

[SRRM18] Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen, and Ivan Martinovic. Analysis of reflexive eye movements for fast replay-resistant biometric authentication. *ACM Transactions on Privacy and Security (TOPS)*, 22(1):4:1–4:??, January 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/citation.cfm?id=3281745`.

Sethumadhavan:2012:CHD

[SRT12] Simha Sethumadhavan, Ryan Roberts, and Yannis Tsividis. A case for hybrid discrete-continuous architectures. *IEEE Computer Architecture Letters*, 11(1):1–4, January/June 2012. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Saklikar:2010:IFV

[SS10a] Samir Saklikar and Subir Saha. Identity federation for VoIP systems. *Journal of Computer Security*, 18(4):499–540, ???? 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Saxena:2010:SGC

[SS10b] N. Saxena and C. Seshadhri. From Sylvester–Gallai configurations to rank bounds: Improved black-box identity test for depth-3 circuits. In IEEE [IEE10], pages 21–29. ISBN 1-4244-8525-8. LCCN ???? URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5669376`. IEEE Computer Society Order Number P4244.

Sopka:2010:BTS

[SS10c] Katherine R. Sopka and Elisabeth M. Sopka. The Bonebrake Theological Seminary: Top-secret Manhattan Project site. *Physics in Perspective (PIP)*, 12(3):338–349, September 2010. CODEN PHPEF2. ISSN 1422-6944 (print), 1422-6960 (electronic). URL `http://link.springer.com/article/10.1007/s00016-010-0019-4`.

Szaban:2011:IQB

[SS11] Miroslaw Szaban and Franciszek Seredynski. Improving quality of DES S-boxes by cellular automata-based S-boxes. *The Journal of Supercomputing*, 57(2):216–226, August 2011. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=57&issue=2&spage=216`.

Saxena:2012:BIT

[SS12a] Nitin Saxena and C. Seshadhri. Blackbox identity testing for bounded top-fanin depth-3 circuits: The field doesn't matter. *SIAM Journal on Computing*, 41(5):1285–1298, ???? 2012. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Shparlinski:2012:CSD

[SS12b] Igor E. Shparlinski and Katherine E. Stange. Character sums with division polynomials. *Bulletin canadien de mathématiques = Canadian Mathematical Bulletin*, 55(4):850–??, December 2012. CODEN CMBUA3. ISSN 0008-4395

(print), 1496-4287 (electronic).

Sendrier:2013:HCE

[SS13] Nicolas Sendrier and Dimitris E. Simos. The hardness of code equivalence over $\mathbf{F}_q$ and its application to code-based cryptography. *Lecture Notes in Computer Science*, 7932: 203–216, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-38616-9_14/.

Singh:2015:EST

[SS15] Dilraj Singh and Amardeep Singh. Enhanced secure trusted AODV (ESTA) protocol to mitigate blackhole attack in mobile ad hoc networks. *Future Internet*, 7(3):342–362, September 23, 2015. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/7/3/342.

Sadhya:2017:PRE

[SS17a] Debanjan Sadhya and Sanjay Kumar Singh. Privacy risks ensuing from cross-matching among databases: a case study for soft biometrics. *Information Processing Letters*, 128(??):38–45, December 2017. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019017301436.

Shivani:2017:RIE

[SS17b] J. L. Divya Shivani and Ranjan K. Senapati. Robust image embedded watermarking using DCT and listless SPIHT. *Future Internet*, 9(3):33, July 12, 2017. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/9/3/33.

Siegel:2019:UOC

[SS19] J. E. Siegel and S. Sarma. Using open channels to trigger the invited, unintended consequences of the Internet of Things. *IEEE Security & Privacy*, 17 (3):49–55, May/June 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Singh:2013:QBF

[SSA13] Durgesh Singh, Shivendra Shivani, and Suneeta Agarwal. Quantization-based fragile watermarking using block-wise authentication and pixel-wise recovery scheme for tampered image. *International Journal of Image and Graphics (IJIG)*, 13(2), April 2013. CODEN ???? ISSN 0219-4678.

Smith:2011:SMC

[SSAF11] Matthew Smith, Christian Schridde, Björn Agel, and Bernd Freisleben. Secure mobile communication via identity-based cryptography and server-aided computations. *The Journal of Supercomputing*, 55(2):284–306, February 2011. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=55&issue=2&spage=284.

Sakai:2016:NCS

[SSKL16] K. Sakai, M. Sun, W. Ku, and T. H. Lai. A novel coding scheme for secure communications in distributed RFID systems. *IEEE Transactions on Computers*, 65(2):409–421, February 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Shahandashti:2015:RUP

[SSNS15] Siamak F. Shahandashti, Reihaneh Safavi-Naini, and Nashad Ahmed Safa. Reconciling user privacy and implicit authentication for mobile devices. *Computers & Security*, 53(??):215–233, September 2015. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404815000838.

Sundararajan:2019:SMC

[SSP19] Aditya Sundararajan, Arif I. Sarwat, and Alexander Pons. A survey on modality characteristics, performance evaluation metrics, and security for traditional and wearable biometric systems. *ACM Computing Surveys*, 52(2):39:1–39:??, May 2019. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3309550.

Shrivastava:2012:UIE

[SSPC12] Swapnil Shrivastava, Zia Saquib, Gopinath P., and Peeyush Chomal. Unique identity enabled service delivery through NSDG. *Lecture Notes in Computer Science*, 7452: 103–111, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32701-8_10/.

Strydis:2013:SAP

[SSPL+13] Christos Strydis, Robert M. Seepers, Pedro Peris-Lopez, Dimitrios Siskos, and Ioannis Sourdis. A system architecture, processor, and communication protocol for secure implants. *ACM Transactions on Architecture and Code Optimization*, 10(4):57:1–57:??, December 2013. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic).

Sood:2011:SDI

[SSS11] Sandeep K. Sood, Anil K. Sarje, and Kuldip Singh. A secure dynamic identity based authentication protocol for multi-server architecture. *Journal of Network and Computer Applications*, 34(2):609–618, March 2011. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804510002092.

Saadeh:2018:HAP

[SSSA18] Maha Saadeh, Azzam Sleit, Khair Eddin Sabri, and Wesam Almobaideen. Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities. *Journal of Network and Computer Applications*, 121(??):1–19, November 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518302339.

Spiez:2012:RCT

[SSU12] Stanisław Spież, Marian Srebrny, and Jerzy Urbanowicz. Remarks on the classical threshold secret sharing schemes. *Fundamenta Informaticae*, 114(3–4):345–357, August 2012. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Sahai:2012:DCC

[SSW12] Amit Sahai, Hakan Seyalioglu, and Brent Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. *Lecture Notes in Computer Science*, 7417: 199–217, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32009-5_13/.

Schaffer:2012:EII

[SSY12] J. S. Schaffer, M. L. Stokes, and N. Yan. Enabling an integrated identity from disparate sources. *IBM Journal of Research and Development*, 56(6):6:1–6:10, ???? 2012. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6355654.

Schillewaert:2014:CCA

[ST14] Jeroen Schillewaert and Koen Thas. Construction and comparison of authentication codes. *SIAM Journal on Discrete Mathematics*, 28(1):474–489, ???? 2014. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Shrestha:2015:CIS

[ST15] Ajaya Shrestha and Arun Timalsina. Color image steganography technique using Daubechies discrete wavelet transform. In *2015 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, December 2015.

Shen:2016:RMM

[ST16] Wuqiang Shen and Shaohua Tang. RGB, a mixed multivariate signature scheme. *The Computer Journal*, 59(4):439–451, April 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/59/4/439`.

Sethumadhavan:2019:SA

[ST19] S. Sethumadhavan and M. Tiwari. Secure architectures. *IEEE Micro*, 39 (4):6–7, July/August 2019. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Stallings:2011:C

[Sta11a] William Stallings. Ciphers. *WIREs Computational Statistics*, 3(5):239–250, May/June 2011. CODEN ???? ISSN 1939-0068 (print), 1939-5108 (electronic).

Stallings:2011:CNS

[Sta11b] William Stallings. *Cryptography and network security: principles and practice*. Prentice-Hall, Inc., Upper Saddle River, NJ 07458, USA, fifth edition, 2011. ISBN 0-13-609704-9. xxiii + 719 pp. LCCN TK5105.59 .S713 2011.

Stanoyevitch:2011:ICM

[Sta11c] Alexander Stanoyevitch. *Introduction to cryptography with mathematical foundations and computer implementations*. Discrete mathematics and its applications. Chapman and Hall/CRC, Boca Raton, FL, USA, 2011. ISBN 1-4398-1763-4 (hardcover). xix + 649 pp. LCCN QA268 .S693 2011.

Stanek:2012:TEM

[Sta12] Martin Stanek. Threshold encryption into multiple ciphertexts. *Lecture Notes in Computer Science*, 6888:62–72, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27901-0_6/.

Staff:2013:ITD

[Sta13] S. Staff. Inside TAO: Documents reveal top NSA hacking unit. *Der Spiegel*, ??(??):??, December 29, 2013. URL http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html.

Stewart:2011:CCI

[STC11] James Michael Stewart, Ed Tittel, and Mike Chapple. *CISSP: Certified Information Systems Security Professional Study Guide*. John Wiley and Sons, Inc., New York, NY, USA, fifth edition, 2011. ISBN 0-470-94498-6. ???? pp. LCCN QA76.3 .T5735 2011. URL http://catalogimages.wiley.com/images/db/jimages/9780470944981.jpg.

Steel:2015:APF

[Ste15a] Graham Steel. Automated proof and flaw-finding tools in cryptography. *IEEE Security & Privacy*, 13(2):81–83, March/April 2015. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://www.computer.org/csdl/mags/sp/2015/02/msp2015020081-abs.html.

Stenn:2015:SNT

[Ste15b] Harlan Stenn. Securing Network Time Protocol. *Communications of the Association for Computing Machinery*, 58(2):48–51, February 2015. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2015/2/182654/fulltext.

Stipcevic:2011:QRN

[Sti11] M. Stipcevic. Quantum random number generators and their use in cryptography. In *2011 Proceedings of the 34th International Convention MIPRO*, pages 1474–1479. 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=5967293.

Stickney:2015:CBS

[Sti15] Zephorene Stickney. Code breakers: The secret service. *Wheaton Quarterly*, ??(??):??, Summer 2015. URL https://wheatoncollege.edu/

news/code-breakers-secret-service/.

Stiles:2019:HSB

[Sti19] D. Stiles. The hardware security behind Azure Sphere. *IEEE Micro*, 39(2):20–28, March/April 2019. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Stolte:2012:EDA

[Sto12] Daniel Stolte. Experts determine age of book 'nobody can read'. *UANews*, February 11, 2012. URL http://uanews.org/node/37825; http://www.rdmag.com/News/2011/02/Materials-Testing-Experts-determine-age-of-book-nobody-can-read/.

Suciu:2012:SED

[Suc12] Dan Suciu. SQL on an encrypted database: technical perspective. *Communications of the Association for Computing Machinery*, 55(9):102, September 2012. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Sung:2011:DCE

[Sun11] Jaechul Sung. Differential cryptanalysis of eight-round SEED. *Information Processing Letters*, 111(10):474–478, April 30, 2011. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Sun:2016:NEB

[Sun16] Shuliang Sun. A novel edge based image steganography with 2^k correction and Huffman encoding. *Information Processing Letters*, 116(2):93–99, February 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019015001738.

Shen:2015:CSC

[SVCV15] Emily Shen, Mayank Varia, Robert K. Cunningham, and W. Konrad Vesey. Cryptographically secure computation. *Computer*, 48(4):78–81, April 2015. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/csdl/mags/co/2015/04/mco2015040078-abs.html.

Song:2016:IAR

[SVG16] Yang Song, Arun Venkataramani, and Lixin Gao. Identifying and addressing reachability and policy attacks in "Secure" BGP. *IEEE/ACM Transactions on Networking*, 24(5):2969–2982, October 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Shmueli:2014:IDE

[SVGE14] Erez Shmueli, Ronen Vaisenberg, Ehud Gudes, and Yuval Elovici. Implementing a database encryption solution, design and implementation issues. *Computers & Security*, 44(??):33–50, July 2014. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404814000509`.

Svozil:2014:NCC

[Svo14] Karl Svozil. Non-contextual chocolate balls versus value indefinite quantum cryptography. *Theoretical Computer Science*, 560 (part 1)(??):82–90, December 4, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397514006975`.

Svaba:2010:PKC

[SvT10] Pavol Svaba and Tran van Trung. Public key cryptosystem MST_1tn3: cryptanalysis and realization. Technical report 2010,2, Institut für Experimentelle Mathematik, Universität Duisburg-Essen, Duisburg, Germany, 2010. 37 pp.

ShanmugaPriya:2019:PAS

[SVY19] S. ShanmugaPriya, A. Valarmathi, and D. Yuvaraj. The personal authentication service and security enhancement for optimal strong password. *Concurrency and Computation: Practice and Experience*, 31(14):e5009:1–e5009:??, July 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Shi:2019:LWW

[SWF+19] Y. Shi, W. Wei, H. Fan, M. H. Au, and X. Luo. A light-weight white-box encryption scheme for securing distributed embedded devices. *IEEE Transactions on Computers*, 68 (10):1411–1427, October 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Shoufan:2010:NCA

[SWM+10] A. Shoufan, T. Wink, H. G. Molter, S. A. Huss, and E. Kohnert. A novel cryptoprocessor architecture for the McEliece public-key cryptosystem. *IEEE Transactions on Computers*, 59(11):1533–1546, November 2010. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/`

stamp/stamp.jsp?tp=&arnumber=5477413.

Song:2016:IBS

[SWW+16] Lingwei Song, Jinxia Wei, Licheng Wang, Chenlei Cao, and Xinxin Niu. Identity-based storage management and integrity verify protocol for secure outsourcing in multi-cloud. *Concurrency and Computation: Practice and Experience*, 28(6):1930–1945, April 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Song:2017:PPF

[SWW+17] Wei Song, Bing Wang, Qian Wang, Zhiyong Peng, Wenjing Lou, and Yihui Cui. A privacy-preserved full-text retrieval algorithm over encrypted data for cloud storage applications. *Journal of Parallel and Distributed Computing*, 99(??):14–27, January 2017. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731516300533.

Sheldon:2012:IWN

[SWYP12] Frederick T. Sheldon, John Mark Weber, Seong-Moo Yoo, and W. David Pan. The insecurity of wireless networks. *IEEE Security & Privacy*, 10(4):54–61, July/August 2012. ISSN 1540-7993 (print), 1558-4046 (electronic).

Sha:2019:CED

[SXH+19] Le-Tian Sha, Fu Xiao, Hai-Ping Huang, Yu Chen, and Ru-Chuan Wang. Catching escapers: a detection method for advanced persistent escapers in industry Internet of Things based on identity-based broadcast encryption (IBBE). *ACM Transactions on Embedded Computing Systems*, 18(3):29:1–29:??, June 2019. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3319615.

Su:2016:PSN

[SXL16] Shenghui Su, Tao Xie, and Shuwang Lü. A provably secure non-iterative hash function resisting birthday attack. *Theoretical Computer Science*, 654(??):128–142, November 22, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397516001547.

Sahillioglu:2014:SCM

[SY14] Y. Sahillioğlu and Y. Yemez. Shapes and cryptography: Multiple shape correspondence by dynamic programming. *Computer Graphics Forum*, 33 (7):121–130, October 2014. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Savas:2015:GMA

[SY15a] Erkay Savaş and Cemal Yılmaz. A generic method for the analysis of a class of cache attacks: a case study for AES. *The Computer Journal*, 58(10):2716–2737, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/10/2716`.

Shao:2015:SAS

[SY15b] Zhi-Yi Shao and Bo Yang. On security against the server in designated tester public key encryption with keyword search. *Information Processing Letters*, 115(12):957–961, December 2015. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019015001283`.

Song:2017:SSI

[SYC+17] Jun Song, Fan Yang, Kim-Kwang Raymond Choo, Zhijian Zhuang, and Lizhe Wang. SIPF: a secure installment payment framework for drive-thru Internet. *ACM Transactions on Embedded Computing Systems*, 16(2):52:1–52:??, April 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Seo:2013:PIC

[SYL13] Jae Woo Seo, Dae Hyun Yum, and Pil Joong Lee. Proxy-invisible CCA-secure type-based proxy re-encryption without random oracles. *Theoretical Computer Science*, 491(??):83–93, June 17, 2013. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397512010560`.

SoltaniPanah:2019:CDG

[SYv+19] A. Soltani Panah, A. Yavari, R. van Schyndel, D. Georgakopoulos, and X. Yi. Context-driven granular disclosure control for Internet of Things applications. *IEEE Transactions on Big Data*, 5(3):408–422, September 2019. ISSN 2332-7790.

Song:2017:SAM

[SYW17] Jun Song, Fan Yang, and Lizhe Wang. Secure authentication in motion: a novel online payment framework for drive-thru Internet. *Future Generation Computer Systems*, 76(??):146–158, November 2017. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16301960.

Shuai:2019:AAS

[SYWX19] Mengxia Shuai, Nenghai Yu, Hongxia Wang, and Ling Xiong. Anonymous authentication scheme for smart home environment with provable security. *Computers & Security*, 86(??):132–146, September 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818313701.

Shen:2017:RDP

[SYY+17] Wenting Shen, Guangyang Yang, Jia Yu, Hanlin Zhang, Fanyu Kong, and Rong Hao. Remote data possession checking with privacy-preserving authenticators for cloud storage. *Future Generation Computer Systems*, 76(??):136–145, November 2017. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16304939.

Sui:2014:DAH

[SZDL14] Yan Sui, Xukai Zou, Eliza Y. Du, and Feng Li. Design and analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method. *IEEE Transactions on Computers*, 63 (4):902–916, April 2014. CODEN ITCOB4. ISSN 0018-9340.

Shah:2019:PCB

[SZHY19] Mohsin Shah, Weiming Zhang, Honggang Hu, and Nenghai Yu. Paillier cryptosystem based mean value computation for encrypted domain image processing operations. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 15(3):76:1–76:??, September 2019. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3325194.

Shi:2013:REA

[SZMK13] Qi Shi, Ning Zhang, Madjid Merabti, and Kashif Kifayat. Resource-efficient authentic key establishment in heterogeneous wireless sensor networks. *Journal of Parallel and Distributed Computing*, 73(2):235–249, February 2013. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://

www.sciencedirect.com/science/article/pii/S0743731512002547.

Sun:2017:CPP

[SZQ+17] Jiameng Sun, Binrui Zhu, Jing Qin, Jiankun Hu, and Qianhong Wu. Confidentiality-preserving publicly verifiable computation. *International Journal of Foundations of Computer Science (IJFCS)*, 28(6):799–??, September 2017. CODEN IFCSEN. ISSN 0129-0541.

Shen:2014:ERC

[SZS14] Limin Shen, Futai Zhang, and Yinxia Sun. Efficient revocable certificateless encryption secure in the standard model. *The Computer Journal*, 57(4):592–601, April 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/57/4/592.full.pdf+html.

Sun:2018:RPP

[SZZT18] Weiwei Sun, Jiantao Zhou, Shuyuan Zhu, and Yuan Yan Tang. Robust privacy-preserving image sharing over online social networks (OSNs). *ACM Transactions on Multimedia Computing, Communications, and Applications*, 14(1):14:1–14:??, January 2018. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Tsang:2010:BRR

[TAKS10] Patrick P. Tsang, Man Ho Au, Apu Kapadia, and Sean W. Smith. BLAC: Revoking repeatedly misbehaving anonymous users without relying on TTPs. *ACM Transactions on Information and System Security*, 13(4):39:1–39:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Tamayo:2015:AFH

[Tam15] Matthew Tamayo. Algebraic full homomorphic encryption and resisting Gröbner basis cryptanalysis. *ACM Communications in Computer Algebra*, 49 (2):63, June 2015. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Tan:2011:CTA

[Tan11] Zuowen Tan. Comments on a threshold authenticated encryption scheme. *International Journal of Computer Applications*, 33(2): 132–136, 2011. ISSN 1206-212X (print), 1925-7074 (electronic). URL https://www.tandfonline.com/doi/full/10.2316/Journal.202.2011.2.202-2858.

Tan:2012:SLM

[Tan12a] Shunquan Tan. Steganalysis of LSB matching revisited for consecutive pixels using B-spline functions. *Lecture Notes in Computer Science*, 7128:16–29, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32205-1_4/.

Tan:2012:LCP

[Tan12b] Zuowen Tan. A lightweight conditional privacy-preserving authentication and access control scheme for pervasive computing environments. *Journal of Network and Computer Applications*, 35(6):1839–1846, November 2012. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804512001609.

Tang:2015:ETE

[Tan15a] Qiang Tang. From ephemerizer to timed-ephemerizer: Achieve assured lifecycle enforcement for sensitive data. *The Computer Journal*, 58(4):1003–1020, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/1003.

Tang:2015:HAC

[Tan15b] Zhaohui Tang. Homomorphic authentication codes for network coding. *Concurrency and Computation: Practice and Experience*, 27(15):3892–3911, October 2015. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Tankard:2017:BNK

[Tan17a] Colin Tankard. BYOE: New kid on the block. *Network Security*, 2017(11):20, November 2017. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S135348581730096X.

Tankard:2017:ECB

[Tan17b] Colin Tankard. Encryption as the cornerstone of big data security. *Network Security*, 2017(3):5–7, March 2017. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485817300259.

Tankard:2018:LAA

[Tan18] Colin Tankard. A layered approach to authentication. *Network Security*, 2018(12):20, December 2018. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485818301284.

Toth:2019:SSD

[TAP19] K. C. Toth and A. Anderson-Priddy. Self-sovereign digital identity: A paradigm shift for identity. *IEEE Security & Privacy*, 17(3):17–27, May/June 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Tarnovsky:2010:DSP

[Tar10] Christopher Tarnovsky. Deconstructing a secure processor. BlackHat Briefings, 2010.

Taylor:2014:WSE

[Tay14] Dave Taylor. Work the shell: easy watermarking with ImageMagick. *Linux Journal*, 2014(237): 6:1–6:??, January 2014. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Taylor:2017:EBH

[Tay17] Michael Bedford Taylor. The evolution of Bitcoin hardware. *Computer*, 50 (9):58–66, September 2017. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL https://www.computer.org/csdl/mags/co/2017/09/mco2017090058-abs.html.

Taylor:2019:DST

[Tay19] Adrian Taylor. Decrypting SSL traffic: best practices for security, compliance and productivity. *Network Security*, 2019(8):17–19, August 2019. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485819300984.

Talbi:2018:SIW

[TB18] Mourad Talbi and Med Salim Bouhlel. Secure image watermarking based on LWT and SVD. *International Journal of Image and Graphics (IJIG)*, 18 (4):??, October 2018. ISSN 0219-4678. URL https://www.worldscientific.com/doi/10.1142/S0219467818500213.

Tilli:2015:GCR

[TBCB15] Andrea Tilli, Andrea Bartolini, Matteo Cacciari, and Luca Benini. Guaranteed computational resprinting via model-predictive control. *ACM Transactions on Embedded Computing Systems*, 14 (3):48:1–48:??, April 2015. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Turan:2018:RES

[TBK+18] Meltem Sönmez Turan, Elaine Barker, John Kelsey, Kerry A. McKay, Mary L. Baish, and Mike Boyle. Recommendation for the entropy sources used for random bit generation. NIST Special Publication 800-90B, National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg, MD, USA, January 2018. URL `https://csrc.nist.gov/publications/detail/sp/800-90b/final`.

Takagi:2019:ISC

[TBL19] Naofumi Takagi, Sylvie Boldo, and Martin Langhammer, editors. *2019 IEEE 26th Symposium on Computer Arithmetic ARITH-26 (2019), Kyoto, Japan, 10–12 June 2019*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, June 2019. ISBN 1-72813-366-1. ISSN 1063-6889.

Treleaven:2017:BTF

[TBY17] Philip Treleaven, Richard Gendal Brown, and Danny Yang. Blockchain technology in finance. *Computer*, 50(9):14–17, September 2017. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `https://www.computer.org/csdl/mags/co/2017/09/mco2017090014.html`.

Tuan:2010:AWB

[TC10] Do Van Tuan and Ui-Pil Chong. Audio watermarking based on advanced Wigner distribution and important frequency peaks. *The International Journal of High Performance Computing Applications*, 24(2):154–163, May 2010. CODEN IHPCFL. ISSN 1094-3420 (print), 1741-2846 (electronic). URL `http://hpc.sagepub.com/content/24/2/154.full.pdf+html`.

Taylor:2011:DR

[TC11] Greg Taylor and George Cox. Digital randomness. *IEEE Spectrum*, 48(9):32–58, September 2011. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic). URL `http://spectrum.ieee.org/semiconductors/processors/behind-intels-new-randomnumber-generator/`.

Tang:2015:CER

[TCL15] Ying-Kai Tang, Sherman S. M. Chow, and Joseph K. Liu. Comments on 'Efficient Revocable Certificateless Encryption Secure in the Standard Model'. *The Computer Journal*, 58(4):779–781, April 2015. CODEN

CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/779.

Testa:2019:SFE

[TCMLN19] Rafael Luiz Testa, Cléber Gimenez Corrêa, Ariane Machado-Lima, and Fátima L. S. Nunes. Synthesis of facial expressions in photographs: Characteristics, approaches, and challenges. *ACM Computing Surveys*, 51(6):124:1–124:??, February 2019. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3292652.

Tan:2017:JDC

[TCN+17] Rui Tan, Sheng-Yuan Chiu, Hoang Hai Nguyen, David K. Y. Yau, and Deokwoo Jung. A joint data compression and encryption approach for wireless energy auditing networks. *ACM Transactions on Sensor Networks*, 13(2):9:1–9:??, June 2017. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Tian:2014:DFS

[TCS14] Haibo Tian, Xiaofeng Chen, and Willy Susilo. Deniability and forward secrecy of one-round authenticated key exchange. *The Journal of Supercomputing*, 67(3):671–690, March 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-013-0968-x.

Tiplea:2014:NSC

[TD14] Ferucio Laurentiu Tiplea and Constantin Catalin Dragan. A necessary and sufficient condition for the asymptotic idealness of the GRS threshold secret sharing scheme. *Information Processing Letters*, 114(6):299–303, June 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019014000179.

Tao:2013:SMS

[TDTD13] Chengdong Tao, Adama Diene, Shaohua Tang, and Jintai Ding. Simple matrix scheme for encryption. *Lecture Notes in Computer Science*, 7932:231–242, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-38616-9_16/.

Teng:2018:KPA

[Ten18] Sheng-Hua Teng. 2018

Knuth Prize is awarded to Johan Håstad. *ACM SIGACT News*, 49(3):78–79, September 2018. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Terai:2011:BRB

[Ter11] Saif Terai. Book review: *Foundations of Logic and Mathematics Applications to Computer Science and Cryptography*, by Yves Nievergelt. *ACM SIGACT News*, 42(4):17–21, December 2011. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [Nie02].

Tseng:2019:AMR

[TFS19] Yi-Fan Tseng, Chun-I Fan, and Cheng-Wei Sung. On the anonymity of multi-receiver identity-based encryption based on Fujisaki–Okamoto transformation. *International Journal of Foundations of Computer Science (IJFCS)*, 30(4): 493–509, June 2019. ISSN 0129-0541. URL `https://www.worldscientific.com/doi/10.1142/S0129054119400094`.

Tassa:2012:SDC

[TG12] Tamir Tassa and Ehud Gudes. Secure distributed computation of anonymized views of shared databases. *ACM Transactions on Database Systems*, 37(2):11:1–11:??, May 2012. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Tewari:2017:CNU

[TG17] Aakanksha Tewari and B. B. Gupta. Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *The Journal of Supercomputing*, 73(3): 1085–1102, March 2017. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Theofanos:2016:SUE

[TGC16] Mary Theofanos, Simson Garfinkel, and Yee-Yin Choong. Secure and usable enterprise authentication: Lessons from the field. *IEEE Security & Privacy*, 14(5):14–21, September/October 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL `https://www.computer.org/csdl/mags/sp/2016/05/msp2016050014-abs.html`.

Tian:2016:IBS

[TH16] Miaomiao Tian and Liusheng Huang. Identity-based signatures from lattices: Simpler, faster, shorter. *Fundamenta Informaticae*, 145

(2):171–187, ???? 2016. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Toledo:2013:DFS

[THA+13] Nerea Toledo, Marivi Higuero, Jasone Astorga, Marina Aguado, and Jean Marie Bonnin. Design and formal security evaluation of NeMHIP: a new secure and efficient network mobility management protocol based on the host identity protocol. *Computers & Security*, 32(??):1–18, February 2013. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404812001599.

Tian:2015:IBP

[Tia15] Miaomiao Tian. Identity-based proxy re-signatures from lattices. *Information Processing Letters*, 115(4): 462–467, April 2015. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S002001901400266X.

Tian:2012:TOE

[TJZF12] Hui Tian, Hong Jiang, Ke Zhou, and Dan Feng. Transparency-orientated encoding strategies for Voice-over-IP steganography. *The Computer Journal*, 55(6):702–716, June 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/55/6/702.full.pdf+html.

Thabit:2014:RRW

[TK14] Rasha Thabit and Bee Ee Khoo. Robust reversible watermarking scheme using Slantlet transform matrix. *The Journal of Systems and Software*, 88(??):74–86, February 2014. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121213002380.

Takayasu:2019:PKE

[TK19] Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on RSA: Achieving the Boneh–Durfee bound. *Theoretical Computer Science*, 761(??):51–77, February 21, 2019. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397518305371.

Tuna:2017:SIS

[TKG+17] Gurkan Tuna, Dimitrios G. Kogias, V. Cagri Gungor, Cengiz Gezer, Erhan

Taskin, and Erman Ayday. A survey on information security threats and solutions for Machine to Machine (M2M) communications. *Journal of Parallel and Distributed Computing*, 109(??):142–154, November 2017. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731517301867`.

Tu:2014:EPB

[TKHK14] Hang Tu, Neeraj Kumar, Debiao He, and Jongsung Kim. An efficient password-based three-party authenticated multiple key exchange protocol for wireless mobile networks. *The Journal of Supercomputing*, 70(1): 224–235, October 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://link.springer.com/article/10.1007/s11227-014-1198-6`.

Tani:2012:EQA

[TKM12] Seiichiro Tani, Hirotada Kobayashi, and Keiji Matsumoto. Exact quantum algorithms for the leader election problem. *ACM Transactions on Computation Theory*, 4(1):1:1–1:??, March 2012. CODEN ???? ISSN 1942-3454 (print), 1942-3462 (electronic).

Tu:2013:PAQ

[TKMZ13] Stephen Tu, M. Frans Kaashoek, Samuel Madden, and Nickolai Zeldovich. Processing analytical queries over encrypted data. *Proceedings of the VLDB Endowment*, 6(5): 289–300, March 2013. CODEN ???? ISSN 2150-8097.

Tariq:2014:SBL

[TKR14] Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel. Securing broker-less publish/subscribe systems using identity-based encryption. *IEEE Transactions on Parallel and Distributed Systems*, 25(2):518–528, February 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Tan:2016:ESE

[TLCF16] Jingweijia Tan, Zhi Li, Mingsong Chen, and Xin Fu. Exploring soft-error robust and energy-efficient register file in GPGPUs using resistive memory. *ACM Transactions on Design Automation of Electronic Systems*, 21(2):34:1–34:??, January 2016. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Tsaur:2012:ESM

[TLL12] Woei-Jiunn Tsaur, Jia-Hong Li, and Wei-Bin Lee. An efficient and secure multi-server authentication scheme with key agreement. *The Journal of Systems and Software*, 85(4):876–882, April 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211002810.

Tsai:2013:ZWS

[TLL13] Hung-Hsu Tsai, Yen-Shou Lai, and Shih-Che Lo. A zero-watermark scheme with geometrical invariants using SVM and PSO against geometrical attacks for image protection. *The Journal of Systems and Software*, 86(2):335–348, February 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212002440.

Tetali:2013:MSA

[TLMM13] Sai Deep Tetali, Mohsen Lesani, Rupak Majumdar, and Todd Millstein. MrCrypt: static analysis for secure cloud computations. *ACM SIGPLAN Notices*, 48(10):271–286, October 2013. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). OOPSLA '13 conference proceedings.

Tang:2012:RSS

[TLW12] Zhaohui Tang, Hoon Wei Lim, and Huaxiong Wang. Revisiting a secret sharing approach to network codes. *Lecture Notes in Computer Science*, 7496: 300–317, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33272-2_20/.

Tian:2017:RSP

[TLZ+17] Z. Tian, T. Liu, Q. Zheng, E. Zhuang, M. Fan, and Z. Yang. Reviving sequential program birthmarking for multithreaded software plagiarism detection. *IEEE Transactions on Software Engineering*, PP(99):1, ???? 2017. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7888597.

Tsay:2012:VUL

[TM12] Joe-Kai Tsay and Stig F. Mjølsnes. A vulnerability in the UMTS and LTE authentication and key agreement protocols. *Lecture*

Notes in Computer Science, 7531:65–76, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33704-8_6/.

Tsoutsos:2018:EDM

[TM18] Nektarios Georgios Tsoutsos and Michail Maniatakos. Efficient detection for malicious and random errors in additive encrypted computation. *IEEE Transactions on Computers*, 67(1):16–31, January 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/document/7967774/.

Tang:2015:ECP

[TMC15] Qiang Tang, Hua Ma, and Xiaofeng Chen. Extend the concept of public key encryption with delegated search. *The Computer Journal*, 58(4):724–734, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/724.

Tormo:2013:IMP

[TMGP13] Gines Dolera Tormo, Felix Gomez Marmol, Joao Girao, and Gregorio Martinez Perez. Identity management — in privacy we trust: Bridging the trust gap in eHealth environments. *IEEE Security & Privacy*, 11(6):34–41, November/December 2013. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Terrovitis:2011:LGR

[TMK11] Manolis Terrovitis, Nikos Mamoulis, and Panos Kalnis. Local and global recoding methods for anonymizing set-valued data. *VLDB Journal: Very Large Data Bases*, 20(1):83–106, February 2011. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Terrovitis:2012:PPD

[TMLS12] Manolis Terrovitis, Nikos Mamoulis, John Liagouris, and Spiros Skiadopoulos. Privacy preservation by disassociation. *Proceedings of the VLDB Endowment*, 5(10):944–955, June 2012. CODEN ???? ISSN 2150-8097.

Tao:2018:AAC

[TODQ18] Ming Tao, Kaoru Ota, Mianxiong Dong, and Zhuzhong Qian. AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks.

Journal of Parallel and Distributed Computing, 118 (part 1)(??):107–117, August 2018. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0743731517302587.

Tomb:2016:AVR

[Tom16] Aaron Tomb. Automated verification of real-world cryptographic implementations. *IEEE Security & Privacy*, 14(6):26–33, November/December 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/06/msp2016060026-abs.html.

Toxen:2014:NSS

[Tox14] Bob Toxen. The NSA and Snowden: securing the all-seeing eye. *Communications of the Association for Computing Machinery*, 57 (5):44–51, May 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Tsougenis:2012:PEM

[TPKT12] E. D. Tsougenis, G. A. Papakostas, D. E. Koulouriotis, and V. D. Tourassis. Performance evaluation of moment-based watermarking methods: a review. *The Journal of Systems and Software*, 85(8):1864–1884, August 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212000684.

Tan:2016:BIB

[TPL16] Chik How Tan, Theo Fanuela Prabowo, and Duc-Phong Le. Breaking an ID-based encryption based on discrete logarithm and factorization problems. *Information Processing Letters*, 116(2):116–119, February 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019015001696.

Tang:2014:PAB

[TQL+14] Ming Tang, Zhenlong Qiu, Weijie Li, Weijin Sun, Xiaobo Hu, and Huanguo Zhang. Power analysis based reverse engineering on the secret round function of block ciphers. *Concurrency and Computation: Practice and Experience*, 26(8):1531–1545, June 10, 2014. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Taylor:2011:CAS

[TRD11] Ken Taylor, Scott Rickard,

and Konstantinos Drakakis. Costas arrays: Survey, standardization, and MATLAB toolbox. *ACM Transactions on Mathematical Software*, 37(4):41:1–41:31, February 2011. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Tezcan:2016:IID

[TS16a] Cihangir Tezcan and Ali Aydin Selçuk. Improved improbable differential attacks on ISO standard CLEFIA: Expansion technique revisited. *Information Processing Letters*, 116(2):136–143, February 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019015001659`.

Tschorsch:2016:BBT

[TS16b] F. Tschorsch and B. Scheuermann. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys Tutorials*, 18(3):2084–2123, Third Quarter 2016. ISSN 1553-877X.

Taassori:2018:VRP

[TSB18] Meysam Taassori, Ali Shafiee, and Rajeev Balasubramonian. VAULT: Reducing paging overheads in SGX with efficient integrity verification structures. *ACM SIGPLAN Notices*, 53(2):665–678, February 2018. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Tao:2014:CFS

[TSH14] Jia Tao, Giora Slutzki, and Vasant Honavar. A conceptual framework for secrecy-preserving reasoning in knowledge bases. *ACM Transactions on Computational Logic*, 16(1):3:1–3:??, December 2014. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic).

Toreini:2017:TRP

[TSH17] Ehsan Toreini, Siamak F. Shahandashti, and Feng Hao. Texture to the rescue: Practical paper fingerprinting based on texture patterns. *ACM Transactions on Privacy and Security (TOPS)*, 20(3):9:1–9:??, August 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic).

Tang:2011:IDC

[TSLL11] Xuehai Tang, Bing Sun, Ruilin Li, and Chao Li. Impossible differential cryptanalysis of 13-round CLEFIA-128. *The Journal of Systems and*

Software, 84(7):1191–1196, July 2011. CODEN JSSODM. ISSN 0164-1212.

Tso:2013:SAI

[Tso13] Raylin Tso. Security analysis and improvements of a communication-efficient three-party password authenticated key exchange protocol. *The Journal of Supercomputing*, 66(2): 863–874, November 2013. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-013-0917-8.

Tseng:2012:ERI

[TT12] Yuh-Min Tseng and Tung-Tso Tsai. Efficient revocable ID-based encryption with a public channel. *The Computer Journal*, 55(4):475–486, April 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/55/4/475.full.pdf+html.

Tenca:2018:PIS

[TT18] Alexandre Tenca and Naofumi Takagi, editors. *Proceedings of the 25th International Symposium on Computer Arithmetic, 25–27 June 2018 Amherst, MA, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, June 2018. ISBN 1-5386-2612-8 (USB), 1-5386-2665-9. ISSN 2576-2265. LCCN QA76.9.C62. IEEE catalog number CFP18121-USB.

Tseng:2015:LFI

[TTH15] Yuh-Min Tseng, Tung-Tso Tsai, and Sen-Shan Huang. Leakage-free ID-based signature. *The Computer Journal*, 58(4):750–757, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/750.

Tsai:2010:RLI

[TTL10] H.-H. Tsai, H.-C. Tseng, and Y.-S. Lai. Robust lossless image watermarking based on α-trimmed mean algorithm and support vector machine. *The Journal of Systems and Software*, 83(6):1015–1028, June 2010. CODEN JSSODM. ISSN 0164-1212.

Turing:2018:XYZ

[Tur18] Dermot Turing. *X, Y and Z: the Real Story of How Enigma Was Broken*. The History Press, Gloucestershire, UK, 2018. ISBN 0-7509-8782-0 (hardcover), 0-7509-8967-X (ePub). 319 + 1 pp. LCCN D810.C88 T87 2018.

Tupakula:2015:TES

[TV15] Udaya Tupakula and Vijay Varadharajan. Trust enhanced security for tenant transactions in the cloud environment. *The Computer Journal*, 58 (10):2388–2403, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2388.

Turan:2019:CFF

[TV19] Furkan Turan and Ingrid Verbauwhede. Compact and flexible FPGA implementation of Ed25519 and X25519. *ACM Transactions on Embedded Computing Systems*, 18(3): 24:1–24:??, June 2019. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3312742.

Thorpe:2012:CRB

[TW12] Christopher Thorpe and Steven R. Willis. Cryptographic rule-based trading. *Lecture Notes in Computer Science*, 7397:65–72, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32946-3_6/.

Tripunitara:2014:CKM

[TW14] Mahesh V. Tripunitara and Jeffrey Lok Tin Woo. Composing Kerberos and Multimedia Internet KEYing (MIKEY) for authenticated transport of group keys. *IEEE Transactions on Parallel and Distributed Systems*, 25(4):898–907, April 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Wu:2012:SWG

[tWmC12] Hao tian Wu and Yiu ming Cheung. Secure watermarking on 3D geometry via ICA and orthogonal transformation. *Lecture Notes in Computer Science*, 7110:52–62, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28693-3_4/.

Toor:2018:VQA

[TWNC18] Andeep S. Toor, Harry Wechsler, Michele Nappi, and Kim-Kwang Raymond Choo. Visual question authentication protocol (VQAP). *Computers & Security*, 76(??):285–294, July 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://

www.sciencedirect.com/science/article/pii/S0167404817302547.

Tartary:2011:EIT

[TWZ11] Christophe Tartary, Huaxiong Wang, and Yun Zhang. An efficient and information theoretically secure rational secret sharing scheme based on symmetric bivariate polynomials. *International Journal of Foundations of Computer Science (IJFCS)*, 22 (6):1395–1416, September 2011. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Tian:2012:SSB

[TWZ+12] Huawei Tian, Zheng Wang, Yao Zhao, Rongrong Ni, and Lunming Qin. Spread spectrum-based multi-bit watermarking for free-view video. *Lecture Notes in Computer Science*, 7128: 156–166, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32205-1_14/.

Trost:2016:OPC

[TX16] William R. Trost and Guangwu Xu. On the optimal pre-computation of window NAF for Koblitz curves. *IEEE Transactions on Computers*, 65(9):2918–2924, September 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Tan:2016:CCA

[TY16a] Syh-Yuan Tan and Wun-She Yap. Cryptanalysis of a CP–ABE scheme with policy in normal forms. *Information Processing Letters*, 116(7): 492–495, July 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019016300126.

Tolba:2016:GMA

[TY16b] Mohamed Tolba and Amr M. Youssef. Generalized MitM attacks on full TWINE. *Information Processing Letters*, 116(2):128–135, February 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019015001660.

Trammel:2012:DTP

[TYK+12] John Trammel, Ümit Yalçinalp, Andrei Kalfas, James Boag, and Dan Brotsky. Device token protocol for persistent authentication shared across applications. *Lecture Notes in Computer Science*, 7592: 230–243, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-

3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33427-6_20/.

Tian:2017:ORA

[TYM+17] Yangguang Tian, Guomin Yang, Yi Mu, Shiwei Zhang, Kaitai Liang, and Yong Yu. One-round attribute-based key exchange in the multi-party setting. *International Journal of Foundations of Computer Science (IJFCS)*, 28(6):725–??, September 2017. CODEN IFCSEN. ISSN 0129-0541.

Teh:2016:STD

[TZTC16] Pin Shen Teh, Ning Zhang, Andrew Beng Jin Teoh, and Ke Chen. A survey on touch dynamics authentication in mobile devices. *Computers & Security*, 59(??):210–235, June 2016. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404816300256.

Ehatisham-ul-Haq:2018:CAS

[uHAN+18] Muhammad Ehatisham ul Haq, Muhammad Awais Azam, Usman Naeem, Yasar Amin, and Jonathan Loo. Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. *Journal of Network and Computer Applications*, 109(??):24–35, May 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518300717.

Uzunkol:2018:SWU

[UK18] Osmanbey Uzunkol and Mehmet Sabir Kiraz. Still wrong use of pairings in cryptography. *Applied Mathematics and Computation*, 333(??):467–479, September 15, 2018. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300318302352.

Unruh:2015:RQT

[Unr15] Dominique Unruh. Revocable quantum timed-release encryption. *Journal of the ACM*, 62(6):49:1–49:??, December 2015. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

UlHassan:2019:DPR

[URK+19] Muneeb Ul Hassan, Mubashir Husain Rehmani, Ramamohanarao Kotagiri, Jiekui Zhang, and Jinjun Chen. Differential privacy for renewable energy resources based smart metering. *Journal of Parallel and Distributed Computing*, 131(??):69–80, September 2019. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731518309201.

Ueno:2019:TBP

[USH19] R. Ueno, M. Suzuki, and N. Homma. Tackling biased PUFs through biased masking: a debiasing method for efficient fuzzy extractor. *IEEE Transactions on Computers*, 68 (7):1091–1104, July 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Uto:2013:MRI

[Uto13] Nelson Uto. A methodology for retrieving information from malware encrypted output files: Brazilian case studies. *Future Internet*, 5(2):140–167, April 25, 2013. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/5/2/140.

Ulutas:2011:MIS

[UUN11] Mustafa Ulutas, Güzin Ulutas, and Vasif V. Nabiyev. Medical image security and EPR hiding using Shamir's secret sharing scheme. *The Journal of Systems and Software*, 84 (3):341–353, March 2011. CODEN JSSODM. ISSN 0164-1212.

Ulutas:2013:ISI

[UUN13] Mustafa Ulutas, Güzin Ulutas, and Vasif V. Nabiyev. Invertible secret image sharing for gray level and dithered cover images. *The Journal of Systems and Software*, 86(2):485–500, February 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212002701.

Vaikuntanathan:2011:CBN

[Vai11] V. Vaikuntanathan. Computing blindfolded: New developments in fully homomorphic encryption. In IEEE [IEE11b], pages 5–16. ISBN 1-4577-1843-X. LCCN ????

Vaikuntanathan:2012:HCE

[Vai12] Vinod Vaikuntanathan. How to compute on encrypted data. *Lecture Notes in Computer Science*, 7668:1–15, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34931-7_1/.

Vigil:2015:IAN

[VBC+15] Martín Vigil, Johannes Buchmann, Daniel Cabarcas, Christian Weinert, and Alexander Wiesmaier. Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: a survey. *Computers & Security*, 50(??): 16–32, May 2015. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404814001849.

Venkataramani:2016:DHC

[VCD16] Guru Venkataramani, Jie Chen, and Milos Doroslovacki. Detecting hardware covert timing channels. *IEEE Micro*, 36(5):17–27, September/October 2016. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL https://www.computer.org/csdl/mags/mi/2016/05/mmi2016050017-abs.html.

Valamehr:2012:IRM

[VCK+12] Jonathan Valamehr, Melissa Chase, Seny Kamara, Andrew Putnam, Dan Shumow, Vinod Vaikuntanathan, and Timothy Sherwood. Inspection resistant memory: architectural support for security from physical examination. *ACM SIGARCH Computer Architecture News*, 40(3): 130–141, June 2012. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic). ISCA '12 conference proceedings.

Vatajelu:2016:SMB

[VDB+16] Elena Ioana Vatajelu, Giorgio Di Natale, Mario Barbareschi, Lionel Torres, Marco Indaco, and Paolo Prinetto. STT–MRAM-based PUF architecture exploiting magnetic tunnel junction fabrication-induced variability. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 13(1):5:1–5:??, December 2016. CODEN ???? ISSN 1550-4832.

vandeGraaf:2017:LTT

[vdG17] Jeroen van de Graaf. Long-term threats to ballot privacy. *IEEE Security & Privacy*, 15(3): 40–47, May/June 2017. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2017/03/msp2017030040-abs.html.

vanDam:2011:TQC

[vDKS11] Wim van Dam, Vivian M. Kendon, and Simone Severini, editors. *Theory of quantum computation,* *communication, and cryptography: 5th conference, TQC 2010, Leeds, UK, April 13–15, 2010, revised selected papers*, volume 6519 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011. ISBN 3-642-18072-8 (softcover). LCCN ????

Visegrady:2014:SCV

[VDO14] T. Visegrady, S. Dragone, and M. Osborne. Stateless cryptography for virtual environments. *IBM Journal of Research and Development*, 58(1):5:1–5:10, January–February 2014. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

vanderWalt:2018:CSI

[vdWEG18] Estee van der Walt, J. H. P. Eloff, and Jacomine Grobler. Cybersecurity: Identity deception detection on social media platforms. *Computers & Security*, 78(??):76–89, September 2018. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404818306503`.

VenafiLabs:2014:VLQ

[Ven14] Venafi Labs. Venafi Labs Q3 Heartbleed threat research analysis. Web site., 2014. URL `https://www.venafi.com/assets/pdf/wp/Venafi_Labs_Q3_Heartbleed_Threat_Research_Analysis.pdf`.

Vergnaud:2017:CAB

[Ver17] Damien Vergnaud. Comment on ‘Attribute-Based Signatures for Supporting Anonymous Certification’ by N. Kaaniche and M. Laurent (ESORICS 2016). *The Computer Journal*, 60(12):1801–1808, December 1, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `https://academic.oup.com/comjnl/article/60/12/1801/3861971`.

Vetter:2010:ABV

[Vet10] Ron Vetter. Authentication by biometric verification. *Computer*, 43 (2):28–29, February 2010. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Vo:2019:ISA

[VFFHF19] Tri Hoang Vo, Woldemar Fuhrmann, Klaus-Peter Fischer-Hellmann, and Steven Furnell. Identity-as-a-service: An adaptive security infrastructure and privacy-preserving user identity for the cloud environment. *Future Internet*, 11(5):116, May 15, 2019. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/11/5/116.

Voulgaris:2019:BTI

[VFS+19] Spyros Voulgaris, Nikos Fotiou, Vasilios A. Siris, George C. Polyzos, Mikael Jaatinen, and Yannis Oikonomidis. Blockchain technology for intelligent environments. *Future Internet*, 11(10):213, October 11, 2019. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/11/10/213.

Venkatakrishnan:2017:DRB

[VFV17a] Shaileshh Bojja Venkatakrishnan, Giulia Fanti, and Pramod Viswanath. Dandelion: Redesigning the Bitcoin network for anonymity. *Proceedings of the ACM on Measurement and Analysis of Computing Systems (POMACS)*, 1(1): 22:1–22:??, June 2017. CODEN ???? ISSN 2476-1249. URL http://dl.acm.org/citation.cfm?id=3084459.

Venkatakrishnan:2017:DRBb

[VFV17b] Shaileshh Bojja Venkatakrishnan, Giulia Fanti, and Pramod Viswanath. Dandelion: Redesigning the Bitcoin network for anonymity. *Proceedings of the ACM on Measurement and Analysis of Computing Systems (POMACS)*, 1(1): 22:1–22:34, June 2017. CODEN ???? ISSN 2476-1249. URL http://dl.acm.org/citation.cfm?id=3084459.

Vernize:2015:MNI

[VGA15] Grazielle Vernize, André Luiz Pires Guedes, and Luiz Carlos Pessoa Albini. Malicious nodes identification for complex network based on local views. *The Computer Journal*, 58(10):2476–2491, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2476.

Vijayarajan:2019:BKB

[VGA19] R. Vijayarajan, P. Gnanasivam, and R. Avudaiammal. Bio-key based AES for personalized image cryptography. *The Computer Journal*, 62 (11):1695–1705, November 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/11/1695/5436925.

Vrakas:2014:OUI

[VGL14] Nikos Vrakas, Dimitris Geneiatakis, and Costas

Lambrinoudakis. Obscuring users' identity in VoIP/IMS environments. *Computers & Security*, 43(??):145–158, June 2014. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404814000510`.

Viennot:2014:MSG

[VGN14] Nicolas Viennot, Edward Garcia, and Jason Nieh. A measurement study of Google Play. *ACM SIGMETRICS Performance Evaluation Review*, 42(1): 221–233, June 2014. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Vasisht:2018:DEU

[VJH+18] Deepak Vasisht, Anubhav Jain, Chen-Yu Hsu, Zachary Kabelac, and Dina Katabi. Duet: Estimating user position and identity in smart homes using intermittent and incomplete RF-Data. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2(2): 1–21, July 2018. CODEN ???? ISSN 2474-9567 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3214287`.

Vu:2015:NAN

[VKC15] Hai L. Vu, Kenneth K. Khaw, and Tsong Yueh Chen. A new approach for network vulnerability analysis. *The Computer Journal*, 58(4):878–891, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/4/878`.

Vgena:2019:TAL

[VKK+19] Katerina Vgena, Angeliki Kitsiou, Christos Kalloniatis, Dimitris Kavroudakis, and Stefanos Gritzalis. Toward addressing location privacy issues: New affiliations with social and location attributes. *Future Internet*, 11(11):234, November 01, 2019. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/11/11/234`.

Vasiliadis:2017:DIS

[VKPI17] Giorgos Vasiliadis, Lazaros Koromilas, Michalis Polychronakis, and Sotiris Ioannidis. Design and implementation of a stateful network packet processing framework for GPUs. *IEEE/ACM Transactions on Networking*, 25(1):610–623, February 2017. CODEN IEANEP. ISSN

1063-6692 (print), 1558-2566 (electronic).

Vleju:2012:CCA

[Vle12] Mircea Boris Vleju. A client-centric ASM-based approach to identity management in cloud computing. *Lecture Notes in Computer Science*, 7518: 34–43, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-33999-8_5/`.

Vivek:2014:CSC

[VM14] Srinivas Vivek and C. E. Veni Madhavan. Cubic Sieve Congruence of the Discrete Logarithm Problem, and fractional part sequences. *Journal of Symbolic Computation*, 64(??): 22–34, August 2014. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0747717113001703`.

Vliegen:2015:SRD

[VMV15] Jo Vliegen, Nele Mentens, and Ingrid Verbauwhede. Secure, remote, dynamic reconfiguration of FPGAs. *ACM Transactions on Reconfigurable Technology and Systems*, 7(4):8:1–8:??, January 2015. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Veloudis:2016:NPH

[VN16] Simeon Veloudis and Nimal Nissanke. A novel permission hierarchy for RBAC for dealing with SoD in MAC models. *The Computer Journal*, 59(4):462–492, April 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/59/4/462`.

Vollala:2017:EEM

[VN17] Satyanarayana Vollala and Ramasubramanian N. Energy efficient modular exponentiation for public-key cryptography based on bit forwarding techniques. *Information Processing Letters*, 119(??):25–38, March 2017. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019016301715`.

VonMaurich:2015:IQM

[VOG15] Ingo Von Maurich, Tobias Oder, and Tim Güneysu. Implementing QC–MDPC McEliece encryption. *ACM Transactions on Embedded Computing Systems*, 14 (3):44:1–44:??, April 2015. CODEN ???? ISSN 1539-

9087 (print), 1558-3465 (electronic).

Varadharajan:2018:AUR

[VOGB18] V. S. Varadharajan, D. S. Onge, C. Guß, and G. Beltrame. Over-the-air updates for robotic swarms. *IEEE Software*, 35(2):44–50, March/April 2018. CODEN IESOEG. ISSN 0740-7459 (print), 1937-4194 (electronic).

vanRijswijk-Deij:2017:PIE

[vRDHSP17] Roland van Rijswijk-Deij, Kaspar Hageman, Anna Sperotto, and Aiko Pras. The performance impact of elliptic curve cryptography on DNSSEC validation. *IEEE/ACM Transactions on Networking*, 25 (2):738–750, April 2017. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Vembuselvi:2011:LLL

[VS11] C. Vembuselvi and S. Selvakumar. LISISAP: link level signature based secure anonymous protocol for prevention of traffic analysis attacks. *ACM SIGSOFT Software Engineering Notes*, 36(2):1–10, March 2011. CODEN SFENDP. ISSN 0163-5948 (print), 1943-5843 (electronic).

Vassilev:2016:ESU

[VS16] Apostol Vassilev and Robert Staples. Entropy as a service: Unlocking cryptography's full potential. *Computer*, 49(9):98–102, September 2016. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL `https://www.computer.org/csdl/mags/co/2016/09/mco2016090098-abs.html`.

Voris:2019:AAU

[VSB+19] Jonathan Voris, Yingbo Song, Malek Ben Salem, Shlomo Hershkop, and Salvatore Stolfo. Active authentication using file system decoys and user behavior modeling: results of a large scale study. *Computers & Security*, 87(??):Article 101412, November 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404818311258`.

Vivek:2012:CSE

[VSR12] S. Sree Vivek, S. Sharmila Deva Selvi, and C. Pandu Rangan. Compact stateful encryption schemes with ciphertext verifiability. *Lecture Notes in Computer Science*, 7631: 87–104, 2012. CODEN LNCSD9. ISSN

0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34117-5_6/.

Vlachos:2015:DPC

[VSV15] Michail Vlachos, Johannes Schneider, and Vassilios G. Vassiliadis. On data publishing with clustering preservation. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 9(3):23:1–23:??, April 2015. CODEN ???? ISSN 1556-4681 (print), 1556-472X (electronic).

vanTilborg:2011:ECS

[vTJ11] Henk C. A. van Tilborg and Sushil Jajodia, editors. *Encyclopedia of Cryptography and Security*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2011. ISBN 1-4419-5905-X (print), 1-4419-5906-8 (e-book). xl + 1416 pp. LCCN ????

Viswanathan:2018:EEG

[VTY18] Sreejaya Viswanathan, Rui Tan, and David K. Y. Yau. Exploiting electrical grid for accurate and secure clock synchronization. *ACM Transactions on Sensor Networks*, 14(2):12:1–12:??, July 2018. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Vuagnoux:2010:CAC

[Vua10] Martin Vuagnoux. *Computer Aided Cryptanalysis from Ciphers to Side Channels*. Thèse, École polytechnique fédérale de Lausanne (EPFL), Lausanne, 2010. 191 pp.

vanVredendaal:2016:RMM

[vV16] Christine van Vredendaal. Reduced memory meet-in-the-middle attack against the NTRU private key. *LMS Journal of Computation and Mathematics*, 19 (A):43–57, 2016. CODEN ???? ISSN 1461-1570. URL https://www.cambridge.org/core/product/2FD6898DA25DD88B007F12A56421BA73.

VanDijkhuizen:2018:SNT

[VV18] Niels Van Dijkhuizen and Jeroen Van Der Ham. A survey of network traffic anonymisation techniques and implementations. *ACM Computing Surveys*, 51(3):52:1–52:??, July 2018. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Vazirani:2019:FDI

[VV19] Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution. *Communications of the Association for*

Computing Machinery, 62 (4):133, April 2019. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL https://cacm.acm.org/magazines/2019/4/235624/fulltext.

Valente:2019:SSA

[VWC19] J. Valente, M. A. Wynn, and A. A. Cardenas. Stealing, spying, and abusing: Consequences of attacks on Internet of Things devices. *IEEE Security & Privacy*, 17(5):10–21, September/October 2019. ISSN 1540-7993 (print), 1558-4046 (electronic).

Wagstaff:2010:C

[Wag10] Samuel S. Wagstaff, Jr. *Cryptanalysis*, chapter 11, pages 1–16. Volume 2 of Atallah and Blanton [AB10b], second edition, 2010. ISBN 1-58488-820-2. LCCN QA76.9.A43 A433 2010. URL http://www.crcnetbase.com/doi/abs/10.1201/9781584888215-c11.

Wagner:2016:TPF

[Wag16] David Wagner. Technical perspective: Fairness and the coin flip. *Communications of the Association for Computing Machinery*, 59(4):75, April 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2016/4/200173/fulltext.

Woo:2019:UEM

[WAK+19] Simon S. Woo, Ron Artstein, Elsi Kaiser, Xiao Le, and Jelena Mirkovic. Using episodic memory for user authentication. *ACM Transactions on Privacy and Security (TOPS)*, 22(2):11:1–11:??, April 2019. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3308992.

Walter:2018:RCS

[Wal18] Kenny Walter. Researchers close security vulnerability in popular encryption program. *R&D Magazine*, ??(??):??, August 9, 2018. URL https://www.rdmag.com/article/2018/08/researchers-close-security-vulnerability-popular-encryption-program.

Wang:2010:NSB

[Wan10] Xiang Wang. A new SDVS based on NTRUSign. In Cheng-Xiang Wang, editor, *Proceedings of the 2010 International Conference on Communications and Mobile Computing (CMC). 12–14 April 2010, Shenzhen, China*, pages 205–?? IEEE Computer Society Press, 1109 Spring

Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 1-4244-6327-0. LCCN ???? URL http://ieeexplore.ieee.org/servlet/opac?punumber=5471195.

Wang:2013:CRA

[Wan13] Honggang Wang. Communication-resource-aware adaptive watermarking for multimedia authentication in wireless multimedia sensor networks. *The Journal of Supercomputing*, 64 (3):883–897, June 2013. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-010-0500-5.

Wang:2014:IIA

[Wan14] Huaqun Wang. Insecurity of 'Improved Anonymous Multi-Receiver Identity-Based Encryption'. *The Computer Journal*, 57(4): 636–638, April 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/57/4/636.full.pdf+html. See [Chi12].

Wang:2018:LRI

[Wan18a] Zhiwei Wang. Leakage resilient ID-based proxy re-encryption scheme for access control in fog computing. *Future Generation Computer Systems*, 87(??):679–685, October 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17310075.

Wang:2018:PPA

[Wan18b] Zhiwei Wang. A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity. *Future Generation Computer Systems*, 82(??):342–348, May 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17307495.

Ward:2011:CCM

[War11] Mark Ward. Code-cracking machine returned to life. *BBC News*, May 27, 2011. URL http://www.bbc.co.uk/news/technology-13566878.

Watt:2010:IPI

[Wat10] Stephen M. Watt, editor. *ISSAC 2010: Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, July 25–28, 2010, Munich, Germany*. ACM Press, New York, NY 10036, USA, 2010. ISBN

1-4503-0150-9. LCCN QA76.95 .I59 2010.

Waters:2012:FER

[Wat12] Brent Waters. Functional encryption for regular languages. *Lecture Notes in Computer Science*, 7417:218–235, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32009-5_14/.

Watts:2014:ICB

[Wat14a] Steve Watts. Intelligent combination — the benefits of tokenless two-factor authentication. *Network Security*, 2014(8):17–20, August 2014. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485814700820.

Watts:2014:PYI

[Wat14b] Steve Watts. Protecting your identity when working remotely. *Network Security*, 2014(1):5–7, January 2014. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485814700054.

Watts:2015:HGA

[Wat15] Steve Watts. The holy grail of authentication. *Network Security*, 2015(12):18–19, December 2015. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485815301136.

Wang:2012:PCE

[WB12] Qingju Wang and Andrey Bogdanov. The provable constructive effect of diffusion switching mechanism in CLEFIA-type block ciphers. *Information Processing Letters*, 112(11):427–432, June 15, 2012. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019012000555.

Weisse:2017:RLC

[WBA17] Ofir Weisse, Valeria Bertacco, and Todd Austin. Regaining lost cycles with HotCalls: a fast interface for SGX secure enclaves. *ACM SIGARCH Computer Architecture News*, 45(2):81–93, May 2017. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Wright:2010:USP

[WBC+10] Charles V. Wright, Lucas Ballard, Scott E. Coull, Fabian Monrose, and Gerald M. Masson. Uncovering spoken phrases in encrypted voice over IP conversations. *ACM Transactions on Information and System Security*, 13 (4):35:1–35:??, December 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wu:2018:ESS

[WCCH18] Libing Wu, Biwen Chen, Kim-Kwang Raymond Choo, and Debiao He. Efficient and secure searchable encryption protocol for cloud-based Internet of Things. *Journal of Parallel and Distributed Computing*, 111(??):152–161, January 2018. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S074373151730237X`.

Wang:2019:IFT

[WCD19] Gaoli Wang, Zhenfu Cao, and Xiaolei Dong. Improved fault-tolerant aggregate signatures. *The Computer Journal*, 62(4): 481–489, April 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/62/4/481/5139676`.

Wang:2018:SNU

[WCFW18] King-Hang Wang, Chien-Ming Chen, Weicheng Fang, and Tsu-Yang Wu. On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. *The Journal of Supercomputing*, 74(1):65–70, January 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Wei:2018:GCQ

[WCL+18] Chun-Yan Wei, Xiao-Qiu Cai, Bin Liu, Tian-Yin Wang, and Fei Gao. A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure. *IEEE Transactions on Computers*, 67(1):2–8, January 2018. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/document/7962191/`.

Wu:2017:HMA

[WCXZ17] Ying Wu, Jinyong Chang, Rui Xue, and Rui Zhang. Homomorphic MAC from algebraic one-way functions for network coding with small key size. *The Computer Journal*, 60(12):1785–1800, December 1, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/12/1785/3885827.

Wang:2018:SEA

[WDCL18] Haijiang Wang, Xiaolei Dong, Zhenfu Cao, and Dongmei Li. Secure and efficient attribute-based encryption with keyword search. *The Computer Journal*, 61(8):1133–1142, August 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/8/1133/4975828.

Wei:2012:NTB

[WDDW12] Zhuo Wei, Xuhua Ding, Robert Huijie Deng, and Yongdong Wu. No tradeoff between confidentiality and performance: An analysis on H.264/SVC partial encryption. *Lecture Notes in Computer Science*, 7394:72–86, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32805-3_6/.

Wang:2019:FTSa

[WDG19] Leimin Wang, Tiandu Dong, and Ming-Feng Ge. Finite-time synchronization of memristor chaotic systems and its application in image encryption. *Applied Mathematics and Computation*, 347(??):293–305, April 15, 2019. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300318309901.

Wazid:2019:DSK

[WDKV19] Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, and Athanasios V. Vasilakos. Design of secure key management and user authentication scheme for fog computing services. *Future Generation Computer Systems*, 91(??):475–492, February 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X18303959.

Wazid:2018:AKM

[WDV18] Mohammad Wazid, Ashok Kumar Das, and Athanasios V. Vasilakos. Authenticated key management protocol for cloud-assisted body area sensor networks. *Journal of Network and Computer Applications*, 123(??):112–126, December 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518302960.

Wang:2019:SFE

[WDZ19] Xiaofen Wang, Hong-Ning Dai, and Ke Zhang. Secure and flexible economic data sharing protocol based on ID-based dynamic exclusive broadcast encryption in economic system. *Future Generation Computer Systems*, 99(??):177–185, October 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18316145.

Wang:2013:SES

[WDZL13] Guojun Wang, Qiushuang Du, Wei Zhou, and Qin Liu. A scalable encryption scheme for multi-privileged group communications. *The Journal of Supercomputing*, 64(3):1075–1091, June 2013. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-011-0683-4.

West:2015:EC

[Wes15] Tom West. *The Einstein code*. Pan Books, London, UK, 2015. ISBN 1-4472-1034-4 (paperback), 1-4472-4660-8 (ePub e-book). 400 pp. LCCN ????

Wess:2016:JWM

[Wes16] Jane Wess. John Wallis (1616–1703). Mathematics, music theory, and cryptography in 17th century Oxford. Oxford University Mathematical Institute, 9 June 2016. *BSHM Bulletin: Journal of the British Society for the History of Mathematics*, 31 (3):252–253, 2016. CODEN ???? ISSN 1749-8430 (print), 1749-8341 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/17498430.2016.1215868.

Wang:2018:ERS

[WGD18] Hong Wang, Jie Guan, and Lin Ding. On equivalence relations of state diagram of cascade connection of an LFSR into an NFSR. *International Journal of Foundations of Computer Science (IJFCS)*, 29(7):??, November 2018. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054118500235.

Wang:2016:SSS

[WGF16] Xianfang Wang, Jian Gao, and Fang-Wei Fu. Secret sharing schemes from linear codes over $F_p + \nu F_p$. *International Journal of Foundations of Computer Science (IJFCS)*, 27 (5):595–??, August 2016. CODEN IFCSEN. ISSN 0129-0541.

Wang:2010:DVT

[WGJT10] Xiaofeng Wang, Philippe Golle, Markus Jakobsson, and Alex Tsow. Deterring voluntary trace disclosure in re-encryption mix-networks. *ACM Transactions on Information and System Security*, 13(2): 18:1–18:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Wang:2012:BRR

[WgMdZlZ12] Ding Wang, Chun guang Ma, Sen dong Zhao, and Chang li Zhou. Breaking a robust remote user authentication scheme using smart cards. *Lecture Notes in Computer Science*, 7513:110–118, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35606-3_13/.

Wang:2012:SPB

[WgMW12] Ding Wang, Chun guang Ma, and Peng Wu. Secure password-based remote user authentication scheme with non-tamper resistant smart cards. *Lecture Notes in Computer Science*, 7371:114–121, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31540-4_9/.

Wei:2012:NCI

[WGZ+12] Xiaopeng Wei, Ling Guo, Qiang Zhang, Jianxin Zhang, and Shiguo Lian. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *The Journal of Systems and Software*, 85(2):290–299, February 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211002147.

Wang:2017:DRM

[WH17] Yi Wang and Yajun Ha. A DFA-resistant and masked PRESENT with area optimization for RFID applications. *ACM Transactions on Embedded Computing Systems*, 16(4): 102:1–102:??, August 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Wang:2018:GAD

[WH18] Lin Wang and Zhi Hu. On graph algorithms for degeneracy test and recursive description of stream ciphers. *Fundamenta Informaticae*, 160(3):343–359, ???? 2018. CODEN FUMAAJ. ISSN 0169-2968

(print), 1875-8681 (electronic).

Wang:2015:EFF

[WHC+15] Wei Wang, Yin Hu, Lianmu Chen, Xinming Huang, and B. Sunar. Exploring the feasibility of fully homomorphic encryption. *IEEE Transactions on Computers*, 64(3):698–706, March 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Wang:2017:DVP

[WHJ17] Huaqun Wang, Debiao He, and Yimu Ji. Designated-verifier proof of assets for Bitcoin exchange using elliptic curve cryptography. *Future Generation Computer Systems*, ??(??):??, ???? 2017. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X1731350X`.

Wei:2016:PAB

[WHLH16] Jianghong Wei, Xinyi Huang, Wenfen Liu, and Xuexian Hu. Practical attribute-based signature: Traceability and revocability. *The Computer Journal*, 59(11):1714–1734, November 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/59/11/1714`.

Wei:2017:CES

[WHLH17] Jianghong Wei, Xinyi Huang, Wenfen Liu, and Xuexian Hu. Cost-effective and scalable data sharing in cloud storage using hierarchical attribute-based encryption with forward security. *International Journal of Foundations of Computer Science (IJFCS)*, 28(7):843–??, November 2017. CODEN IFCSEN. ISSN 0129-0541.

Wu:2012:DAA

[WHN+12] Hongjun Wu, Tao Huang, Phuong Ha Nguyen, Huaxiong Wang, and San Ling. Differential attacks against stream cipher ZUC. *Lecture Notes in Computer Science*, 7658: 262–277, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-34961-4_17/`.

Wang:2012:FOP

[WHY+12] Xu An Wang, Xinyi Huang, Xiaoyuan Yang, Longfei Liu, and Xuguang Wu. Further observation on proxy re-encryption with keyword search. *The Journal of Systems and*

Software, 85(3):643–654, March 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211002433.

Wang:2012:NFS

[WHZ12] Hui Wang, Anthony T. S. Ho, and Xi Zhao. A novel fast self-restoration semi-fragile watermarking algorithm for image content authentication resistant to JPEG compression. *Lecture Notes in Computer Science*, 7128:72–85, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32205-1_8/.

Wang:2019:RSI

[WHZ+19] Ping Wang, Xing He, Yushu Zhang, Wenying Wen, and Ming Li. A robust and secure image sharing scheme with personal identity information embedded. *Computers & Security*, 85(??):107–121, August 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404819300914.

Willyard:2011:MM

[Wil11] C. Willyard. Me, myself, or I. *IEEE Spectrum*, 48(6):52–84, June 2011. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Williams:2018:FPD

[Wil18] Michael Williams. The first public discussion of the secret Colossus Project. *IEEE Annals of the History of Computing*, 40(1):84–87, January/March 2018. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic). URL https://www.computer.org/csdl/mags/an/2018/01/man2018010084.pdf.

Winder:2017:ROS

[Win17] Davey Winder. Researchers open sliding window to completely break libgcrypt RSA-1024. Web blog., July 6, 2017. URL https://www.scmagazineuk.com/researchers-open-sliding-window-to-completely-break-libgcrypt-rsa-1024/article/673178/. See [BBG+17].

Wang:2019:MBN

[WJ19] Qian Wang and Chenhui Jin. A method to bound the number of active S-boxes for a kind of AES-like structure. *The Computer Journal*, 62(8):1121–1131, August 2019. CODEN

CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/8/1121/5319150.

Wang:2018:VMF

[WK18] Nana Wang and Mohan Kankanhalli. 2D vector map fragile watermarking with region location. *ACM Transactions on Spatial Algorithms and Systems (TSAS)*, 4(4):12:1–12:??, October 2018. CODEN ???? ISSN 2374-0353. URL https://dl.acm.org/citation.cfm?id=3239163.

Wang:2016:DRS

[WKB16] Zhen Wang, Mark Karpovsky, and Lake Bu. Design of reliable and secure devices realizing Shamir's secret sharing. *IEEE Transactions on Computers*, 65(8):2443–2455, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Wu:2011:HQI

[WKH11] Chia-Chun Wu, Shang-Juh Kao, and Min-Shiang Hwang. A high quality image sharing with steganography and adaptive authentication scheme. *The Journal of Systems and Software*, 84(12):2196–2207, December 2011. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211001488.

Weissman:2011:LLB

[WL11] Clark Weissman and Timothy Levin. Lessons learned from building a high-assurance crypto gateway. *IEEE Security & Privacy*, 9(1):31–39, January/February 2011. ISSN 1540-7993 (print), 1558-4046 (electronic).

Wang:2012:MCE

[WL12] Jinwei Wang and Shiguo Lian. On multiwatermarking in cloud environment. *Concurrency and Computation: Practice and Experience*, 24(17):2151–2164, December 10, 2012. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Wu:2019:VFS

[WL19] Zhiqiang Wu and Kenli Li. VBTree: forward secure conjunctive queries over encrypted data for cloud computing. *VLDB Journal: Very Large Data Bases*, 28(1):25–46, February 2019. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).

Wei:2012:IRK

[WLC12] Yuechuan Wei, Chao Li, and Dan Cao. Improved related-key rectangle attack on the full HAS-160 encryption mode. *International Journal of Foundations of Computer Science (IJFCS)*, 23(3):733–??, April 2012. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Wang:2011:RBM

[WLDB11] Kai Wang, Guillaume Lavoué, Florence Denis, and Atilla Baskurt. Robust and blind mesh watermarking based on volume moments. *Computers and Graphics*, 35(1):1–19, February 2011. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0097849310001433`.

Wang:2017:CAS

[WLFX17] Changji Wang, Yuan Li, Jian Fang, and Jianguo Xie. Cloud-aided scalable revocable identity-based encryption scheme with ciphertext update. *Concurrency and Computation: Practice and Experience*, 29(20):??, October 25, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Wang:2013:HCL

[WLH13] Kan Wang, Zhe-Ming Lu, and Yong-Jian Hu. A high capacity lossless data hiding scheme for JPEG images. *The Journal of Systems and Software*, 86(7):1965–1975, July 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121213000812`.

Wei:2015:FST

[WLH15] Jianghong Wei, Wenfen Liu, and Xuexian Hu. Forward-secure threshold attribute-based signature scheme. *The Computer Journal*, 58(10):2492–2506, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/10/2492`.

Wei:2014:EEF

[WLS14] Guiyi Wei, Rongxing Lu, and Jun Shao. EFADS: Efficient, flexible and anonymous data sharing protocol for cloud computing with proxy re-encryption. *Journal of Computer and System Sciences*, 80(8):1549–1562, December 2014. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://`

www.sciencedirect.com/science/article/pii/S0022000014000658.

Wang:2011:HAB

[WLWG11] Guojun Wang, Qin Liu, Jie Wu, and Minyi Guo. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. *Computers & Security*, 30(5): 320–331, July 2011. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404811000678.

Wu:2015:TRM

[WLY+15] Guowei Wu, Zuosong Liu, Lin Yao, Jing Deng, and Jie Wang. A trust routing for multimedia social networks. *The Computer Journal*, 58(4):688–699, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/688.

Wang:2017:ABS

[WLY17] Qi Wang, Xiangxue Li, and Yu Yu. Anonymity for Bitcoin from secure escrow address. *IEEE Access*, ??(??): 1, ???? 2017. ISSN 2169-3536.

Wang:2016:LLE

[WLZ+16] Mingzhong Wang, Dan Liu, Liehuang Zhu, Yongjun Xu, and Fei Wang. LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. *Computing*, 98(7): 685–708, July 2016. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Wang:2012:RTC

[WLZL12] Liyun Wang, Hefei Ling, Fuhao Zou, and Zhengding Lu. Real-time compressed-domain video watermarking resistance to geometric distortions. *IEEE MultiMedia*, 19(1):70–79, January/March 2012. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic).

Wang:2017:PPD

[WMC17] Xiaofen Wang, Yi Mu, and Rongmao Chen. Privacy-preserving data search and sharing protocol for social networks through wireless applications. *Concurrency and Computation: Practice and Experience*, 29(7):??, April 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Wu:2012:PSC

[WMS+12] Wei Wu, Yi Mu, Willy Susilo, Xinyi Huang, and Li Xu. A provably secure construction of certificate-based encryption from certificateless encryption. *The Computer Journal*, 55(10):1157–1168, October 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/55/10/1157.full.pdf+html.

Watanabe:2014:OAC

[WMU14] Shun Watanabe, Ryutaroh Matsumoto, and Tomohiko Uyematsu. Optimal axis compensation in quantum key distribution protocols over unital channels. *Theoretical Computer Science*, 560 (part 1)(??):91–106, December 4, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397514006987.

Wang:2017:CES

[WMX+17] Xu An Wang, Jianfeng Ma, Fatos Xhafa, Mingwu Zhang, and Xiaoshuang Luo. Cost-effective secure e-health cloud system using identity based cryptographic techniques. *Future Generation Computer Systems*, 67(??):242–254, February 2017. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16302588.

Won:2016:PAA

[WMYR16] Jongho Won, Chris Y. T. Ma, David K. Y. Yau, and Nageswara S. V. Rao. Privacy-assured aggregation protocol for smart metering: a proactive fault-tolerant approach. *IEEE/ACM Transactions on Networking*, 24(3):1661–1674, June 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Wang:2015:HAD

[WOLP15] Xing Wang, Nga Lam Or, Ziyan Lu, and Derek Pao. Hardware accelerator to detect multi-segment virus patterns. *The Computer Journal*, 58(10):2443–2460, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2443.

Wu:2012:UFS

[WOLS12] Xiaotian Wu, Duanhao Ou, Qiming Liang, and Wei Sun. A user-friendly secret image sharing scheme with reversible steganography based on cellular automata. *The Journal of Systems and Software*, 85(8):1852–1863, August 2012. CODEN JS-

SODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212000696.

Wendzel:2015:CME

[WP15] S. Wendzel and C. Palmer. Creativity in mind: Evaluating and maintaining advances in network steganographic research. *J.UCS: Journal of Universal Computer Science*, 21(12): 1684–??, ???? 2015. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL http://www.jucs.org/jucs_21_12/creativity_in_mind_evaluating.

Wang:2017:PPK

[WP17] Yujue Wang and Hwee-Hwa Pang. Probabilistic public key encryption for controlled equijoin in relational databases. *The Computer Journal*, 60(4): 600–612, March 23, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/4/600/2354608.

Wang:2016:SEP

[WPZM16] Xinlei Wang, Amit Pande, Jindan Zhu, and Prasant Mohapatra. STAMP: Enabling privacy-preserving location proofs for mobile users. *IEEE/ACM Transactions on Networking*, 24 (6):3276–3289, December 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Wu:2013:FTR

[WQZ+13] Qianhong Wu, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, and Jesús A. Manjón. Fast transmission to remote cooperative groups: a new key management paradigm. *IEEE/ACM Transactions on Networking*, 21(2):621–633, April 2013. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Wu:2016:CBE

[WQZ+16] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farras, and J. A. Manjon. Contributory broadcast encryption with efficient encryption and short ciphertexts. *IEEE Transactions on Computers*, 65(2):466–479, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Wei:2015:TPE

[WR15] Lei Wei and Michael K. Reiter. Toward practical encrypted email that supports private, regular-expression searches. *International Journal of In-*

formation Security, 14(5): 397–416, October 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-014-0268-3; http://link.springer.com/content/pdf/10.1007/s10207-014-0268-3.pdf.

Wani:1970:PEA

[WRP70] Abdul Raoof Wani, Q. P. Rana, and Nitin Pandey. Performance evaluation and analysis of advanced symmetric key cryptographic algorithms for cloud computing security. In Kanad Ray, Tarun K. Sharma, Sanyog Rawat, R. K. Saini, and Anirban Bandyopadhyay, editors, *Soft Computing: Theories and Applications: Proceedings of SoCTA 2017*, pages 261–270. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1970. ISBN 981-13-0588-9 (print), 981-13-0589-7 (e-book). ISSN 2194-5357 (print), 2194-5365 (electronic). LCCN QA76.9.S63. URL http://link.springer.com/10.1007/978-981-13-0589-4.

Wu:2012:RGB

[WS12] Xiaotian Wu and Wei Sun. Random grid-based visual secret sharing for general access structures with cheat-preventing ability. *The Journal of Systems and Software*, 85(5):1119–1134, May 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211003220.

Williams:2013:APC

[WS13] Peter Williams and Radu Sion. Access privacy and correctness on untrusted storage. *ACM Transactions on Information and System Security*, 16 (3):12:1–12:??, November 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Whitworth:2014:SPC

[WS14] Jeff Whitworth and Shan Suthaharan. Security problems and challenges in a machine learning-based hybrid big data processing network systems. *ACM SIGMETRICS Performance Evaluation Review*, 41(4):82–85, March 2014. CODEN ???? ISSN 0163-5999 (print), 1557-9484 (electronic).

Woodworth:2019:SSS

[WS19] Jason W. Woodworth and Mohsen Amini Salehi. S3BD: Secure semantic search over encrypted big data in the cloud. *Con-*

currency and Computation: Practice and Experience, 31(11):e5050:1–e5050:??, June 10, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Wang:2015:RSA

[WSA15] Yang Wang, Willy Susilo, and Man Ho Au. Revisiting security against the arbitrator in optimistic fair exchange. *The Computer Journal*, 58(10):2665–2676, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2665.

Wang:2014:NDH

[WSC14] Zhiwei Wang, Guozi Sun, and Danwei Chen. A new definition of homomorphic signature for identity management in mobile cloud computing. *Journal of Computer and System Sciences*, 80(3):546–553, May 2014. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000013001190.

Wang:2019:CPB

[WSL+19] Licheng Wang, Xiaoying Shen, Jing Li, Jun Shao, and Yixian Yang. Cryptographic primitives in blockchains. *Journal of Network and Computer Applications*, 127(??):43–58, February 1, 2019. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S108480451830362X.

Wu:2016:BPK

[WSQ+16] Qianhong Wu, Yang Sun, Bo Qin, Jiankun Hu, Weiran Liu, Jianwei Liu, and Yong Ding. Batch public key cryptosystem with batch multi-exponentiation. *Future Generation Computer Systems*, 62(??):196–204, September 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X15003933.

Watanabe:2012:ITT

[WSS12] Yohei Watanabe, Takenobu Seito, and Junji Shikata. Information-theoretic timed-release security: Key-agreement, encryption, and authentication codes. *Lecture Notes in Computer Science*, 7412:167–186, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32284-6_10/.

Wei:2019:VFA

[WSS+19] Shih-En Wei, Jason Saragih, Tomas Simon, Adam W. Harley, Stephen Lombardi, Michal Perdoch, Alexander Hypes, Dawei Wang, Hernan Badino, and Yaser Sheikh. VR facial animation via multiview image translation. *ACM Transactions on Graphics*, 38 (4):67:1–67:??, July 2019. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

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 Computer Science*, 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/.

Wu:2010:EUA

[WT10a] Tsu-Yang Wu and Yuh-Min Tseng. An efficient user authentication and key exchange protocol for mobile client–server environment. *Computer Networks (Amsterdam, Netherlands: 1999)*, 54(9):1520–1530, June 17, 2010. CODEN ???? ISSN 1389-1286.

Wu:2010:IBM

[WT10b] Tsu-Yang Wu and Yuh-Min Tseng. An ID-based mutual authentication and key exchange protocol for low-power mobile devices. *The Computer Journal*, 53(7):1062–1070, September 2010. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/cgi/content/abstract/53/7/1062; http://comjnl.oxfordjournals.org/cgi/reprint/53/7/1062.

Wang:2013:NMC

[WT13] Qichun Wang and Chik How Tan. A new method to construct Boolean functions with good cryptographic properties. *Information Processing Letters*, 113(14–16):567–571, July/August 2013. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013001348.

Wu:2012:RIB

[WTT12] Tsu-Yang Wu, Yuh-Min Tseng, and Tung-Tso Tsai. A revocable ID-based authenticated group key exchange protocol with resistant to malicious participants. *Computer Networks*

(Amsterdam, Netherlands: 1999), 56(12):2994–3006, August 16, 2012. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128612001995.

Wu:2016:LTN

[Wu16] Felix Wu. Law and technology: No easy answers in the fight over iPhone decryption. *Communications of the Association for Computing Machinery*, 59(9):20–22, September 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2016/9/206250/fulltext.

Wu:2017:SPM

[Wu17] Wei-Chen Wu. A secret push messaging service in VANET clouds. *The Journal of Supercomputing*, 73 (7):3085–3097, July 2017. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Wu:2012:AST

[WW12] Shengbao Wu and Mingsheng Wang. Automatic search of truncated impossible differentials for word-oriented block ciphers. *Lecture Notes in Computer Science*, 7668: 283–302, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34931-7_17/.

Willis:2013:IFI

[WW13] Karl D. D. Willis and Andrew D. Wilson. InfraStructs: fabricating information inside physical objects for imaging in the terahertz region. *ACM Transactions on Graphics*, 32(4): 138:1–138:??, July 2013. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Wang:2014:ATF

[WW14] Ding Wang and Ping Wang. On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. *Computer Networks (Amsterdam, Netherlands: 1999)*, 73(??):41–57, November 14, 2014. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128614002643.

Wen:2014:MZC

[WWBC14] Long Wen, Meiqin Wang, Andrey Bogdanov, and Huaifeng Chen. Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard. *Information Processing Letters*, 114(6): 322–330, June 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019014000088.

Wang:2011:MMW

[WWC+11] Yini Wang, Sheng Wen, Silvio Cesare, Wanlei Zhou, and Yang Xiang. The microcosmic model of worm propagation. *The Computer Journal*, 54 (10):1700–1720, October 2011. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/54/10/1700.full.pdf+html.

Weng:2012:NCC

[WWHL12] Zhiwei Weng, Jian Weng, Kai He, and Yingkai Li. New chosen ciphertext secure public key encryption in the standard model with public verifiability. *Lecture Notes in Computer Science*, 6839:170–176, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-25944-9_22.

Wahaballa:2014:MLS

[WWL+14] Abubaker Wahaballa, Osman Wahballa, Fagen Li, Mohammed Ramadan, and Zhiguang Qin. Multiple-layered securities using steganography and cryptography. *International Journal of Computer Applications*, 36(3):93–100, 2014. ISSN 1206-212X (print), 1925-7074 (electronic). URL https://www.tandfonline.com/doi/full/10.2316/Journal.202.2014.3.202-3917.

Werner:2017:CIM

[WWW17] Jorge Werner, Carla Merkle Westphall, and Carlos Becker Westphall. Cloud identity management: a survey on privacy strategies. *Computer Networks (Amsterdam, Netherlands: 1999)*, 122(??):29–42, July 20, 2017. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128617301664.

Wang:2011:CIB

[WWYY11] Xu An Wang, Jian Weng, Xiaoyuan Yang, and Yanjiang Yang. Cryptanalysis of an identity based broadcast encryption scheme without random oracles. *Information Processing Letters*, 111(10): 461–464, April 30, 2011.

CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Wang:2011:CHI

[WWYZ11] Xu An Wang, Jian Weng, Xiaoyuan Yang, and Minqing Zhang. Cryptanalysis of an (hierarchical) identity based parallel key-insulated encryption scheme. *The Journal of Systems and Software*, 84(2):219–225, February 2011. CODEN JSSODM. ISSN 0164-1212.

Wu:2017:EAK

[WXK+17] Fan Wu, Lili Xu, Saru Kumari, Xiong Li, Jian Shen, Kim-Kwang Raymond Choo, Mohammad Wazid, and Ashok Kumar Das. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. *Journal of Network and Computer Applications*, 89(??):72–85, July 1, 2017. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804516303150.

Wang:2017:FWA

[WXL+17] Ran Wang, Guangquan Xu, Bin Liu, Yan Cao, and Xiaohong Li. Flow watermarking for anti-noise and multistream tracing in anonymous networks. *IEEE MultiMedia*, 24(4):38–47, October/December 2017. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL https://www.computer.org/csdl/mags/mu/2017/04/mmu2017040038-abs.html.

Wang:2016:SHI

[WXLY16] Wei Wang, Peng Xu, Hui Li, and Laurence Tianruo Yang. Secure hybrid-indexed search for high efficiency over keyword searchable ciphertexts. *Future Generation Computer Systems*, 55(??):353–361, February 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X14001484.

Wang:2019:CSS

[WXMZ19] Xu An Wang, Fatos Xhafa, Jianfeng Ma, and Zhiheng Zheng. Controlled secure social cloud data sharing based on a novel identity based proxy re-encryption plus scheme. *Journal of Parallel and Distributed Computing*, 130(??):153–165, August 2019. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731519302345.

Wang:2019:NTB

[WXSH19] Chen Wang, Lu Xiao, Jian Shen, and Rui Huang. Neighborhood trustworthiness-based vehicle-to-vehicle authentication scheme for vehicular ad hoc networks. *Concurrency and Computation: Practice and Experience*, 31(21):e4643:1–e4643:??, November 10, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Wang:2017:SRS

[WXY+17] Wei Wang, Peng Xu, Laurence Tianruo Yang, Willy Susilo, and Jinjun Chen. Securely reinforcing synchronization for embedded online contests. *ACM Transactions on Embedded Computing Systems*, 16 (2):58:1–58:??, April 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Wang:2010:IIB

[WY10] Xu An Wang and Xiaoyuan Yang. On the insecurity of an identity based proxy re-encryption scheme. *Fundamenta Informaticae*, 98 (2–3):277–281, April 2010. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Weir:2012:AVC

[WY12] Jonathan Weir and WeiQi Yan. Authenticating visual cryptography shares using 2D barcodes. *Lecture Notes in Computer Science*, 7128:196–210, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32205-1_17/`.

Wang:2014:NAI

[WYCF14] Xiaojing Wang, Qizhao Yuan, Hongliang Cai, and Jiajia Fang. A new approach to image sharing with high-security threshold structure. *Journal of the ACM*, 61(6):39:1–39:??, November 2014. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Weir:2012:IHV

[WYK12] Jonathan Weir, Weiqi Yan, and Mohan S. Kankanhalli. Image hatching for visual cryptography. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 8(2S):32:1–32:??, September 2012. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Wang:2013:NSW

[WYL13] Xiaogang Wang, Ming Yang, and Junzhou Luo. A novel sequential watermark detection model for efficient traceback of secret network attack flows. *Journal of Network and Computer Applications*, 36(6):1660–1670, November 2013. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804513000246.

Wei:2014:IDC

[WYL14] Yuechuan Wei, Xiaoyuan Yang, and Chao Li. Impossible differential cryptanalysis on cipher E2. *Concurrency and Computation: Practice and Experience*, 26(8):1477–1489, June 10, 2014. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Wu:2018:SMI

[WYL18] Pin Wu, Yang Yang, and Xiaoqiang Li. StegNet: Mega image steganography capacity with deep convolutional network. *Future Internet*, 10(6):54, June 15, 2018. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/10/6/54.

Wei:2016:APS

[WYML16] Jiannan Wei, Guomin Yang, Yi Mu, and Kaitai Liang. Anonymous proxy signature with hierarchical traceability. *The Computer Journal*, 59(4):559–569, April 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/4/559.

Wang:2013:BSB

[WYW+13] Xiangyang Wang, Hongying Yang, Jing Wang, Lili Chen, and Panpan Niu. Bayesian segmentation based local geometrically invariant image watermarking. *Fundamenta Informaticae*, 128(4):475–501, October 2013. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (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:2017:RRA

[WYZ+17] YiPeng Wang, Xiaochun Yun, Yongzheng Zhang, Liwei Chen, and Tianning Zang. Rethinking robust and accurate application protocol identification. *Computer Networks (Amsterdam, Netherlands:*

1999), 129 (part 1)(??): 64–78, December 24, 2017. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128617303572`.

Wen:2011:DSH

[WZ11] Yamin Wen and Fangguo Zhang. Delegatable secret handshake scheme. *The Journal of Systems and Software*, 84 (12):2284–2292, December 2011. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121211001580`.

Wei:2015:CPK

[WZ15] Puwen Wei and Yuliang Zheng. On the construction of public key encryption with sender recovery. *International Journal of Foundations of Computer Science (IJFCS)*, 26(1):1–??, January 2015. CODEN IFCSEN. ISSN 0129-0541.

Wang:2016:SAP

[WZC16] Minqian Wang, Zhenfeng Zhang, and Cheng Chen. Security analysis of a privacy-preserving decentralized ciphertext-policy attribute-based encryption scheme. *Concurrency and Computation: Practice and Experience*, 28(4):1237–1245, March 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Wang:2018:AMB

[WZCC18] Rong Wang, Yan Zhu, Tung-Shou Chen, and Chin-Chen Chang. An authentication method based on the turtle shell algorithm for privacy-preserving data mining. *The Computer Journal*, 61(8):1123–1132, August 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/61/8/1123/4925401`.

Wu:2019:PFI

[WZCH19] Libing Wu, Yubo Zhang, Kim-Kwang Raymond Choo, and Debiao He. Pairing-free identity-based encryption with authorized equality test in online social networks. *International Journal of Foundations of Computer Science (IJFCS)*, 30(4):647–664, June 2019. ISSN 0129-0541. URL `https://www.worldscientific.com/doi/10.1142/S0129054119400185`.

Weng:2013:VWI

[WZLW13] Chi-Yao Weng, Yu Hong Zhang, Li Chun Lin, and Shiuh-Jeng Wang. Visible watermarking images in high quality of data hiding. *The Journal of Supercomputing*, 66(2):1033–1048, November 2013. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-013-0969-9.

Wei:2012:CSO

[WZM12a] Fushan Wei, Zhenfeng Zhang, and Chuangui Ma. Corrigendum to "Gateway-oriented password-authenticated key exchange protocol in the standard model' [J. Syst. Softw. **85** (March (3)) (2012) 760–768]. *The Journal of Systems and Software*, 85(9):2192, September 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121212001550. See [WZM12b].

Wei:2012:GOP

[WZM12b] Fushan Wei, Zhenfeng Zhang, and Chuangui Ma. Gateway-oriented password-authenticated key exchange protocol in the standard model. *The Journal of Systems and Software*, 85(3):760–768, March 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211002597.

Wang:2012:NIS

[WZXL12] Xiaofeng Wang, Nanning Zheng, Jianru Xue, and Zhenli Liu. A novel image signature method for content authentication. *The Computer Journal*, 55(6):686–701, June 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/55/6/686.full.pdf+html.

Xiong:2013:NIB

[XCL13] Hu Xiong, Zhong Chen, and Fagen Li. New identity-based three-party authenticated key agreement protocol with provable security. *Journal of Network and Computer Applications*, 36(2):927–932, March 2013. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804512002184.

Xu:2014:AHA

[XGLM14] Chang Xu, Hua Guo, Zhoujun Li, and Yi Mu. Affiliation-hiding authenticated asymmetric group key agreement based on short signature. *The Computer Journal*, 57

(10):1580–1590, October 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/57/10/1580.

Xu:2012:APA

[XHC+12] Zhi Xu, Hungyuan Hsu, Xin Chen, Sencun Zhu, and Ali R. Hurson. AK-PPM: An authenticated packet attribution scheme for mobile ad hoc networks. *Lecture Notes in Computer Science*, 7462: 147–168, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33338-5_8/.

Xu:2014:TBH

[XHCH14] Li Xu, Yuan He, Xiaofeng Chen, and Xinyi Huang. Ticket-based handoff authentication for wireless mesh networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 73(??):185–194, November 14, 2014. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128614002886.

Xi:2012:MDA

[XHH12] Kai Xi, Jiankun Hu, and Fengling Han. Mobile device access control: an improved correlation based face authentication scheme and its Java ME application. *Concurrency and Computation: Practice and Experience*, 24(10):1066–1085, July 2012. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Xue:2014:LDP

[XHM14] Kaiping Xue, Peilin Hong, and Changsha Ma. A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. *Journal of Computer and System Sciences*, 80(1):195–206, February 2014. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000013001426.

Xue:2017:CNC

[XHX+17] Kaiping Xue, Jianan Hong, Yingjie Xue, David S. L. Wei, Nenghai Yu, and Peilin Hong. CABE: A new comparable attribute-based encryption construction with 0-encoding and 1-encoding. *IEEE Transactions on Computers*, 66 (9):1491–1503, September 2017. CODEN IT-

COB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/document/7896558/.

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).

Xie:2012:RAA

[Xie12a] Yulai Xie. Review of *Applied Algebra: Codes, Ciphers and Discrete Algorithms*, by Darel W. Hardy, Fred Richman, and Carol L. Walker. *ACM SIGACT News*, 43(3):25–27, September 2012. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Xie:2012:RBA

[Xie12b] Yulai Xie. Review of *Applied Algebra: Codes, Ciphers and Discrete Algorithms*, by Darel W. Hardy, Fred Richman, and Carol L. Walker. *ACM SIGACT News*, 43(3):25–27, September 2012. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Xiong:2012:PPK

[Xio12] Kaiqi Xiong. The performance of public key-based authentication protocols. *Lecture Notes in Computer Science*, 7645: 206–219, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34601-9_16/.

Xu:2017:GKG

[XJR+17] Weitao Xu, Chitra Javali, Girish Revadigar, Chengwen Luo, Neil Bergmann, and Wen Hu. Gait-Key: a gait-based shared secret key generation protocol for wearable devices. *ACM Transactions on Sensor Networks*, 13(1):6:1–6:??, February 2017. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Xu:2016:CIB

[XJW+16] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin. Conditional identity-based broadcast proxy re-encryption and its application to cloud email. *IEEE Transactions on Computers*, 65(1):66–79, ???? 2016. CODEN

ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Xu:2013:PKE

[XJWW13] Peng Xu, Hai Jin, Qianhong Wu, and Wei Wang. Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack. *IEEE Transactions on Computers*, 62 (11):2266–2277, November 2013. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Xu:2019:TPT

[XLC+19] Lingling Xu, Jin Li, Xiaofeng Chen, Wanhua Li, Shaohua Tang, and HaoTian Wu. Tc-PEDCKS: Towards time controlled public key encryption with delegatable conjunctive keyword search for Internet of Things. *Journal of Network and Computer Applications*, 128(??):11–20, February 15, 2019. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518303850.

Xu:2012:AHA

[XLM+12] Chang Xu, Zhoujun Li, Yi Mu, Hua Guo, and Tao Guo. Affiliation-hiding authenticated asymmetric group key agreement. *The Computer Journal*, 55(10):1180–1191, October 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/55/10/1180.full.pdf+html.

Xue:2018:SNN

[XLP+18] W. Xue, H. Li, Y. Peng, J. Cui, and Y. Shi. Secure k nearest neighbors query for high-dimensional vectors in outsourced environments. *IEEE Transactions on Big Data*, 4(4): 586–599, December 2018. ISSN 2332-7790.

Xiong:2009:PSI

[XLQ09] H. Xiong, F. Li, and Z. Qin. Provably secure identity based threshold signature without random oracles. *International Journal of Computer Applications*, 31(4): 290–295, 2009. ISSN 1206-212X (print), 1925-7074 (electronic). URL https://www.tandfonline.com/doi/full/10.1080/1206212X.2009.11441953.

Xiang:2016:EMP

[XLWZ16] Xinyin Xiang, Hui Li, Mingyu Wang, and Xingwen Zhao. Efficient multiparty concurrent signature from lattices. *Information Processing Letters*, 116(8):

497–502, August 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019016300138.

Xue:2013:TCB

[XMHD13] Kaiping Xue, Changsha Ma, Peilin Hong, and Rong Ding. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *Journal of Network and Computer Applications*, 36(1):316–323, January 2013. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804512001403.

Xie:2013:ECP

[XMLC13] X. Xie, H. Ma, J. Li, and X. Chen. An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing. *J.UCS: Journal of Universal Computer Science*, 19(16): 2349–??, ???? 2013. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL http://www.jucs.org/jucs_19_16/an_efficient_ciphertext_policy.

Xu:2017:EOS

[XMY+17] Rui Xu, Kirill Morozov, Yanjiang Yang, Jianying Zhou, and Tsuyoshi Takagi. Efficient outsourcing of secure k-nearest neighbour query over encrypted database. *Computers & Security*, 69(??):65–83, August 2017. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404816301651.

Xiang:2014:PBA

[XNG+14] Yong Xiang, I. Natgunanathan, Song Guo, Wanlei Zhou, and S. Nahavandi. Patchwork-based audio watermarking method robust to de-synchronization attacks. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 22(9):1413–1423, September 2014. CODEN ???? ISSN 2329-9290.

Xia:2015:SPK

[XNKG15] Q. Xia, J. Ni, A. J. B. A. Kanpogninge, and J. C. Gee. Searchable public-key encryption with data sharing in dynamic groups for mobile cloud storage. *J.UCS: Journal of Universal Computer Science*, 21 (3):440–??, ???? 2015. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL http:/

/www.jucs.org/jucs_21_3/searchable_public_key_encryption.

Xiang:2018:SSA

[XNP+18] Y. Xiang, I. Natgunanathan, D. Peng, G. Hua, and B. Liu. Spread spectrum audio watermarking using multiple orthogonal PN sequences and variable embedding strengths and polarities. *IEEE/ ACM Transactions on Audio, Speech, and Language Processing*, 26(3):529–539, March 2018. ISSN 2329-9290.

Xiang:2015:SSB

[XNRG15] Yong Xiang, I. Natgunanathan, Yue Rong, and Song Guo. Spread spectrum-based high embedding capacity watermarking method for audio signals. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 23(12):2228–2237, December 2015. CODEN ???? ISSN 2329-9290.

Xiong:2011:CIB

[XQL11] Hu Xiong, Zhiguang Qin, and Fagen Li. Cryptanalysis of an identity based signcryption without random oracles. *Fundamenta Informaticae*, 107(1):105–109, January 2011. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Xin:2010:IEB

[XSWC10] Hong Xin, Zhu Shujing, Chen Weibin, and Jian Chongjun. An image encryption base on non-linear pseudo-random number generator. In *2010 International Conference on Computer Application and System Modeling (ICCASM)*, volume 9, pages V9–238–V9–241. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5623043.

Xiao:2010:TAT

[XTK10] Xiaokui Xiao, Yufei Tao, and Nick Koudas. Transparent anonymization: Thwarting adversaries who know the algorithm. *ACM Transactions on Database Systems*, 35(2):8:1–8:??, April 2010. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Xu:2019:DAB

[XTZ+19] Qian Xu, Chengxiang Tan, Wenye Zhu, Ya Xiao, Zhijie Fan, and Fujia Cheng. Decentralized attribute-based conjunctive keyword search scheme with online/offline encryption and outsource decryption for cloud computing. *Future Generation*

Computer Systems, 97(??): 306–326, August 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18329613.

Xie:2012:ORI

[XW12] Min Xie and Libin Wang. One-round identity-based key exchange with Perfect Forward Security. *Information Processing Letters*, 112(14–15):587–591, August 15, 2012. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019012001196.

Xie:2013:SIP

[XW13] Yongming Xie and Guojun Wang. Special issue papers: Practical distributed secret key generation for delay tolerant networks. *Concurrency and Computation: Practice and Experience*, 25(14):2067–2079, September 25, 2013. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Xiong:2012:CBP

[XWDN12] Kaiqi Xiong, Ronghua Wang, Wenliang Du, and Peng Ning. Containing bogus packet insertion attacks for broadcast authentication in sensor networks. *ACM Transactions on Sensor Networks*, 8(3):20:1–20:??, July 2012. CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Xu:2017:SEP

[XWK+17] Zhiyan Xu, Libing Wu, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, and Debiao He. A secure and efficient public auditing scheme using RSA algorithm for cloud storage. *The Journal of Supercomputing*, 73(12):5285–5309, December 2017. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Xu:2016:CCP

[XWLJ16] Jie Xu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin. Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, 27(1): 119–129, January 2016. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL http://www.computer.org/csdl/trans/td/2016/01/07010954-abs.html. See comments [XWS17].

Xiong:2017:CCC

[XWS17] Hu Xiong, Qiang Wang,

and Jianfei Sun. Comments on “Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation”. *Information Processing Letters*, 127(??):67–70, November 2017. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019017301308`. See [XWLJ16].

Xia:2016:SDM

[XWSW16] Zhihua Xia, Xinhui Wang, Xingming Sun, and Qian Wang. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. *IEEE Transactions on Parallel and Distributed Systems*, 27(2):340–352, February 2016. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL `http://www.computer.org/csdl/trans/td/2016/02/07039216-abs.html`.

Xie:2014:SCP

[XWXC14] Qi Xie, Guilin Wang, Fubiao Xia, and Deren Chen. Self-certified proxy convertible authenticated encryption: formal definitions and a provably secure scheme. *Concurrency and Computation: Practice and Experience*, 26(5): 1038–1051, April 10, 2014. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Xu:2018:SKS

[XWY+18] Li Xu, Chi-Yao Weng, Lun-Pin Yuan, Mu-En Wu, Raylin Tso, and Hung-Min Sun. A shareable keyword search over encrypted data in cloud computing. *The Journal of Supercomputing*, 74(3):1001–1023, March 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Xu:2018:DFH

[XWZ+18] Jian Xu, Laiwen Wei, Yu Zhang, Andi Wang, Fucai Zhou, and Chong zhi Gao. Dynamic fully homomorphic encryption-based Merkle tree for lightweight streaming authenticated data structures. *Journal of Network and Computer Applications*, 107(??):113–124, April 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804518300286`.

Xiao:2016:REM

[XWZW16] Chen Xiao, Lifeng Wang, Mengjiao Zhu, and Wendong Wang. A resource-efficient multimedia encryption scheme for embedded video sensing system based on unmanned aircraft. *Journal of Network and Computer Applications*, 59(??):117–125, January 2016. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804515001654.

Xu:2019:LAM

[XXCY19] Zisang Xu, Cheng Xu, Haixian Chen, and Fang Yang. A lightweight anonymous mutual authentication and key agreement scheme for WBAN. *Concurrency and Computation: Practice and Experience*, 31(14):e5295:1–e5295:??, July 25, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Xiong:2015:SRE

[XXX15] Lizhi Xiong, Zhengquan Xu, and Yanyan Xu. A secure re-encryption scheme for data services in a cloud computing environment. *Concurrency and Computation: Practice and Experience*, 27(17):4573–4585, December 10, 2015. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Xie:2012:DPK

[XXZ12] Xiang Xie, Rui Xue, and Rui Zhang. Deterministic public key encryption and identity-based encryption from lattices in the auxiliary-input setting. *Lecture Notes in Computer Science*, 7485:1–18, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32928-9_1/.

Xiao:2018:KRL

[XY18] Dianyan Xiao and Yang Yu. Klepto for ring-LWE encryption. *The Computer Journal*, 61(8):1228–1239, August 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/8/1228/5035449.

Xu:2019:SIC

[XYML19] Shengmin Xu, Guomin Yang, Yi Mu, and Ximeng Liu. A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. *Future Generation Computer Systems*, 97(??):284–294, August 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18320922.

Xing-Yuan:2011:PRS

[XYXYX11] Wang Xing-Yuan, Qin

Xue, and Xie Yi-Xin. Pseudo-random sequences generated by a class of one-dimensional smooth map. *Chinese Physics Letters*, 28 (8):080501, 2011. CODEN CPLEEU. ISSN 0256-307X (print), 1741-3540 (electronic). URL http://stacks.iop.org/0256-307X/28/i=8/a=080501.

Xiao:2019:NEA

[XZL+19] C. Xiao, L. Zhang, W. Liu, L. Cheng, P. Li, Y. Pan, and N. Bergmann. NV-eCryptfs: Accelerating enterprise-level cryptographic file system with non-volatile memory. *IEEE Transactions on Computers*, 68(9):1338–1352, September 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Xu:2015:ORA

[XZLW15] Chang Xu, Liehuang Zhu, Zhoujun Li, and Feng Wang. One-round affiliation-hiding authenticated asymmetric group key agreement with semi-trusted group authority. *The Computer Journal*, 58 (10):2509–2519, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2509.

Xiong:2019:PPH

[XZP+19] Hu Xiong, Yanan Zhao, Li Peng, Hao Zhang, and Kuo-Hui Yeh. Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing. *Future Generation Computer Systems*, 97(??):453–461, August 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19300172.

Xiong:2012:CLR

[XZY+12] Hao Xiong, Cong Zhang, Tsz Hon Yuen, Echo P. Zhang, Siu Ming Yiu, and Sihan Qing. Continual leakage-resilient dynamic secret sharing in the split-state model. *Lecture Notes in Computer Science*, 7618:119–130, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34129-8_11/.

Xiao:2018:FEI

[XZZ18] Chang Xiao, Cheng Zhang, and Changxi Zheng. FontCode: Embedding information in text documents using glyph perturbation. *ACM Transactions on Graphics*, 37(2):15:1–15:??, July 2018. CODEN

ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Yoo:2017:PQD

[Y+17] Y. Yoo et al. A post-quantum digital signature scheme based on supersingular isogenies. Cryptology ePrint Archive report, 2017. URL `http://eprint.iacr.org/2017/186`.

Yaacoubi:2019:REM

[Yaa19] Omar Yaacoubi. The rise of encrypted malware. *Network Security*, 2019(5):6–9, May 2019. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1353485819300595`.

Yamaguchi:2012:EVC

[Yam12] Yasushi Yamaguchi. An extended visual cryptography scheme for continuous-tone images. *Lecture Notes in Computer Science*, 7128:228–242, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32205-1_19/`.

Yu:2015:SDS

[YAM+15] Yong Yu, Man Ho Au, Yi Mu, Willy Susilo, and Huai Wu. Secure delegation of signing power from factorization. *The Computer Journal*, 58(4):867–877, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/4/867`.

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`.

Yang:2011:PQC

[Yan11] Bo-Yin Yang, editor. *Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 — December 2, 2011. Proceedings*, volume 7071 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011. CODEN LNCSD9. ISBN 3-642-25404-7. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http:/`

/www.springerlink.com/content/978-3-642-25404-8.

Yang:2014:BEB

[Yan14] Yang Yang. Broadcast encryption based non-interactive key distribution in MANETs. *Journal of Computer and System Sciences*, 80(3):533–545, May 2014. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000013001189.

Yang:2011:GSS

[YC11] Ching-Nung Yang and Yu-Ying Chu. A general (k, n) scalable secret image sharing scheme with the smooth scalability. *The Journal of Systems and Software*, 84(10):1726–1733, October 2011. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211001105.

Yang:2012:PST

[YC12] Jun-Han Yang and Tian-Jie Cao. Provably secure three-party password authenticated key exchange protocol in the standard model. *The Journal of Systems and Software*, 85(2):340–350, February 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211002172.

Yang:2016:EBB

[YCC16] Ching-Nung Yang, Cheng-Hua Chen, and Song-Ruei Cai. Enhanced Boolean-based multi secret image sharing scheme. *The Journal of Systems and Software*, 116(??):22–34, June 2016. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121215000205.

Yi:2017:ZCL

[YCL17] Wentan Yi, Shaozhen Chen, and Yuchen Li. Zero-correlation linear cryptanalysis of SAFER block cipher family using the undisturbed bits. *The Computer Journal*, 60(4):613–624, March 23, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/4/613/2354610.

Yuan:2013:PVQ

[YCM+13] Lihua Yuan, Chao-Chih Chen, Prasant Mohapatra, Chen-Nee Chuah, and Krishna Kant. A proxy view of quality of Domain Name Service, poisoning attacks and survival strategies. *ACM Transactions on Internet Technology (TOIT)*, 12(3):9:1–9:??, May 2013. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Yu:2016:DNF

[YCR16] Jiangshan Yu, Vincent Cheval, and Mark Ryan. DTKI: a new formalized PKI with verifiable trusted parties. *The Computer Journal*, 59(11):1695–1713, November 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/11/1695.

Yao:2015:LAB

[YCT15] Xuanxia Yao, Zhi Chen, and Ye Tian. A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Computer Systems*, 49(??):104–112, August 2015. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X14002039.

Yuen:2012:IBE

[YCZY12] Tsz Hon Yuen, Sherman S. M. Chow, Ye Zhang, and Siu Ming Yiu. Identity-based encryption resilient to continual auxiliary leakage. *Lecture Notes in Computer Science*, 7237:117–134, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/accesspage/chapter/10.1007/978-3-642-29011-4_8; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_9/.

Yu:2017:PDA

[YD17] Meng-Day (Mandel) Yu and Srinivas Devadas. Pervasive, dynamic authentication of physical items. *Communications of the Association for Computing Machinery*, 60(4):32–39, April 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2017/4/215034/fulltext.

Yasuda:2015:MQC

[YDH+15] Takanori Yasuda, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi, and Kouichi Sakurai. A multivariate quadratic challenge toward post-quantum generation cryptography. *ACM Communications in Computer Algebra*, 49(3):105–107, September 2015. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Yao:2019:CTC

[YDV19] Fan Yao, Miloš Doroslovački, and Guru Venkataramani. Covert timing channels exploiting cache coherence hardware: Characterization and defense. *International Journal of Parallel Programming*, 47(4):595–620, August 2019. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic).

Yan:2016:DEB

[YDY+16] Zheng Yan, Wenxiu Ding, Xixun Yu, Haiqi Zhu, and Robert H. Deng. Deduplication on encrypted big data in cloud. *IEEE Transactions on Big Data*, 2(2): 138–150, ???? 2016. CODEN ???? ISSN 2332-7790.

Ye:2010:ACC

[Ye10] Guodong Ye. Another constructed chaotic image encryption scheme based on Toeplitz matrix and Hankel matrix. *Fundamenta Informaticae*, 101(4):321–333, December 2010. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Yamada:2012:PBR

[YE12] Takaaki Yamada and Isao Echizen. PC-based realtime video watermark embedding system independent of platform for parallel computing. *Lecture Notes in Computer Science*, 7110:15–33, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-28693-3_2/`.

Ye:2014:NIE

[Ye14] Ruisong Ye. A novel image encryption scheme based on generalized multisawtooth maps. *Fundamenta Informaticae*, 133 (1):87–104, January 2014. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Yekhanin:2010:LDC

[Yek10] Sergey Yekhanin. *Locally Decodable Codes and Private Information Retrieval Schemes*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-14357-1 (hardcover), 3-642-14358-X (e-book). ISSN 1619-7100 (print), 2197-845X (electronic). xii + 82 pp. LCCN QA76.9.A25 Y45 2010eb. URL `http://www.springerlink.com/content/978-3-642-14358-8`.

Yoshida:2012:OGT

[YFF12] Maki Yoshida, Toru Fujiwara, and Marc Fossorier.

Optimum general threshold secret sharing. *Lecture Notes in Computer Science*, 7412:187–204, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32284-6_11/`.

Yu:2012:EPF

[YFK+12] Jia Yu, Fanyu, Kong, Xiangguo Cheng, Rong Hao, and Jianxi Fan. Erratum to the paper: Forward-Secure Identity-Based Public-Key Encryption without Random Oracles. *Fundamenta Informaticae*, 114(1):103, January 2012. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic). See [YKC+11].

Yang:2017:CCS

[YFT17] Kun Yang, Domenic Forte, and Mark M. Tehranipoor. CDTA: a comprehensive solution for counterfeit detection, traceability, and authentication in the IoT supply chain. *ACM Transactions on Design Automation of Electronic Systems*, 22(3):42:1–42:??, May 2017. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Yang:2018:RRE

[YFT18] Kun Yang, Domenic Forte, and Mark Tehranipoor. ReSC: an RFID-Enabled solution for defending IoT supply chain. *ACM Transactions on Design Automation of Electronic Systems*, 23(3):29:1–29:??, April 2018. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Yuce:2017:AFI

[YGD+17] Bilgiday Yuce, Nahid Farhady Ghalaty, Chinmay Deshpande, Harika Santapuri, Conor Patrick, Leyla Nazhandali, and Patrick Schaumont. Analyzing the fault injection sensitivity of secure embedded software. *ACM Transactions on Embedded Computing Systems*, 16(4):95:1–95:??, August 2017. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Yang:2015:SHI

[YGFL15] Zhen Yang, Kaiming Gao, Kefeng Fan, and Yingxu Lai. Sensational headline identification by normalized cross entropy-based metric. *The Computer Journal*, 58(4):644–655, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/4/644`.

Ye:2017:VCS

[YGS+17] Katherine Q. Ye, Matthew Green, Naphat Sanguansin, Lennart Beringer, Adam Petcher, and Andrew W. Appel. Verified correctness and security of mbedTLS HMAC-DRBG. In ACM, editor, *Proceedings of CCS 17, October 30–November 3, 2017, Dallas, TX, USA*, pages 1–14. ACM Press, New York, NY 10036, USA, 2017. ISBN 1-4503-4946-3. LCCN ???? URL `http://www.cs.princeton.edu/~appel/papers/verified-hmac-drbg.pdf`.

Ye:2016:IEA

[YH16] Guodong Ye and Xiaoling Huang. An image encryption algorithm based on autoblocking and electrocardiography. *IEEE MultiMedia*, 23(2):64–71, April/June 2016. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166 (electronic). URL `https://www.computer.org/csdl/mags/mu/2016/02/mmu2016020064-abs.html`.

Yang:2018:RKF

[YHHM18] Li Yang, Ziyi Han, Zhengan Huang, and Jianfeng Ma. A remotely keyed file encryption scheme under mobile cloud computing. *Journal of Network and Computer Applications*, 106(??):90–99, March 15, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804517304241`.

Yang:2016:IHA

[YHHS16] Xu Yang, Xinyi Huang, Jinguang Han, and Chunhua Su. Improved handover authentication and key pre-distribution for wireless mesh networks. *Concurrency and Computation: Practice and Experience*, 28(10):2978–2990, July 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Yu:2010:IBF

[YHK+10] Jia Yu, Rong Hao, Fanyu Kong, Xiangguo Cheng, Huawei Zhao, and Chen Yangkui. Identity-based forward secure threshold signature scheme based on mediated RSA. *International Journal of Computer Applications*, 32(4):469–475, 2010. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.2316/Journal.202.2010.4.202-2927`.

Yang:2016:EHA

[YHL16] Xu Yang, Xinyi Huang, and Joseph K. Liu. Efficient handover authentication with user anonymity and untraceability for mobile cloud computing. *Future Generation Computer Systems*, 62(??):190–195, September 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X15003088.

Yao:2019:RSA

[YHSW19] Jiaying Yao, Zhigeng Han, Muhammad Sohail, and Liangmin Wang. A robust security architecture for SDN-based 5G networks. *Future Internet*, 11(4):85, March 28, 2019. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/11/4/85.

Yang:2014:MDF

[YI14] Ying Yang and Ioannis Ivrissimtzis. Mesh discriminative features for 3D steganalysis. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 10(3):27:1–27:??, April 2014. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Yamada:2017:EPA

[YI17] Asahiko Yamada and Tatsuro Ikeda. Enhanced PKI authentication with trusted product at claimant. *Computers & Security*, 67(??):324–334, June 2017. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404817300044.

Youn:2018:DAH

[YJC18] Taek-Young Youn, Nam-Su Jho, and Ku-Young Chang. Design of additive homomorphic encryption with multiple message spaces for secure and practical storage services over encrypted data. *The Journal of Supercomputing*, 74(8):3620–3638, August 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Yang:2018:CPG

[YJSL18] Hongbin Yang, Shuxiong Jiang, Wenfeng Shen, and Zhou Lei. Certificateless provable group shared data possession with comprehensive privacy preservation for cloud storage. *Future Internet*, 10(6):49, June 07, 2018. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/10/6/49.

Yang:2016:TCP

[YK16] Baijian Justin Yang and Brian Kirk. Try-CybSI: A platform for trying out cybersecurity. *IEEE Se-*

curity & Privacy, 14(4): 74–75, July/August 2016. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic). URL https://www.computer.org/csdl/mags/sp/2016/04/msp2016040074-abs.html.

Yassein:2016:FSB

[YKA16] M. B. Yassein, Y. Khamayseh, and M. AbuJazoh. Feature selection for black hole attacks. *J.UCS: Journal of Universal Computer Science*, 22(4):521–??, ???? 2016. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL http://www.jucs.org/jucs_22_4/feature_selection_for_black.

Yoo:2010:IRR

[YKBS10] Sang-Kyung Yoo, Deniz Karakoyunlu, Berk Birand, and Berk Sunar. Improving the robustness of ring oscillator TRNGs. *ACM Transactions on Reconfigurable Technology and Systems*, 3(2):9:1–9:??, May 2010. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Yu:2011:FSI

[YKC+11] Jia Yu, Fanyu Kong, Xiangguo Cheng, Rong Hao, and Jianxi Fan. Forward-secure identity-based public-key encryption without random oracles. *Fundamenta Informaticae*, 111(2):241–256, April 2011. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic). See erratum [YFK+12].

Yu:2012:IRI

[YKC+12] Jia Yu, Fanyu Kong, Xiangguo Cheng, Rong Hao, and Jianxi Fan. Intrusion-resilient identity-based signature: Security definition and construction. *The Journal of Systems and Software*, 85(2):382–391, February 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211002342.

Young:2013:TPC

[YKGK13] Maxwell Young, Aniket Kate, Ian Goldberg, and Martin Karsten. Towards practical communication in Byzantine-resistant DHTs. *IEEE/ACM Transactions on Networking*, 21(1):190–203, February 2013. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Yang:2018:AIW

[YKK18] Zhi-Fang Yang, Chih-Ting Kuo, and Te-Hsi Kuo. Authorization identification by watermarking in log-polar coordinate system. *The Computer Journal*, 61 (11):1710–1723, November 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/11/1710/4993056.

Yum:2012:OPE

[YKKL12] Dae Hyun Yum, Duk Soo Kim, Jin Seok Kim, and Pil Joong Lee. Order-preserving encryption for non-uniformly distributed plaintexts. *Lecture Notes in Computer Science*, 7115: 84–97, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27890-7_7/.

Yoshino:2012:SIP

[YKNS12] Masayuki Yoshino, Noboru Kunihiro, Ken Naganuma, and Hisayoshi Sato. Symmetric inner-product predicate encryption based on three groups. *Lecture Notes in Computer Science*, 7496:215–234, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33272-2_14/.

Yum:2011:ACO

[YL11] Dae Hyun Yum and Pil Joong Lee. On the average cost of order-preserving encryption based on hypergeometric distribution. *Information Processing Letters*, 111(19):956–959, October 15, 2011. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019011001906.

Yi:2017:ICM

[YL17] Haibo Yi and Weijian Li. On the importance of checking multivariate public key cryptography for side-channel attacks: The case of enTTS scheme. *The Computer Journal*, 60(8): 1197–1209, August 1, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/8/1197/2996413.

Yuen:2013:ELT

[YLA+13] Tsz Hon Yuen, Joseph K. Liu, Man Ho Au, Willy Susilo, and Jianying Zhou. Efficient linkable and/or threshold ring signature without random oracles. *The Computer Journal*, 56(4):407–421, April 2013. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.

org/content/56/4/407.full.pdf+html.

Yang:2012:WSI

[YLL+12] Chunfang Yang, Fenlin Liu, Shiguo Lian, Xiangyang Luo, and Daoshun Wang. Weighted stego-image steganalysis of messages hidden into each bit plane. *The Computer Journal*, 55(6):717–727, June 2012. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/55/6/717.full.pdf+html.

Yang:2018:NSS

[YLL+18] Zheng Yang, Chao Liu, Wanping Liu, Daigu Zhang, and Song Luo. A new strong security model for stateful authenticated group key exchange. *International Journal of Information Security*, 17(4):423–440, August 2018. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-017-0373-1.

You:2012:DDS

[YLS12] Ilsun You, Jong-Hyouk Lee, and Kouichi Sakurai. DSSH: Digital signature based secure handover for network-based mobility management. *International Journal of Computer Systems Science and Engineering*, 27(3):??, ???? 2012. CODEN CSSEEI. ISSN 0267-6192.

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.

Yi:2013:ETS

[YLW13] Xun Yi, San Ling, and Huaxiong Wang. Efficient two-server password-only authenticated key exchange. *IEEE Transactions on Parallel and Distributed Systems*, 24(9):1773–1782, 2013. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Yu:2016:CBE

[YLZ+16] Qihong Yu, Jiguo Li, Yichen Zhang, Wei Wu, Xinyi Huang, and Yang Xiang. Certificate-based encryption resilient to key leakage. *The Journal of Systems and Soft-

ware, 116(??):101–112, June 2016. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121215001326.

Yagan:2016:WSN

[YM16] Osman Yagan and Armand M. Makowski. Wireless sensor networks under the random pairwise key predistribution scheme: Can resiliency be achieved with small key rings? *IEEE/ACM Transactions on Networking*, 24 (6):3383–3396, December 2016. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Yan:2018:FPS

[YM18] Qiuchen Yan and Stephen McCamant. Fast PokeEMU: Scaling generated instruction tests using aggregation and state chaining. *ACM SIGPLAN Notices*, 53(3):71–83, March 2018. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Yao:2019:ACC

[YM19] Zhongyuan Yao and Yi Mu. ACE with compact ciphertext size and decentralized sanitizers. *International Journal of Foundations of Computer Science (IJFCS)*, 30(4):531–549, June 2019. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054119400112.

Yakubu:2017:SSN

[YMA17] Abukari M. Yakubu, Namunu C. Maddage, and Pradeep K. Atrey. Securing speech noise reduction in outsourced environment. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 13(4):51:1–51:??, October 2017. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Yu:2017:ACA

[YMC+17] Gang Yu, Xiaoxiao Ma, Zhenfu Cao, Guang Zeng, and Wenbao Han. Accountable CP-ABE with public verifiability: How to effectively protect the outsourced data in cloud. *International Journal of Foundations of Computer Science (IJFCS)*, 28(6): 705–??, September 2017. CODEN IFCSEN. ISSN 0129-0541.

Ying:2013:PPB

[YMM13] Bidi Ying, Dimitrios Makrakis, and Hussein T. Mouftah. Privacy preserving broadcast message authentication protocol for VANETs. *Journal of Network and Computer Appli-*

cations, 36(5):1352–1364, September 2013. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804512001439`.

Yu:2010:PSI

[YMSH10] Gang Yu, Xiaoxiao Ma, Yong Shen, and Wenbao Han. Provable secure identity based generalized signcryption scheme. *Theoretical Computer Science*, 411(40–42):3614–3624, September 6, 2010. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Yu:2011:CLE

[YMWS11] Yong Yu, Yi Mu, Guilin Wang, and Ying Sun. Cryptanalysis of an off-line electronic cash scheme based on proxy blind signature. *The Computer Journal*, 54(10):1645–1651, October 2011. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/54/10/1645.full.pdf+html`.

Ying:2019:LRU

[YN19] Bidi Ying and Amiya Nayak. Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography. *Journal of Network and Computer Applications*, 131(??):66–74, April 1, 2019. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804519300256`.

Young:2015:DWE

[YNQ15] Vinson Young, Prashant J. Nair, and Moinuddin K. Qureshi. DEUCE: Write-efficient encryption for non-volatile memories. *ACM SIGPLAN Notices*, 50(4):33–44, April 2015. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Yavuz:2012:BFB

[YNR12a] Attila A. Yavuz, Peng Ning, and Michael K. Reiter. BAF and FI-BAF: Efficient and publicly verifiable cryptographic schemes for secure logging in resource-constrained systems. *ACM Transactions on Information and System Security*, 15(2):9:1–9:??, July 2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Yavuz:2012:ECR

[YNR12b] Attila A. Yavuz, Peng Ning, and Michael K. Reiter. Efficient, compromise resilient and append-only cryptographic schemes for secure audit logging. *Lecture Notes in Computer Science*, 7397:148–163, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32946-3_12/.

Yu:2016:SSD

[YNX+16] Yong Yu, Jianbing Ni, Qi Xia, Xiaofen Wang, Haomiao Yang, and Xiaosong Zhang. SDIVIP^2: shared data integrity verification with identity privacy preserving in mobile clouds. *Concurrency and Computation: Practice and Experience*, 28 (10):2877–2888, July 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Yong:2011:SPP

[Yon11] J. Yong. Security and privacy preservation for mobile E-learning via digital identity attributes. *J.UCS: Journal of Universal Computer Science*, 17(2):296–??, ???? 2011. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL http://www.jucs.org/jucs_17_2/security_and_privacy_preservation.

Yoneyama:2012:ORA

[Yon12] Kazuki Yoneyama. One-round authenticated key exchange with strong forward secrecy in the standard model against constrained adversary. *Lecture Notes in Computer Science*, 7631:69–86, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34117-5_5/.

Yang:2017:SAS

[YPRI17] Ying Yang, Ruggero Pintus, Holly Rushmeier, and Ioannis Ivrissimtzis. A 3D steganalytic algorithm and steganalysis-resistant watermarking. *IEEE Transactions on Visualization and Computer Graphics*, 23(2):1002–1013, February 2017. CODEN ITVGEA. ISSN 1077-2626 (print), 1941-0506 (electronic), 2160-9306. URL https://www.computer.org/csdl/trans/tg/2017/02/07399411-abs.html.

Yang:2012:EMA

[YQH12] Rui Yang, Zhenhua Qu, and Jiwu Huang. Exposing MP3 audio forgeries using frame offsets. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 8(2S):35:1–35:??, September 2012. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Yin:2017:QPE

[YQOL17] Hui Yin, Zheng Qin, Lu Ou, and Keqin Li. A query privacy-enhanced and secure search scheme over encrypted data in cloud computing. *Journal of Computer and System Sciences*, 90(??):14–27, December 2017. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0022000016301301`.

Yin:2019:SCM

[YQZ+19] Hui Yin, Zheng Qin, Jixin Zhang, Lu Ou, Fangmin Li, and Keqin Li. Secure conjunctive multi-keyword ranked search over encrypted cloud data for multiple data owners. *Future Generation Computer Systems*, 100(??):689–700, November 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X17321192`.

Yengisetty:2011:AVC

[YR11] Subba Rao V. Yengisetty and Bimal K. Roy. Applications of visual cryptography. *International Journal of Parallel, Emergent and Distributed Systems: IJPEDS*, 26(5):429–442, 2011. CODEN ???? ISSN 1744-5760 (print), 1744-5779 (electronic).

Yi:2016:IPA

[YRT+16] Xun Yi, Fang-Yu Rao, Zahir Tari, Feng Hao, Elisa Bertino, Ibrahim Khalil, and Albert Y. Zomaya. ID2S password-authenticated key exchange protocols. *IEEE Transactions on Computers*, 65(12):3687–3701, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Yang:2012:SAK

[YS12] Zheng Yang and Jörg Schwenk. Strongly authenticated key exchange protocol from bilinear groups without random oracles. *Lecture Notes in Computer Science*, 7496: 264–275, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-33272-2_17/`.

Yumbul:2015:EEP

[YS15] Kazim Yumbul and Erkay Savaş. Enhancing an embedded processor core for efficient and isolated execution of cryptographic algorithms. *The Computer Journal*, 58(10):2368–2387, October 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2368.

Yang:2015:EPS

[YSC+15] Bin Yang, Xingming Sun, Xianyi Chen, Jianjun Zhang, and Xu Li. Exposing photographic splicing by detecting the inconsistencies in shadows. *The Computer Journal*, 58(4):588–600, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/588.

Yang:2016:ECV

[YSC16] Ching-Nung Yang, Li-Zhe Sun, and Song-Ruei Cai. Extended color visual cryptography for black and white secret image. *Theoretical Computer Science*, 609 (part 1)(??):143–161, January 4, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397515008452.

Yang:2018:HEP

[YSF+18] Kun Yang, Haoting Shen, Domenic Forte, Swarup Bhunia, and Mark Tehranipoor. Hardware-enabled pharmaceutical supply chain security. *ACM Transactions on Design Automation of Electronic Systems*, 23(2):23:1–23:??, January 2018. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Yao:2014:NCR

[YSJL14] Hongyi Yao, Danilo Silva, Sidharth Jaggi, and Michael Langberg. Network codes resilient to jamming and eavesdropping. *IEEE/ACM Transactions on Networking*, 22(6):1978–1987, December 2014. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Yeh:2010:TRR

[YSL+10] Kuo-Hui Yeh, Chunhua Su, N. W. Lo, Yingjiu Li, and Yi-Xiang Hung. Two robust remote user authentication protocols using smart cards. *The Journal of Systems and Software*, 83(12):2556–2565, December 2010. CODEN JSSODM. ISSN 0164-1212.

Yuen:2014:TCT

[YSM14] Tsz Hon Yuen, Willy Susilo, and Yi Mu. Towards a cryptographic treatment of publish/subscribe systems. *Journal of Computer Security*,

22(1):33–67, ???? 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Yang:2019:ISO

[YSQM19] Haining Yang, Jiameng Sun, Jing Qin, and Jixin Ma. An improved scheme for outsourced computation with attribute-based encryption. *Concurrency and Computation: Practice and Experience*, 31(21): e4833:1–e4833:??, November 10, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Ylonen:2014:SAA

[YSS14] Tatu Ylonen, Karen Scarfone, and Murugiah Souppaya. Security of automated access management using Secure Shell (SSH). Technical report NISTIR 7966 (draft), National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 2014. URL `http://csrc.nist.gov/publications/drafts/nistir-7966/nistir_7966_draft.pdf`.

Yang:2011:CCK

[YT11a] Guomin Yang and Chik How Tan. Certificateless cryptography with KGC trust level 3. *Theoretical Computer Science*, 412(39): 5446–5457, September 9, 2011. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Yang:2011:CPK

[YT11b] Guomin Yang and Chik How Tan. Certificateless public key encryption: a new generic construction and two pairing-free schemes. *Theoretical Computer Science*, 412(8–10):662–674, March 4, 2011. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Yamada:2012:UEW

[YT12] Takaaki Yamada and Yoshiyasu Takahashi. Use of “emergable watermarks” as copy indicators for securing video content. *Lecture Notes in Computer Science*, 7128:181–195, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-32205-1_16/`.

Yi:2016:VSF

[YT16] Haibo Yi and Shaohua Tang. Very small FPGA processor for multivariate signatures. *The Computer Journal*, 59(7):1091–1101, July 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://`

comjnl.oxfordjournals.org/content/59/7/1091.

Ye:2018:VBA

[YTF+18] Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Willy Wolff, Adam J. Aviv, and Zheng Wang. A video-based attack for Android pattern lock. *ACM Transactions on Privacy and Security (TOPS)*, 21(4):19:1–19:??, October 2018. ISSN 2471-2566 (print), 2471-2574 (electronic). URL https://dl.acm.org/citation.cfm?id=3230740.

Yeh:2017:SIB

[YTH17] Lo-Yao Yeh, Woei-Jiunn Tsaur, and Hsin-Han Huang. Secure IoT-based, incentive-aware emergency personnel dispatching scheme with weighted fine-grained access control. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 9(1):10:1–10:??, October 2017. CODEN ???? ISSN 2157-6904 (print), 2157-6912 (electronic).

Yang:2014:IBI

[YTM+14] Guomin Yang, Chik How Tan, Yi Mu, Willy Susilo, and Duncan S. Wong. Identity based identification from algebraic coding theory. *Theoretical Computer Science*, 520(??):51–61, February 6, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397513006786.

Yang:2011:ACD

[YTP11] Yang Yang, Xiaohu Tang, and Udaya Parampalli. Authentication codes from difference balanced functions. *International Journal of Foundations of Computer Science (IJFCS)*, 22(6):1417–1429, September 2011. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Yasuda:2012:ASM

[YTS12] Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Sakurai. Application of scalar multiplication of Edwards curves to pairing-based cryptography. *Lecture Notes in Computer Science*, 7631:19–36, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34117-5_2/.

Yang:2018:IAC

[YWF18] Xiaokun Yang, Wujie Wen, and Ming Fan. Improving AES core performance via an advanced ASBUS protocol. *ACM Journal on Emerging Technolo-*

gies in Computing Systems (JETC), 14(1):6:1–6:??, March 2018. CODEN ???? ISSN 1550-4832.

Yan:2019:IFF

[YWJ+19] Hongyang Yan, Yu Wang, Chunfu Jia, Jin Li, Yang Xiang, and Witold Pedrycz. IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT. *Future Generation Computer Systems*, 95(??): 344–353, June 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X1830997X`.

Yao:2010:IDA

[YWK+10a] Lin Yao, Lei Wang, Xiangwei Kong, Guowei Wu, and Feng Xia. An inter-domain authentication scheme for pervasive computing environment. *Computers and Mathematics with Applications*, 60(2):234–244, July 2010. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122110000210`.

Yao:2010:ASP

[YWK10b] Yurong Yao, Edward Watson, and Beverly K. Kahn. Application service providers: market and adoption decisions. *Communications of the Association for Computing Machinery*, 53(7):113–117, July 2010. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Yan:2017:PIS

[YWL+17] Jianhua Yan, Licheng Wang, Jing Li, Muzi Li, Yixan Yang, and Wenbin Yao. Pre-image sample algorithm with irregular Gaussian distribution and construction of identity-based signature. *Concurrency and Computation: Practice and Experience*, 29(20):??, October 25, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Ye:2019:NCA

[YWM19] T. Ye, Y. Wei, and W. Meier. A new cube attack on MORUS by using division property. *IEEE Transactions on Computers*, 68(12):1731–1740, December 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Yang:2015:RCI

[YWNW15] Hong-Ying Yang, Xiang-Yang Wang, Pan-Pan Niu, and Ai-Long Wang. Robust color image watermarking using geometric invariant quaternion polar harmonic transform. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 11(3):40:1–40:??, January 2015. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Wang:2011:RDA

[yWpNyL11] Xiang yang Wang, Pan pan Niu, and Ming yu Lu. A robust digital audio watermarking scheme using wavelet moment invariance. *The Journal of Systems and Software*, 84(8): 1408–1421, August 2011. CODEN JSSODM. ISSN 0164-1212.

Wang:2013:RBC

[yWpWyYpN13] Xiang yang Wang, Chun peng Wang, Hong ying Yang, and Pan pan Niu. A robust blind color image watermarking in quaternion Fourier transform domain. *The Journal of Systems and Software*, 86(2):255–277, February 2013. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121212002312`.

Yu:2012:NWM

[YWT+12] Zhiwei Yu, Chaokun Wang, Clark Thomborson, Jianmin Wang, Shiguo Lian, and Athanasios V. Vasilakos. A novel watermarking method for software protection in the cloud. *Software—Practice and Experience*, 42(4):409–430, ???? 2012. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Yang:2010:CRS

[YWW10] Cheng-Hsing Yang, Shiuh-Jeng Wang, and Chi-Yao Weng. Capacity-raising steganography using multi-pixel differencing and pixel-value shifting operations. *Fundamenta Informaticae*, 98(2–3):321–336, April 2010. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Wang:2018:CIW

[yWXyZ+18] Xiang yang Wang, Huan Xu, Si yu Zhang, Lin lin Liang, Pan pan Niu, and Hong ying Yang. A color image watermarking approach based on synchronization correction. *Fundamenta Informaticae*, 158 (4):385–407, ???? 2018. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Yang:2019:SCC

[YWY+19] Haomiao Yang, Xiaofen Wang, Chun Yang, Xin Cong, and You Zhang. Securing content-centric networks with content-based encryption. *Journal of Network and Computer Applications*, 128(??):21–32, February 15, 2019. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518303874.

Yan:2012:SMA

[YWYZ12] Diqun Yan, Rangding Wang, Xianmin Yu, and Jie Zhu. Steganography for MP3 audio by exploiting the rule of window switching. *Computers & Security*, 31(5):704–716, July 2012. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404812000673.

Yu:2012:SME

[YWZ+12] Jia Yu, Shuguang Wang, Huawei Zhao, Minglei Shu, Jialiang Lv, and Qiang Guo. A simultaneous members enrollment and revocation protocol for secret sharing schemes. *Lecture Notes in Computer Science*, 7299:190–197, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-30428-6_16/.

Yang:2018:EEC

[YWZ+18] Wencheng Yang, Song Wang, Guanglou Zheng, Junaid Chaudhry, and Craig Valli. ECB4CI: an enhanced cancelable biometric system for securing critical infrastructures. *The Journal of Supercomputing*, 74(10):4893–4909, October 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Yu:2016:CDI

[YXA+16] Yong Yu, Liang Xue, Man Ho Au, Willy Susilo, Jianbing Ni, Yafang Zhang, Athanasios V. Vasilakos, and Jian Shen. Cloud data integrity checking with an identity-based auditing mechanism from RSA. *Future Generation Computer Systems*, 62(??):85–91, September 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X16300164.

Yang:2018:PBC

[YXA+18] Rupeng Yang, Qiuliang Xu, Man Ho Au, Zuoxia Yu, Hao Wang, and Lu Zhou. Position based cryptography with location privacy: a step for Fog Computing. *Future Generation Computer Systems*, 78 (part 2)(??):799–

806, January 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X17311032.

Ye:2018:ISS

[YXD18] Jun Ye, Zheng Xu, and Yong Ding. Image search scheme over encrypted database. *Future Generation Computer Systems*, 87(??):251–258, October 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X17324354.

Yoon:2011:SBC

[YY11] Eun-Jun Yoon and Kee-Young Yoo. A secure broadcasting cryptosystem and its application to grid computing. *Future Generation Computer Systems*, 27(5):620–626, May 2011. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Yoon:2013:RBB

[YY13] Eun-Jun Yoon and Kee-Young Yoo. Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. *The Journal of Supercomputing*, 63(1):235–255, January 2013. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-010-0512-1.

Young:2017:PSC

[YY17a] Adam L. Young and Moti Yung. Privacy and security: Cryptovirology: the birth, neglect, and explosion of ransomware. *Communications of the Association for Computing Machinery*, 60(7):24–26, July 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2017/7/218875/fulltext.

Yu:2017:PFS

[YY17b] Huifang Yu and Bo Yang. Pairing-free and secure certificateless signcryption scheme. *The Computer Journal*, 60(8):1187–1196, August 1, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/8/1187/2979229.

Yildiz:2017:BLF

[YYK+17] Muhammet Yildiz, Berrin Yanikoğlu, Alisher Kholmatov, Alper Kanak, Umut Uludağ, and Hakan

Erdoğan. Biometric layering with fingerprints: Template security and privacy through multi-biometric template fusion. *The Computer Journal*, 60(4):573–587, March 23, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `https://academic.oup.com/comjnl/article/60/4/573/2354606`.

Yang:2019:NPP

[YYK+19] Xu Yang, Xun Yi, Ibrahim Khalil, Hui Cui, Xuechao Yang, Surya Nepal, Xinyi Huang, and Yali Zeng. A new privacy-preserving authentication protocol for anonymous web browsing. *Concurrency and Computation: Practice and Experience*, 31(21):e4706:1–e4706:??, November 10, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Yesilyurt:2015:RWM

[YYO15] Murat Yesilyurt, Yildiray Yalman, and A. Turan Ozcerit. A robust watermarking method for MPEG-4 based on kurtosis. *The Computer Journal*, 58(7):1645–1655, July 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/7/1645`.

Yang:2013:ECS

[yYqWqZC13] Xiao yuan Yang, Li qiang Wu, Min qing Zhang, and Xiao-Feng Chen. An efficient CCA-secure cryptosystem over ideal lattices from identity-based encryption. *Computers and Mathematics with Applications*, 65(9):1254–1263, May 2013. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122112001447`.

Yang:2016:EPA

[YYS+16] Guangyang Yang, Jia Yu, Wenting Shen, Qianqian Su, Zhangjie Fu, and Rong Hao. Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability. *The Journal of Systems and Software*, 113(??):130–139, March 2016. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S016412121500268X`.

Yu:2019:PSI

[YYW19] Yong Yu, Guomin Yang, and Huaxiong Wang. Preface: Special issue cryptography and provable security. *International Journal of Foundations of Computer Science (IJFCS)*, 30 (4):489–492, June 2019. CODEN IFCSEN. ISSN 0129-0541. URL `https://www.worldscientific.com/doi/10.1142/S0129054119020027`.

Yang:2012:LUC

[YZ12] Bo Yang and Mingwu Zhang. LR-UESDE: a continual-leakage resilient encryption with unbounded extensible set delegation. *Lecture Notes in Computer Science*, 7496: 125–142, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-33272-2_9/`.

Yang:2017:SKS

[YZCT17] Yang Yang, Xianghan Zheng, Victor Chang, and Chunming Tang. Semantic keyword searchable proxy re-encryption for postquantum secure cloud storage. *Concurrency and Computation: Practice and Experience*, 29(19):??, October 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Yan:2019:HDS

[YZDZ19] Z. Yan, L. Zhang, W. DING, and Q. Zheng. Heterogeneous data storage management with deduplication in cloud computing. *IEEE Transactions on Big Data*, 5(3):393–407, September 2019. ISSN 2332-7790.

Yang:2018:CDD

[YZL+18] Yang Yang, Xianghan Zheng, Ximeng Liu, Shangping Zhong, and Victor Chang. Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system. *Future Generation Computer Systems*, 84(??):160–176, July 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X1730554X`.

Yang:2012:BPN

[YZLC12] Shuguo Yang, Yongbin Zhou, Jiye Liu, and Danyang Chen. Back propagation neural network based leakage characterization for practical security analysis of cryptographic implementations. *Lecture Notes in Computer Science*, 7259:169–185, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31912-9_12/`.

Yang:2012:NIB

[YZX+12] Geng Yang, Qiang Zhou, Xiaolong Xu, Jian Xu, and Chunming Rong. A novel identity-based key management and encryption scheme for distributed system. *Lecture Notes in Computer Science*, 7672: 123–138, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35362-8_11/.

Yang:2014:PST

[YZZ+14] Haomin Yang, Yaoxue Zhang, Yuezhi Zhou, Xiaoming Fu, Hao Liu, and Athanasios V. Vasilakos. Provably secure three-party authenticated key agreement protocol using smart cards. *Computer Networks (Amsterdam, Netherlands: 1999)*, 58(??):29–38, January 15, 2014. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128613002867.

Zhai:2017:EEI

[ZAAB17] Xiaojun Zhai, Amine Ait Si Ali, Abbes Amira, and Faycal Bensaali. ECG encryption and identification based security solution on the Zynq SoC for connected health systems. *Journal of Parallel and Distributed Computing*, 106(??):143–152, August 2017. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731516301927.

Zufiria:2017:GLM

[ZÁC17] Pedro J. Zufiria and José A. Álvarez-Cubero. Generalized lexicographic MultiObjective combinatorial optimization. Application to cryptography. *SIAM Journal on Optimization*, 27(4):2182–2201, ???? 2017. CODEN SJOPE8. ISSN 1052-6234 (print), 1095-7189 (electronic).

Zidaric:2019:HOA

[ZAG19] Nusa Zidaric, Mark Aagaard, and Guang Gong. Hardware optimizations and analysis for the WG-16 cipher with tower field arithmetic. *IEEE Transactions on Computers*, 68 (1):67–82, ???? 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL https://ieeexplore.ieee.org/document/8409309/.

Zajac:2019:HEM

[Zaj19] Pavol Zajac. Hybrid encryption from McEliece cryptosystem with pseudo-random error vector. *Fundamenta Informaticae*, 169 (4):345–360, ???? 2019. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Zoni:2018:CSC

[ZBPF18] Davide Zoni, Alessandro Barenghi, Gerardo Pelosi, and William Fornaciari. A comprehensive side-channel information leakage analysis of an in-order RISC CPU microarchitecture. *ACM Transactions on Design Automation of Electronic Systems*, 23(5): 57:1–57:??, October 2018. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Zhang:2011:TNT

[ZBR11] Zhenxia Zhang, Azzedine Boukerche, and Hussam Ramadan. TEASE: a novel Tunnel-based sEcure Authentication SchemE to support smooth handoff in IEEE 802.11 wireless networks. *Journal of Parallel and Distributed Computing*, 71(7):897–905, July 2011. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731510002686.

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).

Zhang:2013:RMS

[ZC13] En Zhang and Yongquan Cai. Rational multi-secret sharing scheme in standard point-to-point communication networks. *International Journal of Foundations of Computer Science (IJFCS)*, 24(6):879–??, September 2013. CODEN IFCSEN. ISSN 0129-0541.

Zhang:2015:PCL

[ZCC15] Zongyang Zhang, Sherman S. M. Chow, and Zhenfu Cao. Post-challenge leakage in public-key encryption. *Theoretical Computer Science*, 572(??):25–49, March 23, 2015. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397515000377.

Zhang:2012:TCS

[ZCS+12] Zhifang Zhang, Yeow Meng

Chee, San Ling, Mulan Liu, and Huaxiong Wang. Threshold changeable secret sharing schemes revisited. *Theoretical Computer Science*, 418(1):106–115, February 10, 2012. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397511008206.

Zhang:2019:EPK

[ZCL+19] Kai Zhang, Jie Chen, Hyung Tae Lee, Haifeng Qian, and Huaxiong Wang. Efficient public key encryption with equality test in the standard model. *Theoretical Computer Science*, 755(??):65–80, January 10, 2019. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S030439751830464X.

Zhang:2014:GCS

[ZCLL14] Yinghui Zhang, Xiaofeng Chen, Jin Li, and Hui Li. Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 75 (part A)(??):192–211, December 24, 2014. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128614003648.

Zhang:2015:IAI

[ZCWS15] Zhi-Kai Zhang, Michael Cheng Yi Cho, Zong-Yu Wu, and Shiuhpyng Winston Shieh. Identifying and authenticating IoT objects in a natural context. *Computer*, 48(8):81–83, August 2015. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://csdl.computer.org/csdl/mags/co/2015/08/mco2015080081-abs.html.

Zhou:2019:SAN

[ZCZ+19] Lu Zhou, Jiageng Chen, Yidan Zhang, Chunhua Su, and Marino Anthony James. Security analysis and new models on the intelligent symmetric key encryption. *Computers & Security*, 80(??):14–24, January 2019. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404818309647.

Zeng:2019:PKE

[ZCZQ19] Ming Zeng, Jie Chen, Kai Zhang, and Haifeng Qian. Public key encryption with equality test via hash proof system. *Theoretical Computer Science*, 795(??):20–35, November 26, 2019. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397519303822.

Zhang:2018:SSH

[ZDHZ18] Yinghui Zhang, Robert H. Deng, Gang Han, and Dong Zheng. Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things. *Journal of Network and Computer Applications*, 123(??):89–100, December 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518302935.

Zhang:2012:AOP

[ZDL12] Jiuling Zhang, Beixing Deng, and Xing Li. Additive order preserving encryption based encrypted documents ranking in secure cloud storage. *Lecture Notes in Computer Science*, 7332:58–65, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31020-1_8/.

Zhou:2016:IBP

[ZDW+16] Yunya Zhou, Hua Deng, Qianhong Wu, Bo Qin, Jianwei Liu, and Yong Ding. Identity-based proxy re-encryption version 2: Making mobile access easy in cloud. *Future Generation Computer Systems*, 62(??):128–139, September 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X15003076.

Zetter:2014:CZD

[Zet14] Kim Zetter. *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Crown, New York, NY, USA, 2014. ISBN 0-7704-3617-X (hardcover), 0-7704-3619-6 (paperback), 0-7704-3618-8 (e-book). ???? pp. LCCN UG593 .Z48 2014.

Zhou:2018:SAE

[ZFH+18] Yukun Zhou, Dan Feng, Yu Hua, Wen Xia, Min Fu, Fangting Huang, and Yucheng Zhang. A similarity-aware encrypted deduplication scheme with flexible access control in the cloud. *Future Generation Computer Systems*, 84(??):177–189, July 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S016773939X17309238.

Zhao:2010:PSA

[ZG10] Jianjie Zhao and Dawu Gu. Provably secure authenticated key exchange protocol under the CDH assumption. *The Journal of Systems and Software*, 83 (11):2297–2304, November 2010. CODEN JSSODM. ISSN 0164-1212.

Zhou:2016:HFD

[ZGC16] Peng Zhou, Xiaojing Gu, and Rocky K. C. Chang. Harvesting file download exploits in the Web: a hacker's view. *The Computer Journal*, 59(4):522–540, April 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/4/522.

Zhou:2018:CBG

[ZGCZ18] Caixue Zhou, Guangyong Gao, Zongmin Cui, and Zhiqiang Zhao. Certificate-based generalized ring signcryption scheme. *International Journal of Foundations of Computer Science (IJFCS)*, 29(6):1063–1088, September 2018. ISSN 0129-0541. URL https://www.worldscientific.com/doi/10.1142/S0129054118500211.

Zhang:2018:AAG

[ZGL+18a] Qikun Zhang, Yong Gan, Lu Liu, Xianmin Wang, Xiangyang Luo, and Yuanzhang Li. An authenticated asymmetric group key agreement based on attribute encryption. *Journal of Network and Computer Applications*, 123(??):1–10, December 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518302704.

Zhang:2018:PPE

[ZGL+18b] Yin Zhang, Raffaele Gravina, Huimin Lu, Massimo Villari, and Giancarlo Fortino. PEA: Parallel electrocardiogram-based authentication for smart healthcare systems. *Journal of Network and Computer Applications*, 117(??):10–16, September 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804518301693.

Gao:2012:DES

[zGXW12] Chong zhi Gao, Dongqing Xie, and Baodian Wei. Deniable encryptions secure against adaptive chosen ciphertext attack. *Lecture Notes in Computer Science*, 7232:46–62, 2012.

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29101-2_4/.

Zadeh:2015:ASP

[ZH15] Abdulah Abdulah Zadeh and Howard M. Heys. Application of simple power analysis to stream ciphers constructed using feedback shift registers. *The Computer Journal*, 58(4):961–972, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/961.

Zhang:2012:LDC

[Zha12] Haibin Zhang. Length-doubling ciphers and tweakable ciphers. *Lecture Notes in Computer Science*, 7341:100–116, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31284-7_7/.

Zhang:2015:BYO

[Zha15a] Hongwen Zhang. Bring your own encryption: balancing security with practicality. *Network Security*, 2015(1):18–20, January 2015. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1353485815700115.

Zhang:2015:STR

[Zha15b] Zhiyong Zhang. Security, trust and risk in multimedia social networks. *The Computer Journal*, 58(4):515–517, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/515.

Zhao:2017:RAS

[ZHH+17] Caidan Zhao, Minmin Huang, Lianfen Huang, Xiaojiang Du, and Mohsen Guizani. A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 128(??):164–171, December 9, 2017. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128617302347.

Zhang:2011:PFB

[ZHL+11] Peng Zhang, Jiankun Hu, Cai Li, Mohammed Bennamoun, and Vijayakumar Bhagavatula. A pitfall in fingerprint biocryptographic key generation. *Computers & Security*, 30(5):311–319, July 2011. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404811000459`.

Zhu:2015:IDM

[ZHL15] Hui Zhu, Cheng Huang, and Hui Li. Information diffusion model based on privacy setting in online social networking services. *The Computer Journal*, 58(4):536–548, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/58/4/536`.

Zhao:2010:IFU

[ZHS10] Xi Zhao, Anthony Tung Shuen Ho, and Yun Q. Shi. Image forensics using generalised Benford's Law for improving image authentication detection rates in semi-fragile watermarking. *International Journal of Digital Crime and Forensics*, 2(2):1–20, ???? 2010. CODEN ???? ISSN 1941-6210 (print), 1941-6229 (electronic). URL `https://dblp.org/db/journals/ijdcf/ijdcf2.html#ZhaoHS10`.

Zhang:2019:REU

[ZHS+19] Jun Zhang, Rui Hou, Wei Song, Sally A. Mckee, Zhen Jia, Chen Zheng, Mingyu Chen, Lixin Zhang, and Dan Meng. RAGuard: an efficient and user-transparent hardware mechanism against ROP attacks. *ACM Transactions on Architecture and Code Optimization*, 15(4):50:1–50:??, January 2019. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3280852`.

Zhu:2016:SCI

[ZHT16] Youwen Zhu, Zhiqiu Huang, and Tsuyoshi Takagi. Secure and controllable k-NN query over encrypted cloud data with key confidentiality. *Journal of Parallel and Distributed Computing*, 89(??):1–12, March 2016. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0743731515002105`.

Zhu:2013:TSC

[Zhu13] Wen Tao Zhu. Towards secure and communication-efficient broadcast encryption systems. *Journal of Network and Computer Applications*, 36(1):178–

186, January 2013. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804512002159.

Zhou:2015:EPP

[ZHW15] Zhibin Zhou, Dijiang Huang, and Zhijie Wang. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption. *IEEE Transactions on Computers*, 64(1):126–138, January 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Zhang:2016:PPV

[ZHW+16] Lei Zhang, Chuanyan Hu, Qianhong Wu, Josep Domingo-Ferrer, and Bo Qin. Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response. *IEEE Transactions on Computers*, 65(8):2562–2574, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (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 nonvolatile main memory. *IEEE Micro*, 39(1):44–51, January/February 2019. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Zimand:2010:SEC

[Zim10] Marius Zimand. Simple extractors via constructions of cryptographic pseudo-random generators. *Theoretical Computer Science*, 411(10):1236–1250, March 4, 2010. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Zhang:2011:FBP

[ZJ11] Meng Zhang and Niraj K. Jha. FinFET-based power management for improved DPA resistance with low overhead. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 7(3):10:1–10:??, August 2011. CODEN ???? ISSN 1550-4832.

Zeng:2014:NFC

[ZJ14] Shengke Zeng and Shaoquan Jiang. A new framework for conditionally anonymous ring signature. *The Computer Journal*, 57(4):567–578, April 2014. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.

org/content/57/4/567.full.pdf+html.

Zhou:2012:CBF

[ZL12] Qing Zhou and Xiaofeng Liao. Collision-based flexible image encryption algorithm. *The Journal of Systems and Software*, 85(2):400–407, February 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0164121211002329.

Zhang:2019:CCF

[ZL19] X. Zhang and Y. Lao. On the construction of composite finite fields for hardware obfuscation. *IEEE Transactions on Computers*, 68(9):1353–1364, September 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Zhou:2015:PPS

[ZLDC15] Jun Zhou, Xiaodong Lin, Xiaolei Dong, and Zhenfu Cao. PSMPA: Patient self-controllable and multilevel privacy-preserving cooperative authentication in distributed-healthcare cloud computing system. *IEEE Transactions on Parallel and Distributed Systems*, 26(6):1693–1703, June 2015. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL http://csdl.computer.org/csdl/trans/td/2015/06/06779640-abs.html.

Zhao:2012:IAS

[ZLDD12] Yifan Zhao, Swee-Won Lo, Robert H. Deng, and Xuhua Ding. An improved authentication scheme for H.264/SVC and its performance evaluation over nonstationary wireless mobile networks. *Lecture Notes in Computer Science*, 7645:192–205, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34601-9_15/.

Zhao:2014:TAH

[ZLDD14] Yifan Zhao, Swee-Won Lo, Robert H. Deng, and Xuhua Ding. Technique for authenticating H.264/SVC and its performance evaluation over wireless mobile networks. *Journal of Computer and System Sciences*, 80(3):520–532, May 2014. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000013001177.

Zhang:2012:EEF

[ZLH+12] Yunmei Zhang, Joseph K. Liu, Xinyi Huang, Man Ho

Au, and Willy Susilo. Efficient escrow-free identity-based signature. *Lecture Notes in Computer Science*, 7496:161–174, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33272-2_11/.

Zhang:2015:RBA

[ZLQ15] Jiliang Zhang, Yaping Lin, and Gang Qu. Reconfigurable binding against FPGA replay attacks. *ACM Transactions on Design Automation of Electronic Systems*, 20(2):33:1–33:??, February 2015. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Zhang:2012:CCB

[ZLW+12] Leo Yu Zhang, Chengqing Li, Kwok-Wo Wong, Shi Shu, and Guanrong Chen. Cryptanalyzing a chaos-based image encryption algorithm using alternate structure. *The Journal of Systems and Software*, 85(9):2077–2085, September 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/science/article/pii/S016412121200101X.

Zhu:2017:PSN

[ZLW+17] Youwen Zhu, Xingxin Li, Jian Wang, Yining Liu, and Zhiguo Qu. Practical secure naïve Bayesian classification over encrypted big data in cloud. *International Journal of Foundations of Computer Science (IJFCS)*, 28(6):683–??, September 2017. CODEN IFCSEN. ISSN 0129-0541.

Zhang:2010:ESP

[ZLY10] Jianhong Zhang, Chenglian Liu, and Yixian Yang. An efficient secure proxy verifiably encrypted signature scheme. *Journal of Network and Computer Applications*, 33(1):29–34, January 2010. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804509001039.

Zhou:2019:LIB

[ZLY+19] Lu Zhou, Xiong Li, Kuo-Hui Yeh, Chunhua Su, and Wayne Chiu. Lightweight IoT-based authentication scheme in cloud computing circumstance. *Future Generation Computer Systems*, 91(??):244–251, February 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://

www.sciencedirect.com/science/article/pii/S0167739X18307878.

Zhang:2016:TLT

[ZM16] Mingwu Zhang and Yi Mu. Token-leakage tolerant and vector obfuscated IPE and application in privacy-preserving two-party point/polynomial evaluations. *The Computer Journal*, 59 (4):493–507, April 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/4/493.

Zhang:2018:SPF

[ZM18] Jianhong Zhang and Jian Mao. On the security of a pairing-free certificateless signcryption scheme. *The Computer Journal*, 61(4):469–471, April 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/4/469/4107198.

Zhang:2017:FGA

[ZML17] Rui Zhang, Hui Ma, and Yao Lu. Fine-grained access control system based on fully outsourced attribute-based encryption. *The Journal of Systems and Software*, 125 (??):344–353, March 2017. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL //www.sciencedirect.com/science/article/pii/S0164121216302606.

Zhang:2010:NSS

[ZMM+10] Qing Zhang, John McCullough, Justin Ma, Nabil Schear, Michael Vrable, Amin Vahdat, Alex C. Snoeren, Geoffrey M. Voelker, and Stefan Savage. Neon: system support for derived data management. *ACM SIGPLAN Notices*, 45(7): 63–74, July 2010. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Zielinska:2014:TS

[ZMS14] Elzbieta Zielińska, Wojciech Mazurczyk, and Krzysztof Szczypiorski. Trends in steganography. *Communications of the Association for Computing Machinery*, 57(3):86–95, March 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Zhang:2016:CAH

[ZMW16] Leyou Zhang, Yi Mu, and Qing Wu. Compact anonymous hierarchical identity-based encryption with constant size private keys. *The Computer Journal*, 59(4):452–461, April 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/4/452.

Zaeem:2017:MAI

[ZMYB17] Razieh Nokhbeh Zaeem, Monisha Manoharan, Yongpeng Yang, and K. Suzanne Barber. Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers & Security*, 65(??):50–63, March 2017. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404816301559.

Zafar:2010:GRN

[ZOC10] Fahad Zafar, Marc Olano, and Aaron Curtis. GPU random numbers via the Tiny Encryption Algorithm. In ????, editor, *HPG '10 Proceedings of the Conference on High Performance Graphics, Saarbrucken, Germany, June 25–27, 2010*, pages 133–141. Eurographics Association, Aire-la-Ville, Switzerland, 2010. ISBN ???? LCCN ???? URL http://www.cs.umbc.edu/~olano/papers/GPUTEA.pdf.

Zorpette:2012:BEC

[Zor12] Glenn Zorpette. The beginning of the end of cash [special report]. *IEEE Spectrum*, 49(6):27–29, June 2012. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Zhang:2017:PPN

[ZOSZ17] Yuankai Zhang, Adam O'Neill, Micah Sherr, and Wenchao Zhou. Privacy-preserving network provenance. *Proceedings of the VLDB Endowment*, 10(11): 1550–1561, August 2017. CODEN ???? ISSN 2150-8097.

Zavattoni:2015:SIA

[ZPM+15] E. Zavattoni, L. J. Dominguez Perez, S. Mitsunari, A. H. Sanchez-Ramirez, T. Teruya, and F. Rodriguez-Henriquez. Software implementation of an attribute-based encryption scheme. *IEEE Transactions on Computers*, 64(5):1429–1441, ???? 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Zheng:2016:EUV

[ZPW16] Nan Zheng, Aaron Paloski, and Haining Wang. An efficient user verification system using angle-based mouse movement biometrics. *ACM Transactions on Information and System Security*, 18(3):11:1–11:??, April 2016. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Zhao:2012:SSS

[ZPWY12] Dawei Zhao, Haipeng Peng, Cong Wang, and Yixian Yang. A secret sharing scheme with a short share realizing the (t, n) threshold and the adversary structure. *Computers and Mathematics with Applications*, 64(4):611–615, August 2012. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122111011382`.

Zhou:2017:IBB

[ZPXX17] Fucai Zhou, Su Peng, Jian Xu, and Zifeng Xu. Identity-based batch provable data possession with detailed analyses. *International Journal of Foundations of Computer Science (IJFCS)*, 28(6):743–??, September 2017. CODEN IFCSEN. ISSN 0129-0541.

Zenger:2016:AKE

[ZPZ+16] Christian T. Zenger, Mario Pietersz, Jan Zimmer, Jan-Felix Posielek, Thorben Lenze, and Christof Paar. Authenticated key establishment for low-resource devices exploiting correlated random channels. *Computer Networks (Amsterdam, Netherlands: 1999)*, 109 (part 1)(??):105–123, November 9, 2016. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1389128616301943`.

Zhang:2016:SBA

[ZQD16] Yue Zhang, Jing Qin, and Lihua Du. A secure biometric authentication based on PEKS. *Concurrency and Computation: Practice and Experience*, 28 (4):1111–1123, March 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Zhang:2015:MAA

[ZQQ15] G. Zhang, J. Qin, and S. Qazi. Multi-authority attribute-based encryption scheme from lattices. *J.UCS: Journal of Universal Computer Science*, 21 (3):483–??, ???? 2015. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL `http://www.jucs.org/jucs_21_3/multi_authority_attribute_based`.

Zhang:2010:EMO

[ZQWZ10] Lei Zhang, Bo Qin, Qianhong Wu, and Futai Zhang. Efficient many-to-one authentication with certificateless aggregate signatures. *Computer Networks (Amsterdam, Netherlands: 1999)*, 54(14):2482–2491, October 6, 2010. CODEN ???? ISSN 1389-1286.

Zmudzinski:2012:WEU

[ZS12] Sascha Zmudzinski and Martin Steinebach. Watermark embedding using audio fingerprinting. *Lecture Notes in Computer Science*, 7228:63–79, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31971-6_4/.

Zhao:2012:SSM

[ZSA12] Hong Zhao, Yun Q. Shi, and Nirwan Ansari. Steganography in streaming multimedia over networks. *Lecture Notes in Computer Science*, 7110: 96–114, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28693-3_7/.

Zhou:2019:LIN

[ZSH+19] Lu Zhou, Chunhua Su, Zhi Hu, Sokjoon Lee, and Hwajeong Seo. Lightweight implementations of NIST p-256 and SM2 ECC on 8-bit resource-constraint embedded device. *ACM Transactions on Embedded Computing Systems*, 18(3): 23:1–23:??, June 2019. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3236010.

Zheng:2018:GDP

[ZSMS18] Zhigao Zheng, Nitin Saxena, K. K. Mishra, and Arun Kumar Sangaiah. Guided dynamic particle swarm optimization for optimizing digital image watermarking in industry applications. *Future Generation Computer Systems*, 88(??):92–106, November 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18307945.

Zanon:2019:FKC

[ZSP+19] G. H. M. Zanon, M. A. Simplicio, G. C. C. F. Pereira, J. Doliskani, and P. S. L. M. Barreto. Faster key compression for isogeny-based cryptosystems. *IEEE Transactions on Computers*, 68(5):688–701, May 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Zhang:2012:EHO

[ZSW+12] Wentao Zhang, Bozhan Su, Wenling Wu, Dengguo Feng, and Chuankun Wu. Extending higher-order integral: An efficient unified algorithm of constructing integral distinguishers for block ciphers. *Lecture Notes in Computer Science*, 7341:117–134, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31284-7_8/`.

Zhou:2018:TPW

[ZSW+18a] Lu Zhou, Chunhua Su, Yamin Wen, Weijie Li, and Zheng Gong. Towards practical white-box lightweight block cipher implementations for IoTs. *Future Generation Computer Systems*, 86(??):507–514, September 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X17326705`.

Zuo:2018:CSA

[ZSW+18b] Cong Zuo, Jun Shao, Guiyi Wei, Mande Xie, and Min Ji. CCA-secure ABE with outsourced decryption for fog computing. *Future Generation Computer Systems*, 78 (part 2)(??):730–738, January 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X16304745`.

Zhou:2019:LCP

[ZSY19] Lu Zhou, Chunhua Su, and Kuo-Hui Yeh. A lightweight cryptographic protocol with certificateless signature for the Internet of Things. *ACM Transactions on Embedded Computing Systems*, 18(3):28:1–28:??, June 2019. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3301306`.

Zhang:2014:NCM

[ZT14] Miao Zhang and Xiaojun Tong. A new chaotic map based image encryption schemes for several image formats. *The Journal of Systems and Software*, 98(??):140–154, December 2014. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0164121214001915`.

Zhu:2015:PPD

[ZTL15] Hong Zhu, Shengli Tian, and Kevin Lü. Privacy-preserving data publication with features of independent ℓ-diversity. *The Computer Journal*, 58(4):549–571, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://`

comjnl.oxfordjournals.org/content/58/4/549.

Zwattendorfer:2012:CBL

[ZTSR12] Bernd Zwattendorfer, Arne Tauber, Klaus Stranacher, and Peter Reichstädter. Cross-border legal identity management. *Lecture Notes in Computer Science*, 7443:149–161, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33489-4_13/.

Zhang:2016:EEA

[ZTZ16] Liping Zhang, Shanyu Tang, and Shaohui Zhu. An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks. *Journal of Network and Computer Applications*, 59(??):126–133, January 2016. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804515001666.

Zhou:2016:SRB

[ZVG16] Lan Zhou, Vijay Varadharajan, and K. Gopinath. A secure role-based cloud storage system for encrypted patient-centric health records. *The Computer Journal*, 59 (11):1593–1611, November 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/11/1593.

Zhou:2014:SAC

[ZVH14] Lan Zhou, Vijay Varadharajan, and Michael Hitchens. Secure administration of cryptographic role-based access control for large-scale cloud storage systems. *Journal of Computer and System Sciences*, 80(8):1518–1533, December 2014. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000014000634.

Zhang:2015:FAA

[ZW15] Zhiyong Zhang and Kanliang Wang. A formal analytic approach to credible potential path and mining algorithms for multimedia social networks. *The Computer Journal*, 58(4):668–678, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/668.

Zhang:2014:LFL

[ZWM14] Mingwu Zhang, Chunzhi Wang, and Kirill Morozov. LR-FEAD: leakagetolerating and attribute-hiding functional encryption mechanism with delegation in affine subspaces. *The Journal of Supercomputing*, 70(3):1405–1432, December 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-014-1234-6.

Zhang:2011:AGK

[ZWQ+11] Lei Zhang, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer, and Úrsula González-Nicolás. Asymmetric group key agreement protocol for open networks and its application to broadcast encryption. *Computer Networks (Amsterdam, Netherlands: 1999)*, 55(15):3246–3255, October 27, 2011. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128611002283.

Zhou:2018:QTA

[ZWS+18] Lu Zhou, Quanlong Wang, Xin Sun, Piotr Kulicki, and Arcangelo Castiglione. Quantum technique for access control in cloud computing II: Encryption and key distribution. *Journal of Network and Computer Applications*, 103(??):178–184, February 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804517303922.

Zilberberg:2013:PCM

[ZWT13] Omer Zilberberg, Shlomo Weiss, and Sivan Toledo. Phase-change memory: an architectural perspective. *ACM Computing Surveys*, 45(3):29:1–29:33, June 2013. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Zhang:2015:FER

[ZWTM15] Mingwu Zhang, Chunzhi Wang, Tsuyoshi Takagi, and Yi Mu. Functional encryption resilient to hard-to-invert leakage. *The Computer Journal*, 58(4):735–749, April 2015. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/4/735.

Zhang:2017:FBI

[ZWWW17] Yunpeng Zhang, Chengyou Wang, Xiaoli Wang, and Min Wang. Feature-based image watermarking algorithm using SVD and APBT for copyright protection. *Future Internet*, 9(2):13, April 19, 2017. CODEN ???? ISSN 1999-

5903. URL https://www.mdpi.com/1999-5903/9/2/13.

Zhang:2013:LPP

[ZWY+13] Ye Zhang, Wai-Kit Wong, S. M. Yiu, Nikos Mamoulis, and David W. Cheung. Lightweight privacy-preserving peer-to-peer data integration. *Proceedings of the VLDB Endowment*, 6(3): 157–168, January 2013. CODEN ???? ISSN 2150-8097.

Zhang:2019:MAA

[ZWY+19] Xiao Zhang, Faguo Wu, Wang Yao, Zhao Wang, and Wenhua Wang. Multi-authority attribute-based encryption scheme with constant-size ciphertexts and user revocation. *Concurrency and Computation: Practice and Experience*, 31(21):e4678:1–e4678:??, November 10, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Zhang:2017:FWI

[ZWZ17a] Heng Zhang, Chengyou Wang, and Xiao Zhou. Fragile watermarking for image authentication using the characteristic of SVD. *Algorithms (Basel)*, 10(1), March 2017. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL https://www.mdpi.com/1999-4893/10/1/27.

Zhang:2017:RIW

[ZWZ17b] Heng Zhang, Chengyou Wang, and Xiao Zhou. A robust image watermarking scheme based on SVD in the spatial domain. *Future Internet*, 9(3):45, August 07, 2017. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/9/3/45.

Zhou:2011:PSA

[ZX11] Tao Zhou and Jing Xu. Provable secure authentication protocol with anonymity for roaming service in global mobility networks. *Computer Networks (Amsterdam, Netherlands: 1999)*, 55(1):205–213, January 7, 2011. CODEN ???? ISSN 1389-1286.

Zhang:2016:PAG

[ZXH16] Yuexin Zhang, Yang Xiang, and Xinyi Huang. Password-authenticated group key exchange: a cross-layer design. *ACM Transactions on Internet Technology (TOIT)*, 16(4):24:1–24:??, December 2016. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Zhang:2014:EFH

[ZXJ+14] Xiaojun Zhang, Chunxiang Xu, Chunhua Jin, Run Xie, and Jining Zhao. Efficient fully homomorphic encryption from RLWE with an extension to a threshold encryption scheme. *Future Generation Computer Systems*, 36(??):180–186, July 2014. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X13002422`.

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`.

Zhang:2018:AKE

[ZXW+18] Yuexin Zhang, Yang Xiang, Tao Wang, Wei Wu, and Jian Shen. An over-the-air key establishment protocol using keyless cryptography. *Future Generation Computer Systems*, 79 (part 1)(??):284–294, 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167739X1630752X`.

Zhang:2018:VPA

[ZXWA18] Yuexin Zhang, Yang Xiang, Wei Wu, and Abdulhameed Alelaiwi. A variant of password authenticated key exchange protocol. *Future Generation Computer Systems*, 78 (part 2)(??):699–711, January 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X17302145`.

Zhang:2016:DEP

[ZXYL16] Rui Zhang, Rui Xue, Ting Yu, and Ling Liu. Dynamic and efficient private keyword search over inverted index-based encrypted data. *ACM Transactions on Internet Technology (TOIT)*, 16(3):21:1–21:??, August 2016. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Zhang:2011:SIR

[ZXZ+11] Jun Zhang, Yang Xiang, Wanlei Zhou, Lei Ye, and Yi Mu. Secure image retrieval based on visual content and watermarking protocol. *The Computer Journal*, 54(10):1661–1674, October 2011. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/54/10/1661.full.pdf+html`.

Zhou:2017:CLR

[ZY17a] Yanwei Zhou and Bo Yang. Continuous leakage-resilient public-key encryption scheme with CCA security. *The Computer Journal*, 60(8): 1161–1172, August 1, 2017. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL https://academic.oup.com/comjnl/article/60/8/1161/2882687.

Zhou:2017:LRC

[ZY17b] Yanwei Zhou and Bo Yang. Leakage-resilient CCA2-secure certificateless public-key encryption scheme without bilinear pairing. *Information Processing Letters*, 130(??):16–24, February 2017. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019017301680.

Zhang:2017:GFD

[ZYC+17] Jian Zhang, Yang Yang, Yanjiao Chen, Jing Chen, and Qian Zhang. A general framework to design secure cloud storage protocol using homomorphic encryption scheme. *Computer Networks (Amsterdam, Netherlands: 1999)*, 129 (part 1)(??):37–50, December 24, 2017. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128617303328.

Zheng:2010:PS

[ZYD10] Yuliang Zheng, Moti Yung, and Alexander W. Dent, editors. *Practical Signcryption*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-540-89409-8, 3-540-89411-X (e-book). xviii + 274 pp. LCCN QA76. 9. A25 P73 2010.

Zhan:2017:NKG

[ZYGT17] Furui Zhan, Nianmin Yao, Zhenguo Gao, and Guozhen Tan. A novel key generation method for wireless sensor networks based on system of equations. *Journal of Network and Computer Applications*, 82(??):114–127, March 15, 2017. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804517300395.

Zhan:2018:EKG

[ZYGY18] Furui Zhan, Nianmin Yao, Zhenguo Gao, and Haitao Yu. Efficient key generation leveraging wireless channel reciprocity for MANETs. *Journal of Network and Computer Ap-*

plications, 103(??):18–28, February 1, 2018. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804517303909.

Zhou:2019:CLR

[ZYH+19] Yanwei Zhou, Bo Yang, Hongxia Hou, Lina Zhang, Tao Wang, and Mingxiao Hu. Continuous leakage-resilient identity-based encryption with tight security. *The Computer Journal*, 62(8):1092–1105, August 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/8/1092/5288324.

Zhang:2010:ASL

[ZYL+10] Youtao Zhang, Jun Yang, Weijia Li, Linzhang Wang, and Lingling Jin. An authentication scheme for locating compromised sensor nodes in WSNs. *Journal of Network and Computer Applications*, 33(1):50–62, January 2010. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1084804509000976.

Zhou:2018:CLR

[ZYM18] Yanwei Zhou, Bo Yang, and Yi Mu. Continuous leakage-resilient identity-based encryption without random oracles. *The Computer Journal*, 61(4):586–600, April 1, 2018. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/61/4/586/4824746.

Zhou:2019:GCC

[ZYM19] Yanwei Zhou, Bo Yang, and Yi Mu. The generic construction of continuous leakage-resilient identity-based cryptosystems. *Theoretical Computer Science*, 772(??):1–45, June 7, 2019. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397518307096.

Zhang:2013:BLR

[ZYT13] Mingwu Zhang, Bo Yang, and Tsuyoshi Takagi. Bounded leakage-resilient functional encryption with hidden vector predicate. *The Computer Journal*, 56 (4):464–477, April 2013. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/56/4/464.full.pdf+html.

Zhao:2019:LRC

[ZYY19] Yi Zhao, Yong Yu, and

Bo Yang. Leakage resilient CCA security in stronger model: Branch hidden ABO-LTFs and their applications. *The Computer Journal*, 62(4):631–640, April 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://academic.oup.com/comjnl/article/62/4/631/5272751`.

Zhang:2019:LRH

[ZYZ+19] Yinghui Zhang, Menglei Yang, Dong Zheng, Tiantian Zhang, Rui Guo, and Fang Ren. Leakage-resilient hierarchical identity-based encryption with recipient anonymity. *International Journal of Foundations of Computer Science (IJFCS)*, 30(5):665–681, August 2019. CODEN IFCSEN. ISSN 0129-0541. URL `https://www.worldscientific.com/doi/10.1142/S0129054119400197`.

Zhang:2011:EPK

[ZZ11] Bo Zhang and Fangguo Zhang. An efficient public key encryption with conjunctive-subset keywords search. *Journal of Network and Computer Applications*, 34(1):262–267, January 2011. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804510001293`.

Zhao:2012:FCS

[ZZ12] Xingwen Zhao and Fangguo Zhang. Fully CCA2 secure identity-based broadcast encryption with black-box accountable authority. *The Journal of Systems and Software*, 85(3):708–716, March 2012. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S016412121100255X`.

Zhang:2015:ITS

[ZZ15] Jie Zhang and Futai Zhang. Information-theoretical secure verifiable secret sharing with vector space access structures over bilinear groups and its applications. *Future Generation Computer Systems*, 52(??):109–115, November 2015. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167739X14002477`.

Zheng:2015:EPT

[ZZC15] Minghui Zheng, Huihua Zhou, and Jing Chen. An efficient protocol for two-party explicit authenticated key agreement. *Concurrency and Computation: Practice and Experience*, 27(12):2954–2963, August 25, 2015. CODEN CCPEBO. ISSN 1532-0626

(print), 1532-0634 (electronic).

Zhou:2017:ENQ

[ZZC17] Lu Zhou, Youwen Zhu, and Aniello Castiglione. Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner. *Computers & Security*, 69(??): 84–96, August 2017. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167404816301663.

Zhuang:2014:SCA

[ZZCJ14] Yixin Zhuang, Ming Zou, Nathan Carr, and Tao Ju. Shapes and cryptography: Anisotropic geodesics for live-wire mesh segmentation. *Computer Graphics Forum*, 33(7):111–120, October 2014. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Zaidan:2017:NDW

[ZZKA17] B. B. Zaidan, A. A. Zaidan, H. Abdul. Karim, and N. N. Ahmad. A new digital watermarking evaluation and benchmarking methodology using an external group of evaluators and multi-criteria analysis based on 'large-scale data'. *Software—Practice and Experience*, 47(10): 1365–1392, October 2017. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Zhu:2018:CAC

[ZZL+18] Biaokai Zhu, Jumin Zhao, Dengao Li, Hong Wang, Ruiqin Bai, Yanxia Li, and Hao Wu. Cloud access control authentication system using dynamic accelerometers data. *Concurrency and Computation: Practice and Experience*, 30 (20):e4474:1–e4474:??, October 25, 2018. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Zhu:2019:ICR

[ZZL+19] Youwen Zhu, Yue Zhang, Xingxin Li, Hongyang Yan, and Jing Li. Improved collusion-resisting secure nearest neighbor query over encrypted data in cloud. *Concurrency and Computation: Practice and Experience*, 31(21): e4681:1–e4681:??, November 10, 2019. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

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.

Zeng:2019:SAE

[ZZQ+19] Ming Zeng, Kai Zhang, Haifeng Qian, Xiaofeng Chen, and Jie Chen. A searchable asymmetric encryption scheme with support for Boolean queries for cloud applications. *The Computer Journal*, 62(4):563–578, April 2019. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://academic.oup.com/comjnl/article/62/4/563/5253754.

Zhang:2019:LAS

[ZZY+19] Liping Zhang, Lanchao Zhao, Shuijun Yin, Chi-Hung Chi, Ran Liu, and Yixin Zhang. A lightweight authentication scheme with privacy protection for smart grid communications. *Future Generation Computer Systems*, 100(??):770–778, November 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X19310398.