# A Bibliography of Papers in *Lecture Notes in Computer Science* (2013): Volumes 7126–??

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: http://www.math.utah.edu/~beebe/

25 April 2024
Version 1.03

## Title word cross-reference

2 [15]. $F_q$ [35].

**-Party** [15].

**5th** [41].

**Achieve** [22]. **against** [36]. **Algorithm** [29]. **Algorithms** [23]. **Anonymous** [33]. **Application** [6, 35]. **Arguments** [18]. **Attack** [28]. **Attacks** [36]. **Attribute** [8]. **Attribute-Based** [8]. **Authenticated** [30].

**Back** [39]. **Based** [24, 8, 26, 28, 31, 35, 36]. **Bath** [40]. **Becomes** [9]. **Big** [20]. **Bounded** [4].

**Calculemus** [40]. **Chain** [2]. **Characterization** [14]. **Characterizing** [15].

# References

**Dodis:2013:OWE**

[1] 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`.

**Krenn:2013:CCR**

[2] 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/`.

**Berman:2013:HPR**

[3] 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/`.

**Goyal:2013:CZK**

[4] 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/`.

**Canetti:2013:PCC**

[5] 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/`.

**Chase:2013:SMN**

[6] 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/`.

**Gentry:2013:EMH**

[7] 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`.

**Boyen:2013:ABF**

[8] 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/.

**Brakerski:2013:WHB**

[9] 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/.

**Applebaum:2013:GXG**

[10] 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/.

**Bitansky:2013:WFS**

[11] Nir Bitansky, Dana Dachman-Soled, Sanjam Garg, Abhishek Jain, and Yael Tauman Kalai .... 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/.

**Ananth:2013:SFP**

[12] 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/.

**Papamanthou:2013:SCC**

[13] 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/.

**Asharov:2013:FCF**

[14] 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/.

**Jeffs:2013:CCP**

[15] 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/`.

**Fehr:2013:FCC**

[16] 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/`.

**Mahmoody:2013:LEZ**

[17] 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/`.

**Bitansky:2013:SNI**

[18] 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/`.

**Pass:2013:USP**

[19] 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/`.

**Malkin:2013:SCB**

[20] 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`.

**Anonymous:2013:FM**

[21] Anonymous. Front matter. *Lecture Notes in Computer Science*, 7932:??, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/bfm:978-3-642-38616-9/1.pdf`.

**Baldi:2013:ULC**

[22] 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/`.

**Bernstein:2013:QAS**

[23] Daniel J. Bernstein, Stacey Jeffery, Tanja Lange, and Alexander Meurer. Quantum algorithms for the subset-sum problem. *Lecture Notes in Computer Science*, 7932:16–33, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_2/`.

**Bettaieb:2013:ILB**

[24] Slim Bettaieb and Julien Schrek. Improved lattice-based threshold ring signature scheme. *Lecture Notes in Computer Science*, 7932:34–51, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_3/`.

**Ding:2013:DRH**

[25] Jintai Ding and Bo-Yin Yang. Degree of regularity for HFEv and HFEv-. *Lecture Notes in Computer Science*, 7932:52–66, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_4/`.

**Guneysu:2013:SSR**

[26] Tim Güneysu, Tobias Oder, Thomas Pöppelmann, and Peter Schwabe. Software speed records for lattice-based signatures. *Lecture Notes in Computer Science*, 7932:67–82, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_5/`.

**Laarhoven:2013:SSV**

[27] Thijs Laarhoven, Michele Mosca, and Joop van de Pol. Solving the shortest vector problem in lattices faster using quantum search. *Lecture Notes in*

*Computer Science*, 7932:83–101, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_6/`.

**Landais:2013:EAM**

[28] Grégory Landais and Jean-Pierre Tillich. An efficient attack of a McEliece cryptosystem variant based on convolutional codes. *Lecture Notes in Computer Science*, 7932:102–117, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_7/`.

**Miura:2013:EAS**

[29] Hiroyuki Miura, Yasufumi Hashimoto, and Tsuyoshi Takagi. Extended algorithm for solving underdefined multivariate quadratic equations. *Lecture Notes in Computer Science*, 7932:118–135, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_8/`.

**Mosca:2013:QKD**

[30] 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/`.

**Nie:2013:CHB**

[31] 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/`.

**Perlner:2013:CDI**

[32] Ray Perlner and Daniel Smith-Tone. A classification of differential invariants for multivariate post-quantum cryptosystems. *Lecture Notes in Computer Science*, 7932:165–173, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_11/`.

**Persichetti:2013:SAH**

[33] 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/`.

**Petzoldt:2013:FVI**

[34] Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann. Fast verification for improved versions of the UOV and rainbow signature schemes. *Lecture Notes in Computer Science*, 7932:188–202, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_13/`.

**Sendrier:2013:HCE**

[35] 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/`.

**Strenzke:2013:TAA**

[36] Falko Strenzke. Timing attacks against the syndrome inversion in code-based cryptosystems. *Lecture Notes in Computer Science*, 7932:217–230, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_15/`.

**Tao:2013:SMS**

[37] 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/`.

**Yasuda:2013:MSS**

[38] Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Sakurai. Multivariate signature scheme using quadratic forms. *Lecture Notes in Computer Science*, 7932:243–258, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-38616-9_17/`.

**Anonymous:2013:BM**

[39] Anonymous. Back matter. *Lecture Notes in Computer Science*, 7932:??, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/bbm:978-3-642-38616-9/1.pdf`.

**Carette:2013:ICM**

[40] Jacques Carette, David Aspinall, Christoph Lange, Petr Sojka, and Wolfgang Windsteiger, editors. *Intelligent computer mathematics: MKM, Calculemus, DML, and Systems and Projects 2013, held as part of CICM 2013, Bath, UK, July 8–12, 2013. Proceedings*, volume 7961 of *Lecture notes in computer science*. Springer-Verlag Inc., New York, NY, USA, 2013. ISBN 3-642-39319-5 (paperback), 3-642-39320-9 (e-book). LCCN QA76.9.M35 I58 2013.

**Gaborit:2013:PQC**

[41] Philippe Gaborit, editor. *Post-quantum cryptography: 5th International Workshop, PQCRYPTO 2013, Limoges, France, June 4–7, 2013. Proceedings*, volume 7932 of *Lecture Notes in Computer Science*. Springer-Verlag Inc., New York, NY, USA, 2013. ISBN 3-642-38615-6 (paperback), 3-642-38616-4 (e-book). LCCN ???? URL `http://www.springerlink.com/content/978-3-642-38616-9`.