A Bibliography of Papers in *Lecture Notes in Computer Science* (2011)

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/`

14 October 2017
Version 1.03

Title word cross-reference

References

Anonymous:2011:FM

[1] Anonymous. Front matter. *Lecture Notes in Computer Science*, 6632:??, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/bfm:978-3-642-20465-4/1`.

Cramer:2011:ACT

[2] Ronald Cramer. The arithmetic codex: Theory and applications. *Lecture Notes in Computer Science*, 6632:1, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_1`.

Nguyen:2011:LRA

[3] Phong Q. Nguyen. Lattice reduction algorithms: Theory and practice. *Lecture Notes in Computer Science*, 6632: 2–6, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_2`.

Kiltz:2011:EAH

[4] 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`.

Stehle:2011:MNS

[5] Damien Stehlé and Ron Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. *Lecture Notes in Computer Science*, 6632:27–47, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_4`.

Aranha:2011:FEF

[6] Diego F. Aranha, Koray Karabina, Patrick Longa, Catherine H. Gebotys, and Julio López. Faster explicit formulas for computing pairings over ordinary curves. *Lecture Notes in Computer Science*, 6632:48–68, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_5`.

Moradi:2011:PLV

[7] Amir Moradi, Axel Poschmann, San Ling, Christof Paar, and Huaxiong Wang. Pushing the limits: A very compact and a threshold implementation of AES. *Lecture Notes in Computer Science*, 6632:69–88, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_6.

Boyle:2011:FLR

[8] Elette Boyle, Gil Segev, and Daniel Wichs. Fully leakage-resilient signatures. *Lecture Notes in Computer Science*, 6632:89–108, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_7.

Renauld:2011:FSP

[9] Mathieu Renauld, François-Xavier Standaert, Nicolas Veyrat-Charvillon, and Dina Kamel. A formal study of power variability issues and side-channel attacks for nanoscale devices. *Lecture Notes in Computer Science*, 6632:109–128, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_8.

Gentry:2011:IGF

[10] 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.

Boneh:2011:HSP

[11] Dan Boneh and David Mandell Freeman. Homomorphic signatures for polynomial functions. *Lecture Notes in Computer Science*, 6632:149–168, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_10.

Bendlin:2011:SHE

[12] 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.

Schage:2011:TPS

[13] Sven Schäge. Tight proofs for signature schemes without random oracles. *Lecture Notes in Computer Science*, 6632:189–206, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_12.

Catalano:2011:APF

[14] Dario Catalano, Dario Fiore, and Bogdan Warinschi. Adaptive pseudo-free groups and applications. *Lecture Notes in Computer Science*, 6632:207–223, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_13.

Fuchsbauer:2011:CSV

[15] 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.

Bouman:2011:SAW

[16] 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.

Ahmadi:2011:SKC

[17] 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.

Obana:2011:AOC

[18] 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.

Leander:2011:LHS

[19] Gregor Leander. On linear hulls, statistical saturation attacks, PRESENT and a cryptanalysis of PUFFIN. *Lecture Notes in Computer Science*, 6632:303–322, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_18.

Dodis:2011:DEM

[20] Yevgeniy Dodis and John Steinberger. Domain extension for MACs beyond the birthday barrier. *Lecture Notes in Computer Science*, 6632:323–342, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_19.

Sepehrdad:2011:SAR

[21] Pouyan Sepehrdad, Serge Vaudenay, and Martin Vuagnoux. Statistical attack on RC4. *Lecture Notes in Computer Science*, 6632:343–363, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_20.

Becker:2011:IGA

[22] Anja Becker, Jean-Sébastien Coron, and Antoine Joux. Improved generic algorithms for hard knapsacks. *Lecture Notes in Computer Science*, 6632:364–385, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_21.

shelat:2011:TOS

[23] Abhi shelat and Chih hao Shen. Two-output secure computation with malicious adversaries. *Lecture Notes in Computer Science*, 6632:386–405, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_22.

Ishai:2011:ENI

[24] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, and Amit Sahai. Efficient non-interactive secure computation. *Lecture Notes in Computer Science*, 6632:406–425, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_23.

Asharov:2011:TGT

[25] Gilad Asharov, Ran Canetti, and Carmit Hazay. Towards a game theoretic view of secure computation. *Lecture Notes in Computer Science*, 6632:426–445, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_24.

Lindell:2011:HEU

[26] Yehuda Lindell. Highly-efficient universally-composable commitments based on the DDH assumption. *Lecture Notes in Computer Science*, 6632:446–466, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_25.

Unruh:2011:CCB

[27] Dominique Unruh. Concurrent composition in the bounded quantum storage model. *Lecture Notes in Computer Science*, 6632:467–486, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_26.

Ristenpart:2011:CCL

[28] Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton. Careful with composition: Limitations of the indifferentiability framework. *Lecture Notes in Computer Science*, 6632:487–506, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_27.

Malkin:2011:ECS

[29] 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.

Applebaum:2011:KDM

[30] Benny Applebaum. Key-dependent message security: Generic amplification and completeness. *Lecture Notes in Computer Science*, 6632:527–546, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_29.

Lewko:2011:UHA

[31] 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:2011:DAB

[32] 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.

Wee:2011:TRC

[33] Hoeteck Wee. Threshold and revocation cryptosystems via extractable hash proofs. *Lecture Notes in Computer Science*, 6632:589–609, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_32.

Durmuth:2011:DEN

[34] 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.

Anonymous:2011:BM

[35] Anonymous. Back matter. *Lecture Notes in Computer Science*, 6632:??, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/bbm:978-3-642-20465-4/1.

Kopetz:2011:WLB

[36] Hermann Kopetz. What I learned from Brian. *Lecture Notes in Computer Science*, 6875:1–6, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_1/; http://link.springer.com/content/pdf/bfm:978-3-642-24541-1/1.pdf.

Lloyd:2011:BRB

[37] John L. Lloyd and Tom Anderson. Brian Randell: a biographical note. *Lecture Notes in Computer Science*, 6875:7–14, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_2/.

Aviienis:2011:BRA

[38] Algirdas Avi ienis. On building a referee's avatar. *Lecture Notes in Computer Science*, 6875:15–22, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_3/.

Campbell-Kelly:2011:TPI

[39] Martin Campbell-Kelly. From theory to practice: The invention of programming, 1947–51. *Lecture Notes in Computer Science*, 6875:23–37, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_4/.

Lomet:2011:TLA

[40] David Lomet. Transactions: From local atomicity to atomicity in the cloud. *Lecture Notes in Computer Science*, 6875:38–52, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_5/.

Rushby:2011:DM

[41] John Rushby. From DSS to MILS. *Lecture Notes in Computer Science*, 6875:53–57, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_6/.

Swade:2011:PEC

[42] Doron Swade. Pre-electronic computing. *Lecture Notes in Computer Science*, 6875:58–83, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_7/.

Wichmann:2011:WW

[43] Brian Wichmann. Whetstone wanderings. *Lecture Notes in Computer Science*, 6875:84–92, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_8/.

Bacon:2011:URT

[44] Jean Bacon, Andrei Iu. Bejan, Alastair R. Beresford, David Evans, and Richard J. Gibbens. Using real-time road traffic data to evaluate congestion. *Lecture Notes in Computer Science*, 6875:93–117, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_9/.

Bantre:2011:FTA

[45] Jean-Pierre Banâtre, Christine Morin, and Thierry Priol. Fault tolerant autonomic computing systems in a chemical setting. *Lecture Notes in Computer Science*, 6875:118–129, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_10/.

Bell:2011:CEY

[46] Gordon Bell. Out of a closet: The early years of The Computer Museum. *Lecture Notes in Computer Science*, 6875:130–146, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_11/.

Burns:2011:TFM

[47] Alan Burns and Sanjoy Baruah. Timing faults and mixed criticality systems. *Lecture Notes in Computer Science*, 6875:147–166, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_12/.

Ceruzzi:2011:PBR

[48] Paul E. Ceruzzi. Professor Brian Randell and the history of computing. *Lecture Notes in Computer Science*, 6875:167–173, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_13/.

Coffman:2011:CSF

[49] Ed Coffman. Computer storage fragmentation: Pioneering work of Brian Randell. *Lecture Notes in Computer Science*, 6875:174–184, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_14/.

Conway:2011:IAR

[50] Lynn Conway. IBM-ACS: Reminiscences and lessons learned from a 1960's supercomputer project. *Lecture Notes in Computer Science*, 6875:185–224, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_15/.

Courtois:2011:BEM

[51] Pierre-Jacques Courtois. The Belgian Electronic Mathematical Machine (1951–1962): an account. *Lecture Notes in Computer Science*, 6875:225–237, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_16/.

Dacier:2011:RDF

[52] Marc Dacier. On the resilience of the dependability framework to the intrusion of new security threats. *Lecture Notes in Computer Science*, 6875:238–250, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_17/.

Denning:2011:VFT

[53] Peter J. Denning. Virtual fault tolerance. *Lecture Notes in Computer Science*, 6875:251–260, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_18/.

Hoare:2011:RB

[54] Tony Hoare. Recovery blocks. *Lecture Notes in Computer Science*, 6875:261–266, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_19/.

Horning:2011:DWP

[55] J. J. Horning. The development and writing of "process structuring". *Lecture Notes in Computer Science*, 6875:267–272, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-24541-1_20/.

Kiayias:2011:TCC

[56] 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 Inc., New York, NY, USA, 2011. ISBN 3-642-19073-1. LCCN ????

vanDam:2011:TQC

[57] 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 Inc., New York, NY, USA, 2011. ISBN 3-642-18072-8 (softcover). LCCN ????