A Bibliography of Papers in *Lecture Notes in Computer Science* (2005) (Part 1 of 4)

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

Wang:2005:ECS

[1] Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin. Efficient collision search attacks on SHA-0. *Lecture Notes in Computer Science*, 3621:1–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wang:2005:FCF

[2] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. *Lecture Notes in Computer Science*, 3621:17–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dwork:2005:PPW

[3] Cynthia Dwork, Moni Naor, and Hoeteck Wee. Pebbling and proofs of work. *Lecture Notes in Computer Science*, 3621:37–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pietrzak:2005:CDI

[4] Krzysztof Pietrzak. Composition does not imply adaptive security. *Lecture Notes in Computer Science*, 3621:55–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Granger:2005:DLP

[5] R. Granger and F. Vercauteren. On the discrete logarithm problem on algebraic tori. *Lecture Notes in Computer Science*, 3621:66–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Myasnikov:2005:PAB

[6] Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. A practical attack on a braid group based cryptographic protocol. *Lecture Notes in Computer Science*, 3621:86–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lu:2005:CCA

[7] Yi Lu, Willi Meier, and Serge Vaudenay. The conditional correlation attack: A

practical attack on Bluetooth encryption. *Lecture Notes in Computer Science*, 3621: 97–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pass:2005:UCN

[8] Rafael Pass and abhi shelat. Unconditional characterizations of non-interactive zero-knowledge. *Lecture Notes in Computer Science*, 3621:118–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Alwen:2005:IFR

[9] Joë Alwen, Giuseppe Persiano, and Ivan Visconti. Impossibility and feasibility results for zero knowledge with public keys. *Lecture Notes in Computer Science*, 3621: 135–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fischlin:2005:CEN

[10] Marc Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. *Lecture Notes in Computer Science*, 3621:152–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Camenisch:2005:FTO

[11] Jan Camenisch and Anna Lysyanskaya. A formal treatment of onion routing. *Lecture Notes in Computer Science*, 3621: 169–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Peng:2005:SES

[12] Kun Peng, Colin Boyd, and Ed Dawson. Simple and efficient shuffling with provable correctness and ZK privacy. *Lecture Notes in Computer Science*, 3621:188–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Abdalla:2005:SER

[13] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. *Lecture Notes in Computer Science*, 3621:205–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ostrovsky:2005:PSS

[14] Rafail Ostrovsky and William E. Skeith III. Private searching on streaming data. *Lecture Notes in Computer Science*, 3621: 223–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kissner:2005:PPS

[15] Lea Kissner and Dawn Song. Privacy-preserving set operations. *Lecture Notes in Computer Science*, 3621:241–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Boneh:2005:CRB

[16] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. *Lecture Notes in Computer Science*, 3621:258–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hwang:2005:GTS

[17] Jung Yeon Hwang, Dong Hoon Lee, and Jongin Lim. Generic transformation for scalable broadcast encryption schemes. *Lecture Notes in Computer Science*, 3621: 276–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Juels:2005:APD

[18] Ari Juels and Stephen A. Weis. Authenticating pervasive devices with human protocols. *Lecture Notes in Computer Science*, 3621:293–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vaudenay:2005:SCI

[19] Serge Vaudenay. Secure communications over insecure channels based on short authenticated strings. *Lecture Notes in Computer Science*, 3621:309–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cramer:2005:CMS

[20] Ronald Cramer, Vanesa Daza, Ignacio Gracia, Jorge Jiménez Urroz, Gregor Leander, Jaume Martí-Farré, and Carles Padró. On codes, matroids and secure multi-party computation from linear secret sharing schemes. *Lecture Notes in Computer Science*, 3621:327–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cramer:2005:BBS

[21] Ronald Cramer, Serge Fehr, and Martijn Stam. Black-box secret sharing from primitive sets in algebraic number fields. *Lecture Notes in Computer Science*, 3621: 344–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Barak:2005:SCA

[22] Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, and Tal Rabin. Secure computation without authentication. *Lecture Notes in Computer Science*, 3621:361–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Damgaard:2005:CRM

[23] Ivan Damgård and Yuval Ishai. Constant-round multiparty computation using a black-box pseudorandom generator. *Lecture Notes in Computer Science*, 3621: 378–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Barkol:2005:SCC

[24] Omer Barkol and Yuval Ishai. Secure computation of constant-depth circuits with applications to database search problems. *Lecture Notes in Computer Science*, 3621:395–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Boldyreva:2005:ARO

[25] Alexandra Boldyreva and Marc Fischlin. Analysis of random oracle instantiation scenarios for OAEP and other practical schemes. *Lecture Notes in Computer Science*, 3621:412–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Coron:2005:MDR

[26] Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, and Prashant Puniya. Merkle–Damgård revisited: How to construct a hash function. *Lecture Notes in Computer Science*, pages 430–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dodis:2005:GIF

[27] Yevgeniy Dodis, Roberto Oliveira, and Krzysztof Pietrzak. On the generic insecurity of the full domain hash. *Lecture Notes in Computer Science*, pages 449–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wolf:2005:NML

[28] Stefan Wolf and Jürg Wullschleger. New monotones and lower bounds in unconditional two-party computation. *Lecture Notes in Computer Science*, pages 467–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Holenstein:2005:OWS

[29] Thomas Holenstein and Renato Renner. One-way secret-key agreement and applications to circuit polarization and immunization of public-key encryption. *Lecture Notes in Computer Science*, pages 478–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Damgaard:2005:QCN

[30] Ivan Damgård, Thomas Brochmann Pedersen, and Louis Salvail. A quantum cipher with near optimal key-recycling. *Lecture Notes in Computer Science*, pages 494–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chevallier-Mames:2005:ECB

[31] Benoît Chevallier-Mames. An efficient CDH-based signature scheme with a tight security reduction. *Lecture Notes in Computer Science*, pages 511–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:2005:ISA

[32] Mihir Bellare, Krzysztof Pietrzak, and Phillip Rogaway. Improved security analyses for CBC MACs. *Lecture Notes in Computer Science*, pages 527–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Krawczyk:2005:HHP

[33] Hugo Krawczyk. HMQV: A high-performance secure Diffie–Hellman protocol. *Lecture Notes in Computer Science*, pages 546–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Abramov:2005:RLS

[34] S. A. Abramov, M. Bronstein, and D. E. Khmelnov. On regular and logarithmic solutions of ordinary linear differential systems. *Lecture Notes in Computer Science*, 3718:1–12, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/11555964_1.pdf`; `http://link.springer.com/content/pdf/bfm:978-3-540-32070-8/1.pdf`.

Basu:2005:CBN

[35] Saugata Basu and Michael Kettner. Computing the Betti numbers of arrangements in practice. *Lecture Notes in Computer Science*, 3718:13–31, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/11555964_2.pdf`.

Belyaeva:2005:MSN

[36] I. N. Belyaeva, N. A. Chekanov, A. A. Gusev, V. A. Rostovtsev, Yu. A. Ukolov, Y. Uwano, and S. I. Vinitsky. A MAPLE symbolic-numeric program for solving the 2D-eigenvalue problem by a self-consistent basis method. *Lecture Notes in Computer Science*, 3718:32–39, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/11555964_3.pdf`.

Berghammer:2005:ROB

[37] Rudolf Berghammer and Frank Neumann. RelView — an OBDD-based computer algebra system for relations. *Lecture Notes in Computer Science*, 3718:40–51, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_4.pdf.

Borges-Quintana:2005:UGB

[38] M. Borges-Quintana, M. A. Borges-Trenard, and E. Martínez-Moro. On the use of Gröbner bases for computing the structure of finite Abelian groups. *Lecture Notes in Computer Science*, 3718:52–64, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_5.pdf.

Bruno:2005:NFI

[39] Alexander D. Bruno and Victor F. Edneral. Normal forms and integrability of ODE systems. *Lecture Notes in Computer Science*, 3718:65–74, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_6.pdf.

Buse:2005:RBM

[40] Laurent Busé, Houssam Khalil, and Bernard Mourrain. Resultant-based methods for plane curves intersection problems. *Lecture Notes in Computer Science*, 3718:75–92, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_7.pdf.

Cattani:2005:SCS

[41] Carlo Cattani, Evgenii A. Grebenikov, and Alexander N. Prokopenya. Symbolic calculations in studying the stability of dynamically symmetric satellite motion. *Lecture Notes in Computer Science*, 3718:93–104, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_8.pdf.

Chibisov:2005:GOG

[42] Dmytro Chibisov, Victor Ganzha, Ernst W. Mayr, and Evgenii V. Vorozhtsov. Generation of orthogonal grids on curvilinear trimmed regions in constant time. *Lecture Notes in Computer Science*, 3718:105–114, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_9.pdf.

Chibisov:2005:CAN

[43] Dmytro Chibisov, Victor Ganzha, Sergey Pankratov, and Christoph Zenger. Computer algebra in nanosciences: Modeling electronic states in quantum dots. *Lecture Notes in Computer Science*, 3718:115–124, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_10.pdf.

Chtcherba:2005:CDR

[44] Arthur D. Chtcherba, Deepak Kapur, and Manfred Minimair. Cayley–Dixon resultant matrices of multi-univariate composed polynomials. *Lecture Notes in Computer Science*, 3718:125–137, 2005. CODEN LNCSD9. ISSN 0302-9743

(print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_11.pdf.

Eigenwillig:2005:DAP

[45] Arno Eigenwillig, Lutz Kettner, Werner Krandick, Kurt Mehlhorn, and Susanne Schmitt .... A Descartes algorithm for polynomials with bit-stream coefficients. *Lecture Notes in Computer Science*, 3718:138–149, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_12.pdf.

Emiris:2005:RSB

[46] Ioannis Z. Emiris and Elias P. Tsigaridas. Real solving of bivariate polynomial systems. *Lecture Notes in Computer Science*, 3718:150–161, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_13.pdf.

Gago-Vargas:2005:NCC

[47] J. Gago-Vargas, M. I. Hartillo-Hermoso, and J. M. Ucha-Enríquez. Nouvelle cuisine for the computation of the annihilating ideal of f^s. *Lecture Notes in Computer Science*, 3718:162–173, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_14.pdf.

Gerdt:2005:JLM

[48] Vladimir P. Gerdt and Yuri A. Blinkov. Janet-like monomial division. *Lecture Notes in Computer Science*, 3718:174–183, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_15.pdf.

Gerdt:2005:JLG

[49] Vladimir P. Gerdt and Yuri A. Blinkov. Janet-like Gröbner bases. *Lecture Notes in Computer Science*, 3718:184–195, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_16.pdf.

Gomez:2005:CDM

[50] Domingo Gómez, Jaime Gutierrez, and Álvar Ibeas. Circulant digraphs and monomial ideals. *Lecture Notes in Computer Science*, 3718:196–207, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_17.pdf.

Gonzalez–Diaz:2005:ATA

[51] Rocio Gonzalez-Diaz, Belen Medrano, Pedro Real, and Javier Sánchez-Peláez. Algebraic topological analysis of time-sequence of digital images. *Lecture Notes in Computer Science*, 3718:208–219, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_18.pdf.

Gonzalez–Vega:2005:HSP

[52] Laureano Gonzalez-Vega, Carlo Traverso, and Alberto Zanoni. Hilbert stratification and parametric Gröbner bases. *Lecture Notes in Computer Science*, 3718:220–235, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_19.pdf.

Grebenicov:2005:ISP

[53] E. A. Grebenicov, D. Kozak-Skoworodkin, and M. Jakubiak. Investigation of the stability problem for the critical cases of the Newtonian many-body problem. *Lecture Notes in Computer Science*, 3718:236–243, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/11555964_20.pdf.