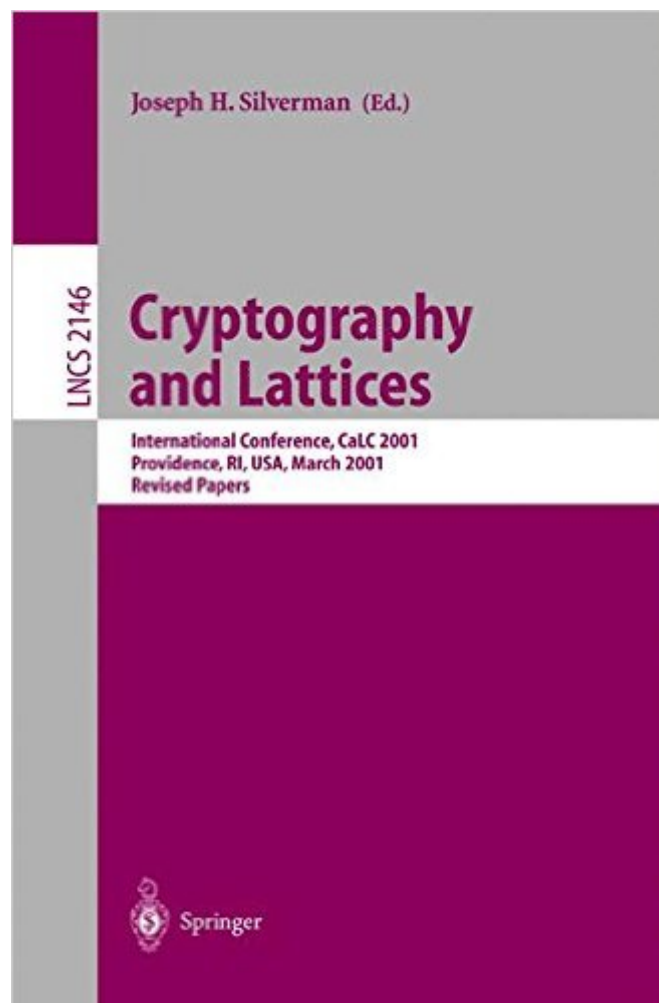


The book was found

# Cryptography And Lattices: International Conference, CaLC 2001, Providence, RI, USA, March 29-30, 2001. Revised Papers (Lecture Notes In Computer Science)



## Synopsis

These are the proceedings of CaLC2001, the first conference devoted to cryptography and lattices.

We have long believed that the importance of lattices

and lattice reduction in cryptography, both for cryptographic construction and

cryptographic analysis, merits a gathering devoted to this topic. The enthusiastic

response that we received from the program committee, the invited speakers, the

many people who submitted papers, and the 90 registered participants amply

confirmed the widespread interest in lattices and their cryptographic applications.

We thank everyone whose involvement made CaLC such a successful event;

in particular we thank Natalie Johnson, Larry Larrivee, Doreen Pappas, and the

Brown University Mathematics Department for their assistance and support. March 2001

Jeffrey Hoëstein, Jill Pipher, Joseph Silverman VI Preface Organization

CaLC2001 was organized by the Department of Mathematics at Brown University.

The program chairs express their thanks to the program committee and the

additional external referees for their help in selecting the papers for CaLC2001.

The program chairs would also like to thank NTRU Cryptosystems for providing

financial support for the conference. Program Committee Don Coppersmith IBM Research

Jeffrey Hoëstein (co-chair), Brown University and NTRU Cryptosystems Arjen Lenstra Citibank, USA

Phong Nguyen ENS Andrew Odlyzko AT&T Labs Research Joseph H. Silverman (co-chair),

Brown University and NTRU Cryptosystems External Referees

Ali Akhavi, Glenn Durfee, Nick Howgrave-Graham, Daniele Micciancio Sponsoring Institutions

NTRU Cryptosystems, Inc., Burlington, MA Table of Contents An Overview of the Sieve Algorithm

for the Shortest Lattice Vector Problem 1 Miklos Ajtai, Ravi Kumar, and Dandapani Sivakumar Low

Secret Exponent RSA Revisited ..... 4 Johannes Blömer and Alexander May

Finding Small Solutions to Small Degree Polynomials ..... 20 Don Coppersmith Fast

Reduction of Ternary Quadratic Forms ..... 32 Friedrich Eisenbrand and Günter

Rote Factoring Polynomials and 0-1 Vectors ..... 45 Mark van Hoeij Approximate

Integer Common Divisors ..... 51 Nick Howgrave-Graham Segment LLL-Reduction

of Lattice Bases ..... 67 Henrik Koy and Claus Peter Schnorr Segment LLL-Reduction

with Floating Point Orthogonalization ..... 81 Henrik Koy and Claus Peter Schnorr The Insecurity

of Nyberg-Rueppel and Other DSA-Like Signature Schemes with Partially Known

Nonces ..... 97 Edwin El Mahassni, Phong Q. Nguyen, and Igor E. Shparlinski

Dimension Reduction Methods for Convolution Modular Lattices ..... 110 Alexander May and

Joseph H. Silverman Improving Lattice Based Cryptosystems Using the Hermite Normal Form : 126  
Daniele Micciancio The Two Faces of Lattices in Cryptology:..... 146 Phong Q.

## Book Information

Series: Lecture Notes in Computer Science (Book 2146)

Paperback: 224 pages

Publisher: Springer; 2001 edition (June 13, 2008)

Language: English

ISBN-10: 3540424881

ISBN-13: 978-3540424888

Product Dimensions: 6.1 x 0.5 x 9.2 inches

Shipping Weight: 12.6 ounces (View shipping rates and policies)

Average Customer Review: Be the first to review this item

Best Sellers Rank: #8,781,659 in Books (See Top 100 in Books) #92 inÂ Books > Computers & Technology > Programming > Software Design, Testing & Engineering > Coding Theory #957 inÂ Books > Computers & Technology > Security & Encryption > Encryption #1007 inÂ Books > Computers & Technology > Security & Encryption > Cryptography

[Download to continue reading...](#)

Cryptography and Lattices: International Conference, CaLC 2001, Providence, RI, USA, March 29-30, 2001. Revised Papers (Lecture Notes in Computer Science) Practical Aspects of Declarative Languages: Third International Symposium, PADL 2001 Las Vegas, Nevada, March 11-12, 2001 Proceedings (Lecture Notes in Computer Science) Large-Scale Scientific Computing: 6th International Conference, LSSC 2007, Sozopol, Bulgaria, June 5-9, 2007, Revised Papers (Lecture Notes in Computer Science) Software Reuse for Dynamic Systems in the Cloud and Beyond: 14th International Conference on Software Reuse, ICSR 2015, Miami, FL, USA, January 4-6, ... (Lecture Notes in Computer Science) System Analysis and Modeling: Models and Reusability: 8th International Conference, SAM 2014, Valencia, Spain, September 29-30, 2014. Proceedings (Lecture Notes in Computer Science) Database and Expert Systems Applications: 13th International Conference, DEXA 2002, Aix-en-Provence, France, September 2-6, 2002. Proceedings (Lecture Notes in Computer Science) Automated Reasoning with Analytic Tableaux and Related Methods: 16th International Conference, TABLEAUX 2007, Aix en Provence, France, July 3-6, 2007, Proceedings (Lecture Notes in Computer Science) Entity-Relationship Approach - ER '94. Business Modelling and Re-Engineering: 13th International Conference on the Entity-Relationship Approach,

... (Lecture Notes in Computer Science) Software Reuse: Methods, Techniques, and Tools: 8th International Conference, ICSR 2004, Madrid, Spain, July 5-9, 2004, Proceedings (Lecture Notes in Computer Science) Safe and Secure Software Reuse: 13th International Conference on Software Reuse, ICSR 2013, Pisa, Italy, June 18-20, 2013, Proceedings (Lecture Notes in Computer Science) Cellular Automata: 8th International Conference on Cellular Automata for Research and Industry, ACRI 2008, Yokohama, Japan, September 23-26, 2008, Proceedings (Lecture Notes in Computer Science) Reuse of Off-the-Shelf Components: 9th International Conference on Software Reuse, ICSR 2006, Torino, Italy, June 12-15, 2006, Proceedings (Lecture Notes in Computer Science) Software Reuse: Advances in Software Reusability: 6th International Conference, ICSR-6 Vienna, Austria, June 27-29, 2000 Proceedings (Lecture Notes in Computer Science) Dynamical Vision: ICCV 2005 and ECCV 2006 Workshops, WDV 2005 and WDV 2006, Beijing, China, October 21, 2005, Graz, Austria, May 13, 2006, Revised Papers (Lecture Notes in Computer Science) Mobile Entity Localization and Tracking in GPS-less Environments: Second International Workshop, MELT 2009, Orlando, FL, USA, September 30, 2009, Proceedings (Lecture Notes in Computer Science) Proceedings of the Fourth European Conference on Software Maintenance and Reengineering: Reengineering Week Zurich University of Zurich, Switzerland February 29-March 3-March 2, 2000 Trends in Distributed Systems: CORBA and Beyond: International Workshop TreDS '96 Aachen, Germany, October 1 - 2, 1996; Proceedings (Lecture Notes in Computer Science) Ada 95 Reference Manual. Language and Standard Libraries: International Standard ISO/IEC 8652:1995 (E) (Lecture Notes in Computer Science) Eurocode '90: International Symposium on Coding Theory and Applications : Proceedings (Lecture Notes in Computer Science) Solar Wind Nine: Proceedings of the Ninth International Solar Wind Conference: Nantucket, Massachusetts, 5-9 October 1998 (AIP Conference Proceedings / Astronomy and Astrophysics)

[Dmca](#)