



**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Singapore*

*Tokyo*

Joseph H. Silverman (Ed.)

# Cryptography and Lattices

International Conference, CaLC 2001  
Providence, RI, USA, March 29-30, 2001  
Revised Papers



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Joseph H. Silverman  
Brown University, Mathematics Department - Box 1917  
Providence, RI 02912, USA  
E-mail: [jhs@math.brown.edu](mailto:jhs@math.brown.edu)

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Cryptography and lattices : international conference, revised papers / CaLC 2001, Providence, RI, USA, March 29 - 30, 2001. Joseph H. Silverman (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2001  
(Lecture notes in computer science ; Vol. 2146)  
ISBN 3-540-42488-1

CR Subject Classification (1998): E.3, F.2.1, F.2.2, G.1, I.1.2, G.2, K.4.4

ISSN 0302-9743

ISBN 3-540-42488-1 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York  
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2001  
Printed in Germany

Typesetting: Camera-ready by author, date conversion by Christian Grosche, Hamburg  
Printed on acid-free paper      SPIN 10840224      06/3142      5 4 3 2 1 0

## Preface

These are the proceedings of CaLC 2001, 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 Hoffstein, Jill Pipher, Joseph Silverman

## Organization

CaLC 2001 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 CaLC 2001. The program chairs would also like to thank NTRU Cryptosystems for providing financial support for the conference.

### Program Committee

- Don Coppersmith <dcopper@us.ibm.com>  
IBM Research
- Jeffrey Hoffstein (co-chair) <jhoff@math.brown.edu>, <jhoff@ntru.com>  
Brown University and NTRU Cryptosystems
- Arjen Lenstra <arjen.lenstra@citicorp.com>  
Citibank, USA
- Phong Nguyen <Phong.Nguyen@ens.fr>  
ENS
- Andrew Odlyzko <amo@research.att.com>  
AT&T Labs Research
- Joseph H. Silverman (co-chair) <jhs@math.brown.edu>, <jhs@ntru.com>  
Brown University and NTRU Cryptosystems

### External Referees

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

### Sponsoring Institutions

NTRU Cryptosystems, Inc., Burlington, MA <www.ntru.com>

# Table of Contents

An Overview of the Sieve Algorithm for the Shortest Lattice Vector Problem <i>Miklós Ajtai, Ravi Kumar, and Dandapani Sivakumar</i>	1
Low Secret Exponent RSA Revisited <i>Johannes Blömer and Alexander May</i>	4
Finding Small Solutions to Small Degree Polynomials <i>Don Coppersmith</i>	20
Fast Reduction of Ternary Quadratic Forms <i>Friedrich Eisenbrand and Günter Rote</i>	32
Factoring Polynomials and 0-1 Vectors <i>Mark van Hoeij</i>	45
Approximate Integer Common Divisors <i>Nick Howgrave-Graham</i>	51
Segment LLL-Reduction of Lattice Bases <i>Henrik Koy and Claus Peter Schnorr</i>	67
Segment LLL-Reduction with Floating Point Orthogonalization <i>Henrik Koy and Claus Peter Schnorr</i>	81
The Insecurity of Nyberg-Rueppel and Other DSA-Like Signature Schemes with Partially Known Nonces <i>Edwin El Mahassni, Phong Q. Nguyen, and Igor E. Shparlinski</i>	97
Dimension Reduction Methods for Convolution Modular Lattices <i>Alexander May and Joseph H. Silverman</i>	110
Improving Lattice Based Cryptosystems Using the Hermite Normal Form <i>Daniele Micciancio</i>	126
The Two Faces of Lattices in Cryptology <i>Phong Q. Nguyen and Jacques Stern</i>	146
A 3-Dimensional Lattice Reduction Algorithm <i>Igor Semaev</i>	181
The Shortest Vector Problem in Lattices with Many Cycles <i>Mårten Trolin</i>	194
Multisequence Synthesis over an Integral Domain <i>Li-ping Wang and Yue-fei Zhu</i>	206
<b>Author Index</b>	219