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
Miklós Ajtai, Ravi Kumar, and Dandapani Sivakumar .................................................. 1

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

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

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

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

Approximate Integer Common Divisors
Nick Howgrave-Graham ......................................................................................................... 51

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

Segment LLL-Reduction with Floating Point Orthogonalization
Henrik Koy and Claus Peter Schnorr .................................................................................... 81

The Insecurity of Nyberg-Rueppel and Other DSA-Like Signature Schemes
with Partially Known Nonces
Edwin El Mahassni, Phong Q. Nguyen, and Igor E. Shparlinski .......................................... 97

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

Improving Lattice Based Cryptosystems Using the Hermite Normal Form
Daniele Micciancio .................................................................................................................. 126

The Two Faces of Lattices in Cryptology
Phong Q. Nguyen and Jacques Stern .................................................................................... 146

A 3-Dimensional Lattice Reduction Algorithm
Igor Semaev .......................................................................................................................... 181

The Shortest Vector Problem in Lattices with Many Cycles
Mårten Trolin .......................................................................................................................... 194

Multisequence Synthesis over an Integral Domain
Li-ping Wang and Yue-fei Zhu ............................................................................................ 206

Author Index .......................................................................................................................... 219