

Table of Contents

An Overveiw 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
Author Index	219

Cryptography and Lattices

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

Silverman, J.H. (Ed.)

2001, VIII, 224 p., Softcover

ISBN: 978-3-540-42488-8