# Table of Contents

An Overview of the Sieve Algorithm for the Shortest Lattice Vector Problem .......................... 1
   Miklós 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. Nguyen and Jacques Stern

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

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

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

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