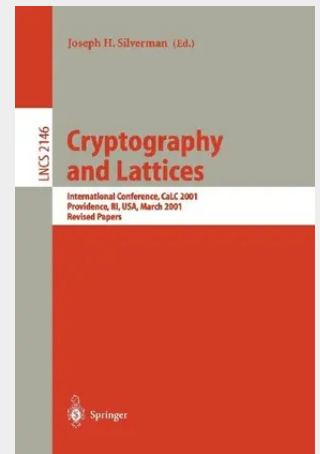


Cryptography and Lattices

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

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 Guntör 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.

An Overview of the Sieve Algorithm for the Shortest Lattice Vector Problem.- Low Secret Exponent RSA Revisited.- Finding Small Solutions to Small Degree Polynomials.- Fast Reduction of Ternary Quadratic Forms.- Factoring Polynomials and 0-1 Vectors.- Approximate Integer Common Divisors.- Segment LLL-Reduction of Lattice Bases.- Segment LLL-Reduction with Floating Point Orthogonalization.- The Insecurity of Nyberg-Rueppel and Other DSA-Like Signature Schemes with Partially Known Nonces.- Dimension Reduction Methods for Convolution Modular Lattices.- Improving Lattice Based Cryptosystems Using the Hermite Normal Form.- The Two Faces of Lattices in Cryptology.- A 3-Dimensional Lattice Reduction Algorithm.- The Shortest Vector Problem in Lattices with Many Cycles.- Multisequence Synthesis over an Integral Domain.



53,49 €

49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540424888

Medium: Buch

ISBN: 978-3-540-42488-8

Verlag: Springer

Erscheinungstermin: 15.08.2001

Sprache(n): Englisch

Auflage: 1. Auflage 2001

Serie: Lecture Notes in Computer Science

Produktform: Kartoniert

Gewicht: 359 g

Seiten: 224

Format (B x H): 155 x 235 mm

