

1. Record Nr.	UNISA996465808103316
Titolo	Cryptography and Lattices [[electronic resource]] : International Conference, CaLC 2001, Providence, RI, USA, March 29-30, 2001. Revised Papers / / edited by Joseph H. Silverman
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2001
ISBN	3-540-44670-2
Edizione	[1st ed. 2001.]
Descrizione fisica	1 online resource (VIII, 224 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2146
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Computers Algorithms Computer science—Mathematics Cryptology Computation by Abstract Devices Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science Symbolic and Algebraic Manipulation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	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

