1. Record Nr.	UNISA996465944303316
Titolo	Algorithmic Number Theory [[electronic resource]] : 4th International Symposium, ANTS-IV Leiden, The Netherlands, July 2-7, 2000 Proceedings / / edited by Wieb Bosma
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2000
ISBN	3-540-44994-9
Edizione	[1st ed. 2000.]
Descrizione fisica	1 online resource (IX, 612 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1838
Disciplina	512/.7
Soggetti	Number theory Data encryption (Computer science) Algorithms Computer science—Mathematics Number Theory Cryptology Algorithm Analysis and Problem Complexity Symbolic and Algebraic Manipulation Discrete Mathematics in Computer Science
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 and index.
Nota di contenuto	Invited Talks -- The Complexity of Some Lattice Problems -- Rational Points Near Curves and Small Nonzero | x 3 ? y 2| via Lattice Reduction -- Coverings of Curves of Genus 2 -- Lattice Reduction in Cryptology: An Update -- Contributed Papers -- Construction of Secure C ab Curves Using Modular Curves -- Curves over Finite Fields with Many Rational Points Obtained by Ray Class Field Extensions -- New Results on Lattice Basis Reduction in Practice -- Baby-Step Giant-Step Algorithms for Non-uniform Distributions -- On Powers as Sums of Two Cubes -- Factoring Polynomials over ?-Adic Fields -- Strategies in Filtering in the Number Field Sieve -- Factoring Polynomials over Finite Fields and Stable Colorings of Tournaments -- Computing Special Values of Partial Zeta Functions -- Construction of Tables of Quartic Number Fields -- Counting Discriminants of Number Fields of Degree

up to Four -- On Reconstruction of Algebraic Numbers -- Dissecting a Sieve to Cut Its Need for Space -- Counting Points on Hyperelliptic Curves over Finite Fields -- Modular Forms for GL(3) and Galois Representations -- Modular Symbols and Hecke Operators -- Fast Jacobian Group Arithmetic on C ab Curves -- Lifting Elliptic Curves and Solving the Elliptic Curve Discrete Logarithm Problem -- A One Round Protocol for Tripartite Diffie–Hellman -- On Exponential Sums and Group Generators for Elliptic Curves over Finite Fields -- Component Groups of Quotients of J 0(N) -- Fast Computation of Relative Class Numbers of CM-Fields -- On Probable Prime Testing and the Computation of Square Roots mod n -- Improving Group Law Algorithms for Jacobians of Hyperelliptic Curves -- Central Values of Artin L-Functions for Quaternion Fields -- The Pseudoprimes up to 1013 -- Computing the Number of Goldbach Partitions up to 5 108 -- Numerical Verification of the Brumer-Stark Conjecture -- Explicit Models of Genus 2 Curves with Split CM -- Reduction in Purely Cubic Function Fields of Unit Rank One -- Factorization in the Composition Algebras -- A Fast Algorithm for Approximately Counting Smooth Numbers -- Computing All Integer Solutions of a General Elliptic Equation -- A Note on Shanks's Chains of Primes -- Asymptotically Fast Discrete Logarithms in Quadratic Number Fields -- Asymptotically Fast GCD Computation in ?[i].