1. Record Nr. UNINA9910143627003321

Titolo	Cryptography and Lattices : 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

Many Cycles -- Multisequence Synthesis over an Integral Domain.

Sommario/riassunto

ThesearetheproceedingsofCaLC2001,the'rstconferencedevotedtocr-tographyandlattices. Wehavelongbelievedthattheimportanceofflatticesandlatticereductionincryptography, bothforcryptographicconstructionand cryptographicanalysis, meritsagatheringdevotedtothistopic. Theenthusiastic responsethatwereceivedfromtheprogramcommittee,theinvitedspeakers, the manypeoplewhosubmittedpapers, andthe90registeredparticipantsamply con'rmedthewidespreadinterestinlatticesandtheircryptographicappli-tions. WethankeveryonewhoseinvolvementmadeCaLCsuchasuccessfulevent; inparticularwethankNatalieJohnson,LarryLarrivee,DoreenPappas,andthe BrownUniversityMathematicsDepartmentfortheirassistanceandsupport. March2001 Je'reyHo'stein,JillPipher,JosephSilverman VI Preface Organization CaLC2001wasorganizedbytheDepartmentofMathematicsatBrownUniv-sity. Theprogramchairsexpresstheirthankstotheprogramcommiteeandthe additionalexternalrefereesfortheirhelpinselectingthepapersforCaLC2001 . TheprogramchairswouldalsoliketothankNTRUCryptosystemsforprovidin g ?nancialsupportfortheconference. Program Commitee DonCoppersmith IBMResearch Je'reyHo'stein(co-chair), BrownUniversityandNTRUCryptosystems ArjenLenstra Citibank,USA PhongNguyen ENS AndrewOdlyzko AT&TLabsResearch JosephH. Silverman(co-chair), BrownUniversityandNTRUCryptosystems External Referees AliAkhavi,GlennDurfee,NickHowgrave-Graham, DanieleMicciancio Sponsoring Institutions NTRUCryptosystems,Inc. , Burlington,MA Table of Contents An Overveiw of the Sieve Algorithm forthe Shortest Lattice Vector Problem 1 Miklos Ajtai, Ravi Kumar, and Dandapani Sivakumar Low Secret Exponent RSA Revisited :::::::::::::::::::::::::::::::: 4 Johannes Bl¨ omer and Alexander May Finding Small Solutions to Small Degree Polynomials:::::::::::::::::: 20 Don Coppersmith Fast Reduction of Ternary Quadratic Forms:::::::::::::::::::::::::: 32 Friedrich Eisenbrand and Gunt ¨ er Rote Factoring Polynomialsand 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 TheInsecurity ofNyberg-Rueppel andOther DSA-LikeSignatureSchemes 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.