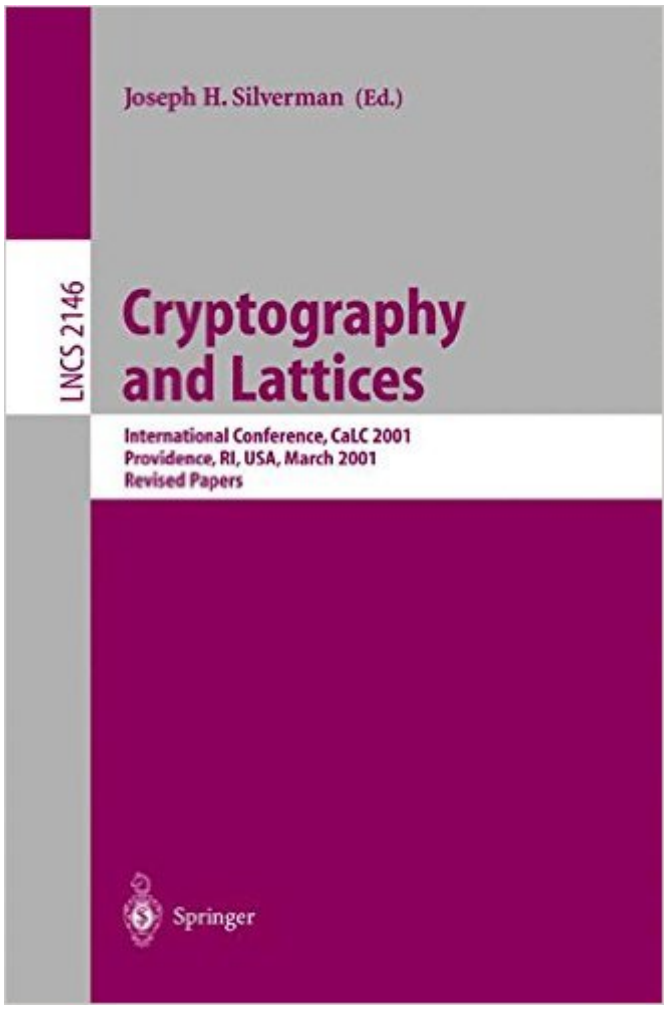
Cryptography And Lattices: International Conference, CaLC 2001, Providence, RI, USA, March 29-30, 2001. Revised Papers (Lecture Notes In Computer Science)



Synopsis

ThesearetheproceedingsofCaLC2001,the?rstconferencedevotedtocr- tographyandlattices. Wehavelongbelievedthattheimportanceoflattices andlatticereductionincryptography,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. TheprogramchairswouldalsoliketothankNTRUCryptosystemsforproviding ?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 BlÂ¨ 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 Â¨ 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

Book Information

Series: Lecture Notes in Computer Science (Book 2146)

Paperback: 224 pages

Publisher: Springer; 2001 edition (June 13, 2008)

Language: English

ISBN-10: 3540424881

ISBN-13: 978-3540424888

Product Dimensions: 6.1 x 0.5 x 9.2 inches

Shipping Weight: 12.6 ounces (View shipping rates and policies)

Average Customer Review: Be the first to review this item

Best Sellers Rank: #8,781,659 in Books (See Top 100 in Books) #92 inÂ Books > Computers & Technology > Programming > Software Design, Testing & Engineering > Coding Theory #957 inÂ Books > Computers & Technology > Security & Encryption > Encryption #1007 inÂ Books > Computers & Technology > Security & Encryption > Cryptography

... (Lecture Notes in Computer Science) Software Reuse: Methods, Techniques, and Tools: 8th International Conference, ICSR 2004, Madrid, Spain, July 5-9, 2004, Proceedings (Lecture Notes in Computer Science) Safe and Secure Software Reuse: 13th International Conference on Software Reuse, ICSR 2013,Pisa, Italy, June 18-20, 2013, Proceedings (Lecture Notes in Computer Science) Cellular Automata: 8th International Conference on Cellular Automata for Research and Industry, ACRI 2008, Yokohama, Japan, September 23-26, 2008, Proceedings (Lecture Notes in Computer Science) Reuse of Off-the-Shelf Components: 9th International Conference on Software Reuse, ICSR 2006, Torino, Italy, June 12-15, 2006, Proceedings (Lecture Notes in Computer Science) Software Reuse: Advances in Software Reusability: 6th International Conference, ICSR-6 Vienna, Austria, June 27-29, 2000 Proceedings (Lecture Notes in Computer Science) Dynamical Vision: ICCV 2005 and ECCV 2006 Workshops, WDV 2005 and WDV 2006, Beijing, China, October 21, 2005, Graz, Austria, May 13, 2006, Revised Papers (Lecture Notes in Computer Science) Mobile Entity Localization and Tracking in GPS-less Environnments: Second International Workshop, MELT 2009, Orlando, FL, USA, September 30, 2009, Proceedings (Lecture Notes in Computer Science) Proceedings of the Fourth European Conference on Software Maintenance and Reengineering: Reengineering Week Zurich University of Zurich, Switzerland February 29-March 3-March 2, 2000 Trends in Distributed Systems: CORBA and Beyond: International Workshop TreDS ’96 Aachen, Germany, October 1 - 2, 1996; Proceedings (Lecture Notes in Computer Science) Ada 95 Reference Manual. Language and Standard Libraries: International Standard ISO/IEC 8652:1995 (E) (Lecture Notes in Computer Science) Eurocode ’90: International Symposium on Coding Theory and Applications : Proceedings (Lecture Notes in Computer Science) Solar Wind Nine: Proceedings of the Ninth International Solar Wind Conference: Nantucket, Massachusetts, 5-9 October 1998 (AIP Conference Proceedings / Astronomy and Astrophysics)