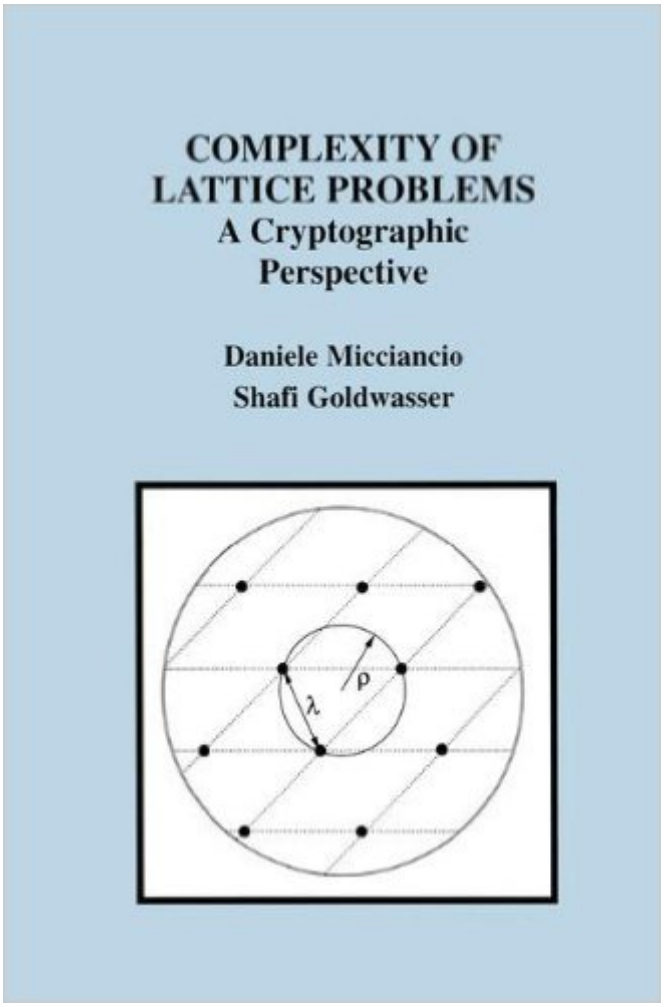
Complexity Of Lattice Problems: A Cryptographic Perspective (The Springer International Series In Engineering And Computer Science)



Synopsis

Lattices are geometric objects that can be pictorially described as the set of intersection points of an infinite, regular n-dimensional grid. DeÂ- spite their apparent simplicity, lattices hide a rich combinatorial strucÂ- ture, which has attracted the attention of great mathematicians over the last two centuries. Not surprisingly, lattices have found numerous apÂ- plications in mathematics and computer science, ranging from number theory and Diophantine approximation, to combinatorial optimization and cryptography. The study of lattices, specifically from a computational point of view, was marked by two major breakthroughs: the development of the LLL lattice reduction algorithm by Lenstra, Lenstra and Lovasz in the early 80's, and Ajtai's discovery of a connection between the worst-case and average-case hardness of certain lattice problems in the late 90's. The LLL algorithm, despite the relatively poor quality of the solution it gives in the worst case, allowed to devise polynomial time solutions to many classical problems in computer science. These include, solving integer programs in a fixed number of variables, factoring polynomials over the rationals, breaking knapsack based cryptosystems, and finding solutions to many other Diophantine and cryptanalysis problems.

Book Information

Series: The Springer International Series in Engineering and Computer Science (Book 671)
Hardcover: 220 pages
Publisher: Springer; 2002 edition (March 31, 2002)
Language: English
ISBN-10: 0792376889
ISBN-13: 978-0792376880
Product Dimensions: 6.1 x 0.6 x 9.2 inches
Shipping Weight: 8.8 ounces (View shipping rates and policies)
Average Customer Review: Be the first to review this item
Best Sellers Rank: #4,610,754 in Books (See Top 100 in Books) #57 inÂ Books > Computers & Technology > Programming > Software Design, Testing & Engineering > Coding Theory #598 inÂ Books > Computers & Technology > Security & Encryption > Encryption #632 inÂ Books > Computers & Technology > Security & Encryption > Cryptography

Complexity of Lattice Problems: A Cryptographic Perspective (The Springer International Series in Engineering and Computer Science) Iterative Detection: Adaptivity, Complexity Reduction, and

Applications (The Springer International Series in Engineering and Computer Science) Draw in Perspective: Step by Step, Learn Easily How to Draw in Perspective (Drawing in Perspective, Perspective Drawing, How to Draw 3D, Drawing 3D, Learn to Draw 3D, Learn to Draw in Perspective) Turbo Codes: Principles and Applications (The Springer International Series in Engineering and Computer Science) Sigma Delta Modulators: Nonlinear Decoding Algorithms and Stability Analysis (The Springer International Series in Engineering and Computer Science) Turbo Coding (The Springer International Series in Engineering and Computer Science) Simply Complexity: A Clear Guide to Complexity Theory Information Security Intelligence: Cryptographic Principles & Applications Understanding Voice Problems: A Physiological Perspective for Diagnosis and Treatment (Understanding Voice Problems: Phys Persp/ Diag & Treatment) Descriptive Complexity (Texts in Computer Science) Structure and Interpretation of Computer Programs - 2nd Edition (MIT Electrical Engineering and Computer Science) Entity-Relationship Approach - ER '94. Business Modelling and Re-Engineering: 13th International Conference on the Entity-Relationship Approach, ... (Lecture Notes in Computer Science) Python: Python Programming For Beginners - The Comprehensive Guide To Python Programming: Computer Programming, Computer Language, Computer Science Python: Python Programming For Beginners - The Comprehensive Guide To Python Programming: Computer Programming, Computer Language, Computer Science (Machine Language) Chinese Lattice Designs (Dover Pictorial Archive) The New Book of Chinese Lattice Designs (Dover Pictorial Archives) The Crystal Lattice: Phonons, Solitons, Dislocations, Superlattices Practice Problems for the Civil Engineering PE Exam: A Companion to the Civil Engineering Reference Manual, 15th Ed A PROLOG Database System (Electronic & Electrical Engineering Research Studies. Computer Engineering Series ; 3) Numerical Optimization (Springer Series in Operations Research and Financial Engineering)