The LLL Algorithm [Survey and Applications /

Nguyen, Phong Q.

Springer Berlin Heidelberg,
2010

Monografía

The LLL algorithm is a polynomial-time lattice reduction algorithm, named after its inventors, Arjen Lenstra, Hendrik Lenstra and László Lovász. The algorithm has revolutionized computational aspects of the geometry of numbers since its introduction in 1982, leading to breakthroughs in fields as diverse as computer algebra, cryptology and algorithmic number theory. This book consists of 15 survey chapters on computational aspects of Euclidean lattices and their main applications. Topics covered include polynomial factorization, lattice reduction algorithms, applications in number theory, integer programming, provable security, lattice-based cryptography and complexity. The authors include many detailed motivations, explanations and examples, and the contributions are largely self-contained. The book will be of value to a wide range of researchers and graduate students working in related fields of theoretical computer science and mathematics

Título: The LLL Algorithm Recurso electrónico-En línea] Survey and Applications edited by Phong Q. Nguyen, Brigitte Vallée

Editorial: Berlin, Heidelberg Springer Berlin Heidelberg 2010

Descripción física: XIV, 496 p. digital

Tipo Audiovisual: Computer science Data structures (Computer science) Computer software Computational complexity Algorithms Number theory Mathematical optimization Computer Science Data Structures, Cryptology and Information Theory Algorithms Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science Number Theory Optimization

Mención de serie: Information Security and Cryptography 1619-7100

Documento fuente: Springer eBooks

Nota general: Computer Science (Springer-11645)

Solving RSA and Factorization Problems: A Survey -- Lattice-Based Cryptanalysis -- Inapproximability Results for Computational Problems on Lattices -- On the Complexity of Lattice Problems with Polynomial Approximation Factors -- Cryptographic Functions from Worst-Case Complexity Assumptions

Restricciones de acceso: Accesible sólo para usuarios de la UPV

Tipo recurso electrónico: Recurso a texto completo

Detalles del sistema: Forma de acceso: Web

ISBN: 9783642022951

Autores: Vallée, Brigitte

Entidades: SpringerLink (Servicio en línea)

Enlace a formato físico adicional: Printed edition 9783642022944

Punto acceso adicional serie-Título: Information Security and Cryptography 1619-7100
