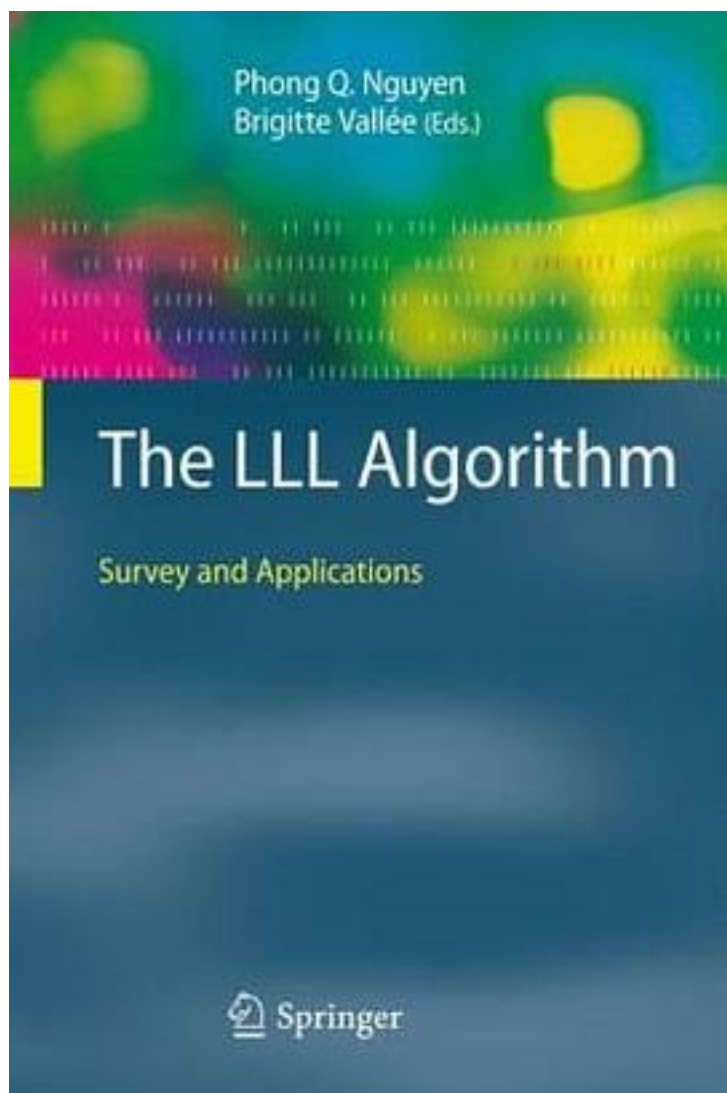


The LLL Algorithm



[The LLL Algorithm_ 下载链接1](#)

著者:Phong Q. Nguyen

出版者:

出版时间:2012

装帧:

isbn:9783642022944

The LLL algorithm is a polynomial-time lattice reduction algorithm, named after its inventors, Arjen Lenstra, Hendrik Lenstra and LAszlA3 LovAsz. 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.

作者介绍:

目录:

[The LLL Algorithm_下载链接1](#)

标签

数学

计算机科学

计算机

算法

The

LLL

Algorithm

2012

评论

[The LLL Algorithm_下载链接1](#)

书评

[The LLL Algorithm_下载链接1](#)