

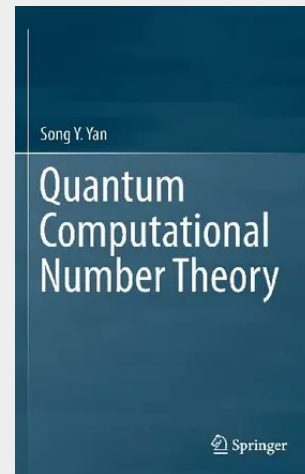
Quantum Computational Number Theory

This book provides a comprehensive introduction to advanced topics in the computational and algorithmic aspects of number theory, focusing on applications in cryptography. Readers will learn to develop fast algorithms, including quantum algorithms, to solve various classic and modern number theoretic problems. Key problems include prime number generation, primality testing, integer factorization, discrete logarithms, elliptic curve arithmetic, conjecture and numerical verification.

The author discusses quantum algorithms for solving the Integer Factorization Problem (IFP), the Discrete Logarithm Problem (DLP), and the Elliptic Curve Discrete Logarithm Problem (ECDLP) and for attacking IFP, DLP and ECDLP based cryptographic systems. Chapters also cover various other quantum algorithms for Pell's equation, principal ideal, unit group, class group, Gauss sums, prime counting function, Riemann's hypothesis and the BSD conjecture.

Quantum Computational Number Theory is self-contained and intended to be used either as a graduate text in computing, communications and mathematics, or as a basic reference in the related fields. Number theorists, cryptographers and professionals working in quantum computing, cryptography and network security will find this book a valuable asset.

This book provides a comprehensive introduction to advanced topics in the computational and algorithmic aspects of number theory, focusing on applications in cryptography. Readers will learn to develop fast algorithms, including quantum algorithms, to solve various classic and modern number theoretic problems. Key problems include prime number generation, primality testing, integer factorization, discrete logarithms, elliptic curve arithmetic, conjecture and numerical verification. The author discusses quantum algorithms for solving the Integer Factorization Problem (IFP), the Discrete Logarithm Problem (DLP), and the Elliptic Curve Discrete Logarithm Problem (ECDLP) and for attacking IFP, DLP and ECDLP based cryptographic systems. Chapters also cover various other quantum algorithms for Pell's equation, principal ideal, unit group, class group, Gauss sums, prime counting function, Riemann's hypothesis and the BSD conjecture. *Quantum Computational Number Theory* is self-contained and intended to be used either as a graduate text in computing, communications and mathematics, or as a basic reference in the related fields. Number theorists, cryptographers and professionals working in quantum computing, cryptography and network security will find this book a valuable asset.



106,99 €

99,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783319258218

Medium: Buch

ISBN: 978-3-319-25821-8

Verlag: Springer

Erscheinungstermin: 06.01.2016

Sprache(n): Englisch

Auflage: 1. Auflage 2015

Produktform: Gebunden

Gewicht: 5207 g

Seiten: 252

Format (B x H): 160 x 241 mm

