1. Record Nr. UNINA9910633996003321

Autore	Zheng Zhiyong
Titolo	Modern Cryptography Volume 2 : A Classical Introduction to Informational and Mathematical Principle
Pubbl/distr/stampa	2022 Singapore : , : Springer, , 2023 ©2023
Edizione	[1st ed.]
Descrizione fisica	1 electronic resource (191 p.)
Collana	Financial Mathematics and Fintech
Classificazione	BUS039000MAT003000
Altri autori (Persone)	TianKun LiuFengxia
Soggetti	Macroeconomics Applied mathematics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	This open access book covers the most cutting-edge and hot research topics and fields of post-quantum cryptography. The main purpose of this book is to focus on the computational complexity theory of lattice ciphers, especially the reduction principle of Ajtai, in order to fill the gap that post-quantum ciphers focus on the implementation of encryption and decryption algorithms, but the theoretical proof is insufficient. In Chapter 3, Chapter 4 and Chapter 6, author introduces the theory and technology of LWE distribution, LWE cipher and homomorphic encryption in detail. When using random analysis tools, there is a problem of "ambiguity" in both definition and algorithm. The greatest feature of this book is to use probability distribution to carry out rigorous mathematical definition and mathematical demonstration for various unclear or imprecise expressions, so as to make it a rigorous theoretical system for classroom teaching and dissemination. Chapters 5 and 7 further expand and improve the theory of cyclic lattice, ideal lattice and generalized NTRU cryptography. This book is used as a professional book for graduate students majoring in mathematics and cryptography, as well as a reference book for

scientific and technological personnel engaged in cryptography research.