1. Record Nr. UNINA9911046012703321

Titolo	Mathematical Foundations for Post-Quantum Cryptography : Crypto-Math CREST / / edited by Tsuyoshi Takagi, Masato Wakayama, Noboru Kunihiro, Keisuke Tanaka, Kazufumi Kimoto, Momonari Kudo
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2026
ISBN	9789819612185
Edizione	[1st ed. 2026.]
Descrizione fisica	1 online resource (IX, 496 p. 46 illus., 25 illus. in color.)
Collana	Mathematics for Industry, , 2198-3518 ; ; 40
Disciplina	530.15
Soggetti	Mathematical physics Geometry, Algebraic Number theory Mathematical Physics Algebraic Geometry Computational Number Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1. Algebraic Geometry -- 2. Number Theory -- 3. Theory of Computation -- 4. Quantum Computation -- 5. Quantum Field Theory -- 6. Mathematical Physics -- 7. Representation Theory -- 8. Lattice Theory -- 9. Multivariate Polynomial Theory -- 10. Data Encryption -- 11. Digital Signature -- 12. Searchable Encryption -- 13. Obfuscation -- 14. Privacy Protection -- 15. Copyright Protection -- 16. ID-based Encryption.
Sommario/riassunto	This open access book presents mathematical foundations for cryptography securely used in the era of quantum computers. In particular, this book aims to deepen the basic mathematics of post-quantum cryptography, model the strongest possible attacks such as side-channel attacks, and construct cryptographic protocols that guarantee security against such attacks. This book is a sequel of the successful book entitled by ``Mathematical Modeling for Next-Generation Cryptography - CREST Crypto-Math Project'' which was published in 2018. The book is suitable for use in an advanced graduate course in mathematical cryptography and as a reference book

for experts.