1. Record Nr. UNISA996466557703316

Autore	Takagi Tsuyoshi
Titolo	International Symposium on Mathematics, Quantum Theory, and Cryptography [[electronic resource]] : Proceedings of MQC 2019 / / edited by Tsuyoshi Takagi, Masato Wakayama, Keisuke Tanaka, Noboru Kunihiro, Kazufumi Kimoto, Yasuhiko Ikematsu
Pubbl/distr/stampa	Springer Nature, 2021 Singapore : , : Springer Singapore : , : Imprint : Springer, , 2021
ISBN	981-15-5191-X
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (XII, 274 p. 83 illus., 24 illus. in color.)
Collana	Mathematics for Industry, , 2198-350X ; ; 33
Disciplina	519
Soggetti	Applied mathematics Engineering mathematics Data structures (Computer science) Quantum computers Computer security Mathematical and Computational Engineering Data Structures and Information Theory Quantum Computing Systems and Data Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Sustainable Cryptography -- What Kind of Insight Provide Analytical Solutions of Quantum Models? -- Emerging Ultrastrong Coupling between Light and Matter Observed in Circuit Quantum Electrodynamics -- Quantum Random Numbers Generated by a Cloud Superconducting Quantum Computer -- Quantum Factoring Algorithm: Resource Estimation and Survey of Experiments -- A Review of Secret Key Distribution Based on Bounded Observability -- Towards Constructing Fully Homomorphic Encryption without Ciphertext Noise from Group Theory -- Number Theoretic Study in Quantum Interactions -- From the Bloch Sphere to Phase Space Representations with the Gottesman-Kitaev-Preskill Encoding -- A Data Concealing Technique

with Random Noise Disturbance and A Restoring Technique for the Concealed Data by Stochastic Process Estimation.

Sommario/riassunto

This open access book presents selected papers from International Symposium on Mathematics, Quantum Theory, and Cryptography (MQC), which was held on September 25-27, 2019 in Fukuoka, Japan. The international symposium MQC addresses the mathematics and quantum theory underlying secure modeling of the post quantum cryptography including e.g. mathematical study of the light-matter interaction models as well as quantum computing. The security of the most widely used RSA cryptosystem is based on the difficulty of factoring large integers. However, in 1994 Shor proposed a quantum polynomial time algorithm for factoring integers, and the RSA cryptosystem is no longer secure in the quantum computing model. This vulnerability has prompted research into post-quantum cryptography using alternative mathematical problems that are secure in the era of quantum computers. In this regard, the National Institute of Standards and Technology (NIST) began to standardize post-quantum cryptography in 2016. This book is suitable for postgraduate students in mathematics and computer science, as well as for experts in industry working on post-quantum cryptography.