1. Record Nr. UNINA9910492144603321

Titolo	Post-Quantum Cryptography : 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings / / edited by Jung Hee Cheon, Jean-Pierre Tillich
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-81293-6
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (502 pages)
Collana	Security and Cryptology, , 2946-1863 ; ; 12841
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Computer engineering Computer networks Data protection Cryptology Computer Engineering and Networks Computer Communication Networks Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Code-Based Cryptography -- Decoding supercodes of Gabidulin codes and applications to cryptanalysis -- LESS-FM: Fine-tuning Signatures from a Code-based Cryptographic Group Action -- Classical and Quantum algorithms for generic Syndrome Decoding problems and applications to the Lee metric -- Multivariate Cryptography -- Improving Thomae-Wolf Algorithm for Solving Underdetermined -- Multivariate Quadratic Polynomial Problem -- New Practical Multivariate Signatures from a Nonlinear Modifier -- On the Effect of Projection on Rank Attacks in Multivariate Cryptography -- Quantum Algorithms -- Quantum Key Search for Ternary LWE -- A fusion algorithm for solving the hidden shift problem in finite abelian groups -- The “quantum annoying” property of password-authenticated key exchange protocols -- Implementation and Side channel attack -- Differential Power

Analysis of the Picnic Signature Scheme -- Implementation of Lattice Trapdoors on Modules and Applications -- Verifying Post-Quantum Signatures in 8 KiB of RAM -- Fast NEON-based multiplication for lattice-based NIST Post-Quantum Cryptography finalists -- Isogeny -- CSI-RAShi: Distributed key generation for CSIDH -- SimS: a Simplification of SiGamal -- Memory Optimization Techniques for Computing Discrete Logarithms in Compressed SIKE -- Lattice-Based Cryptography -- Generating cryptographically-strong random lattice bases and recognizing rotations of Z -- Zero-Knowledge Proofs for Committed Symmetric Boolean Functions -- Short Identity-Based Signatures with Tight Security from Lattices -- On Removing Rejection Conditions in Practical Lattice-Based Signatures -- Secure Hybrid Encryption In the Standard Model from Hard Learning Problems -- Cryptanalysis -- Attack on Beyond-Birthday-Bound MACs in Quantum Setting -- An algebraic approach to the Rank Support Learning problem -- Quantum Indistinguishability for Public Key Encryption -- A Practical Adaptive Key Recovery Attack on the LGM (GSW-like) Cryptosystem.

Sommario/riassunto

This volume constitutes the proceedings of the 12th International Conference on post-quantum cryptography, PQCrypto 2021, held in Daejeon, South Korea in July 2021. The 25 full papers presented in this volume were carefully reviewed and selected from 65 submissions. They cover a broad spectrum of research within the conference's scope, including code-, hash-, isogeny-, and lattice-based cryptography, multivariate cryptography, and quantum cryptanalysis.