1.

Record Nr.	UNINA9910349311503321
Titolo	Post-Quantum Cryptography : 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019 Revised Selected Papers / / edited by Jintai Ding, Rainer Steinwandt
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-25510-7
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (XIII, 418 p. 581 illus., 18 illus. in color.)
Collana	Security and Cryptology, , 2946-1863 ; ; 11505
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Data protection Computers Computer engineering Computer networks Cryptology Data and Information Security Computing Milieux Computer Engineering and Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes Index.
Nota di contenuto	Finding closest lattice vectors using approximate Voronoi cells -- Evaluating the Potential for Hardware Acceleration of Four NTRU Based Key Encapsulation Mechanisms Using Software/Hardware Codesign -- Forward-Secure Group Signatures from Lattices -- Towards Practical Microcontroller Implementation of the Signature Scheme Falcon -- Round5: Compact and Fast Post-Quantum Public-Key Encryption -- The impact of error dependencies on Ring/Mod-LWE/LWR based schemes -- Direct CCA-Secure KEM and Deterministic PKE from Plain LWE -- Recovering short secret keys of RLCE in polynomial time -- Cryptanalysis of an NTRU-based Proxy Encryption Scheme from ASIACCS'15 -- On the Complexity of Superdetermined Minrank Instances -- Constant-Round Group Key Exchange from the Ring-RLWE

Assumption -- Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange -- Tighter security proofs for generic key encapsulation mechanism in the quantum random oracle model -- (Tightly) QCCA-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model -- Faster SeaSign signatures through improved rejection sampling -- Thomas Decru, Lorenz Panny, and Frederik Vercauteren Genus Two Isogeny Cryptography -- On Lions and Elligators: An efficient constant-time implementation of CSIDH -- Quantum security of hash functions and property-preservation of iterated hashing -- Improved Quantum Multicollision-Finding Algorithm -- Preventing timing attacks against RQC using constant time decoding of Gabidulin codes -- A traceable ring signature scheme based on coding theory -- On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders.

Sommario/riassunto

This book constitutes the refereed proceedings of the 9th International Workshop on Post-Quantum Cryptography, PQCrypto 2018, held in Fort Lauderdale, FL, USA, in April 2018. The 24 revised full papers presented were carefully reviewed and selected from 97 submissions. The papers are organized in topical sections on Lattice-based Cryptography, Learning with Errors, Cryptanalysis, Key Establishment, Isogeny-based Cryptography, Hash-based cryptography, Code-based Cryptography.