1. Record Nr. UNINA9910484107803321

Titolo	Post-Quantum Cryptography : 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013, Proceedings / / edited by Philippe Gaborit
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-38616-4
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (X, 259 p. 17 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 7932
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Data protection Quantum computers Electronic data processing - Management Algorithms Cryptology Data and Information Security Quantum Computing IT Operations
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures -- Quantum Algorithms for the Subset-Sum Problem -- Improved Lattice-Based Threshold Ring Signature Scheme -- Degree of Regularity for HFEv and HFEv- -- Software Speed Records for Lattice-Based Signatures -- Solving the Shortest Vector Problem in Lattices Faster Using Quantum Search -- An Efficient Attack of a McEliece Cryptosystem Variant Based on Convolutional -- Extended Algorithm for Solving Underdefined Multivariate Quadratic Equations -- Quantum Key Distribution in the Classical Authenticated Key Exchange Framework -- Cryptanalysis of Hash-Based Tamed Transformation and Minus Signature Scheme -- A Classification of Differential Invariants for Multivariate Post-quantum Cryptosystems -- Secure and Anonymous

	Hybrid Encryption from Coding Theory -- Fast Verification for Improved Versions of the UOV and Rainbow Signature Schemes -- The Hardness of Code Equivalence over Fq and Its Application to Code-Based Cryptography -- Timing Attacks against the Syndrome Inversion in Code-Based Cryptosystems -- Simple Matrix Scheme for Encryption -- Multivariate Signature Scheme Using Quadratic Forms.
Sommario/riassunto	This book constitutes the refereed proceedings of the 5th International Workshop on Post-Quantum Cryptography, PQCrypto 2013, held in Limoges, France, in June 2013. The 17 revised full papers presented were carefully reviewed and selected from 24 submissions. The papers cover all technical aspects of cryptographic research related to the future world with large quantum computers such as code-based cryptography, lattice-based cryptography, multivariate cryptography, cryptanalysis or implementations.