1. Record Nr. UNINA9910484277803321

Titolo	Post-quantum cryptography : third international workshop, PQcrypto 2010, Darmstadt, Germany, May 25-28, 2010. proceedings / / Nicolas Sendrier (ed.)
Pubbl/distr/stampa	New York, : Springer, 2010
ISBN	1-280-38644-4 9786613564368 3-642-12929-3
Edizione	[1st ed.]
Descrizione fisica	1 online resource (X, 241 p. 27 illus.)
Collana	Lecture notes in computer science, , 0302-9743 ; ; 6061
Altri autori (Persone)	SendrierNicolas
Disciplina	005.82
Soggetti	Computers - Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cryptanalysis of Multivariate Systems -- Properties of the Discrete Differential with Cryptographic Applications -- Growth of the Ideal Generated by a Quadratic Boolean Function -- Mutant Zhuang-Zi Algorithm -- Cryptanalysis of Two Quartic Encryption Schemes and One Improved MFE Scheme -- Cryptanalysis of Code-Based Systems -- Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes -- Grover vs. McEliece -- Information-Set Decoding for Linear Codes over F q -- A Timing Attack against the Secret Permutation in the McEliece PKC -- Practical Power Analysis Attacks on Software Implementations of McEliece -- Design of Encryption Schemes -- Key Exchange and Encryption Schemes Based on Non-commutative Skew Polynomials -- Designing a Rank Metric Based McEliece Cryptosystem -- Secure Variants of the Square Encryption Scheme -- Low-Reiter: Niederreiter Encryption Scheme for Embedded Microcontrollers -- Design of Signature Schemes -- Strongly Unforgeable Signatures and Hierarchical Identity-Based Signatures from Lattices without Random Oracles -- Proposal of a Signature Scheme Based on STS Trapdoor -- Selecting Parameters for the Rainbow Signature Scheme.