1. Record Nr. UNISA996465880003316

Titolo	Post-Quantum Cryptography [[electronic resource]] : Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010, Proceedings / / edited by Nicolas Sendrier
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	1-280-38644-4 9786613564368 3-642-12929-3
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (X, 241 p. 27 illus.)
Collana	Security and Cryptology ; ; 6061
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer communication systems Management information systems Computer science Algorithms Computer security Operating systems (Computers) Cryptology Computer Communication Networks Management of Computing and Information Systems Algorithm Analysis and Problem Complexity Systems and Data Security Operating Systems Darmstadt <2010>
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.