| | |
|---|---|
| 1. Record Nr. | UNISA996465875803316 |
| Titolo | Public Key Cryptography - PKC 2010 [[electronic resource] ] : 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010, Proceedings / / edited by Phong Q. Nguyen, David Pointcheval |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010 |
| ISBN | 1-280-38648-7<br>9786613564405<br>3-642-13013-5 |
| Edizione | [1st ed. 2010.] |
| Descrizione fisica | 1 online resource (XIII, 519 p. 34 illus.) |
| Collana | Security and Cryptology ; ; 6056 |
| Disciplina | 005.82 |
| Soggetti | Computer communication systems<br>Data encryption (Computer science)<br>Management information systems<br>Computer science<br>Algorithms<br>Computer security<br>Computer science—Mathematics<br>Computer Communication Networks<br>Cryptology<br>Management of Computing and Information Systems<br>Algorithm Analysis and Problem Complexity<br>Systems and Data Security<br>Discrete Mathematics in Computer Science<br>Paris <2010> |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Bibliographic Level Mode of Issuance: Monograph |
| Nota di bibliografia | Includes bibliographical references and index. |
| Nota di contenuto | Encryption I -- Simple and Efficient Public-Key Encryption from Computational Diffie-Hellman in the Standard Model -- Constant Size Ciphertexts in Threshold Attribute-Based Encryption -- Cryptanalysis -- Algebraic Cryptanalysis of the PKC’2009 Algebraic Surface |

Cryptosystem -- Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA -- Implicit Factoring with Shared Most Significant and Middle Bits -- Protocols I -- On the Feasibility of Consistent Computations -- Multi-query Computationally-Private Information Retrieval with Constant Communication Rate -- Further Observations on Optimistic Fair Exchange Protocols in the Multi-user Setting -- Network Coding -- Secure Network Coding over the Integers -- Preventing Pollution Attacks in Multi-source Network Coding -- Tools -- Groth–Sahai Proofs Revisited -- Constant-Round Concurrent Non-Malleable Statistically Binding Commitments and Decommitments -- Elliptic Curves -- Faster Squaring in the Cyclotomic Subgroup of Sixth Degree Extensions -- Faster Pairing Computations on Curves with High-Degree Twists -- Efficient Arithmetic on Hessian Curves -- Lossy Trapdoor Functions -- CCA Proxy Re-Encryption without Bilinear Maps in the Standard Model -- More Constructions of Lossy and Correlation-Secure Trapdoor Functions -- Chosen-Ciphertext Security from Slightly Lossy Trapdoor Functions -- Protocols II -- Efficient Set Operations in the Presence of Malicious Adversaries -- Text Search Protocols with Simulation Based Security -- Discrete Logarithm -- Solving a 676-Bit Discrete Logarithm Problem in GF(36n ) -- Using Equivalence Classes to Accelerate Solving the Discrete Logarithm Problem in a Short Interval -- Encryption II -- Functional Encryption for Inner Product: Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation -- Security of Encryption Schemes in Weakened Random Oracle Models -- Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes -- Signatures -- Unlinkability of Sanitizable Signatures -- Confidential Signatures and Deterministic Signcryption -- Identity-Based Aggregate and Multi-Signature Schemes Based on RSA -- Lattice Mixing and Vanishing Trapdoors: A Framework for Fully Secure Short Signatures and More.