1. Record Nr. UNINA9910144206703321

Titolo	Public Key Cryptography -- PKC 2004 : 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004 / / edited by Feng Bao, Robert Deng, Jianying Zhou
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	1-280-30691-2 9786610306916 3-540-24632-0
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (XIII, 459 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2947
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer communication systems Algorithms Computers and civilization Management information systems Computer science Cryptology Computer Communication Networks Algorithm Analysis and Problem Complexity Computers and Society Management of Computing and Information Systems
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	A Generalized Wiener Attack on RSA -- Cryptanalysis of a Public-Key Encryption Scheme Based on the Polynomial Reconstruction Problem -- Faster Scalar Multiplication on Koblitz Curves Combining Point Halving with the Frobenius Endomorphism -- Application of Montgomery's Trick to Scalar Multiplication for Elliptic and Hyperelliptic Curves Using a Fixed Base Point -- Fast Arithmetic on Jacobians of Picard Curves -- Undeniable Signatures Based on Characters: How to Sign with One Bit -- Efficient Extension of Standard Schnorr/RSA Signatures into

Universal Designated-Verifier Signatures -- Constructing Committed Signatures from Strong-RSA Assumption in the Standard Complexity Model -- Constant Round Authenticated Group Key Agreement via Distributed Computation -- Efficient ID-based Group Key Agreement with Bilinear Maps -- New Security Results on Encrypted Key Exchange -- New Results on the Hardness of Diffie-Hellman Bits -- Short Exponent Diffie-Hellman Problems -- Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups -- Algebraic Attacks over GF(2 k), Application to HFE Challenge 2 and Sflash-v2 -- Secret Exponent Attacks on RSA-type Schemes with Moduli N=p r q -- General Group Authentication Codes and Their Relation to “Unconditionally-Secure Signatures” -- From Digital Signature to ID-based Identification/Signature -- Identity-Based Threshold Decryption -- An Efficient Signature Scheme from Bilinear Pairings and Its Applications -- An RSA Family of Trap-Door Permutations with a Common Domain and Its Applications -- A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation -- Efficient, Verifiable Shuffle Decryption and Its Requirement of Unlinkability -- A Point Compression Method for Elliptic Curves Defined over GF(2 n) -- On the Optimal Parameter Choice for Elliptic Curve Cryptosystems Using Isogeny -- On the Security of Multiple Encryption or CCA-security+CCA-security=CCA-security? -- QuasiModo: Efficient Certificate Validation and Revocation -- A Distributed Online Certificate Status Protocol with a Single Public Key -- A First Approach to Provide Anonymity in Attribute Certificates -- A Nonuniform Algorithm for the Hidden Number Problem in Subgroups -- Cryptographic Randomized Response Techniques -- A Correct, Private, and Efficient Mix Network.