1. Record Nr. UNINA9910143640503321

Titolo	Public Key Cryptography : Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2000, Melbourne, Victoria, Australia, January 18-20, 2000, Proceedings / / edited by Hideki Imai, Yuliang Zheng
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2000
ISBN	3-540-46588-X
Edizione	[1st ed. 2000.]
Descrizione fisica	1 online resource (XIV, 490 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1751
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Computer programming Operating systems (Computers) Algorithms Computer networks Management information systems Computer science Cryptology Programming Techniques Operating Systems Algorithm Analysis and Problem Complexity Computer Communication Networks 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 Practical and Secure Fault-Tolerant Conference-Key Agreement Protocol -- An Efficient NICE-Schnorr-Type Signature Scheme -- Identification of Bad Signatures in Batches -- Some Remarks on a Fair Exchange Protocol -- Gaudry’s Variant against C ab Curves -- An Identification Scheme Based on Sparse Polynomials -- A State-Based Model for Certificate Management Systems -- Confidence Valuation in a Public-Key Infrastructure Based on Uncertain Evidence -- The

Composite Discrete Logarithm and Secure Authentication -- Chosen-Ciphertext Security for Any One-Way Cryptosystem -- Short Proofs of Knowledge for Factoring -- Secure and Practical Tree-Structure Signature Schemes Based on Discrete Logarithms -- All-or-Nothing Transform and Remotely Keyed Encryption Protocols -- Security of Public Key Certificate Based Authentication Protocols -- Efficient Implementation of Schoof's Algorithm in Case of Characteristic 2 -- Key Recovery in Third Generation Wireless Communication Systems -- Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications -- Certificates of Recoverability with Scalable Recovery Agent Security -- Design Validations for Discrete Logarithm Based Signature Schemes -- Optimally Efficient Accountable Time-Stamping -- "Pseudorandom Intermixing": A Tool for Shared Cryptography -- RSA-Based Auto-recoverable Cryptosystems -- Efficient and Fresh Certification -- Efficient Zero-Knowledge Proofs of Knowledge without Intractability Assumptions -- Cryptographic Approaches to Privacy in Forensic DNA Databases -- Making Hash Functions from Block Ciphers Secure and Efficient by Using Convolutional Codes -- Fast Implementation of Elliptic Curve Arithmetic in GF(p n) -- An Auction Protocol Which Hides Bids of Losers -- Forward Secrecy and Its Application to Future Mobile Communications Security -- Selecting Cryptographic Key Sizes -- A Structured ElGamal-Type Multisignature Scheme.