1. Record Nr. UNISA996465687603316

Titolo	Public Key Cryptography [[electronic resource]] : 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001, Cheju Island, Korea, February 13-15, 2001. Proceedings / / edited by Kwangjo Kim
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2001
ISBN	3-540-44586-2
Edizione	[1st ed. 2001.]
Descrizione fisica	1 online resource (XII, 428 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1992
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Algorithms Computer communication systems Operating systems (Computers) Management information systems Computer science Cryptology Algorithm Analysis and Problem Complexity Computer Communication Networks Operating Systems 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 at the end of each chapters and index.
Nota di contenuto	On the Security o a Williams Based Public Key Encryption Scheme -- Semantically Secure McEliece Public-Key Cryptosystems -Conversions for McEliece PKC - -- IND-CCA Public Key Schemes Equivalent to Factoring n =pq -- Identification, Signature and Signcryption Using High Order Residues Modulo an RSA Composite -- On the Security o Lenstra' s Variant o DSA without Long Inversions -- Fast Irreducibility and Subgroup Membership Testing in XTR -- A New Aspect for Security Notions: Secure Randomness in Public-Key Encryption Schemes -- The Gap-Problems: A New Class of Problems for the Security of

Cryptographic Schemes -- A Generalisation, a Simpli.cation and Some Applications of Paillier's Probabilistic Public-Key System -- Marking: A Privacy Protecting Approach Against Blackmailing -- Cryptanalysis of Two Sparse Polynomial Based Public Key Cryptosystems -- Cryptanalysis of PKP: A New Approach -- Cryptanalysis of a Digital Signature Scheme on ID-Based Key-Sharing Infrastructures -- Loopholes in Two Public Key Cryptosystems Using the Modular Group -- Efficient Revocation in Group Signatures -- A Public-Key Traitor Tracing Scheme with Revocation Using Dynamic Shares -- Efficient Asymmetric Self-Enforcement Scheme with Public Traceability -- Adaptive Security for the Additive-Sharing Based Proactive RSA -- Robust Forward-Secure Signature Schemes with Proactive Security -- Equitability in Retroactive Data Confiscation versus Proactive Key Escrow -- A PVSS as Hard as Discrete Log and Shareholder Separability -- One Round Threshold Discrete-Log Key Generation without Private Channels -- Remarks on Mix-Network Based on Permutation Networks -- New Key Recovery in WAKE Protocol -- Redundant Representation of Finite Fields -- Compact Encoding of Non-adjacent Forms with Applications to Elliptic Curve Cryptography -- Efficient Implementation of Elliptic Curve Cryptosystems on the TI MSP430x33x Family of Microcontrollers -- Secure Server-Aided Signature Generation -- Efficient Long-Term Validation of Digital Signatures -- A Novel Systolic Architecture for an Efficient RSA Implementation.

Sommario/riassunto

This book constitutes the refereed proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2001, held in Cheju Island, Korea in February 2001. The 30 revised full papers presented were carefully reviewed and selected from 67 submissions. The papers address all current issues in public key cryptography, ranging from mathematical foundations to implementation issues.