1. Record Nr. UNINA9910144913803321

Titolo	Information Security [[electronic resource]] : First International Workshop, ISW'97, Tatsunokuchi, Ishikawa Japan, September 17-19, 1997, Proceedings / / edited by Eiji Okamoto, George Davida, Masahiro Mambo
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1998
ISBN	3-540-69767-5
Edizione	[1st ed. 1998.]
Descrizione fisica	1 online resource (XII, 364 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1396
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer security Algorithms Computer networks Operating systems (Computers) Cryptology Systems and Data Security Algorithm Analysis and Problem Complexity Computer Communication Networks Operating Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	A general theory of codes, II: Paradigms and homomorphisms -- Improving the higher order differential attack and cryptanalysis of the KN cipher -- An optimised linear attack on pseudorandom generators using a non-linear combiner -- Cryptanalysis of message authentication codes -- The least witness of a composite number -- Fast algorithm for finding a small root of a quadratic modular equation -- Modified Finite Automata Public Key Cryptosystem -- Modified ElGamal cryptosystem -- Remarks on blind decryption -- High-speed cryptography -- Secure applications of low-entropy keys -- A key escrow system of the RSA cryptosystem -- A key escrow system with protecting user's privacy by blind decoding -- Some recent research

aspects of threshold cryptography -- A high-speed small RSA encryption LSI with low power dissipation -- The case for a secure multi-application smart card operating system -- An augmented family of cryptographic Parity Circuits -- A new byte-oriented block cipher -- Practice-oriented provable-security -- A framework for the management of information security -- Specifying security in a composite system -- On rough sets and inference analysis -- Arbitrated unconditionally secure authentication scheme with multi-senders -- Group signatures for hierarchical multigroups -- Threshold proxy signature schemes -- Signcryption and its applications in efficient public key solutions -- A new digital cash scheme based on blind Nyberg-Rueppel digital signature -- An incremental payment method for internet based streaming real-time media -- A new identity-based key exchange protocol minimizing computation and communication -- The application of ID-based key distribution systems to an elliptic curve -- On reconciliation of discrepant sequences shared through quantum mechanical channels.

Sommario/riassunto

This book constitutes the strictly refereed post-workshop proceedings of the First International Workshop on Information Security, ISW'98, held in Tatsunokuchi, Ishikawa, Japan, in September 1997. The volume presents six invited surveys together with 25 thoroughly revised full papers selected from 39 submissions. Among the topics covered are public-key cryptosystems, cryptoanalysis, digital signatures, hardware/software implementation, key management, key sharing, security management, electronic commerce, and quantum cryptology.