1. Record Nr. UNINA9910144924703321

Titolo	Information Security and Privacy [[electronic resource]] : Second Australasian Conference, ACISP '97, Sydney, NSW, Australia, July 7-9, 1997 Proceedings / / edited by Vijav Varadharajan, Josef Pieprzyk, Yi Mu
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1997
ISBN	3-540-69237-1
Edizione	[1st ed. 1997.]
Descrizione fisica	1 online resource (XIII, 343 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1270
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer engineering Management information systems Computer science Operating systems (Computers) Computer networks Electrical engineering Cryptology Computer Engineering Management of Computing and Information Systems Operating Systems Computer Communication Networks Communications Engineering, Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Trusted third parties for secure electronic commerce — Are they needed -- Prospectives for modelling trust in information security -- Analysis and implementation of a formal authorization policy design approach -- An approach to dynamic domain and type enforcement -- Purpose-oriented access control model in object-based systems -- User Access Domain Management System-ADAMS -- Revocation of unread e-mail in an untrusted network -- Security issues in

asynchronous transfer mode -- A method to implement a denial of service protection base -- ProtectOS: Operating system and hardware support for small objects -- Practical memory checkers for stacks, queues and deques -- Using cyclotomic polynomials to construct efficient discrete logarithm cryptosystems over finite fields -- A new hash function based on block cipher -- New lower bounds on nonlinearity and a class of highly nonlinear functions -- On the security of self-synchronous ciphers -- Inefficiency of variant characteristics for substitution-permutation networks with position permutations -- Secret sharing with reusable polynomials -- A message authentication code based on latin squares -- Characterization of (k, n) multi-receiver authentication -- Cryptanalysis of adaptive arithmetic coding encryption schemes -- Fast correlation attacks and multiple linear approximations -- Verifiable escrowed signature -- Democratic key escrow scheme -- Design and analyses of two basic protocols for use in TTP-based Key escrow -- Protection of data and delegated keys in digital distribution -- New micropayment schemes based on Pay Words -- On key agreement and conference key agreement -- Identity-based and self-certified key-exchange protocols -- Enabling technology for the trading of MPEG-encoded Video -- Image distribution method with embedded identifier scheme for copyright protection.

Sommario/riassunto

This book constitutes the refereed proceedings of the Second Australasian Conference on Information Security and Privacy, ACISP'97, held in Sydney, NSW, Australia, in July 1997. The 20 revised full papers presented were carefully selected for inclusion in the proceedings. The book is divided into sections on security models and access control, network security, secure hardware and implementation issues, cryptographic functions and ciphers, authentication codes and secret sharing systems, cryptanalysis, key escrow, security protocols and key management, and applications.