1. Record Nr. UNISA996466119703316

Titolo	Information Security and Privacy [[electronic resource]] : Third Australasian Conference, ACISP'98, Brisbane, Australia July 13-15, 1998, Proceedings / / edited by Colin Boyd, Ed Dawson
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1998
ISBN	3-540-69101-4
Edizione	[1st ed. 1998.]
Descrizione fisica	1 online resource (XII, 432 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1438
Disciplina	005.8
Soggetti	Computer security Computer communication systems Data encryption (Computer science) Management information systems Computer science Application software Electrical engineering Systems and Data Security Computer Communication Networks Cryptology Management of Computing and Information Systems Information Systems Applications (incl. Internet) 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	A review of the SESAME development -- The security of public key cryptosystems based on integer factorization -- A uniform approach to securing Unix applications using SESAME -- Integrated management of network and host based security mechanisms -- Covert distributed computing using Java through Web Spoofing -- Differential cryptanalysis of a block cipher -- On private-key cryptosystems based on product codes -- Key schedules of iterative block ciphers -- Low-cost secure server connection with limited-privilege clients -- A

solution to open standard of PKI -- Comparison of commitment schemes used in mix-mediated anonymous communication for preventing pool-mode attacks -- Correlation attacks on up/down cascades -- A stream cipher based on linear feedback over GF(28) -- A probabilistic correlation attack on the shrinking generator -- Bounds and constructions for A3-code with multi-senders -- Rotation-symmetric functions and fast hashing -- How to improve the nonlinearity of bijective S-boxes -- Object modeling of cryptographic algorithms with UML -- Adapting an electronic purse for internet payments -- LITESET: A light-weight secure electronic transaction protocol -- Applications of linearised and sub-linearised polynomials to information security -- Protocol failures related to order of encryption and signature computation of discrete logarithms in RSA groups -- Protection against EEPROM modification attacks -- Trends in quantum cryptography in Czech Republic -- A high level language for conventional access control models -- Fast access control decisions from delegation certificate databases -- Meta objects for access control: Role-based principals -- A dynamically typed access control model -- Efficient identity-based conference key distribution protocols -- A formal model for systematic design of key establishment protocols -- Key establishment protocols for secure mobile communications: A selective survey -- Detecting key-dependencies -- Secret sharing in multilevel and compartmented groups -- On construction of cumulative secret sharing schemes -- A comment on the efficiency of secret sharing scheme over any finite abelian group -- A user identification system using signature written with mouse -- On Zhang's nonrepudiable proxy signature schemes.

Sommario/riassunto

This book constitutes the refereed proceedings of the Third Australasian Conference on Information Security and Privacy, ACISP'98, held in Brisbane, Australia, in Kuly 1998. The volume presents 35 revised full papers selected from a total of 66 submissions; also included are two invited contributions. The book is divided in sections on network security, block ciphers, stream ciphers, authorization codes and Boolean functions, software security and electronic commerce, public key cryptography, hardware, access control, protocols, secret sharing, and digital signatures.