1. Record Nr. UNINA9910143592803321

Titolo	Information Security and Privacy : 6th Australasian Conference, ACISP 2001, Sydney, Australia, July 11-13, 2001. Proceedings / / edited by Vijay Varadharajan, Yi Mu
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2001
ISBN	3-540-47719-5
Edizione	[1st ed. 2001.]
Descrizione fisica	1 online resource (XI, 522 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2119
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Management information systems Computer science Computer networks Algorithms Computers and civilization Systems and Data Security Cryptology Management of Computing and Information Systems Computer Communication Networks Algorithm Analysis and Problem Complexity Computers and Society
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 Few Thoughts on E-Commerce -- New CBC-MAC Forgery Attacks -- Cryptanalysis of a Public Key Cryptosystem Proposed at ACISP 2000 -- Improved Cryptanalysis of the Self-Shrinking Generator -- Attacks Based on Small Factors in Various Group Structures -- On Classifying Conference Key Distribution Protocols -- Pseudorandomness of MISTY-Type Transformations and the Block Cipher KASUMI -- New Public-Key Cryptosystem Using Divisor Class Groups -- First Implementation of Cryptographic Protocols Based on Algebraic Number Fields -- Practical

Key Recovery Schemes -- Non-deterministic Processors -- Personal Secure Booting -- Evaluation of Tamper-Resistant Software Deviating from Structured Programming Rules -- A Strategy for MLS Workflow -- Condition-Driven Integration of Security Services -- SKETHIC: Secure Kernel Extension against Trojan Horses with Informat ion-Carrying Codes -- Secure and Private Distribution of Online Video and Some Related Cryptographic Issues -- Private Information Retrieval Based on the Subgroup Membership Problem -- A Practical English Auction with One-Time Registration -- A User Authentication Scheme with Identity and Location Privacy -- An End-to-End Authentication Protocol in Wireless Application Protocol -- Error Detection and Authentication in Quantum Key Distribution -- An Axiomatic Basis for Reasoning about Trust in PKIs -- A Knowledge-Based Approach to Internet Authorizations -- Applications of Trusted Review to Information Security -- Network Security Modeling and Cyber Attack Simulation Methodology -- Cryptographic Salt: A Countermeasure against Denial-of-Service Attacks -- Enhanced Modes of Operation for the Encryption in High-Speed Networks and Their Impact on QoS -- Improving the Availability of Time-Stamping Services -- Randomness Required for Linear Threshold Sharing Schemes Defined over Any Finite Abelian Group -- Democratic Systems -- Efficient and Unconditionally Secure Verifiable Threshold Changeable Scheme -- Provably Secure Distributed Schnorr Signatures and a (t, n) Threshold Scheme for Implicit Certificates -- How to Construct Fail-Stop Confirmer Signature Schemes -- Signature Schemes Based on 3rd Order Shift Registers -- Anonymous Statistical Survey of Attributes -- Secure Mobile Agent Using Strong Non-designated Proxy Signature -- Elliptic Curve Based Password Authenticated Key Exchange Protocols -- Elliptic Curve Cryptography on a Palm OS Device -- Reducing Certain Elliptic Curve Discrete Logarithms to Logarithms in a Finite Field.