

1. Record Nr.	UNINA9910767558003321
Titolo	Information Security and Privacy : 5th Australasian Conference, ACISP 2000, Brisbane, Australia, July 10-12, 2000, Proceedings // edited by Ed Dawson, Andrew Clark, Colin Boyd
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2000
ISBN	3-540-45030-0
Edizione	[1st ed. 2000.]
Descrizione fisica	1 online resource (XIII, 488 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1841
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer networks Management information systems Computer science Operating systems (Computers) Algorithms Cryptology Computer Communication Networks Management of Computing and Information Systems Operating Systems Algorithm Analysis and Problem Complexity
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	Network Security I -- Protecting Confidentiality against Trojan Horse Programs in Discretionary Access Control System -- Towards a New Authorisation Paradigm for Extranets -- Custom Safety Policies in Safe Erlang -- Public Key Cryptography -- A Proposal of a New Public Key Cryptosystem Using Matrices over a Ring -- Secure Length-Saving ElGamal Encryption under the Computational Diffie-Hellman Assumption -- Efficient Scalar Multiplications on Elliptic Curves without Repeated Doublings and Their Practical Performance -- Network Security II -- High Performance Agile Crypto Modules -- A Three-Party HTTP Proxy to Support Internet Content Regulation -- Cryptographic Implementation Issues -- Cryptanalysis of the m – Permutation

Protection Schemes -- An Implementation of Bitsliced DES on the Pentium MMXTM Processor -- Electronic Commerce I -- Securing Large E-Commerce Networks -- Passive Entities: A Strategy for Electronic Payment Design -- Key Recovery -- Key Recovery System for the Commercial Environment -- A Key Escrow Scheme with Time-Limited Monitoring for One-Way Communication -- Public Key Infrastructure -- Key Management for Secure Multicast with Dynamic Controller -- PKI Seeks a Trusting Relationship -- The PKI Specification Dilemma: A Formal Solution -- Boolean Functions -- Iterative Probabilistic Cryptanalysis of RC4 Keystream Generator -- Security Weaknesses in a Randomized Stream Cipher -- Two-Stage Optimisation in the Design of Boolean Functions -- Intrusion Detection -- A Novel Engine for Various Intrusion Detection Methods -- Codes -- Construction and Categories of Codes -- Digital Signatures I -- Cryptanalysis of Polynomial Authentication and Signature Scheme -- Secure Transactions with Mobile Agents in Hostile Environments -- A Multisignature Scheme with Message Flexibility, Order Flexibility and Order Verifiability -- Secret Sharing I -- Light Weight Broadcast Exclusion Using Secret Sharing -- Cheating Prevention in Secret Sharing -- On Multiplicative Secret Sharing Schemes -- Digital Signatures II -- On the Security of the RSA-Based Multisignature Scheme for Various Group Structures -- Fail-Stop Confirmer Signatures -- An Extremely Small and Efficient Identification Scheme -- Protocols -- An Anonymous Electronic Bidding Protocol Based on a New Convertible Group Signature Scheme -- AKA Protocols for Mobile Communications -- Electronic Commerce II -- A Three Phased Schema for Sealed Bid Auction System Design -- An Online Public Auction Protocol Protecting Bidder Privacy -- Secret Sharing II -- Algorithms to Speed Up Computations in Threshold RSA -- Sharing Block Ciphers -- Keynote Papers -- All Sail, No Anchor, I: Cryptography, Risk, and e-Commerce -- Professional Ethics in a Security and Privacy Context -- the Perspective of a National Computing Society.
