1. Record Nr. UNINA9910143452003321

Titolo	Information security and privacy : 12th australasian conference, acisp 2007, townsville, australia, july 2-4, 2007 : proceedings / / edited by Josef Pieprzyk, Rei Safavi-Naini, Jennifer Seberry
Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [1999] Â©1999
ISBN	1-280-80455-6 9786610804559 3-540-48970-3
Edizione	[1st ed. 1999.]
Descrizione fisica	1 online resource (336 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1587
Disciplina	005.8
Soggetti	Privacy, Right of Data protection Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Boolean Functions -- Boolean Function Design Using Hill Climbing Methods -- Enumeration of Correlation Immune Boolean Functions -- On the Symmetric Property of Homogeneous Boolean Functions -- Key Management -- Publicly Verifiable Key Escrow with Limited Time Span -- Accelerating Key Establishment Protocols for Mobile Communication -- Conference Key Agreement from Secret Sharing -- Cryptanalysis -- On m-Permutation Protection Scheme against Modification Attack -- Inversion Attack and Branching -- Signatures -- Fail-Stop Threshold Signature Schemes Based on Elliptic Curves -- Divertible Zero-Knowledge Proof of Polynomial Relations and Blind Group Signature -- Repudiation of Cheating and Non-repudiation of Zhang's Proxy Signature Schemes -- RSA Cryptosystems -- On the Security of an RSA Based Encryption Scheme -- Generalised Cycling Attacks on RSA and Strong RSA Primes -- RSA Acceleration with Field Programmable Gate Arrays -- Group Cryptography -- Changing Thresholds in the Absence of Secure Channels -- A Self-Certified Group-Oriented Cryptosystem without a Combiner -- Network Security -- Companion Viruses and the

Macintosh: Threats and Countermeasures -- An Implementation of a Secure Version of NFS Including RBAC -- Electronic Commerce -- Group Signatures and Their Relevance to Privacy-Protecting Offline Electronic Cash Systems -- Effient Electronic Cash Using Batch Signatures -- Evolution of Fair Non-repudiation with TTP -- Access Control -- Authorization in Object Oriented Databases -- An Analysis of Access Control Models -- Odds and Ends -- Efficient Identity Based Parameter Selection for Elliptic Curve Cryptosystems -- Characterization of Optimal Authentication Codes with Arbitration -- A Functional Cryptosystem Using a Group Action.