1. Record Nr.	UNISA996465900103316
Titolo	Information Security and Privacy [[electronic resource]] : 8th Australasian Conference, ACISP 2003, Wollongong, Australia, July 9-11, 2003, Proceedings / / edited by Rei Safavi-Naini, Jennifer Seberry
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2003
ISBN	3-540-45067-X
Edizione	[1st ed. 2003.]
Descrizione fisica	1 online resource (XII, 540 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2727
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer communication systems Operating systems (Computers) Coding theory Information theory Algorithms Management information systems Computer science Cryptology Computer Communication Networks Operating Systems Coding and Information Theory Algorithm Analysis and Problem Complexity Management of Computing and Information Systems
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	Privacy and Anonymity -- Grouping Verifiable Content for Selective Disclosure -- Evaluation of Anonymity of Practical Anonymous Communication Networks -- An Anonymous Credential System and a Privacy-Aware PKI -- Flaws in Some Robust Optimistic Mix-Nets -- Invited Talk (I) -- The Unsolvable Privacy Problem and Its Implications for Security Technologies -- Elliptic Curves -- The Security of Fixed versus Random Elliptic Curves in Cryptography -- Cryptanalysis of the

Full Version Randomized Addition-Subtraction Chains -- Generic GF (2m) Arithmetic in Software and Its Application to ECC -- An Addition Algorithm in Jacobian of C 34 Curve -- Crytpanalysis (I) -- Amplified Differential Power Cryptanalysis on Rijndael Implementations with Exponentially Fewer Power Traces -- Differential Fault Analysis on AES Key Schedule and Some Countermeasures -- On the Pseudorandomness of KASUMI Type Permutations -- Theoretical Analysis of ?2 Attack on RC6 -- Mobile and Network Security -- A Typed Theory for Access Control and Information Flow Control in Mobile Systems -- Provably Secure Mobile Key Exchange: Applying the Canetti-Krawczyk Approach -- Mobile PKI: A PKI-Based Authentication Framework for the Next Generation Mobile Communications -- Practical Pay TV Schemes -- Cooperative Routers against DoS Attacks -- Detecting Distributed Denial of Service Attacks by Sharing Distributed Beliefs -- Malicious ICMP Tunneling: Defense against the Vulnerability -- On Fair E-cash Systems Based on Group Signature Schemes -- Invited Talk (II) -- A Taxonomy of Single Sign-On Systems -- Cryptanalysis (II) -- Key Recovery Attacks on the RMAC, TMAC, and IACBC -- Key Recovery Attacks on NTRU without Ciphertext Validation Routine -- Permanent Fault Attack on the Parameters of RSA with CRT -- Backdoor Attacks on Black-Box Ciphers Exploiting Low-Entropy Plaintexts -- Signature -- Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings -- Digital Signature Schemes with Restriction on Signing Capability -- On the Exact Security of Multi-signature Schemes Based on RSA -- Cryptosystems (I) -- A Length-Flexible Threshold Cryptosystem with Applications -- Separating Encryption and Key Issuance in Digital Rights Management Systems -- An Efficient Revocation Scheme with Minimal Message Length for Stateless Receivers -- Parallel Authentication and Public-Key Encryption -- Invited Talk (III) -- Is Cross-Platform Security Possible? -- Cryptosystems (II) -- A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems -- Cryptanalysis of a New Cellular Automata Cryptosystem -- A CCA2 Secure Key Encapsulation Scheme Based on 3rd Order Shift Registers -- Clock-Controlled Shrinking Generator of Feedback Shift Registers -- Key Management -- EPA: An Efficient Password-Based Protocol for Authenticated Key Exchange -- Constructing General Dynamic Group Key Distribution Schemes with Decentralized User Join -- Robust Software Tokens — Yet Another Method for Securing User’s Digital Identity -- Theory and Hash Functions -- Public-Key Cryptosystems Based on Class Semigroups of Imaginary Quadratic Non-maximal Orders -- New Constructions for Resilient and Highly Nonlinear Boolean Functions -- On Parallel Hash Functions Based on Block-Cipher -- Square Hash with a Small Key Size.

Sommario/riassunto

This book constitutes the refereed proceedings of the 8th Australasian Conference on Information Security and Privacy, ACISP 2003, held in Wollongong, Australia, in July 2003. The 42 revised full papers presented together with 3 invited contributions were carefully reviewed and selected from 158 submissions. The papers are organized in topical sections on privacy and anonymity, elliptic curve cryptography, cryptanalysis, mobile and network security, digital signatures, cryptosystems, key management, and theory and hash functions.