1. Record Nr. UNISA996465735503316

Titolo	Information Security and Privacy [[electronic resource]] : 13th Australasian Conference, ACISP 2008, Wollongong, Australia, July 7-9, 2008, Proceedings / / edited by Yi Mu, Willy Susilo, Jennifer Seberry
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
ISBN	3-540-70500-7
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XIII, 480 p.)
Collana	Security and Cryptology ; ; 5107
Disciplina	005.82
Soggetti	Data encryption (Computer science) Management information systems Computer science Computer security Computer communication systems Coding theory Information theory Algorithms Cryptology Management of Computing and Information Systems Systems and Data Security Computer Communication Networks Coding and Information Theory 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	New Paradigms for Password Security -- Enforcing User-Aware Browser-Based Mutual Authentication with Strong Locked Same Origin Policy -- Secure Biometric Authentication with Improved Accuracy -- A Critical Analysis and Improvement of AACS Drive-Host Authentication -- Comparing the Pre- and Post-specified Peer Models for Key Agreement -- Efficient One-Round Key Exchange in the Standard Model -- On the Improvement of the BDF Attack on LSBS-RSA -- Public-Key

Cryptosystems with Primitive Power Roots of Unity -- Relationship between Two Approaches for Defining the Standard Model PA-ness -- Distributed Verification of Mixing - Local Forking Proofs Model -- Fully-Simulatable Oblivious Set Transfer -- Efficient Disjointness Tests for Private Datasets -- Efficient Perfectly Reliable and Secure Message Transmission Tolerating Mobile Adversary -- Methods for Linear and Differential Cryptanalysis of Elastic Block Ciphers -- Multidimensional Linear Cryptanalysis of Reduced Round Serpent -- Cryptanalysis of Reduced-Round SMS4 Block Cipher -- On the Unprovable Security of 2-Key XCBC -- Looking Back at a New Hash Function -- Non-linear Reduced Round Attacks against SHA-2 Hash Family -- Collisions for Round-Reduced LAKE -- Preimage Attacks on Step-Reduced MD5 -- Linear Distinguishing Attack on Shannon -- Recovering RC4 Permutation from 2048 Keystream Bytes if j Is Stuck -- Related-Key Chosen IV Attacks on Grain-v1 and Grain-128 -- Signature Generation and Detection of Malware Families -- Reducing Payload Scans for Attack Signature Matching Using Rule Classification -- Implicit Detection of Hidden Processes with a Feather-Weight Hardware-Assisted Virtual Machine Monitor -- FormatShield: A Binary Rewriting Defense against Format String Attacks -- Advanced Permission-Role Relationship in Role-Based Access Control -- Enhancing Micro-Aggregation Technique by Utilizing Dependence-Based Information in Secure Statistical Databases -- Montgomery Residue Representation Fault-Tolerant Computation in GF(2 k) -- A Tree-Based Approach for Computing Double-Base Chains -- Extractors for Jacobians of Binary Genus-2 Hyperelliptic Curves -- Efficient Modular Arithmetic in Adapted Modular Number System Using Lagrange Representation.

Sommario/riassunto

This book constitutes the refereed proceedings of the 13th Australasian Conference on Information Security and Privacy, ACISP 2008, held in Wollongong, Australia, in July 2008. The 33 revised full papers presented were carefully reviewed and selected from 111 submissions. The papers cover a range of topics in information security, including authentication, key management, public key cryptography, privacy, anonymity, secure communication, ciphers, network security, elliptic curves, hash functions, and database security.