1. Record Nr. UNISA996465890403316

Titolo	Information Security, Practice and Experience [[electronic resource]] : 6th International Conference, ISPEC 2010, Seoul, Korea, May 12-13, 2010, Proceedings / / edited by Jin Kwak, Robert H. Deng, Guilin Wang, Yoojae Won
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	1-280-38641-X 9786613564337 3-642-12827-0
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (XIII, 399 p. 68 illus.)
Collana	Security and Cryptology ; ; 6047
Disciplina	004.6
Soggetti	Computer communication systems Data encryption (Computer science) Management information systems Computer science Algorithms Computers and civilization Computer security Computer Communication Networks Cryptology Management of Computing and Information Systems Algorithm Analysis and Problem Complexity Computers and Society Systems and Data Security
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	Cryptanalysis -- Improved Related-Key Boomerang Attacks on Round-Reduced Threefish-512 -- Integral Attacks on Reduced-Round ARIA Block Cipher -- A New Class of RC4 Colliding Key Pairs with Greater Hamming Distance -- On the Security of NOEKEON against Side Channel Cube Attacks -- Algorithms and Implementations (I) -- On

Fast and Approximate Attack Tree Computations -- Width-3 Joint Sparse Form -- Accelerating Inverse of GF(2 n) with Precomputation -- Algorithms and Implementations (II) -- Concurrent Error Detection Architectures for Field Multiplication Using Gaussian Normal Basis -- The Elliptic Curve Discrete Logarithm Problems over the p-adic Field and Formal Groups -- A New Efficient Algorithm for Computing All Low Degree Annihilators of Sparse Polynomials with a High Number of Variables -- Network Security -- Host-Based Security Sensor Integrity in Multiprocessing Environments -- Using Purpose Capturing Signatures to Defeat Computer Virus Mutating -- Rate-Based Watermark Traceback: A New Approach -- Locally Multipath Adaptive Routing Protocol Resilient to Selfishness and Wormholes -- Access Control -- Security Analysis and Validation for Access Control in Multi-domain Environment Based on Risk -- A Proposal of Appropriate Evaluation Scheme for Exchangeable CAS (XCAS), -- Identity Management -- A Trustworthy ID Management Mechanism in Open Market -- BioID: Biometric-Based Identity Management -- Trust Management -- Privacy Preserving of Trust Management Credentials Based on Trusted Computing -- Mitigating the Malicious Trust Expansion in Social Network Service -- Public Key Cryptography -- An Efficient Convertible Undeniable Signature Scheme with Delegatable Verification -- Certificateless KEM and Hybrid Signcryption Schemes Revisited -- A Deniable Group Key Establishment Protocol in the Standard Model -- Threshold Password-Based Authenticated Group Key Exchange in Gateway-Oriented Setting -- Security Applications -- Binary Image Steganographic Techniques Classification Based on Multi-class Steganalysis -- Game Theoretic Resistance to Denial of Service Attacks Using Hidden Difficulty Puzzles -- Attacking and Improving on Lee and Chiu’s Authentication Scheme Using Smart Cards -- Protection Profile for Secure E-Voting Systems.