

1. Record Nr.	UNISA996465906903316
Titolo	Information Security Applications [[electronic resource]] : 9th International Workshop, WISA 2008, Jeju Island, Korea, September 23-25, 2008, Revised Selected Papers // edited by Kiwook Sohn, Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-00306-0
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XI, 334 p.)
Collana	Security and Cryptology ; ; 5379
Classificazione	DAT 465f SS 4800
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Data protection Computer networks Algorithms Electronic data processing—Management Computers, Special purpose Cryptology Data and Information Security Computer Communication Networks IT Operations Special Purpose and Application-Based 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	Smart Card and Secure Hardware(1) -- Using Templates to Attack Masked Montgomery Ladder Implementations of Modular Exponentiation -- Template Attacks on ECDSA -- Compact ASIC Architectures for the 512-Bit Hash Function Whirlpool -- Wireless and Sensor Network Security(1) -- Improved Constant Storage Self-healing Key Distribution with Revocation in Wireless Sensor Network -- Advances in Ultralightweight Cryptography for Low-Cost RFID Tags:

Gossamer Protocol -- Securing Layer-2 Path Selection in Wireless Mesh Networks -- Public Key Crypto Applications -- Public Key Authentication with Memory Tokens -- Certificate-Based Signatures: New Definitions and a Generic Construction from Certificateless Signatures -- Cryptanalysis of Mu et al.'s and Li et al.'s Schemes and a Provably Secure ID-Based Broadcast Signcryption (IBBSC) Scheme -- Privacy and Anonymity -- Sanitizable and Deletable Signature -- An Efficient Scheme of Common Secure Indices for Conjunctive Keyword-Based Retrieval on Encrypted Data -- Extension of Secret Handshake Protocols with Multiple Groups in Monotone Condition -- N/W Security and Intrusion Detection -- Pseudorandom-Function Property of the Step-Reduced Compression Functions of SHA-256 and SHA-512 -- A Regression Method to Compare Network Data and Modeling Data Using Generalized Additive Model -- A Visualization Technique for Installation Evidences Containing Malicious Executable Files Using Machine Language Sequence -- Application Security and Trust Management -- Image-Feature Based Human Identification Protocols on Limited Display Devices -- Ternary Subset Difference Method and Its Quantitative Analysis -- Data Deletion with Provable Security -- Smart Card and Secure Hardware(2) -- A Probing Attack on AES -- On Avoiding ZVP-Attacks Using Isogeny Volcanoes -- Security Analysis of DRBG Using HMAC in NIST SP 800-90 -- Wireless and Sensor Network Security(2) -- Compact Implementation of SHA-1 Hash Function for Mobile Trusted Module -- An Improved Distributed Key Management Scheme in Wireless Sensor Networks -- Protection Profile for Connected Interoperable DRM Framework.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 9th International Workshop on Information Security Applications, WISA 2008, held in Jeju Island, Korea, during September 23-25, 2008. The 24 revised full papers presented were carefully reviewed and selected from a total of 161 submissions. The papers are organized in topical sections on smart card and secure hardware, wireless and sensor network security, public key crypto applications, privacy and anonymity, n/w security and intrusion detection, as well as application security and trust management.
