1. Record Nr. UNISA996466254603316

Titolo	Information Security Applications [[electronic resource]] : 8th International Workshop, WISA 2007, Jeju Island, Korea, August 27-29, 2007, Revised Selected Papers / / edited by Kim Sehun, Moti Yung, Hyung-Woo Lee
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	3-540-77535-8
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XIII, 388 p.)
Collana	Security and Cryptology ; ; 4867
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Data protection Algorithms Computer networks 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	Public Key Crypto Applications -- Universal ? T Pairing Algorithm over Arbitrary Extension Degree -- Convertible Undeniable Proxy Signatures: Security Models and Efficient Construction -- Secret Signatures: How to Achieve Business Privacy Efficiently? -- Biometrics/Information Hiding -- Implementation of BioAPI Conformance Test Suite Using BSP Testing Model -- Information Hiding in Software with Mixed Boolean-Arithmetic Transforms -- Geometrically Invariant Image Watermarking in the DWT Domain -- Secure Hardware -- Implementation of LSM-

Based RBAC Module for Embedded System -- Iteration Bound Analysis and Throughput Optimum Architecture of SHA-256 (384,512) for Hardware Implementations -- A Compact Architecture for Montgomery Elliptic Curve Scalar Multiplication Processor -- Secure Systems -- Windows Vault: Prevention of Virus Infection and Secret Leakage with Secure OS and Virtual Machine -- An Architecture Providing Virtualization-Based Protection Mechanisms Against Insider Attacks -- Detecting Motifs in System Call Sequences -- Wireless and Mobile Security -- Comparative Studies in Key Disagreement Correction Process on Wireless Key Agreement System -- Breaking 104 Bit WEP in Less Than 60 Seconds -- Efficient Implementation of the Pairing on Mobilephones Using BREW -- Application Security/Secure Systems -- Security Analysis of MISTY1 -- A Generic Method for Secure SBox Implementation -- On the Security of a Popular Web Submission and Review Software (WSaR) for Cryptology Conferences -- Access Control/DB Security -- Authorization Constraints Specification of RBAC -- Dynamic Access Control Research for Inter-operation in Multi-domain Environment Based on Risk -- A Compositional Multiple Policies Operating System Security Model -- Smart Cards/Secure Systems -- Longer Randomly Blinded RSA Keys May Be Weaker Than Shorter Ones -- Differential Power Analysis of HMAC Based on SHA-2, and Countermeasures -- Provably Secure Countermeasure Resistant to Several Types of Power Attack for ECC -- Anonymity and P2P Security -- Risk & Distortion Based K-Anonymity -- Optimizing Quality Levels and Development Costs for Developing an Integrated Information Security System -- ICRep: An Incentive Compatible Reputation Mechanism for P2P Systems.

Sommario/riassunto

The 8th International Workshop on Information Security Applications (WISA 2007) was held on Jeju Island, Korea during August 27–29, 2007. The workshop was sponsored by the Korea Institute of Information Security and Cryptology (KIISC), the Electronics and Telecommunications Research Institute (ETRI) and the Ministry of Information and Communication (MIC). WISAaimsatprovidingaforumforprofessionalsfromacademiaandindustry to present their work and to exchange ideas. The workshop covers all technical aspects of security applications, including cryptographic and non-cryptographic techniques. We were very pleased and honored to serve as the Program Committee Co-chairs of WISA 2007. The Program Committee received 95 papers from 20 countries, and accepted 27 papers for the full presentation track. The papers were selected after an extensive and careful refereeing process in which each paper was reviewed by at least three members of the Program Committee. In addition to the contributed papers, the workshop had three special talks. Moti Yung gave a tutorial talk, entitled “Somebody You Know: The Fourth Factor of Authentication.” Kihong Park and Nasir Memon gave invited talks, entitled “Reactive Zero-Day Attack Protection” and “Securing Biometric T- plates,” respectively. Many people deserve our gratitude for their generous contributions to the success of the workshop. We would like to thank all the people involved in the technical program and in organizing the workshop. We are very grateful to the ProgramCommitteemembersandtheexternalrefereesfortheir timeande?orts in reviewing the submissions and selecting the accepted papers. We also express our special thanks to the Organizing Committee members for their hard work in organizing the workshop.