1. Record Nr. UNINA9910483065303321

Titolo	Information Security Applications : 10th International Workshop, WISA 2009, Busan, Korea, August 25-27, 2009, Revised Selected Papers / / edited by Heung Youl Youm, Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	1-280-38536-7 9786613563286 3-642-10838-5
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XIII, 386 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 5932
Altri autori (Persone)	YoumHeung Youl YungMoti
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Computer networks Computer science - Mathematics Discrete mathematics Data protection Algorithms Cryptology Computer Communication Networks Discrete Mathematics in Computer Science Data and Information Security Mathematical Applications in Computer Science
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	Multimedia Security -- Protecting IPTV Service Network against Malicious Rendezvous Point -- Design and Implementation of SIP-aware Security Management System -- Device Security -- Application Management Framework in User Centric Smart Card Ownership Model -- When Compromised Readers Meet RFID -- HW Implementation Security -- Coding Schemes for Arithmetic and Logic Operations - How

Robust Are They? -- Mechanism behind Information Leakage in Electromagnetic Analysis of Cryptographic Modules -- EM Side-Channel Attacks on Commercial Contactless Smartcards Using Low-Cost Equipment -- Applied Cryptography -- Identity-Based Identification Scheme Secure against Concurrent-Reset Attacks without Random Oracles -- Construction of Odd-Variable Boolean Function with Maximum Algebraic Immunity -- Efficient Publicly Verifiable Secret Sharing with Correctness, Soundness and ZK Privacy -- ID-Based Adaptive Oblivious Transfer -- Side Channel Attacks -- Unknown Plaintext Template Attacks -- On Comparing Side-Channel Preprocessing Techniques for Attacking RFID Devices -- You Cannot Hide behind the Mask: Power Analysis on a Provably Secure S-Box Implementation -- A Comparative Study of Mutual Information Analysis under a Gaussian Assumption -- Cryptograptanalysis -- Finding Collisions for a 45-Step Simplified HAS-V -- Non-linear Error Detection for Finite State Machines -- Quadratic Equations from a Kind of S-boxes -- Cryptanalysis of a Multivariate Public Key Encryption Scheme with Internal Perturbation Structure -- Anonymity/Authentication/Access Control -- Towards Privacy Aware Pseudonymless Strategy for Avoiding Profile Generation in VANET -- A Selectable k-Times Relaxed Anonymous Authentication Scheme -- PUF-Based Authentication Protocols – Revisited -- Mediated Ciphertext-Policy Attribute-Based Encryption andIts Application -- Network Security -- Securing Remote Access Inside Wireless Mesh Networks -- Detecting Ringing-Based DoS Attacks on VoIP Proxy Servers -- USN Middleware Security Model -- Practical Broadcast Authentication Using Short-Lived Signatures in WSNs.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 10th International Workshop on Information Security Applications, WISA 2009, held in Busan, Korea, during August 25-27, 2009. The 27 revised full papers presented were carefully reviewed and selected from a total of 79 submissions. The papers are organized in topical sections on mutlimedia security, device security, HW implementation security, applied cryptography, side channel attacks, cryptograptanalysis, anonymity/authentication/access controll, and network security.