1.

Record Nr.	UNINA9910484509403321
Titolo	Information Security Applications : 6th International Workshop, WISA 2005, Jeju Island, Korea, August 22-24, 2005, Revised Selected Papers / / edited by Jooseok Song, Taekyoung Kwon
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-33153-0
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XII, 378 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 3786
Altri autori (Persone)	SongJooSeok KwonTaekyoung YungMoti
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Operating systems (Computers) Algorithms Computer networks Electronic data processing - Management Computers, Special purpose Cryptology Operating Systems 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	Security Analysis and Attacks -- Security Weakness in Ren et al.’s Group Key Agreement Scheme Built on Secure Two-Party Protocols -- Cryptanalysis of Some Group-Oriented Proxy Signature Schemes -- Application of LFSRs in Time/Memory Trade-Off Cryptanalysis -- System Security -- An Alert Data Mining Framework for Network-Based Intrusion Detection System -- Key Factors Influencing Worm Infection in Enterprise Networks -- Evaluation of the Unified Modeling Language

for Security Requirements Analysis -- Network Security -- A Simple and Efficient Conference Scheme for Mobile Communications -- A Hash-Chain Based Authentication Scheme for Fast Handover in Wireless Network -- Efficient Multicast Stream Authentication for the Fully Adversarial Network Model -- Elastic Security QoS Provisioning for Telematics Applications -- DRM/Software Security -- An Improved Algorithm to Watermark Numeric Relational Data -- Video Fingerprinting System Using Wavelet and Error Correcting Code -- Secure Asymmetric Watermark Detection Without Secret of Modified Pixels -- Kimchi: A Binary Rewriting Defense Against Format String Attacks -- Software Protection Through Dynamic Code Mutation -- Efficient HW Implementation -- Efficient Hardware Implementation of Elliptic Curve Cryptography over GF(p m) -- Developing and Implementing IHPM on IXP 425 Network Processor Platforms -- Analysis on the Clockwise Transposition Routing for Dedicated Factoring Devices -- mCrypton – A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors -- Side-Channel Attacks -- Practical Modifications of Leadbitter et al.'s Repeated-Bits Side-Channel Analysis on (EC)DSA -- A DPA Countermeasure by Randomized Frobenius Decomposition -- DPA Attack on the Improved Ha-Moon Algorithm -- An Efficient Masking Scheme for AES SoftwareImplementations -- Privacy/Anonymity -- Secure Multi-attribute Procurement Auction -- Oblivious Conjunctive Keyword Search -- Efficient, Non-optimistic Secure Circuit Evaluation Based on the ElGamal Encryption -- Efficient Implementation -- New Concept of Authority Range for Flexible Management of Role Hierarchy -- Role-Based Access Control Model for Ubiquitous Computing Environment -- Designing Security Auditing Protocol with Web Browsers.

Sommario/riassunto

This book constitutes the refereed proceedings of the 6th International Workshop on Information Security Applications, WISA 2005, held in Jeju Island, Korea, in August 2005. The 29 revised full papers presented were carefully selected during two rounds of reviewing and improvement from 168 submissions. The papers are organized in topical sections on security analysis and attacks, systems security, network security, DRM/software security, efficient HW implementation, side-channel attacks, privacy/anonymity, and efficient implementation.