1. Record Nr. UNINA9910483628203321

Titolo	Information Security Practice and Experience : 5th International Conference, ISPEC 2009 Xi'an, China, April 13-15, 2009 Proceedings / / edited by Feng Bao, Hui Li, Guilin Wang
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-00843-7
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XIV, 410 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 5451
Altri autori (Persone)	BaoFeng LiHui <1968-> WangGuilin, Dr.
Disciplina	005.8
Soggetti	Data protection Cryptography Data encryption (Computer science) Computer networks Computers and civilization Data and Information Security Cryptology Computer Communication Networks Computers and Society
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	International conference proceedings.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Public Key Encryption -- Efficient and Provable Secure Ciphertext-Policy Attribute-Based Encryption Schemes -- A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length -- RSA-Based Certificateless Public Key Encryption -- Digital Signatures -- Strongly Unforgeable ID-Based Signatures without Random Oracles -- On the Security of a Certificate-Based Signature Scheme and Its Improvement with Pairings -- System Security -- An Empirical Investigation into the Security of Phone Features in SIP-Based VoIP Systems -- Reconstructing a Packed DLL Binary for Static Analysis -- Static Analysis of a Class of Memory Leaks in TrustedBSD MAC Framework -- Applied Cryptography -- Efficient Concurrent n poly

(logn)-Simulatable Argument of Knowledge -- New Constructions for Reusable, Non-erasure and Universally Composable Commitments -- Certificateless Hybrid Signcryption -- On Non-representable Secret Sharing Matroids -- Multimedia Security and DRM -- A Novel Adaptive Watermarking Scheme Based on Human Visual System and Particle Swarm Optimization -- Defending against the Pirate Evolution Attack -- Security Specification for Conversion Technologies of Heterogeneous DRM Systems -- Security Protocols -- Analysing Protocol Implementations -- Measuring Anonymity -- A Hybrid E-Voting Scheme -- Key Exchange and Management -- A Framework for Authenticated Key Exchange in the Standard Model -- Secret Handshake: Strong Anonymity Definition and Construction -- An Extended Authentication and Key Agreement Protocol of UMTS -- Hash-Based Key Management Schemes for MPEG4-FGS -- Hash Functions and MACs -- Twister – A Framework for Secure and Fast Hash Functions -- Preimage Attack on Hash Function RIPEMD -- Full Key-Recovery Attack on the HMAC/NMAC Based on 3 and 4-Pass HAVAL -- Cryptanalysis -- MemorylessRelated-Key Boomerang Attack on the Full Tiger Block Cipher -- Memoryless Related-Key Boomerang Attack on 39-Round SHACAL-2 -- Some New Observations on the SMS4 Block Cipher in the Chinese WAPI Standard -- On the Correctness of an Approach against Side-Channel Attacks -- Network Security -- Ranking Attack Graphs with Graph Neural Networks -- Implementing IDS Management on Lock-Keeper -- Security Applications -- Ensuring Dual Security Modes in RFID-Enabled Supply Chain Systems -- Achieving Better Privacy Protection in Wireless Sensor Networks Using Trusted Computing -- Trusted Privacy Domains – Challenges for Trusted Computing in Privacy-Protecting Information Sharing.

Sommario/riassunto

This book constitutes the refereed proceedings of the 5th International Information Security Practice and Experience Conference, ISPEC 2009, held in Xi'an, China in April 2009. The 34 revised full papers were carefully reviewed and selected from 147 submissions. The papers are organized in topical sections on public key encryption, digital signatures, system security, applied cryptography, multimedia security and DRM, security protocols, key exchange and management, hash functions and MACs, cryptanalysis, network security as well as security applications.