1. Record Nr. UNISA996203621303316

Titolo	Information Security Practice and Experience [[electronic resource]] : 10th International Conference, ISPEC 2014, Fuzhou, China, May 5-8, 2014, Proceedings / / edited by Xinyi Huang, Jianying Zhou
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2014
ISBN	3-319-06320-0
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (XIV, 578 p. 131 illus.)
Collana	Security and Cryptology ; ; 8434
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Management information systems Computer science Computer communication systems Systems and Data Security Cryptology Management of Computing and Information Systems Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Access Control in and Around the Browser -- Improving Thomlinson-Walker's Software Patching Scheme Using Standard Cryptographic and Statistical Tools -- Preserving Receiver-Location Privacy in Wireless Sensor Networks -- Data Security and Privacy in the Cloud -- Forbidden City Model – Towards a Practice Relevant Framework for Designing Cryptographic Protocols -- A CAPTCHA Scheme Based on the Identification of Character Locations -- A Multi process Mechanism of Evading Behavior-Based Bot Detection Approaches -- Obfuscating Encrypted Web Traffic with Combined Objects -- A Website Credibility Assessment Scheme Based on Page Association -- A Methodology for Hook-Based Kernel Level Rootkits -- Precise Instruction-Level Side Channel Profiling of Embedded Processors -- Automated Proof for Authorization Protocols of TPM 2.0 in Computational Model -- SBE – A

Precise Shell code Detection Engine Based on Emulation and Support Vector Machine -- HDROP: Detecting ROP Attacks Using Performance Monitoring Counters -- Efficient Hardware Implementation of MQ Asymmetric Cipher PMI+ on FPGAs -- High-Speed Elliptic Curve Cryptography on the NVIDIA GT200 Graphics Processing Unit -- A Progressive Dual-Rail Routing Repair Approach for FPGA Implementation of Crypto Algorithm -- Fault-Tolerant Linear Collision Attack: A Combination with Correlation Power Analysis -- Implementing a Covert Timing Channel Based on Mimic Function -- Detecting Frame Deletion in H.264 Video -- Efficient Adaptive Oblivious Transfer in UC Framework -- Multi-receiver Authentication Scheme for Multiple Messages Based on Linear Codes -- Efficient Sealed-Bid Auction Protocols Using Verifiable Secret Sharing -- Information-Theoretical Secure Verifiable Secret Sharing with Vector Space Access Structures over Bilinear Groups -- Proofs of Retrievability Based on MRD Codes -- TIMER: Secure and Reliable Cloud Storage against Data Re-outsourcing -- Improvement of a Remote Data Possession Checking Protocol from Algebraic Signatures -- Distributed Pseudo-Random Number Generation and Its Application to Cloud Database -- A Provably Secure Ring Signature Scheme with Bounded Leakage Resilience -- Two-Party (Blind) Ring Signatures and Their Applications -- Efficient Leakage-Resilient Signature Schemes in the Generic Bilinear Group Model -- Attribute-Based Signature with Message Recovery -- Encryption and Key Agreement An Adaptively CCA-Secure Ciphertext-Policy Attribute-Based Proxy Re-Encryption for Cloud Data Sharing -- Multi-recipient Encryption in Heterogeneous Setting -- ACP-lrFEM: Functional Encryption Mechanism with Automatic Control Policy in the Presence of Key Leakage -- Provably Secure Certificateless Authenticated Asymmetric Group Key Agreement -- New Variants of Lattice Problems and Their NP-Hardness -- Improved Preimage Attacks against Reduced HAS-160 -- Modular Inversion Hidden Number Problem Revisited -- On the Recursive Construction of MDS Matrices for Lightweight Cryptography -- On Constructions of Circulant MDS Matrices for Lightweight Cryptography.

Sommario/riassunto

This book constitutes the proceedings of the 10th International Conference on Information Security Practice and Experience, ISPEC 2014, held in Fuzhou, China, in May 2014. The 36 papers presented in this volume were carefully reviewed and selected from 158 submissions. In addition the book contains 5 invited papers. The regular papers are organized in topical sections named: network security; system security; security practice; security protocols; cloud security; digital signature; encryption and key agreement and theory.