1. Record Nr. UNINA9910349408403321

Titolo	Information Security Practice and Experience : 14th International Conference, ISPEC 2018, Tokyo, Japan, September 25-27, 2018, Proceedings / / edited by Chunhua Su, Hiroaki Kikuchi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	9783319998077 3319998072
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (XIV, 624 p. 111 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 11125
Disciplina	005.8
Soggetti	Data protection Cryptography Data encryption (Computer science) Computer networks Computers Artificial intelligence Data and Information Security Cryptology Computer Communication Networks Computing Milieux Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	System Security -- Macros Finder: Do You Remember LOVELETTER -- Time Series Analysis: Unsupervised Anomaly Detection Beyond Outlier Detection -- Universal Wavelet Relative Distortion: A New Counter Forensic Attack on Photo Response Non-Uniformity based Source Camera Identification -- Compact Ring Signature in the Standard Model for Blockchain -- Public key cryptography -- A Generic Construction of Integrated Secure-Channel Free PEKS and PKE -- An Almost Non-Interactive Order Preserving Encryption Scheme -- Leveled Hierarchical Identity-Based Fully Homomorphic Encryption from Learning with

Rounding -- Searchable and functional encryption -- Leakage-Resilient Chosen-Ciphertext Secure Functional Encryption from Garbled Circuits -- Constrained (Verifiable) Pseudorandom Function from Functional Encryption -- Efficient Trapdoor Generation from Multiple Hashing in Searchable Symmetric Encryption (Invited paper) -- (Post-quantum) Signature schemes -- Certificateless Public Key Signature Schemes from Standard Algorithms -- A New Design of Online/Offline Signatures Based on Lattice -- CHQS: Publicly Verifiable Homomorphic Signatures Beyond the Linear Case -- Achieving Almost-Full Security for Lattice-based Fully Dynamic Group Signatures with Verifier-local Revocation -- Entanglement between Hash Encodings and Signatures from ID Schemes with Non-Binary Challenges: a Case Study on Lightweight Code-based Signatures -- Security Protocols -- Efficient Evaluation of Low Degree Multivariate Polynomials in Ring-LWE Homomorphic Encryption Schemes -- Keyword-Based Delegable Proofs of Storage -- A Generic Framework for Accountable Optimistic Fair Exchange Protocol -- Network Security -- Towards Securing Challenge-based Collaborative Intrusion Detection Networks via Message Verification -- A Two-Stage Classifier Approach for Network Intrusion Detection -- DSH: Deniable Secret Handshake Framework -- Authentication -- Non-adaptive Group-Testing Aggregate MAC Scheme -- TMGMap: Designing Touch Movement-based Geographical Password Authentication on Smartphones -- Seeing is believing: authenticating users with what they see and remember -- Side-channel Attacks -- T SM: Elliptic Curve Scalar Multiplication Algorithm Secure against Single-Trace Attacks -- Recovering Memory Access Sequence with Differential Flush+Reload Attack -- Revisiting the Sparsification Technique in Kannan's Embedding Attack on LWE -- Security for Cyber-Physical Systems -- Efficient and Secure Firmware Update/Rollback Method for Vehicular Devices (Invited Paper) -- Regulating IoT messages -- A security cycle clock synchronization method based on mobile reference nodes in Wireless Sensor Networks -- Security in Mobile Environment -- Attribute-based Traceable Anonymous Proxy Signature Strategy for Mobile Healthcare -- Privacy-preserving data collection for mobile phone sensing tasks -- Secure Computation and Data Privacy -- M-ORAM Revisited: Security and Construction Updates -- Secure Computation of Inner Product of Vectors with Distributed Entries & its Applications to SVM -- (k,l)-clustering for Transactional Data Streams Anonymization -- Cryptographic Protocols -- A New Insight - Proxy Re-Encryption under LWE with Strong Anti-Collusion -- Hierarchical Secret Sharing Schemes Secure against Rushing Adversary:nn Cheater Identification and Robustness -- An Efficient and Provably Secure Private Polynomial Evaluation Scheme -- Efficient Traceable Oblivious Transfer and Its Applications.

Sommario/riassunto

This book constitutes the refereed proceedings of the 14th International Conference on Information Security Practice and Experience, ISPEC 2018, held in Tokyo, Japan, in September 2018. The 39 papers presented in this volume were carefully reviewed and selected from 73 submissions. They were organized in topical sections named: system security; public key cryptography; searchable and functional encryption; post-quantum signature schemas; security protocols; network security; authentication; side-channel attacks; security for cyber-physical systems; security in mobile environment; secure computation and data privacy; and cryptographic protocols. .