1. Record Nr. UNINA9910754093503321

Autore	Wang Ding
Titolo	Information and Communications Security : 25th International Conference, ICICS 2023, Tianjin, China, November 18–20, 2023, Proceedings / / edited by Ding Wang, Moti Yung, Zheli Liu, Xiaofeng Chen
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2023
ISBN	981-9973-56-2
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (773 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14252
Altri autori (Persone)	YungMoti LiuZheli ChenXiaofeng
Disciplina	005.73 003.54
Soggetti	Data structures (Computer science) Information theory Database management Data mining Application software Image processing - Digital techniques Computer vision Cryptography Data encryption (Computer science) Data Structures and Information Theory Database Management Data Mining and Knowledge Discovery Computer and Information Systems Applications Computer Imaging, Vision, Pattern Recognition and Graphics Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Symmetric-Key Cryptography -- SAT-aided Differential Cryptanalysis of Lightweight Block Ciphers Midori, MANTIS and QARMA -- Improved

Related-Key Rectangle Attack against the Full AES-192 -- Block Ciphers Classification Based on Randomness Test Statistic Value via LightGBM -- Cryptanalysis of Two White-Box Implementations of the CLEFIA Block Cipher -- PAE: Towards More Efficient and BBB-secure AE From a Single Public Permutation -- Public-Key Cryptography -- A Polynomial-time Attack on G2SIDH -- Improvements of Homomorphic Secure Evaluation of Inverse Square Root -- Oblivious Transfer from Rerandomizable PKE -- Forward Secure Lattice-based Ring Signature Scheme in the Standard Model -- Applied Cryptography -- Secure Multi-Party Computation with Legally-Enforceable Fairness -- On-demand Allocation of Cryptographic Computing Resource with Load Prediction -- Private Message Franking with After Opening Privacy -- Semi-Honest 2-Party Faithful Truncation from Two-Bit Extraction -- Outsourcing Verifiable Distributed Oblivious Polynomial Evaluation from Threshold Cryptography -- Authentication and Authorization -- PiXi: Password Inspiration by Exploring Information -- Security Analysis of Alignment-Robust Cancelable Biometric Scheme for Iris Verification -- A Certificateless Conditional Anonymous Authentication Scheme for Satellite Internet of Things -- BLAC: A Blockchain-based Lightweight Access Control Scheme in Vehicular Social Networks -- Privacy and Anonymity -- Link Prediction-Based Multi-Identity Recognition of Darknet Vendors -- CryptoMask: Privacy-preserving Face Recognition -- Efficient Private Multiset ID Protocols -- Zoomer: A Website Fingerprinting Attack against Tor Hidden Services -- An Enhanced Privacy-preserving Hierarchical Federated Learning Framework for IoV -- Security and Privacy of AI -- Revisiting the Deep Learning-based Eavesdropping Attacks via Facial Dynamics from VR Motion Sensors -- Multi-scale Features Destructive Universal Adversarial Perturbations -- Pixel-Wise Reconstruction of Private Data in Split Federated Learning -- Neural Network Backdoor Attacks Fully Controlled by Composite Natural Utterance Fragments -- Black-Box Fairness Testing with Shadow Models -- Graph Unlearning using Knowledge Distillation -- AFLOW: Developing Adversarial Examples under Extremely Noise-limited Settings -- Learning to Detect Deepfakes via Adaptive Attention and Constrained Difference -- A Novel Deep Ensemble Framework for Online Signature Verification Using Temporal and Spatial Representation -- Blockchain and Cryptocurrencies -- SCOPE: A Cross-Chain Supervision Scheme for Consortium Blockchains -- Subsidy Bridge: Rewarding Cross-blockchain Relayers with Subsidy -- Towards Efficient and Privacy-Preserving Anomaly Detection of Blockchain-based Cryptocurrency Transactions -- Blockchain based Publicly Auditable Multi-Party Computation with Cheater Detection -- BDTS: Blockchain-based Data Trading System -- Illegal Accounts Detection on Ethereum using Heterogeneous Graph Transformer Networks -- System and Network security -- DRoT: A Decentralised Root of Trust for Trusted Networks -- Finding Missing Security Operation Bugs via Program Slicing and Differential Check -- TimeClave: Oblivious In-enclave Time series Processing System -- Efficient and Appropriate Key Generation Scheme in Different IoT Scenarios -- A Fake News Detection Method Based on A Multimodal Cooperative Attention Network.

Sommario/riassunto

This volume LNCS 14252 constitutes the refereed proceedings of 25th International Conference on Information and Communications Security, ICICS 2023, held in Tianjin, China, during November 18–20, 2023. The 38 full papers presented together with 6 short papers were carefully reviewed and selected from 181 submissions. The conference focuses on: Symmetric-Key Cryptography; Public-Key Cryptography; Applied Cryptography; Authentication and Authorization; Privacy and Anonymity; Security and Privacy of AI; Blockchain and Cryptocurrencies;

and System and Network Security.