1. Record Nr. UNISA996696878003316

Autore	Chen Rongmao
Titolo	Information Security and Cryptology : 21st International Conference, Inscrypt 2025, Xi'an, China, October 19-22, 2025, Revised Selected Papers, Part II / / edited by Rongmao Chen, Robert H. Deng, Moti Yung
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2026
ISBN	981-9562-03-1
Edizione	[1st ed. 2026.]
Descrizione fisica	1 online resource (769 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 16409
Altri autori (Persone)	DengRobert H YungMoti
Disciplina	005.8
Soggetti	Data protection Image processing - Digital techniques Computer vision Computer networks Application software Computer networks - Security measures Cryptography Data encryption (Computer science) Data and Information Security Computer Imaging, Vision, Pattern Recognition and Graphics Computer Communication Networks Computer and Information Systems Applications Mobile and Network Security Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Secure Multi-party Computation. -- Quantum-Computation Classical-Communication Commitments from SZK-Hardness. -- Concretely Efficient Constructions for Differentially Private Set Intersection. -- MSFS: Maliciously Secure 3-Party Feature Selection via Mutual Information. -- Adaptive Batched K-out-of-N Oblivious Transfers Extension. -- Programming Equation Systems of Arithmetization-Oriented Primitives with Constraints. -- Anomaly

Detection Methodologies & Models. -- Anomaly Detection for ADS-B Data Based on KAN-LSTM. -- Network Intrusion Detection Method Based on Multi-Scale Feature Clustering and Improved Honey Badger Algorithm. -- SAGE: Spatiotemporal Feature Fusion for Anomaly Detection in Multivariate Time Series. -- MoE-CNN with Dynamic Feature Selection and CSAM for Network Anomaly Detection. -- PP-MTAD: Privacy-Preserving and Efficient Multivariate Time Series Anomaly Detection. -- LogWhisperer: Multi-Log Semantic Similarity Analysis based Intelligent Vehicle Anomaly Detection without Log Template. -- An Early Detection of Risky Crowd Dynamics Scheme Based on Motion Entropy and Scene Semantics. -- Enhancing Explainability in X-IDS through Counterfactuals. -- What Interferes with the Accurate Detection of Origin Hijacking Anomalies?. -- Network Security & Traffic Analysis. -- Verifiable and Privacy-Preserving Deep Packet Inspection for Multiple Rule Service Providers. -- Towards Adaptive Network Defense: A Self-Evolving Threat Detection Framework. -- Early Detection of Malicious Traffic based on Graph Modeling and Spatio-Temporal Attention Approach. -- Revealing the Frailty of Static Benchmarks: The DyNA-IDS Framework for Concept Drift Adaptation in Time-Series Network Intrusion Detection. -- iSSH: Enabling In-Flight SSH Traffic Inspection without Key Escrow. -- Tracing Your Roots: Exploring the Security Issues of Root Certificates in Android TLS Connections. -- Exploring the Root Store Usage in TLS-based Applications. -- LSDBFT: A Loose DAG-based Asynchronous BFT Consensus Algorithm with Fair Ordering. -- FRanCS: A Fair and Randomized Anonymous Network Circuit Selection Mechanism with Blockchain. -- Robust Training of Efficient Traffic Classifier with Noisy Labels. -- A Multimodal Asynchronous Federated Learning Approach for Encrypted Traffic Classification.

Sommario/riassunto

The three-volume set constitutes revised selected papers of the 21st International Conference on Information Security and Cryptology, Inscrypt 2025, held in Xi'an, China, on October 19, 2025. The 79 full papers presented in these proceedings were carefully reviewed and selected from 315 submissions. The papers were organized in the following topical sections: Part I : Post-Quantum Cryptography; Functional Encryption; Cryptanalysis and Implementations I; Cryptanalysis and Implementations II. Part II : Secure Multi-party Computation; Anomaly Detection Methodologies & Models; Network Security & Traffic Analysis. Part III : Privacy Preserving/Enhancing Technologies; AI and Security I; AI and Security II.