1. Record Nr. UNISA996696878403316

| | |
|---|---|
| Autore | Chen Rongmao |
| Titolo | Information Security and Cryptology : 21st International Conference, Inscrypt 2025, Xi'an, China, October 19-22, 2025, Revised Selected Papers, Part III / / edited by Rongmao Chen, Robert H. Deng, Moti Yung |
| Pubbl/distr/stampa | Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2026 |
| ISBN | 981-9562-09-0 |
| Edizione | [1st ed. 2026.] |
| Descrizione fisica | 1 online resource (716 pages) |
| Collana | Lecture Notes in Computer Science, , 1611-3349 ; ; 16410 |
| Altri autori (Persone) | DengRobert H<br>YungMoti |
| Disciplina | 005.8 |
| Soggetti | Data protection<br>Image processing - Digital techniques<br>Computer vision<br>Computer networks<br>Application software<br>Computer networks - Security measures<br>Cryptography<br>Data encryption (Computer science)<br>Data and Information Security<br>Computer Imaging, Vision, Pattern Recognition and Graphics<br>Computer Communication Networks<br>Computer and Information Systems Applications<br>Mobile and Network Security<br>Cryptology |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di contenuto | -- Privacy Preserving/Enhancing Technologies. -- Homomorphic MaxPooling via Bootstrapping for Privacy-Preserving Neural Networks. -- PrivGGM: Private Data Synthesis Using Multivariate Gaussian Generative Models and Fuzzy Rough Sets. -- A Framework for Efficient Enhanced Privacy ID from Group Actions. -- Publicly Verifiable Private Information Retrieval Protocols Based on Function Secret Sharing. -- FH-TEE: Single Enclave for all Applications. -- Comparing and |

Improving Perturbation Mechanisms under Local Differential Privacy. -- Anonymous Attribute-based Multi-keyword Searchable Encryption scheme for Medical Data Sharing using Blockchain. -- Invisible Data Capsule: Bridging On-Chain and Off-Chain Data Collaboration. -- AI and Security I. -- DNNKeyLock: Securing Deep Neural Network Intellectual Property with Steganography and Token Authentication. -- HBS Algorithmic Database Construction: A Chain-of-Thought-Driven Approach. -- EGNNFingers: Explainability-Driven Fingerprinting Framework for GNN Ownership Verification. -- Vertical Federated Convolutional Framework Based on Function Secret Sharing. -- Transferable Dormant Backdoor : Covertly Embedding Transferable Backdoor via Knowledge Distillation in Pre-trained Models. -- Detecting Stealthy Backdoor Attacks in Federated Learning via Wavelet Analysis on Dynamic Dimensions. -- Backdoor Attacks for Geographic Information Science with Principal Component Analysis and Singular Value Decomposition. -- AI and Security II. -- SeqFuzz : Efficient Kernel Directed Fuzzing via Effective Component Inference. -- LLM-DAS: An LLM-Powered Deobfuscation System for ARM Binary Code. -- Dynamic Generation Method of SELinux Policy Based on Knowledge Graph. -- CANalyze-AI: Semantic Zero-Day Detection and Rule Synthesis via LoRA-Fine-Tuned LLM for CAN Security. -- FuzzyHawk: Unveiling Ransomware Behavior Patterns via Graph-Based Fuzzy Matching. -- SC-HNM:Filtering False Negatives for Network Service Embeddings. -- Min-Entropy Estimation for Physical Layer Key Generation: An Empirical Study. -- Dual Modal Featuring Scheme for Learning Based Android Malware Prevention.

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.