1. Record Nr. UNISA996635664003316

Autore	Knechtel Johann
Titolo	Security, Privacy, and Applied Cryptography Engineering : 14th International Conference, SPACE 2024, Kottayam, India, December 14–17, 2024, Proceedings / / edited by Johann Knechtel, Urbi Chatterjee, Domenic Forte
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	9783031804083 3031804082
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (329 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15351
Altri autori (Persone)	ChatterjeeUrbi ForteDomenic
Disciplina	005.8
Soggetti	Data protection Computer networks Image processing - Digital techniques Computer vision Data and Information Security Computer Communication Networks Computer Imaging, Vision, Pattern Recognition and Graphics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Attacks and Countermeasures for Digital Microfluidic Biochips. -- SideLink: Exposing NVLink to Covert- and Side-Channel Attacks. -- Faster and more Energy-Efficient Equation Solvers over GF(2). -- Transferability of Evasion Attacks Against FHE Encrypted Inference. -- Security Analysis of ASCON Cipher under Persistent Faults. -- Privacy-Preserving Graph-Based Machine Learning with Fully Homomorphic Encryption for Collaborative Anti-Money Laundering. -- CoPrIME: Complete Process Isolation using Memory Encryption. -- Online Testing Entropy and Entropy Tests with a Two State Markov Model. -- DLShield: A Defense Approach against Dirty Label Attacks in Heterogeneous Federated Learning. -- Benchmarking Backdoor Attacks on Graph Convolution Neural Networks: A Comprehensive Analysis of Poisoning Techniques. -- Spatiotemporal Intrusion

Detection Systems for IoT Networks. -- High Speed High Assurance implementations of Mutivariate Quadratic based Signatures. -- ”There’ s always another counter”: Detecting Micro-architectural Attacks in a Probabilistically Interleaved Malicious/Benign Setting. -- FPGA-Based Acceleration of Homomorphic Convolution with Plaintext Kernels. -- Post-Quantum Multi-Client Conjunctive Searchable Symmetric Encryption from Isogenies. -- BlockDoor: Blocking Backdoor Based Watermarks in Deep Neural Networks. -- Adversarial Malware Detection. -- ML based Improved Differential Distinguisher with High Accuracy: Application to GIFT-128 and ASCON.

Sommario/riassunto

This book constitutes the refereed proceedings of the 14th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2024, held in Kottayam, India, during December 14–17, 2024. The 8 full papers, 10 short papers and 1 invited paper included in this book were carefully reviewed and selected from 43 submissions. They were organized in topical sections as follows: security, privacy, applied cryptographic engineering, integration of machine learning techniques, reflecting the growing prominence of this approach in contemporary research on security and cryptography, hardware security, the exploration of post-quantum cryptography, and the development of efficient implementations for emerging cryptographic primitives.