1.	Record Nr.	UNINA9910866573503321
	Autore	Andreoni Martin
	Titolo	Applied Cryptography and Network Security Workshops : ACNS 2024 Satellite Workshops, AIBlock, AIHWS, AIoTS, SCI, AAC, SiMLA, LLE, and CIMSS, Abu Dhabi, United Arab Emirates, March 5–8, 2024, Proceedings, Part I / / edited by Martin Andreoni
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
	ISBN	9783031614866 9783031614859
	Edizione	[1st ed. 2024.]
	Descrizione fisica	1 online resource (413 pages)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14586
	Disciplina	005.8
	Soggetti	Data protection Computer engineering Computer networks Computers Cryptography Data encryption (Computer science) Computer networks - Security measures Data and Information Security Computer Engineering and Networks Computing Milieux Cryptology Mobile and Network Security Enginyeria d'ordinadors Xarxes d'ordinadors Protecció de dades Criptografia Congressos Llibres electrònics
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	AIBlock – Application Intelligence and Blockchain Security: An End-to-

End Secure Solution for IoMT Data Exchange -- EasyLog: An Effcient Kernel Logging Service for Machine Learning -- LM-cAPI:A Lite Model based on API Core Semantic Information for Malware Classification -- ACKI NACKI: a Probabilistic Proof-of-Stake consensus protocol with fast finality and parallelization. AIHWS – Artificial Intelligence in Hardware Security: FPGA Implementation of Physically Unclonable Functions based on Multi-threshold Delay Time Measurement Method to Mitigate Modeling Attacks -- Incorporating Cluster Analysis of Feature Vectors for Non-profiled Deep-learning-based Side-channel Attacks -- Creating from Noise: Trace Generations Using Diffusion Model for Side-Channel Attacks -- Diversity Algorithms for Laser Fault Injection -- One for All, All for Ascon: Ensemble-based Deep Learning Side-channel Analysis -- CNN architecture extraction on edge GPU -- Harnessing the Power of LLMs in Hardware Trojan Design -- Everything All At Once: Deep Learning Side-Channel Analysis Optimization Framework -- AIoTS – Artificial Intelligence and Industrial IoT Security: Device Fingerprinting in a Smart Grid CPS -- Power Quality Forecasting of Microgrids using Adaptive Privacy-Preserving Machine Learning -- Evaluation of Lightweight Machine Learning-based NIDS Techniques for Industrial IoT -- Measuring Cyber Resilience of IoT-enabled Critical National Infrastructure -- SCI – Secure Cryptographic Implementation: Towards Discovering Quantum-Threats for Applications using Open-Source Libraries -- Pushing AES-256-GCM to Limits: Design, Implementation and Real FPGA Tests -- Automated Generation of Masked Nonlinear Components: From Lookup Tables to Private Circuits -- A Command-Activated Hardware Trojan Detection Method Based on LU-NAR Framework -- Cross-Correlation Based Trace Segmentation for Clustering Power Analysis on Public Key Cryptosystems -- Fully Hybrid TLSv1.3 in WolfSSL on Cortex-M4.

Sommario/riassunto

This two-volume set LNCS 14586-14587 constitutes the proceedings of eight Satellite Workshops held in parallel with the 22nd International Conference on Applied Cryptography and Network Security, ACNS 2024, held in Abhu Dabhi, United Arab Emirates, during March 5-8, 2024. The 33 full papers and 11 poster papers presented in this volume were carefully reviewed and selected from 62 submissions. They stem from the following workshops: 6th ACNS Workshop on Application Intelligence and Blockchain Security (AIBlock 2024). 5th ACNS Workshop on Artificial Intelligence in Hardware Security (AIHWS 2024). 6th ACNS Workshop on Artificial Intelligence and Industrial IoT Security (AIoTS 2024). 5th ACNS Workshop on Secure Cryptographic Implementation (SCI 2024). 1st Workshop on Advances in Asymmetric Cryptanalysis (AAC 2024). 6th ACNS Workshop on Security in Machine Learning and its Applications (SiMLA 2024). 1st Workshop on Low-Latency Encryption (LLE 2024). 4th ACNS Workshop on Critical Infrastructure and Manufacturing System Security (CIMSS 2024).