1.	Record Nr.	UNINA9910746963303321
	Autore	Zhou Jianying
	Titolo	Applied Cryptography and Network Security Workshops : ACNS 2023 Satellite Workshops, ADSC, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, SiMLA, Kyoto, Japan, June 19–22, 2023, Proceedings / / edited by Jianying Zhou, Lejla Batina, Zengpeng Li, Jingqiang Lin, Eleonora Losiouk, Suryadipta Majumdar, Daisuke Mashima, Weizhi Meng, Stjepan Picek, Mohammad Ashiqur Rahman, Jun Shao, Masaki Shimaoka, Ezekiel Soremekun, Chunhua Su, Je Sen Teh, Aleksei Udovenko, Cong Wang, Leo Zhang, Yury Zhauniarovich
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
	ISBN	3-031-41181-1
	Edizione	[1st ed. 2023.]
	Descrizione fisica	1 online resource (733 pages)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13907
	Altri autori (Persone)	BatinaLejla LiZengpeng LinJingqiang LosioukEleonora MajumdarSuryadipta MashimaDaisuke MengWeizhi PicekStjepan RahmanMohammad Ashiqur
	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
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa

Livello bibliografico	Monografia
Nota di contenuto	ADSC – Automated Methods and Data-driven Techniques in Symmetric-key Cryptanalysis -- Automatic Search Model for Related-Tweakey Impossible Differential Cryptanalysis -- Comprehensive Preimage Security Evaluations on Rijndael-based Hashing -- Conditional Cube Key Recovery Attack on Round-Reduced Xoodyak -- AIBlock – Application Intelligence and Blockchain Security Smart Contract-based E-Voting System Using Homomorphic Encryption and Zero-knowledge Proof -- Preventing Content Cloning in NFT Collections -- NFT Trades in Bitcoin with Off-chain Receipts -- AIHWS – Artificial Intelligence in Hardware Security A Comparison of Multi-task learning and Single-task learning Approaches -- Hide and Seek: Using Occlusion Techniques for Side-Channel Leakage Attribution in CNNs -- Secret Key Recovery Attack on Masked and Shuffled Implementations of CRYSTALS-Kyber and Saber -- SoK: Assisted Fault Simulation Existing Challenges and Opportunities Offered by AI -- Using Model Optimization as Countermeasure against Model Recovery Attacks -- AIoTS – Artificial Intelligence and Industrial IoT Security -- Blockchain-enabled Data Sharing in Connected Autonomous Vehicles for Heterogeneous Networks -- A Security Policy Engine for Building Energy Management Systems -- EARIC: Exploiting ADC Registers in IoT and Control Systems -- CIMSS – Critical Infrastructure and Manufacturing System Security Round-Efficient Security Authentication Protocol for 5G Network -- A Framework for TLS Implementation Vulnerability Testing in 5G -- Safety Watermark: A Defense Tool for Real-Time Digital Forensic Incident Response in Industrial Control Systems -- Leveraging Semantic Relationships to Prioritise Indicators of Compromise in Additive Manufacturing Systems -- WiP: Towards Zero Trust Authentication in Critical Industrial Infrastructures with PRISM -- Cloud S&P – Cloud Security and Privacy slytHErin: An Agile Framework for Encrypted Deep Neural Network Inference -- Trust Management Framework for Containerized Workloads – Applications to 5G Networks -- SCI – Secure Cryptographic Implementation -- cPSIR: Circuit-based Private Stateful Information Retrieval for Private Media Consumption -- A Deep-Learning Approach for Predicting Round Obfuscation in White-Box Block Ciphers -- Efficient Arithmetic for Polynomial Multiplication in Post-Quantum Lattice-based Cryptosystem on RISC-V Platform -- Generic Constructions of Server-Aided Revocable ABE with Verifiable Transformation -- Hybrid Post-Quantum Signatures in Hardware Security Keys -- Multi-Armed SPHINCS+ -- SpanL: Creating Algorithms for Automatic API Misuse Detection with Program Analysis Compositions -- ZKBdf: A ZKBoo-based Quantum-Secure Verifiable Delay Function with Prover-secret -- SecMT – Security in Mobile Technologies -- If you’re scanning this, it’s too late! A QR Code-based Fuzzing Methodology to Identify Input Vulnerabilities In Mobile Apps -- Enabling Lightweight Privilege Separation in Applications with MicroGuards -- SiMLA – Security in Machine Learning and its Applications -- Eliminating Adversarial Perturbations Using Image-to-Image Translation Method -- Federated Learning Approach for Distributed Ransomware Analysis -- Forensic Identification of Android Trojans Using Stacked Ensemble of Deep Neural Networks -- POSTERS -- Ransomware detection mechanism – Project status at the beginning of 2023 -- AuthZit: Multi-Modal Authentication with Visual-Spatial and Text Secrets -- Integration of End-to-End Security and Lightweight-SSL for Enhancing Security and Efficiency of MQTT -- Stopping Run-time

Countermeasures in Cryptographic Primitives -- Swarm-based IoT Network Penetration Testing by IoT Devices -- Advancing Federated Edge Computing with Continual Learning for Secure and Effcient Performance -- A Fine-Grained Metric for Evaluating the Performance of Adversarial Attacks and Defenses -- Integrating Quantum Key Distribution into Hybrid Quantum-Classical Networks -- Adaptive Moving Target Defense: Enhancing Dynamic Perturbation through Voltage Sensitivity Analysis in Power Systems -- PriAuct: Privacy Preserving Auction Mechanism -- Using Verifiable Credentials for Authentication of UAVs in Logistics -- A card-based protocol that lets you know how close two parties are in their opinions (agree/disagree) by using a four-point Likert scale -- Collaborative Authority-Based Searchable Encryption Using Access Control Encryption.

Sommario/riassunto

This book constitutes the proceedings of the satellite workshops held around the 21st International Conference on Applied Cryptography and Network Security, ACNS 2023, held in Kyoto, Japan, in June 2023. The 34 full papers and 13 poster papers presented in this volume were carefully reviewed and selected from 76 submissions. They stem from the following workshops: · 1st ACNS Workshop on Automated Methods and Data-driven Techniques in Symmetric-key Cryptanalysis (ADSC 2023) · 5th ACNS Workshop on Application Intelligence and Blockchain Security (AIBlock 2023) · 4th ACNS Workshop on Artificial Intelligence in Hardware Security (AIHWS 2023) · 5th ACNS Workshop on Artificial Intelligence and Industrial IoT Security (AIoTS 2023) · 3rd ACNS Workshop on Critical Infrastructure and Manufacturing System Security (CIMSS 2023) · 5th ACNS Workshop on Cloud Security and Privacy (Cloud S&P 2023) · 4th ACNS Workshop on Secure Cryptographic Implementation (SCI 2023) · 4th ACNS Workshop on Security in Mobile Technologies (SecMT 2023) · 5th ACNS Workshop on Security in Machine Learning and its Applications (SiMLA 2023).