1. Record Nr. UNINA9910734855503321

Autore	Dolev Shlomi
Titolo	Cyber Security, Cryptology, and Machine Learning : 7th International Symposium, CSCML 2023, Be'er Sheva, Israel, June 29–30, 2023, Proceedings / / edited by Shlomi Dolev, Ehud Gudes, Pascal Paillier
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	3-031-34671-8
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (539 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13914
Altri autori (Persone)	GudesEhud PaillierPascal
Disciplina	005.8
Soggetti	Data protection Application software Computer networks Machine learning Cryptography Data encryption (Computer science) Data and Information Security Computer and Information Systems Applications Computer Communication Networks Machine Learning Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Localhost Detour from Public to Private Networks -- Pseudo-Random Walk on Ideals: Practical Speed-Up in Relation Collection for Class Group Computation -- Efficient Extended GCD and Class Groups from Secure Integer Arithmetic -- On Distributed Randomness Generation in Blockchains -- Efficient Skip Connections Realization for Secure Inference on Encrypted Data -- Single Instance Self-Masking via Permutations A Fusion-Based Framework for Unsupervised Single Image Super-Resolution -- Generating One-Hot Maps under Encryption Building blocks for LSTM homomorphic evaluation with TFHE -- CANdito: Improving Payload-based Detection of Attacks on Controller

Area Networks -- Using Machine Learning Models for Earthquake Magnitude Prediction in California, Japan and Israel -- A Bag of Tokens Neural Network to Predict Webpage Age -- Correlations Between (Nonlinear) Combiners of Input and Output of Random Functions and Permutations (Short Paper) -- PPAuth: A Privacy-Preserving Framework for Authentication of Digital Image -- Robust Group Testing-Based Multiple-Access Protocol for Massive MIMO -- The use of Performance-Counters to perform side-channel attacks -- HAMLET: A Transformer Based Approach for Money Laundering Detection -- Hollow-Pass: A Dual-View Pattern Password Against Shoulder-Surfing Attacks -- Practical Improvements on BKZ Algorithm -- Enhancing Ransomware Classification with Multi-Stage Feature Selection and Data Imbalance Correction -- Short Paper: A Desynchronization-Based Countermeasure Against Side-Channel Analysis of Neural Networks -- New Approach for Sine and Cosine in Secure Fixed-Point Arithmetic -- How Hardened is Your Hardware? Guiding ChatGPT to Generate Secure Hardware Resistant to CWEs -- Evaluating the Robustness of Automotive Intrusion Detection Systems against Evasion Attacks -- On adaptively secure prefix encryption under LWE SigML: Supervised Log Anomaly with Fully Homomorphic Encryption -- HBSS: (Simple) Hash-Based Stateless Signatures -- Hash all the way to the Rescue -- Improving Performance in Space-Hard Algorithms -- A survey of security challenges in Automatic Identification System (AIS) Protocol -- A new interpretation for the GHASH authenticator of AES-GCM -- Fast ORAM with Server-aided Preprocessing and Pragmatic Privacy-Efficiency Trade-off -- Improving Physical Layer Security of Ground Stations Against GEO Satellite Spoofing Attacks -- Midgame Attacks and Defense Against Them -- Deep Neural Networks for Encrypted Inference with TFHE -- On the existence of highly organized communities in networks of locally interacting agents -- Patch or Exploit? NVD Assisted Classification of Vulnerability-Related Github Pages.

Sommario/riassunto

This book constitutes the refereed proceedings of the 7th International Symposium on Cyber Security, Cryptology, and Machine Learning, CSCML 2023, held in Be'er Sheva, Israel, in June 2023. The 21 full and 15 short papers were carefully reviewed and selected from 70 submissions. They deal with the theory, design, analysis, implementation, and application of cyber security, cryptography and machine learning systems and networks, and conceptually innovative topics in these research areas.