1. Record Nr. UNISA996636771503316

Autore	Katsikas Sokratis
Titolo	Information and Communications Security : 26th International Conference, ICICS 2024, Mytilene, Greece, August 26–28, 2024, Proceedings, Part II / / edited by Sokratis Katsikas, Christos Xenakis, Christos Kalloniatis, Costas Lambrinoudakis
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2025
ISBN	9789819788019 9819788013
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (344 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15057
Altri autori (Persone)	XenakisChristos KalloniatisChristos LambrinoudakisCostas
Disciplina	005.73 003.54
Soggetti	Data structures (Computer science) Information theory Database management Data mining Application software Image processing - Digital techniques Computer vision Cryptography Data encryption (Computer science) Data Structures and Information Theory Database Management Data Mining and Knowledge Discovery Computer and Information Systems Applications Computer Imaging, Vision, Pattern Recognition and Graphics Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Crypto & Applied crypto. -- TorHunter: A Lightweight Method for

Efficient Identification of Obfuscated Tor Traffic through Unsupervised Pre-training. -- Two-round Post-quantum Private Equality Test and OT from RLWE-encryption. -- Point Intervention: Improving ACVP Test Vector Generation Through Human Assisted Fuzzing. -- FAMC: Fair and Publicly Auditable Multi-Party Computation with Cheater Detection. -- Homomorphic encryption. -- X-Cipher: Achieving Data Resiliency in Homomorphic Ciphertexts. -- Amortized Functional Bootstrapping for Homomorphic Evaluation of Encrypted Functions. - Tightly Secure Linearly Homomorphic Signature Schemes for Subspace Under DL Assumption in AGM. -- Key agreement protocols and digital signature schemes. -- CoDPoC IP:A Configurable Data Protection Circuit to Support Multiple Key Agreement Scheme. -- Formal analysis of Julia Key Agreement Protocol. -- New Construction of Code-Based Signature Schemes. -- Identity-Based Signature from Lattices without Trapdoors. -- Defences. -- The Emperor is Now Clothed: A Secure Web Governance Framework for User Authentication Between Password Managers and Web Apps. -- HoneyLLM: A Large Language Model-Powered Medium-interaction Honeypot. -- TSR-jack: An In-Browser Crypto-jacking Detection Method Based on Time Series Representation Learning. -- Don’t Abandon the Primary Key: A High-Synchronization and Robust Virtual Primary Key Scheme for Watermarking Relational Databases. -- FirmPorter: Porting RTOSes at the Binary Level for Firmware Re-hosting.

Sommario/riassunto

This two-volume proceedings set LNCS 15056-15057 constitutes the proceedings of 26th International Conference on Information and Communications Security, ICICS 2024, in Mytilene, Greece, during August 26-28, 2024. The 32 full papers presented in this book were carefully selected and reviewed from 123 submissions. They cover topics related to many aspects of security in information and communication systems, ranging from attacks, to defences, to trust issues, to anomaly-based intrusion detection, to privacy preservation, and to theory and applications of various cryptographic techniques. .