1. Record Nr. UNINA9911046554303321

Autore	Nicomette Vincent
Titolo	Computer Security – ESORICS 2025 : 30th European Symposium on Research in Computer Security, Toulouse, France, September 22–24, 2025, Proceedings, Part II / / edited by Vincent Nicomette, Abdelmalek Benzekri, Nora Boulahia-Cuppens, Jaideep Vaidya
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2026
ISBN	3-032-07891-1
Edizione	[1st ed. 2026.]
Descrizione fisica	1 online resource (0 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 16054
Altri autori (Persone)	BenzekriAbdelmalek Boulahia-CuppensNora VaidyaJaideep
Disciplina	005.8
Soggetti	Data protection Cryptography Data encryption (Computer science) Computer networks - Security measures Computer networks Computer systems Data and Information Security Cryptology Security Services Mobile and Network Security Computer Communication Networks Computer System Implementation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- A Certified-Input Mixnet from Two-Party Mercurial Signatures on Randomizable Ciphertexts. -- Tetris! Traceable Extendable Threshold Ring Signatures and More. -- Efficient One-Pass Private Set Intersection from Pairings with Offline Preprocessing. -- Practical Robust Dynamic Searchable Symmetric Encryption Supporting Conjunctive Queries. -- Security Analysis of Covercrypt: A Quantum-Safe Hybrid Key Encapsulation Mechanism for Hidden Access Policies.

-- Anamorphic Monero Transactions: the Threat of Bypassing Anti-Money Laundering Laws. -- Hyperion: Transparent End-to-End Verifiable Voting with Coercion Mitigation. -- Two-Factor Authenticated Key Exchange with Enhanced Security from Post-Quantum Assumptions. -- Concretely Efficient Parallel-accessible DORAM for 100K-sized Array. -- A Symbolic Analysis of Hash Functions Vulnerabilities in Maude-NPA. -- A post-quantum Distributed OPRF from the Legendre PRF. -- TERRA: Trojan-Resilient Reverse-Firewall for Cryptographic Applications. -- Reaction Attack on TFHE: Minimum Number of Oracle Queries and Nearly Optimum Attacking Scheme. -- Predicate-Private Asymmetric Searchable Encryption for Conjunctions from Lattices. -- DEBridge: Towards Secure and Practical Plausibly Deniable Encryption Based on USB Bridge Controller. -- Formalisation of KZG commitment schemes in EasyCrypt. -- UTRA: Universal Token Reusability Attack and Token Unforgeable Delegatable Order-Revealing Encryption. -- Enhanced Key Mismatch Attacks on Lattice-Based KEMs: Multi-bit Inference and Ciphertext Generalization. -- Code Encryption with Intel TME-MK for Control-Flow Enforcement. -- Optimized Privacy-Preserving Multi-Signatures from Discrete Logarithm Assumption. -- Polylogarithmic Polynomial Commitment Scheme over Galois Rings. -- Efficient Homomorphic Evaluation for Non-Polynomial Functions. -- Athena: Accelerating KeySwitch and Bootstrapping for Fully Homomorphic Encryption on CUDA GPU. -- Formally-verified Security against Forgery of Remote Attestation using SSProve. -- SafePath: Encryption-less On-demand Input Path Protection for Mobile Devices. -- Extending Groth16 for Disjunctive Statements.

Sommario/riassunto

This four-volume set LNCS 16053-16056 constitutes the refereed proceedings of the 30th European Symposium on Research in Computer Security, ESORICS 2025, held in Toulouse, France, during September 22–24, 2025. The 100 full papers presented in these proceedings were carefully reviewed and selected from 600 submissions. They were organized in topical sections as follows: AI and Data-Centric Security, Systems and Hardware Security, Privacy, Cryptography and Secure Protocol Design, Blockchain and Financial Security, Privacy Policy and Identity Management, Adversarial and Backdoor Defenses. .