1. Record Nr. UNINA9910983054403321

Titolo	Provable and Practical Security : 18th International Conference, ProvSec 2024, Gold Coast, QLD, Australia, September 25–27, 2024, Proceedings, Part II / / edited by Joseph K. Liu, Liqun Chen, Shi-Feng Sun, Xiaoning Liu
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2025
ISBN	9789819609574 9819609577
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (XVI, 312 p. 47 illus., 22 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14904
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Computer networks Computer networks - Security measures Application software Cryptology Computer Communication Networks Mobile and Network Security Computer and Information Systems Applications
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Tight Security. -- Efficient Variants of TNT with BBB Security. -- ROM Reduction Failures: Reasons and Solutions. -- Quantum-Safe Cryptography. -- BDEC: Enhancing Learning Credibility via Post-Quantum Digital Credentials. -- Semi-Compressed CRYSTALS-Kyber. -- Blocklistable Anonymous Credential for Circuits with Post-Quantum Security. -- Distributed System and Blockchain Security. -- Asynchronous Byzantine Fault Tolerance Reliable Broadcast Based on Directed Acyclic Graph. -- PDTS: Practical Data Trading Scheme in Distributed Environments. -- Communication-Efficient Secure Neural Network via Key-Reduced Distributed Comparison Function. -- Enabling Efficient Cross-Shard Smart Contract Calling via Overlapping.

-- Key Exchange and Privacy. -- Subversion-Resilient Authenticated Key Exchange with Reverse Firewalls. -- On Sealed-bid Combinatorial Auction with Privacy-Preserving Dynamic Programming. -- Short Papers. -- SePEnTra: A secure and privacy-preserving energy trading mechanism in the transactive energy market. -- On Multi-user Security of Lattice-based Signature under Adaptive Corruptions and Key Leakages. -- Reusable Fuzzy Extractor from Isogeny. -- Ensuring Fair Data Trading via Passive Proxy Re-encryption with Smart Contracts. -- DPAC: A New Data-centric Privacy-preserving Access Control Model. -- Improving the Accuracy of Transaction-Based Ponzi Detection on Ethereum. -- A2V: Anonymous and Accountable Voting Framework via Blockchain. -- Quantum Safe Computation-friendly Identity-binding Password Authenticated Key Exchange.

Sommario/riassunto

This book constitutes the proceedings of the 18th International Conference on Provable and Practical Security, ProvSec 2024, which took place in Gold Coast, QLD, Australia, during September 25-27, 2024. The 26 full papers and 8 short papers presented were thoroughly reviewed and selected from the 79 submissions. The papers are organized in the following topical sections: Part I: Multi-Party Computation; Searchable Encryption; Encryption and Signature. Part II : Tight Security; Quantum-Safe Cryptography; Distributed System and Blockchain Security; and Key Exchange and Privacy.