1. Record Nr. UNINA9910983330103321

Autore	Liu Joseph K
Titolo	Provable and Practical Security : 18th International Conference, ProvSec 2024, Gold Coast, QLD, Australia, September 25–27, 2024, Proceedings, Part I / / edited by Joseph K. Liu, Liqun Chen, Shi-Feng Sun, Xiaoning Liu
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2025
ISBN	9789819609543 9819609542
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (592 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14903
Altri autori (Persone)	ChenLiqun SunShi-Feng LiuXiaoning
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	-- Multi-Party Computation. -- SecFloatPlus: More Accurate Floating-Point Meets Secure Two-Party Computation. -- Consecutive Adaptor Signature Scheme: From Two-Party to N-Party Settings. -- Secure Five-party Computation with Private Robustness and Minimal Online Communication. -- Model Extraction Attack on MPC Hardened Vertical Federated Learning. -- Searchable Encryption. -- Verifiable Conjunctive Searchable Symmetric Encryption with Result Pattern Hiding. -- Compressed Cookies: Practical Wildcard Symmetric Searchable Encryption with Optimized Storage. -- Encryption. -- PPA-

DCA: A Privacy-Preserving and Accountable Data Collection and Analysis Scheme Using Decentralized Multi-Client Functional Encryption. -- Ideal Public Key Encryption, Revisited. -- Simple Construction of PEKS from LWE-based IBE in the Standard Model. -- Signature. -- Traceable Ring Signatures: Logarithmic-Size, Without Any Setup, from Standard Assumptions. -- Tightly Secure Identity-based Signature from Cryptographic Group Actions. -- Generic Construction of Withdrawable Signature from Hash-ThenOne-Way Signature. -- Efficient Fork-Free BLS Multi-Signature Scheme with Incremental Signing. -- Threshold Ring Signatures: From DualRing to the t+1 Rings. -- Lattice-Based Non-Interactive Blind Signature Schemes in the Random Oracle Model.

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.