1. Record Nr. UNISA996668470003316

Autore	Susilo Willy
Titolo	Information Security and Privacy : 30th Australasian Conference, ACISP 2025, Wollongong, NSW, Australia, July 14–16, 2025, Proceedings, Part II / / edited by Willy Susilo, Josef Pieprzyk
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2025
ISBN	981-9690-98-6
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (674 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15659
Altri autori (Persone)	PieprzykJosef
Disciplina	005.8
Soggetti	Data protection Computer security Cryptography Data encryption (Computer science) Data protection - Law and legislation Computer networks - Security measures Blockchains (Databases) Data and Information Security Principles and Models of Security Cryptology Privacy Mobile and Network Security Blockchain
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Post-Quantum Cryptography. -- Towards Quantum Security of Hirose Compression Function and Romulus-H. -- Efficient Multi-instance Vector Commitment and Application to Post quantum Signatures. -- Breaking the Shield: Novel Fault Attacks on CRYSTALS-Dilithium. -- Efficient Revocable Identity-Based Encryption from Middle-Product LWE. -- Code-based Fully Dynamic Accountable Ring Signatures and Group Signatures using the Helper Methodology. -- Partial Key Exposure Attacks on UOV and Its Variants. -- Unbounded Multi-Hop Proxy Re-Encryption with HRA Security: An LWEBased

Optimization. -- Fiat-Shamir with Rejection and Rotation. -- Amoeba: More Flexible RLWE-based KEM. -- Get Rid of Templates: A Chosen-Ciphertext Attack on ML-KEM with a DPA-based Self-Comparison Oracle. -- Homomorphic Encryption and Applications. -- Accountability for Server Misbehavior in Homomorphic Secret Sharing. -- High-Precision Homomorphic Modular Reduction for CKKS Bootstrapping. -- Refined Error Management for Gate Bootstrapping. -- Cryptographic Foundations and Number Theory. -- Compact Lifting for NTT-unfriendly Modulus. -- Guaranteed Termination Asynchronous Complete Secret Sharing with Lower Communication and Optimal Resilience. -- Solving Generalized Approximate Divisor Multiples Problems.

Sommario/riassunto

This three-volume set in LNCS constitutes the refereed proceedings of the 30th Australasian Conference on Information Security and Privacy, ACISP 2025, held in Wollongong, NSW, Australia, during July 14–16, 2025. The 54 full papers, 6 short papers and 1 invited paper included in this book were carefully reviewed and selected from 181 submissions. They were organized in topical sections as follows: symmetric-key cryptography and cryptanalysis; public-key encryption; digital signatures and zero knowledge; cryptographic protocols and blockchain; post-quantum cryptography; homomorphic encryption and applications; cryptographic foundations and number theory; privacy enhancing technologies; AI security and privacy; system security.