1. Record Nr. UNINA9911015852603321

Autore	Susilo Willy
Titolo	Information Security and Privacy : 30th Australasian Conference, ACISP 2025, Wollongong, NSW, Australia, July 14–16, 2025, Proceedings, Part I / / edited by Willy Susilo, Josef Pieprzyk
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2025
ISBN	981-9690-95-1
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (723 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15658
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	-- Symmetric-Key Cryptography and Cryptanalysis. -- Forgery Attacks on SipHash. -- Cryptanalysis of Fruit-F: Exploiting Key-Derivation Weaknesses and Initial ization Vulnerabilities. -- Exploring Key-Recovery-Friendly Differential Distinguishers for SM4 and Their Performance in Differential Attacks. -- Inner Product Masked Integral Distinguishers and Integral Sets over Large Finite Fields Applications to MiMC, CIMINION and Chaghri. -- Improved Differential Meet-In-The-Middle Cryptanalysis on SIMON and Piccolo. -- Strengthening Key Scheduling of AES-256 with Minimal Software Modifications. -- Public-

Key Encryption. -- Ideal Transformations for Public Key Encryption. -- Indifferentiability Separations in Ideal Public Key Encryption: Explicit vs Implicit Rejection. -- Digital Signatures and Zero Knowledge. -- Compressed Sigma Protocols: New Model and Aggregation Techniques. -- Glitter: A Fully Adaptive and Tightly Secure Threshold Signature. -- Faster VOLEitH Signatures from All-but-One Vector Commitment and Half Tree. -- Three-Round (Robust) Threshold ECDSA from Threshold CL Encryption. -- Lattice Attack with EHNP: Key Recovery from Two ECDSA Signatures and Breaking the Information-Theoretic Limit. -- Cryptographic Protocols and Blockchain. -- FlexiADKG: A Flexible Asynchronous Distributed Key Generation Protocol with Constant Round Complexity. -- TEAKEX: TESLA-Authenticated Group Key Exchange. -- SoK: A Deep Dive into Anti-Money Laundering Techniques for Blockchain Cryptocurrencies. -- Advanced Temporal Graph Embedding For Detecting Fraudulent Transactions on Complex Blockchain Transactional Networks. -- Walnut: A Generic Framework with Enhanced Scalability for BFT Protocols. -- PPSCCC: Privacy-Preserving Scalable Cross-Chain Communication Among Multiple Blockchains Based on Parent-Child Blockchain.

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.