1.	Record Nr.	UNINA9910731463703321
	Titolo	Information Security and Privacy : 28th Australasian Conference, ACISP 2023, Brisbane, QLD, Australia, July 5–7, 2023, Proceedings / / edited by Leonie Simpson, Mir Ali Rezazadeh Baee
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
	ISBN	3-031-35486-9
	Edizione	[1st ed. 2023.]
	Descrizione fisica	1 online resource (658 pages)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13915
	Disciplina	005.8
	Soggetti	Data protection Data and Information Security
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Symmetric-Key Cryptography -- Improved Differential Cryptanalysis on SPECK Using Plaintext Structures -- Linear Cryptanalysis and Its Variants with Fast Fourier Transformation Technique on MPC/FHE/ZK-Friendly Fp-based Ciphers -- A New Correlation Cube Attack Based on Division Property -- The Triangle Differential Cryptanalysis -- Key Recovery Attacks on Grain-like Keystream Generators with Key Injection -- Related-Cipher Attacks: Applications to Ballet and ANT -- Cryptanalysis of SPEEDY -- Reconsidering Generic Composition: the modes A10, A11 and A12 are insecure -- Exploring Formal Methods for Cryptographic Hash FunctionImplementations -- Public-Key Cryptography -- A Tightly Secure ID-Based Signature Scheme under DL Assumption in AGM -- Compact Password Authenticated Key Exchange from Group Actions -- Multi-key Homomorphic Secret Sharing from LWE without Multi-key HE -- Identity-Based Encryption from Lattices Using Approximate Trapdoors -- Homomorphic Signatures for Subset and Superset Mixed Predicates and Its Applications -- Adaptively Secure Identity-Based Encryption from Middle-Product Learning with Errors -- Post-Quantum Cryptography -- Quantum-access Security of Hash-based Signature Schemes -- Tightly Secure Lattice Identity-Based Signature in the Quantum Random Oracle Model -- Ghidle: Efficient Large-State Block Ciphers for Post-Quantum Security -- Quantum Algorithm for Finding Impossible Differentials and Zero-Correlation

Linear Hulls of Symmetric Ciphers -- Memory-Efficient Quantum Information Set Decoding Algorithm -- Cryptographic Protocols -- CSI-SharK: CSI-FiSh with Sharing-friendly Keys -- Practical Verifiable Random Function with RKA Security -- Statistically Consistent Broadcast Authenticated Encryption with Keyword Search Adaptive Security from Standard Assumptions -- Modular Design of KEM-Based Authenticated Key Exchange -- Reusable, Instant and Private Payment Guarantees for Cryptocurrencies -- System Security -- BinAlign: Alignment Padding based Compiler Provenance Recovery -- Encrypted Network Traffic Classiffication with Higher Order Graph Neural Network.

Sommario/riassunto

This book constitutes the refereed proceedings of the 28th Australasian Conference on Information Security and Privacy, ACISP 2023, held in Brisbane, QLD, Australia, during July 5-7, 2023. The 27 full papers presented were carefully revised and selected from 87 submissions. The papers present and discuss different aspects of symmetric-key cryptography, public-key cryptography, post-quantum cryptography, cryptographic protocols, and system security.