1.

Record Nr.	UNINA9910874664303321
Autore	Zhu Tianqing
Titolo	Information Security and Privacy : 29th Australasian Conference, ACISP 2024, Sydney, NSW, Australia, July 15–17, 2024, Proceedings, Part II / / edited by Tianqing Zhu, Yannan Li
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2024
ISBN	9789819750283
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (464 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14896
Altri autori (Persone)	LiYannan
Disciplina	005.8
Soggetti	Data protection Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Post Quantum Cryptography -- Improved Multimodal Private Signatures from Lattices -- Automatic Quantum Multi collision Distinguishers and Rebound Attacks with Triangulation Algorithm -- Lattice based more general anti leakage model and its application in decentralization -- An Efficient Hardware Implementation of Crystal Dilithium on FPGA -- Pushing the Limit of Vectorized Polynomial Multiplications for NTRU Prime -- Jumping for Berstein Yang Inversion -- DualRing PRF Post Quantum Linkable Ring Signatures from Legendre and Power Residue PRFs -- Faster verifications and smaller signatures Trade offs for Alteq using rejections -- Revisiting the Security of Fiat Shamir Signature Schemes under Superposition Attacks -- Improved Lattice Based Attack on Mersenne Low Hamming Ratio Search Problem -- Cryptanalysis -- New Strategy for Evaluating Differential Clustering Effect of uBlock -- Algebraic Cryptanalysis of the HADES Design Strategy: Application to Poseidon and Poseidon2 -- Revisiting Impossible Differential Cryptanalysis and Expanding the Application of MILP in Impossible Differential Attack -- Secure Protocols -- A Fault Tolerant Content Moderation Mechanism for Secure Messaging System -- Formal Verification of Challenge Flow in EMV 3D Secure -- Size Hiding Computation in the Honest But Curious Model -- Hidden Delta fairness A Novel Notion for Fair Secure Two Party Computation -- ProfistMAC A Protocol Finite State Machine Classifier via Graph Representation --

Subverting Cryptographic Protocols from A Fine Grained Perspective A Case Study on 2 Party ECDSA -- Application Security -- Deep Dive on Relationship between Personality and Password Creation -- Unveiling the Unseen Video Recognition Attacks on Social Software -- An Account Matching Method Based on Hyper Graph.

Sommario/riassunto

This volume constitutes the refereed proceedings of the 29th Australasian Conference, ACISP 2024, held in Sydney, NSW, Australia, during July 15–17, 2024. The 70 full papers were carefully reviewed and selected from 232 submission. They are categorized in the following sections: Post-Quantum Cryptography, Cryptanalysis, Secure Protocols, Application Security. .