1.	Record Nr.	UNISA996696880903316
	Autore	Chen Rongmao
	Titolo	Information Security and Cryptology : 21st International Conference, Inscrypt 2025, Xi'an, China, October 19-22, 2025, Revised Selected Papers, Part I / / edited by Rongmao Chen, Robert H. Deng, Moti Yung
	Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2026
	ISBN	981-9562-06-6
	Edizione	[1st ed. 2026.]
	Descrizione fisica	1 online resource (1132 pages)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 16408
	Altri autori (Persone)	DengRobert H YungMoti
	Disciplina	005.8
	Soggetti	Data protection Image processing - Digital techniques Computer vision Computer networks Application software Computer networks - Security measures Cryptography Data encryption (Computer science) Data and Information Security Computer Imaging, Vision, Pattern Recognition and Graphics Computer Communication Networks Computer and Information Systems Applications Mobile and Network Security Cryptology
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	-- Post-Quantum Cryptography. -- Further Research on Meet-LWE and Its Application to Weakened Kyber. -- Efficient Implementation of Post-Quantum Signature Algorithms for Next Generation of Blockchains. -- Accelerating NTRU-based Bootstrapping with Block Key Distributions. -- Lattice IBE from Non-spherical Gaussian Sampling with Tight Security. -- Fast Multi-key Bootstrapping Instantiated with NTRU and (R)LWE. -- An Area-Performance Balanced

Hardware Accelerator of NTT for Kyber. -- A Framework for Fully Compact Transparent Ring Signature on Lattice and Its Instantiation. -- Tighter Security Proof of Falcon+ in the Quantum Random Oracle Model. -- Speedy Error Reconciliation. -- Functional Encryption. -- A Note on the Simpler Construction to Achieve Dynamic FE via IBE. -- Onion Encryption Revisited: Relations Among Security Notions. -- New Key Combiner Schemes for Multiple Keys. -- Wildcarded Identity-Based Inner Product Encryption Based on SM9. -- Dual-Threshold Verifiable Witness Encryption for Signatures and its Applications. -- Cryptanalysis and Implementations I. -- Improved Quantum Cryptanalysis on Generalized Feistel Structure. -- Algebraic Cryptanalysis on Reduced-round Trivium-LE. -- Automated Periodic Distinguisher Search for AND-RX Ciphers. -- Efficient Reconstruction of S-boxes from Partial Cryptographic Tables via MILP Modeling. -- Quantum Bisimulation-Based Acceleration Method for Quantum Cryptographic Protocol Verification. -- Arithmetic Autocorrelation of Certain Binary Half--sequences. -- Related-Key Rectangle Attacks on Round-Reduced TWINE. -- TwoLayerF: A Two-Layer Framework of PNB-based Key Recovery Attacks on ChaCha. -- Exploring AI-Assisted Cryptanalytic Attacks on Multisets. -- Distributed Quantum Key Recovery Attack on Pseudorandom Functions. -- Cryptanalysis and Implementations II. -- An Area-Efficient Design of ZUC-256 Through Hardware Optimization. -- Revisit Bitslice Implementation of Dummy Shuffling. -- TS-Seg: Temporal-Spatial Feature Fusion Based Side-Channel Trace Segmentation. -- Leakage-abuse Attack Against Substring-SSE with Partially Known Dataset. -- Bit-by-Bit Total Collapse: A Novel Side-Channel Attack on HQC-128 Decapsulation. -- Multi-feature Fusion Leakage Abuse Attacks against Dynamic Searchable Symmetric Encryption. -- A Novel Checking Scheme for Parallel Key Recovery Side-Channel Attack against Kyber.

Sommario/riassunto

The three-volume set constitutes revised selected papers of the 21st International Conference on Information Security and Cryptology, Inscrypt 2025, held in Xi'an, China, on October 19, 2025. The 79 full papers presented in these proceedings were carefully reviewed and selected from 315 submissions. The papers were organized in the following topical sections: Part I : Post-Quantum Cryptography; Functional Encryption; Cryptanalysis and Implementations I; Cryptanalysis and Implementations II. Part II : Secure Multi-party Computation; Anomaly Detection Methodologies & Models; Network Security & Traffic Analysis. Part III : Privacy Preserving/Enhancing Technologies; AI and Security I; AI and Security II.