1.

Record Nr.	UNINA9911047686903321
Autore	Han Jinguang
Titolo	Information and Communications Security : 27th International Conference, ICICS 2025, Nanjing, China, October 29–31, 2025, Proceedings, Part I / / edited by Jinguang Han, Yang Xiang, Guang Cheng, Willy Susilo, Liquan Chen
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2026
ISBN	981-9535-40-9
Edizione	[1st ed. 2026.]
Descrizione fisica	1 online resource (1112 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 16217
Altri autori (Persone)	XiangYang ChengGuang SusiloWilly ChenLiquan
Disciplina	005.73 003.54
Soggetti	Data structures (Computer science) Information theory Database management Data mining Application software Image processing - Digital techniques Computer vision Cryptography Data encryption (Computer science) Data Structures and Information Theory Database Management Data Mining and Knowledge Discovery Computer and Information Systems Applications Computer Imaging, Vision, Pattern Recognition and Graphics Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Cryptography. -- Multi-Signer Locally Verifiable Aggregate

Signature from (Leveled) Multilinear Maps. -- Conditional Attribute-based Encryption with Keyword Search for Pay-Per-Query Commercial Model. -- Lightweight Transparent Zero-Knowledge Proofs for Cross-Domain Statements. -- Public Verifiable Server-Aided Revocable Attribute-Based Encryption. -- New First-Order Secure AES Implementation without Online Fresh Randomness Records. -- SM2-VBKE: Achieving Cryptographic Binding Between Verification Integrity and Key Generation. -- Certificate-Based Quasi-Linearly Homomorphic Signatures: Definition, Construction, and Application to Data Integrity Auditing. -- Zero-Knowledge Protocols with PVC Security: Striking the Balance between Security and Efficiency. -- Attribute-Based Adaptor Signature and Application in Control-based Atomic Swap. -- A Versatile Decentralized Attribute Based Signature Scheme for IoT. -- Post-quantum Cryptography. -- Cross-Domain Lattice-based DAA Scheme with Shared Private-Key for Internet of Things System. -- Compact Adaptively Secure Identity-Based Encryption from Middle-Product Learning with Errors. -- MDKG: Module-lattice-based Distributed Key Generation. -- Turtle Wins Rabbit Again: Faster Modulus Reduction for RNS-CKKS. -- A BGV-subroutinted CKKS Bootstrapping Algorithm without Sine Approximation. -- PolarKyber: Polished Kyber with Smaller Ciphertexts, Greater Security Redundancy, and Lower Decryption Failure Rate. -- Lion: A New Ring Signature Construction from Lattice Gadget. -- Anonymity and Privacy. -- MagWatch: Exposing Privacy Risks in Smartwatches through Electromagnetic Signals. -- Privacy-preserving, Secure and Certificate-based Integrity Auditing for Cloud Storage. -- Unbalanced Private Computation on Set Intersection with Reduced Computation and Communication. -- Artemis: Decentralized, Secure, and Efficient Safety Monitoring with Dynamic Trajectories. -- Privacy-preserving Framework for k-modes Clustering Based on Personalized Local Differential Privacy. -- AnoST: An Anonymous Optimistic Verification System Based on Off-Chain State Transition. -- Privacy-Preserving K-hop Shortest Path Query on Encrypted Graphs Based on Graph Pruning. -- TA-PDC: Provable Data Contribution with Traceable Anonymous for Group Transactions. -- Fine-filter: An Effective Defense against Poisoning Attacks on Frequency Estimation under LDP. -- BioVite: Efficient and Compact Privacy-Preserving Biometric Verification via Fully Homomorphic Encryption. -- Authentication and Authorization. -- Circulation Control Model and Administration for Geospatial Data. -- Identifying Unusual Personal Data in Mobile Apps for Better Privacy Compliance Check. -- Why Biting the Bait? Understanding Bait and Switch UI Dark Patterns in Mobile Apps.

Sommario/riassunto

This three-set volume LNCS 16217-16219 constitutes the refereed proceedings of 27th International Conference on Information and Communications Security, ICICS 2025, held in Nanjing, China, during October 29–31, 2025. The 91 full papers presented in this book were carefully selected and reviewed from 357 submissions. The papers are organized in the following topical sections: Part I: Cryptography; Post-quantum Cryptography; Anonymity and Privacy; Authentication and Authorization. Part II: Blockchain and Cryptocurrencies, System and Network Security, Security and Privacy of AI, Machine Learning for Security. Part III: Attack and Defense; Vulnerability Analysis; Anomaly Detection; Traffic Classification; Steganography and Watermarking.