1.

Record Nr.	UNINA9910634047803321
Titolo	Information Security : 25th International Conference, ISC 2022, Bali, Indonesia, December 18–22, 2022, Proceedings / / edited by Willy Susilo, Xiaofeng Chen, Fuchun Guo, Yudi Zhang, Rolly Intan
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	9783031223907 303122390X
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (522 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13640
Disciplina	005.8
Soggetti	Data protection Computer engineering Computer networks Cryptography Data encryption (Computer science) Computer networks - Security measures Data and Information Security Computer Engineering and Networks Cryptology Mobile and Network Security Seguretat de les xarxes d'ordinadors Congressos Llibres electrònics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cryptography -- Privacy Preserving Computation in Cloud Using Reusable Garbled Oblivious RAMs -- Efficient Private Set Intersection Cardinality Protocol in the Reverse Unbalanced Setting -- Crypto-Steganographic Validity for Additive Manufacturing (3D Printing) Design Files -- Witness Encryption from Smooth Projective Hashing System -- Post-Quantum Cryptography -- More Efficient Adaptively Secure Lattice-based IBE with Equality Test in the Standard Model -- QUIC

	Protocol with Post-Quantum Authentication -- Batched Fully Homomorphic Encryption from TFHE -- Implicit Rejection in Fujisaki-Okamoto: Framework and a Novel Realization -- Cryptanalysis -- Further Cryptanalysis of a Type of RSA Variants -- The SAT-Based Automatic Searching and Experimental Verification for Differential Characteristics with Application to Midori64 -- Efficient Scalar Multiplication on Koblitz Curves with Pre-computation -- Blockchain -- Efficient ECDSA-based Adaptor Signature for Batched Atomic Swaps -- Searching for Encrypted Data on Blockchain: An Efficient, Secure and Fair Realization -- GRUZ : Practical Resource Fair Exchange without Blockchain -- Daric: A Storage Efficient Payment Channel With Punishment Mechanism -- A Blockchain-based Mutual Authentication Protocol for Smart Home -- Email and Web Security -- OblivSend: Secure and Ephemeral File Sharing Services with Oblivious Expiration Control -- EarlyCrow: Detecting APT Malware Command and Control Over HTTP(S) Using Contextual Summaries -- Malware -- ATLAS: A Practical Attack Detection and Live Malware Analysis System for IoT Threat Intelligence -- Dissecting Applications Uninstallers & Removers: Are they effective? -- Representing LLVM-IR in a Code Property Graph -- Why we need a theory of maliciousness: Hardware Performance Counters in security -- Anatomist: Enhanced Firmware Vulnerability Discovery Based on Program State Abnormality Determination With Whole-system Replay -- AI Security -- AspIOC: Aspect-Enhanced Deep Neural Network for Actionable Indicator of Compromise Recognition -- HeHe: Balancing the Privacy and Efficiency in Training CNNs over the Semi-honest Cloud -- Deep Learning Assisted Key Recovery Attack for Round-Reduced Simeck32/64 -- CFL: Cluster Federated Learning in Large-scale Peer-to-Peer Networks -- Bilateral Privacy-Preserving Task Assignment with Personalized Participant Selection for Mobile Crowdsensing -- Communication-Efficient and Secure Federated Learning Based on Adaptive One-bit Compressed Sensing.
Sommario/riassunto	This book constitutes the proceedings of the 25th International Conference on Information Security, ISC 2022, which took place in Bali, Indonesia, in December 2022. The 21 full papers and 8 short papers presented in this volume were carefully reviewed and selected from 72 submissions. The contributions were organized in topical sections as follows: Cryptography; Post-Quantum Cryptography; Cryptanalysis; Blockchain; Email and Web Security; Malware; and AI Security.