1. Record Nr. UNINA9910755086603321

Autore	Deng Jing
Titolo	Cryptology and Network Security : 22nd International Conference, CANS 2023, Augusta, GA, USA, October 31 – November 2, 2023, Proceedings / / edited by Jing Deng, Vladimir Kolesnikov, Alexander A. Schwarzmann
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2023
ISBN	981-9975-63-8
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (593 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14342
Altri autori (Persone)	KolesnikovVladimir SchwarzmannAlexander A
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Computer networks Computer networks - Security measures Data protection Application software Cryptology Computer Communication Networks Mobile and Network Security Data and Information Security Computer and Information Systems Applications
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Schemes I -- Forward Security under Leakage Resilience, Revisited -- Anonymous Broadcast Authentication with Logarithmic-order Ciphertexts from LWE -- Signatures with Delegation -- Basic Primitives -- How to Enumerate LWE Keys as Narrow as in Kyber/Dilithium -- Towards Minimizing Non-linearity in Type-II Generalized Feistel Networks -- Hardness of Learning AES with Gradient-based Methods -- Security -- Privacy-Preserving Digital Vaccine Passport -- Exploiting Android Browser -- Are Current CCPA Compliant Banners Conveying User’s Desired Opt-Out Decisions? An Empirical Study of

Cookie Consent Banners -- MPC with Cards -- Upper Bounds on the Number of Shuffl for Two-Helping-Card Multi-Input AND Protocols -- Free-XOR in Card-based Garbled Circuits -- Hidden Stream Ciphers and TMTO Attacks on TLS 1.3, DTLS 1.3, QUIC, and Signal -- Differetial cryptanalysis with SAT, SMT, MILP, and CP: a detailed comparison for bit-oriented primitives -- Key Filtering in Cube Attacks from the Implementation Aspect -- New Techniques for Modeling SBoxes: An MILP Approach -- Blockchain -- LucidiTEE: A TEE-Blockchain System for Policy-Compliant Multiparty Computation with Fairness -- Improving Privacy of Anonymous Proof-of-Stake Protocols -- Compact Stateful Deterministic Wallet from Isogeny-based Signature featuring Uniquely Rerandomizable Public Keys -- CTA: Confidetial Transactions Protocol with State Accumulator -- MPC and Secret Sharing -- A Plug-n-Play Framework for Scaling Private Set Intersection to Billion-sized Sets -- Lower Bounds on the Share Size of Leakage Resilient Cheating Detectable Secret Sharing -- Schemes II -- Lattice-based Key-Value Commitment scheme with key-binding and key-hiding -- A Practical Forward-Secure DualRing -- Computable Cryptographic Accumulators and Their Application to Attribute Based Encryption -- A Minor Note on Obtaining Simpler iO Constructions via Depleted Obfuscators.

Sommario/riassunto

This book constitutes the refereed proceedings of the 22nd International Conference on Cryptology and Network Security, CANS 2023, which was held in October/November 2023 in Augusta, GA, USA. The 25 papers presented were thoroughly revised and selected from the 54 submissions. They are organized in the following topical sections: Schemes I; Basic Primitives; Security; MPC with Cards; Blockchain; MPC and Secret Sharing; Schemes II.