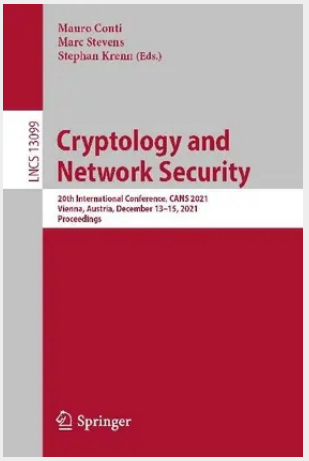
Conti / Stevens / Krenn

Cryptology and Network Security

20th International Conference, CANS 2021, Vienna, Austria, December 13-15, 2021, Proceedings



This book constitutes the refereed proceedings of the 20 International Conference on Cryptology and Network Security, CANS 2021, which was held during December 13-15, 2021. The conference was originally planned to take place in Vienna, Austria, and changed to an online event due to the COVID-19 pandemic.

The 25 full and 3 short papers presented in these proceedings were carefully reviewed and selected from 85 submissions. They were organized in topical sections as follows: Encryption; signatures; cryptographic schemes and protocols; attacks and counter-measures; and attestation and verification.

Encryption.- Cross-Domain Attribute-Based Access Control Encryption.- Grain-128AEADv2: Strengthening the Initialization Against Key Reconstruction.- Partition Oracles from Weak Key Forgeries.- Practical Privacy-Preserving Face Identification based on FunctionHiding Functional Encryption.- The Matrix Reloaded: Multiplication Strategies in FrodoKEM.- Signatures.- BlindOR: An Effcient Lattice-Based Blind Signature Scheme from OR-Proofs.- Effcient Threshold-Optimal ECDSA.- GMMT: A Revocable Group Merkle Multi-Tree Signature Scheme.- Issuer-Hiding Attribute-Based Credentials.- Report and Trace Ring Signatures.- Selectively Linkable Group Signatures - Stronger Security and Preserved Verifiability.- Cryptographic Schemes and Protocols.- FO-like Combiners and Hybrid Post-Quantum Cryptography.- Linear-time oblivious permutations for SPDZ.- On the Higher-bit Version of Approximate Inhomogeneous Short Integer Solution Problem.- Practical Continuously Non-Malleable Randomness Encoders in the Random Oracle Model.- Attacks and Counter-Measures.- Countermeasures against Backdoor Attacks towards Malware Detectors.- Free By Design: On the Feasibility Of Free-Riding Attacks Against Zero-Rated Services.- Function-private Conditional Disclosure of Secrets and Multi-evaluation Threshold Distributed Point Functions.- How Distance-bounding can Detect Internet Traffc Hijacking.- SoK: Secure Memory Allocation.- Toward Learning Robust Detectors from Imbalanced Datasets Leveraging Weighted Adversarial Training.- Towards Quantum Large-Scale Password Guessing on Real-World Distributions.- Attestation and Verification.- Anonymous Transactions with Revocation and Auditing in Hyperledger Fabric.- Attestation Waves: Platform Trust via Remote Power Analysis.- How (not) to Achieve both Coercion Resistance and Cast as Intended Verifiability in Remote eVoting.- Subversion-Resistant Quasi-Adaptive NIZK and Applications to Modular zk-SNARKs.- THC: Practical and Cost-Effective Verification of Delegated Computation.- Tiramisu: Black-Box Simulation Extractable NIZKs in the Updatable CRS Model.

106,99 €
99,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783030925475
Medium: Buch
ISBN: 978-3-030-92547-5
Verlag: Springer
Erscheinungstermin: 09.12.2021
Sprache(n): Englisch
Auflage: 1. Auflage 2021
Serie: Security and Cryptology
Produktform: Kartoniert
Gewicht: 850 g
Seiten: 554
Format (B x H): 155 x 235 mm