1. Record Nr. UNINA9910495212403321

Titolo	Selected Areas in Cryptography : 27th International Conference, Halifax, NS, Canada (Virtual Event), October 21-23, 2020, Revised Selected Papers / / edited by Orr Dunkelman, Michael J. Jacobson, Jr., Colin O'Flynn
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-81652-4
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (727 pages)
Collana	Security and Cryptology, , 2946-1863 ; ; 12804
Disciplina	005.8
Soggetti	Data protection Computer networks Cryptography Data encryption (Computer science) Computer networks - Security measures Data and Information Security Computer Communication Networks Cryptology Security Services Mobile and Network Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Public-key Cryptography -- Efficient Lattice-Based Polynomial Evaluation and Batch ZK Arguments -- FROST: Flexible Round-Optimized Schnorr Threshold Signatures -- Algorithmic Acceleration of B/FV-like Somewhat Homomorphic Encryption for Compute-Enabled RAM -- Obfuscating Finite Automata -- On Index Calculus Algorithms for Subfield Curves -- Symmetric-Key Analysis Weak-Key Distinguishers for AES -- Algebraic Key-Recovery Attacks on Reduced-Round Xoofff -- Improved (Related-key) Differential Cryptanalysis on GIFT -- Boolean Polynomials, BDDs and CRHS Equations - Connecting the Dots with CryptaPath -- Boolean Ring Cryptographic Equation Solving -- Interpolation Cryptanalysis of Unbalanced Feistel Networks

with Low Degree Round Functions -- Unintended Features of APIs: Cryptanalysis of Incremental HMAC -- Quantum Cryptanalysis -- Low-gate Quantum Golden Collision Finding -- Improvements to quantum search techniques for block-ciphers, with applications to AES -- Post-Quantum Constructions -- Not enough LESS: An improved algorithm for solving Code Equivalence Problems over Fq -- Towards Post-Quantum Security for Signal's X3DH Handshake -- Trapdoor DDH groups from pairings and isogenies -- Practical Isogeny-Based Key-exchange with Optimal Tightness -- Symmetric-Key Design -- PRINCEv2 -- Nonce-Misuse Security of the SAEF Authenticated Encryption mode -- WARP : Revisiting GFN for Lightweight 128-bit Block Cipher -- Side Channel Attacks -- Subsampling and Knowledge Distillation on Adversarial Examples: New Techniques for Deep Learning Based Side Channel Evaluations -- Correlation Power Analysis and Higher-order Masking Implementation of WAGE -- On the Influence of Optimizers in Deep Learning-based Side-channel Analysis -- Cryptographic Applications -- On Self-Equivalence Encodings in White-Box Implementations -- Protecting the Privacy of Voters: New Definitions of Ballot Secrecy for E-Voting -- High-Throughput Elliptic Curve Cryptography Using AVX2 Vector Instructions.-.

Sommario/riassunto

This book contains revised selected papers from the 27th International Conference on Selected Areas in Cryptography, SAC 2020, held in Halifax, Nova Scotia, Canada in October 2020. The 27 full papers presented in this volume were carefully reviewed and selected from 52 submissions. They cover the following research areas: design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions, MAC algorithms, and authenticated encryption schemes, efficient implementations of symmetric and public key algorithms, mathematical and algorithmic aspects of applied cryptology, and secure elections and related cryptographic constructions.