1. Record Nr. UNISA996587861603316

Autore	Carlet Claude
Titolo	Selected Areas in Cryptography – SAC 2023 [[electronic resource]] : 30th International Conference, Fredericton, Canada, August 14–18, 2023, Revised Selected Papers / / edited by Claude Carlet, Kalikinkar Mandal, Vincent Rijmen
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-53368-2
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (457 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14201
Altri autori (Persone)	MandalKalikinkar RijmenVincent
Disciplina	005.8
Soggetti	Data protection Computer networks Computer engineering Cryptography Data encryption (Computer science) Data and Information Security Computer Communication Networks Computer Engineering and Networks Cryptology Security Services
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cryptanalysis of Lightweight Ciphers -- More Balanced Polynomials: Cube Attacks on 810- and 825-Round Trivium with Practical Complexities -- A Closer Look at the S-box: Deeper Analysis of Round-Reduced ASCON-HASH -- Improving the Rectangle Attack on GIFT-64 -- Side-Channel Attacks and Countermeasures -- Mask Compression: High-Order Masking on Memory-Constrained Devices -- Not so Difficult in the End: Breaking the Lookup Table-based Affine Masking Scheme -- Threshold Implementations with Non-Uniform Inputs -- Post-Quantum Constructions -- SMAUG: Pushing Lattice-based Key Encapsulation Mechanisms to the Limits -- A Post-Quantum Round-

Optimal Oblivious PRF from Isogenies -- Traceable Ring Signatures from Group Actions: Logarithmic, Flexible, and Quantum Resistant -- Symmetric cryptography and fault attacks -- The Random Fault Model -- Probabilistic Related-Key Statistical Saturation Cryptanalysis -- Compactly Committing Authenticated Encryption Using Encryptment and Tweakable Block Cipher -- Post-Quantum Analysis and Implementations -- Bit Security Analysis of Lattice-Based KEMs under Plaintext-Checking Attacks -- Quantum Cryptanalysis of OTR and OPP: Attacks on Confidentiality, and Key-Recovery -- Fast and Efficient Hardware Implementation of HQC -- Homomorphic encryption -- On the Precision Loss in Approximate Homomorphic Encryption -- Secure Function Extensions to Additively Homomorphic Cryptosystems -- Public-Key Cryptography -- Generalized Implicit Factorization Problem -- Differential Cryptanalysis -- CLAASP: a Cryptographic Library for the Automated Analysis of Symmetric Primitives -- Parallel SAT Framework to Find Clustering of Differential Characteristics and Its Applications -- Deep Learning-Based Rotational-XOR Distinguishers for AND-RX Block Ciphers: Evaluations on Simeck and Simon.

Sommario/riassunto

This book contains revised selected papers from the 30th International Conference on Selected Areas in Cryptography, SAC 2023, held in Fredericton, New Brunswick, Canada, in August 2023. The 21full papers presented in these proceedings were carefully reviewed and selected from 45 submissions. The papers are organized in the following topical sections: Cryptanalysis of Lightweight Ciphers; Side-Channel Attacks and Countermeasures; Post-Quantum Constructions; Symmetric cryptography and fault attacks; Post-Quantum Analysis and Implementations; Homomorphic encryption; Public-Key Cryptography; and Differential Cryptanalysis.