| | | |
|---|---|---|
| 1. | Record Nr. | UNISA996418284503316 |
| | Titolo | Selected Areas in Cryptography – SAC 2019 [[electronic resource] ] : 26th International Conference, Waterloo, ON, Canada, August 12–16, 2019, Revised Selected Papers / / edited by Kenneth G. Paterson, Douglas Stebila |
| | Pubbl/distr/stampa | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020 |
| | ISBN | 3-030-38471-3 |
| | Edizione | [1st ed. 2020.] |
| | Descrizione fisica | 1 online resource (XV, 715 p. 323 illus., 66 illus. in color.) |
| | Collana | Security and Cryptology ; ; 11959 |
| | Disciplina | 001.5436 |
| | Soggetti | Computer security<br>Data protection<br>Computer organization<br>Data structures (Computer science)<br>Artificial intelligence<br>Systems and Data Security<br>Security<br>Computer Systems Organization and Communication Networks<br>Data Structures and Information Theory<br>Artificial Intelligence |
| | Lingua di pubblicazione | Inglese |
| | Formato | Materiale a stampa |
| | Livello bibliografico | Monografia |
| | Nota di contenuto | Block Cipher Modes of Operation and Provable Security -- Looking Back\|My Life as a Mathematician and Cryptographer -- Supersingular Isogeny Key Exchange for Beginners -- Probabilistic Mixture Differential Cryptanalysis on round-reduced AES -- Iterative Differential Characteristic of TRIFLE-BC -- Plaintext Recovery Attacks against XTS Beyond Collisions -- Cryptanalysis of SKINNY in the Framework of the SKINNY 2018-2019 Cryptanalysis Competition -- Algebraic Cryptanalysis of Variants of Frit -- Improved Interpolation Attacks on Cryptographic Primitives of Low Algebraic Degree -- A General Framework for the Related-key Linear Attack against Block Ciphers with Linear Key Schedules -- Towards a Practical Cluster Analysis over |

Encrypted Data -- Breaking the Bluetooth Pairing { The Fixed Coordinate Invalid Curve Attack -- Using TopGear in Overdrive: A more efficient ZKPoK for SPDZ -- On the Real-World Instantiability of Admissible Hash Functions and Effcient Verifiable Random Functions -- Tight Security Bounds for Generic Stream Cipher Constructions -- On the Data Limitation of Small-State Stream Ciphers: Correlation Attacks on Fruit-80 and Plantlet -- A Lightweight Alternative to PMAC -- An Improved Security Analysis on an Indeterminate Equation Public Key Cryptosystem by Evaluation Attacks -- Ternary Syndrome Decoding with Large Weight -- Exploring Trade-offs in Batch Bounded Distance Decoding -- On Quantum Slide Attacks -- XMSS and Embedded Systems: XMSS Hardware Accelerators for RISC-V 1 -- A timing attack on the HQC encryption scheme -- Block-Anti-Circulant Unbalanced Oil and Vinegar -- A DFA Attack on White-Box Implementations of AES with External Encodings -- Parallelizable Authenticated Encryption with Small State Size -- Deep Neural Network Attribution Methods for Leakage Analysis and Symmetric Key Recovery -- BBQ: Using AES in Picnic Signatures -- Towards practical GGM-based PRF from (Module-) Learning-with Rounding.

Sommario/riassunto

This book contains revised selected papers from the 26th International Conference on Selected Areas in Cryptography, SAC 2019, held in Waterloo, ON, Canada, in August 2019. The 26 full papers presented in this volume were carefully reviewed and selected from 74 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, cryptography for the Internet of Things.