1. Record Nr. UNINA9910364955503321

Titolo	Progress in Cryptology – INDOCRYPT 2019 : 20th International Conference on Cryptology in India, Hyderabad, India, December 15–18, 2019, Proceedings / / edited by Feng Hao, Sushmita Ruj, Sourav Sen Gupta
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-35423-7
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (xxiii, 580 pages) : illustrations
Collana	Security and Cryptology ; ; 11898
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Computer networks Application software Coding theory Information theory Data protection Cryptology Computer Communication Networks Computer and Information Systems Applications Coding and Information Theory Security Services Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Constructions : Signatures and Filter Permutators -- PKP-Based Signature scheme -- Modification tolerant signature schemes: location and correction -- Rerandomizable Signatures under Standard Assumption -- Improved Filter Permutators for Efficient FHE: Better Instances and Implementations -- Cryptanalysis : Symmetric Key Ciphers and Hash Functions -- RC4: Non-Randomness in the index j and some results on its Cycles -- Automatic Tool for Searching for

Differential Characteristics in ARX Ciphers and Applications -- Improved Related-Tweakey Rectangle Attacks on Reduced-round Deoxys-BC-384 and Deoxys-I-256-128 -- Some cryptanalytic results on TRIAD -- Cryptanalysis of Round-Reduced KECCAK using Non-Linear Structures -- Protocols : Blockchain, Secure Computation and Blind Coupon Mechanism -- Nummatus : A Privacy Preserving Proof of Reserves Protocol for Quisquis -- Optimality of a Protocol by Feige-Kilian-Naor for Three-Party Secure Computation -- MArBled Circuits: Mixing Arithmetic and Boolean Circuits with Active Security -- A Blind Coupon Mechanism Enabling Veto Voting over Unreliable Networks -- Theory: Oblivious Transfer, Obfuscation and Privacy Amplification -- UC Priced Oblivious Transfer with Purchase Statistics and Dynamic Pricing -- Public-coin Differing-inputs Obfuscator for Hiding-input Point Function with Multi-bit Output and Its Applications -- Privacy Amplification from Non-malleable Codes -- Mathematics : Boolean Functions, Elliptic Curves and Lattices -- Vectorial Boolean Functions with very Low Differential-linear Uniformity using Maiorana-McFarland type Construction -- On the Relationship between Resilient Boolean Functions and Linear Branch Number of S-boxes -- The complete cost of cofactor h=1 -- Revisiting Approximate Polynomial Common Divisor Problem and Noisy Multipolynomial Reconstruction -- Quantum : Algorithms, Attacks and Key Distribution -- Efficient Quantum Algorithms related to Autocorrelation Spectrum -- Quantum Attacks against Type-1 Generalized Feistel Ciphers and Applications to CAST-256 -- Device Independent Quantum Key Distribution using Three-Party Pseudo-Telepathy -- Generalized Approach for Analysing Quantum Key Distribution Experiments -- Hardware : Efficiency, Side-Channel Resistance and PUFs -- Efficient Hardware Implementations of Grain-128AEAD -- Exploring Lightweight Efficiency of ForkAES -- FPGA Implementation and Comparison of Protections against SCAs for RLWE -- Analysis of the Strict Avalanche Criterion in variants of Arbiter-based Physically Unclonable Functions.

Sommario/riassunto

This book constitutes the refereed proceedings of the 20th International Conference on Cryptology in India, INDOCRYPT 2019, held in Hyderabad, India, in December 2019. The 28 revised full papers presented in this book were carefully reviewed and selected from 110 submissions (of which 20 were either rejected without being reviewed or withdrawn before the deadline). The focus of the conference includes works on signatures and filter permutators; symmetric key ciphers and hash functions; blockchain, secure computation and blind coupon mechanism; oblivious transfer, obfuscation and privacy amplification; Boolean functions, elliptic curves and lattices; algorithms, attacks and distribution; and efficiency, side-channel resistance and PUFs.