1. Record Nr. UNINA9910847089003321

Titolo	Progress in Cryptology – INDOCRYPT 2023 : 24th International Conference on Cryptology in India, Goa, India, December 10–13, 2023, Proceedings, Part I / / edited by Anupam Chattopadhyay, Shivam Bhasin, Stjepan Picek, Chester Rebeiro
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-56232-1
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (364 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14459
Disciplina	929
Soggetti	Cryptography Data encryption (Computer science) Computer science - Mathematics Computer science Artificial intelligence Cryptology Mathematics of Computing Theory of Computation Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Symmetric-key cryptography, Hash functions, Authenticated Encryption Modes -- Multimixer-156: Universal Keyed Hashing Based on Integer Multiplication and cyclic shift -- On the Security of Triplex- and Multiplex-type Constructions with Smaller Tweak Size -- From Substitution Box To Threshold -- Tight Security Bound of 2k-LightMAC Plus -- Designing Full-Rate Sponge based AEAD Modes -- Towards Minimizing Tweakable Blockcipher-based Generalized Feistel Networks -- The Patching Landscape of Elisabeth-4 and the Mixed Filter Permutator Paradigm -- Elliptic curves, Zero-knowledge proof, Signatures -- Generating Supersingular Elliptic Curves over Fp with Unknown Endmorphism Ring -- Kummer and Hessian meet in the Field of Characteristic 2 -- Synchronized Aggregate Signature under Standard Assumption in the Random Oracle Model -- Malleable

Commitments from Group Actions and Zero-Knowledge Proofs for Circuits based on Isogenies -- Attacks -- A CP-based Automatic Tool for Instantiating Truncated Differential Characteristics -- Falling into Bytes and Pieces – Cryptanalysis of an Apple Patent Application -- Grover on chosen IV related key attack against GRAIN-128a -- Concrete Time/Memory Trade-Offs in Generalised Stern’s ISD Algorithm -- Practical Aspects of Vertical Side-Channel Analyses on HMAC-SHA-2.

Sommario/riassunto

The two-volume proceedings constitutes the refereed proceedings of the 24th International Conference on Progress in Cryptology, INDOCRYPT 2023, Goa, India, in December 2023. The 26 full papers were carefully reviewed and selected from 74 submissions. They are organized in topical sections as follows: Part One: Symmetric-key cryptography, Hash functions, Authenticated Encryption Modes; Elliptic curves, Zero-knowledge proof, Signatures; Attacks. Part Two: Secure computation, Algorithm hardness, Privacy; Post-quantum cryptography.