1. Record Nr. UNINA9910847089403321

Titolo	Progress in Cryptology – INDOCRYPT 2023 : 24th International Conference on Cryptology in India, Goa, India, December 10–13, 2023, Proceedings, Part II / / edited by Anupam Chattopadhyay, Shivam Bhasin, Stjepan Picek, Chester Rebeiro
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-56235-6
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (277 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14460
Disciplina	929
Soggetti	Cryptography Data encryption (Computer science) Computer science - Mathematics Artificial intelligence Computer science Cryptology Mathematics of Computing Artificial Intelligence Theory of Computation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Secure computation, Algorithm hardness, Privacy -- Threshold-Optimal MPC With Friends and Foes -- Network-Agnostic Perfectly Secure Synchronous Message Transmission Revisited -- Explicit Lower Bounds for Communication Complexity of PSM for Concrete Functions -- Distributed Protocols for Oblivious Transfer and Polynomial Evaluation -- Obfuscating Decision Trees -- Privacy-Preserving Plagiarism Checking -- PURED: A unified framework for resource-hard functions -- Post-quantum cryptography -- Implementing Lattice-Based PQC on Resource-Constrained Processors: A Case Study for Kyber/Saber’s Polynomial Multiplication on ARM CortexM0/M0+ -- Algorithmic Views of Vectorized Polynomial Multipliers – NTRU.
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.