1. Record Nr. UNISA996668469103316

Autore	Nitaj Abderrahmane
Titolo	Progress in Cryptology - AFRICACRYPT 2025 : 16th International Conference on Cryptology in Africa, Rabat, Morocco, July 21–23, 2025, Proceedings / / edited by Abderrahmane Nitaj, Svetla Petkova-Nikova, Vincent Rijmen
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2026
ISBN	9783031972607 9783031972591
Edizione	[1st ed. 2026.]
Descrizione fisica	1 online resource (842 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15651
Altri autori (Persone)	Petkova-NikovaSvetla RijmenVincent
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Computer vision Computer networks - Security measures Data protection Microprogramming Cryptology Computer Vision Mobile and Network Security Data and Information Security Control Structures and Microprogramming
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Homomorphic Encryption. -- Convolution-Friendly Image Compression with FHE. -- Leveled Homomorphic Encryption over Composite Groups. -- Activate Me!: Designing Efficient Activation Functions for Privacy-Preserving Machine Learning with Fully Homomorphic Encryption. -- One-Way Homomorphic Encryption: A Composite Group Approach. -- Cryptanalysis of RSA. -- A Novel Partial Key Exposure Attack on Common Prime RSA. -- Improved Cryptanalysis of an RSA Variant Based on Cubic Pell Curve. -- A New

Generalized Attack on RSA-like Cryptosystems. -- Cryptography Arithmetic. -- An Improvement of the Congruence Solver of Lattice Isomorphism Problem over Totally Real Number Fields and Applications. -- PMNS arithmetic for elliptic curve cryptography. -- Constant-time Integer Arithmetic for SQIsign. -- FPTRU:Optimization of NTRU-Prime and TLS Performance Assessment. -- Side-channel Attacks. -- Simple Power Analysis Attack on SQIsign. -- Correlation power analysis of LESS and CROSS. -- TPL: Power Leakage Model Based on Technology Library. -- Designs. -- Bivariate proximity test-based Asynchronous Verifiable Secret Sharing. -- Behemoth: transparent polynomial commitment scheme with constant opening proof size and verifier time. -- Attribute-based Encryption using Sum-Product Decomposition of Boolean Functions. -- Simultaneously simple universal and indifferentiable hashing to elliptic curves. -- Cryptanalysis. -- Conjunctive Dynamic SSE Schemes under Scrutiny: Exposing Privacy Issues in SDSSE-CQ-S and VCDSSE. -- Efficient and Optimized Modeling of S-Boxes. -- Tearing Solutions for Tree Traversal in Stateful Hash-based Cryptography.

Sommario/riassunto

This book constitutes the refereed proceedings of the 16th International Conference on Cryptology in Africa, AFRICACRYPT 2025, which took place in Rabat, Morocco in July 2025. The 21 full papers presented in this volume were carefully reviewed and selected from 45 submissions. They are grouped into the following topics: Homomorphic Encryption; Cryptanalysis of RSA; Cryptography Arithmetic; Side-channel Attacks; Designs; Cryptanalysis.