1.

Record Nr.	UNINA9910734874503321
Autore	El Mrabet Nadia
Titolo	Progress in Cryptology - AFRICACRYPT 2023 : 14th International Conference on Cryptology in Africa, Sousse, Tunisia, July 19–21, 2023, Proceedings / / edited by Nadia El Mrabet, Luca De Feo, Sylvain Duquesne
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	9783031376795 303137679X
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (518 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14064
Altri autori (Persone)	De FeoLuca DuquesneSylvain
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	Post-quantum cryptography -- MinRank in the Head: Short Signatures from Zero-Knowledge Proofs -- Take your MEDS: Digital Signatures from Matrix Code Equivalence -- Efficient computation of (3^n,3^n)-isogenies -- On the Post-Quantum Security of Classical Authenticated Encryption Schemes -- A Side-Channel Attack against Classic McEliece when loading the Goppa Polynomial -- Symmetric cryptography -- Universal hashing based on field multiplication and (near-)MDS matrices -- Invertible Quadratic Non-Linear Functions over F_p^n via

Multiple Local Maps -- Poseidon2: A Faster Version of the Poseidon Hash Function -- From Unbalanced to Perfect: Implementation of Low Energy Stream Ciphers -- Cryptanalysis -- The special case of cyclotomic fields in quantum algorithms for unit groups -- Improved Cryptanalysis of the Multi-Power RSA Cryptosystem Variant -- Blockchain -- The curious case of the half-half Bitcoin ECDSA nonces -- Maravedí: A Secure and Practical Protocol to Trade Risk for Instantaneous Finality -- Lattice-based cryptography -- ComBo: a Novel Functional Bootstrapping Method for Efficient Evaluation of Nonlinear Functions in the Encrypted Domain -- Concrete Security from Worst-Case to Average-Case Lattice Reductions -- Finding and Evaluating Parameters for BGV -- Quantum Search-to-Decision Reduction for the LWE Problem -- Implementations -- Fast Falcon Signature Generation and Verification Using ARMv8 NEON Instructions -- Benchmarking and Analysing the NIST PQC Lattice-Based Signature Schemes Standards on the ARM Cortex M7 -- Theory -- Impossibilities in Succinct Arguments: Black-box Extraction and More -- Applications of Timed-release Encryption with Implicit Authentication.

Sommario/riassunto

This volume contains the papers accepted for presentation at Africacrypt 2023, the 14th International Conference on the Theory and Application of Cryptographic Techniques in Africa. The 21 full papers included in this book were carefully reviewed and selected from 59 submissions. They were organized in topical sections as follows: Post-quantum cryptography; Symmetric cryptography; Cryptanalysis; Blockchain; Lattice-based cryptography; Implementations; Theory. .