1. Record Nr. UNINA9910726277903321

Autore	El Hajji Said
Titolo	Codes, Cryptology and Information Security : 4th International Conference, C2SI 2023, Rabat, Morocco, May 29–31, 2023, Proceedings / / edited by Said El Hajji, Sihem Mesnager, El Mamoun Souidi
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	9783031330179 9783031330162
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (415 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13874
Altri autori (Persone)	MesnagerSihem SouidiEl Mamoun
Disciplina	003.54
Soggetti	Data protection Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Invited Papers -- Cryptologists should not ignore the history of Al-Andalusia -- Compact Post-Quantum Signatures from Proofs of Knowledge leveraging Structure for the PKP, SD and RSD Problems -- On Catalan Constant Continued Fractions -- Cryptography -- Full Post-Quantum Datagram TLS Handshake in the Internet of Things -- Moderate Classical McEliece keys from quasi-Centrosymmetric Goppa codes -- QCB is Blindly Unforgeable -- A Side-Channel Secret Key Recovery Attack on CRYSTALS-Kyber Using k Chosen Ciphertexts -- A new keyed hash function based on Latin squares and error-correcting codes to authenticate users in smart home environments -- Attack on a Code-based Signature Scheme from QC-LDPC Codes -- Computational results on Gowers U2 and U3 norms of known S-Boxes -- Multi-Input Non-Interactive Functional Encryption: Constructions and Applications -- Indifferentiability of the Confusion-Diffusion Network and the Cascade Block Cipher -- Quantum Cryptanalysis of 5 rounds Feistel schemes and Benes schemes -- Lattice-based accumulator with constant time list update and constant time verification -- Information Security -- Malicious JavaScript detection based on AST analysis and key feature re-sampling in realistic environments -- Searching for Gemstones: Flawed Stegosystems May Hide Promising Ideas -- A Study

for Security of Visual Cryptography -- Forecasting Click Fraud via Machine Learning Algorithms -- An Enhanced Anonymous ECC-based Authentication for Lightweight Application in TMIS -- Discrete Mathematics -- Symmetric 4-adic complexity of quaternary sequences with period 2p n -- Weightwise perfectly balanced functions and nonlinearity -- Chudnovsky-type algorithms over the projective line using generalized evaluation maps -- Coding Theory -- Security enhancement method using shortened error correcting codes -- An Updated Database of Z4 Codes and an Open Problem about Quasi-Cyclic Codes.

Sommario/riassunto

This book constitutes the refereed proceedings of the 4th International Conference on Codes, Cryptology and Information Security, C2SI 2023, held in Rabat, Morocco, during May 29–31, 2023. The 21 full papers included in this book were carefully reviewed and selected from 62 submissions. They were organized in topical sections as follows: Invited Papers, Cryptography, Information Security, Discrete Mathematics, Coding Theory.