1.

Record Nr.	UNINA9910984588803321
Autore	Petkova-Nikova Svetla
Titolo	Arithmetic of Finite Fields : 10th International Workshop, WAIFI 2024, Ottawa, ON, Canada, June 10–12, 2024, Revised Selected Papers / / edited by Svetla Petkova-Nikova, Daniel Panario
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	9783031818240 3031818245
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (634 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15176
Altri autori (Persone)	PanarioDaniel
Disciplina	512.3
Soggetti	Computer science - Mathematics Computer engineering Computer networks Data structures (Computer science) Information theory Data protection Algorithms Symbolic and Algebraic Manipulation Mathematics of Computing Computer Engineering and Networks Data Structures and Information Theory Data and Information Security Design and Analysis of Algorithms
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Invited talks. -- The restricted decoding problem and its application to post-quantum cryptography. -- Algebraic curves over finite fields: rational points and birational invariants. -- An overview of mathematical problems, cryptosystems, and their interconnection. -- Making and breaking post-quantum cryptography from elliptic curve. -- Coding theory. -- Determining the complete weight distributions of some families of cyclic codes. -- Central limit theorem for linear eigenvalue statistics of random matrices from binary linear codes. --

On decoding hyperbolic codes. -- Fast decoding of group testing results from Reed-Solomon d-disjunct matrices. -- Quantum CSS Duadic and Triadic Codes: New Insights and Properties. -- Cryptography and Boolean functions. -- Prescribing traces of primitive elements in finite fields. -- On Cryptographic Properties of a Class of Power Permutations in Odd Characteristic. -- Generating Gaussian pseudorandom noise with binary sequences. -- An FPGA Accelerated Search Method for Maximum Period NLFSRs File. -- On fat linearized polynomials. -- Counting polynomials with distinct roots in finite fields using the subset sum problem. -- Generalized class group actions on oriented elliptic curves with level structure. -- Differential biases, c-differential uniformity, and their relation to differential attacks. -- On the Walsh and Fourier-Hadamard Supports of Boolean functions from a quantum viewpoint. -- Postquantum Cryptography. -- Efficient Batch Post-Quantum Signatures with Crystals Dilithium. -- A Practical Group Signature Scheme based on Rank Metric. -- SMALL: Scalable Matrix OriginAted Large Integer PoLynomial Multiplication Accelerator for Lattice-based Post-Quantum Cryptography.

Sommario/riassunto

This book constitutes the refereed proceedings of the 10th International Workshop on Arithmetic of Finite Fields, WAIFI 2024, held in Ottawa, Ontario, Canada, during June 10–12, 2024. The 17 full papers included in this book were carefully reviewed and selected from 29 submissions. They were organized in topical sections as follows: Invited talks; Coding theory; Cryptography and Boolean functions; and Postquantum Cryptography.