1. Record Nr. UNISA996508672203316

Titolo	Arithmetic of finite fields : 9th International Workshop, WAIFI 2022, Chengdu, China, August 29-September 2, 2022, revised selected papers / / edited by Sihem Mesnager, Zhengchun Zhou
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2023] ©2023
ISBN	3-031-22944-4
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (353 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13638
Disciplina	910.5
Soggetti	Finite fields (Algebra)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Structures in Finite Fields -- On a conjecture on irreducible polynomials over finite fields with restricted coefficients -- On two applications of polynomials xk – cx – d over finite fields and more -- Efficient Finite Field Arithmetic -- Polynomial Constructions of Chudnovsky-Type Algorithms for Multiplication in Finite Fields with Linear Bilinear Complexity -- Reduction-free Multiplication for Finite Fields and Polynomial Rings -- Finite Field Arithmetic in Large Characteristic for Classical and Post-Quantum Cryptography -- Fast enumeration of superspecial hyperelliptic curves of genus 4 with automorphism group V4 -- Coding theory -- Two Classes of Constacyclic Codes with Variable Parameters -- Near MDS Codes with Dimension 4 and Their Application in Locally Recoverable Codes -- Optimal possibly nonlinear 3-PIR codes of small size -- PIR codes from combinatorial structures -- The Projective General Linear Group PGL(2, 5m) and Linear Codes of Length 5m + 1 -- Private Information Retrieval Schemes Using Cyclic Codes -- Two Classes of Optimal Few-Weight Codes over Fq + uFq -- Explicit Non-Malleable Codes from Bipartite Graphs -- Cryptography -- Algebraic Relation of Three MinRank Algebraic Modelings -- Decomposition of Dillon's APN permutation with efficient hardware implementation -- New Versions of Miller-loop Secured against Side-Channel Attacks -- A Class of Power Mappings with Low Boomerang Uniformity -- New Classes of Bent Functions via the Switching Method

	-- Sequences -- Correlation measure of binary sequence families with trace representation -- Linear complexity of generalized cyclotomic sequences with period pnqm -- On the 2-adic complexity of cyclotomic binary sequences with period p2 and 2p2.
Sommario/riassunto	This book constitutes the thoroughly refereed post-workshop proceedings of the 8th International Workshop on the Arithmetic of Finite Field, WAIFI 2022, held in Chengdu, China, in August – September 2022. The 19 revised full papers and 3 invited talks presented were carefully reviewed and selected from 25 submissions. The papers are organized in topical sections: structures in finite fields; efficient finite field arithmetic; coding theory; cryptography; sequences.