1.

Record Nr.	UNISA996466315403316
Titolo	Arithmetic of Finite Fields [[electronic resource]] : 7th International Workshop, WAIFI 2018, Bergen, Norway, June 14-16, 2018, Revised Selected Papers / / edited by Lilya Budaghyan, Francisco Rodríguez-Henríquez
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-030-05153-6
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (X, 309 p. 23 illus., 5 illus. in color.)
Collana	Theoretical Computer Science and General Issues, , 2512-2029 ; ; 11321
Disciplina	512.3
Soggetti	Computer science—Mathematics Cryptography Data encryption (Computer science) Computer networks—Security measures Computer networks Coding theory Information theory Symbolic and Algebraic Manipulation Cryptology Mobile and Network Security Computer Communication Networks Coding and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Pre- and post-quantum diffie-hellman from groups, actions, and isogenies -- A new family of pairing-friendly elliptic curves -- superspecial hyperelliptic curves of genus 4 over small finite fields -- Fast computation of isomorphisms between finite fields using elliptic curves -- construction of some codes suitable for both side channel and fault injection attacks -- On hardware implementation of tang-maitra boolean functions -- rapid hardware design for cryptographic modules with filtering structures over small finite fields -- Sequences

with low correlation -- Vector-valued modular forms on finite upper half planes -- Normal basis exhaustive search -- On symmetry and differential properties of generalized boolean functions -- Characterizations of partially bent and plateaued functions over finite fields -- Codes of length two correcting single errors of limited size II -- Fractional jumps: complete characterisation and an explicit infinite family -- Some sextics of genera five and seven attaining the serre bound -- Direct constructions of (involutory) MDS matrices from block vandermonde and cauchy-like matrices -- Exploiting preprocessing for quantum search to break parameters for MQ cryptosystems.

Sommario/riassunto

This book constitutes the thoroughly refereed post-workshop proceedings of the 7th International Workshop on the Arithmetic of Finite Field, WAIFI 2018, held in Bergen, Norway, in June 2018. The 14 revised full papers and six invited talks presented were carefully reviewed and selected from 26 submissions. The papers are organized in topical sections on invited talks; elliptic curves; hardware implementations; arithmetic and applications of finite fields and cryptography.