1. Record Nr. UNINA9910484408703321

Titolo	Arithmetic of Finite Fields : First International Workshop, WAIFI 2007, Madrid, Spain, June 21-22, 2007, Proceedings / / edited by Claude Carlet, Berk Sunar
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	3-540-73074-5
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XI, 360 p.)
Collana	Theoretical Computer Science and General Issues, , 2512-2029 ; ; 4547
Disciplina	512.3
Soggetti	Coding theory Information theory Cryptography Data encryption (Computer science) Computer science—Mathematics Discrete mathematics Algorithms Coding and Information Theory Cryptology Discrete Mathematics in Computer Science Symbolic and Algebraic Manipulation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Structures in Finite Fields -- Explicit Factorizations of Cyclotomic and Dickson Polynomials over Finite Fields -- Some Notes on d-Form Functions with Difference-Balanced Property -- A Note on Modular Forms on Finite Upper Half Planes -- Efficient Implementation and Architectures -- A Coprocessor for the Final Exponentiation of the ? T Pairing in Characteristic Three -- VLSI Implementation of a Functional Unit to Accelerate ECC and AES on 32-Bit Processors -- Efficient Multiplication Using Type 2 Optimal Normal Bases -- Efficient Finite Field Arithmetic -- Effects of Optimizations for Software Implementations of Small Binary Field Arithmetic -- Software Implementation of Arithmetic in -- Complexity Reduction of Constant

Matrix Computations over the Binary Field -- Towards Optimal Toom-Cook Multiplication for Univariate and Multivariate Polynomials in Characteristic 2 and 0 -- Classification and Construction of Mappings over Finite Fields -- A Construction of Differentially 4-Uniform Functions from Commutative Semifields of Characteristic 2 -- Complete Mapping Polynomials over Finite Field F 16 -- On the Classification of 4 Bit S-Boxes -- The Simplest Method for Constructing APN Polynomials EA-Inequivalent to Power Functions -- Curve Algebra -- New Point Addition Formulae for ECC Applications -- Explicit Formulas for Real Hyperelliptic Curves of Genus 2 in Affine Representation -- The Quadratic Extension Extractor for (Hyper)Elliptic Curves in Odd Characteristic -- Cryptography -- On Kabatianskii-Krouk-Smeets Signatures -- Self-certified Signatures Based on Discrete Logarithms -- Attacking the Filter Generator over GF(2 m) -- Codes -- Cyclic Additive and Quantum Stabilizer Codes -- Determining the Number of One-Weight Cyclic Codes When Length and Dimension Are Given -- Error Correcting Codes from Quasi-Hadamard Matrices -- Fast Computations of Gröbner Bases and Blind Recognitions of Convolutional Codes -- Discrete Structures -- A Twin for Euler’s ? Function in -- Discrete Phase-Space Structures and Mutually Unbiased Bases -- Some Novel Results of p-Adic Component of Primitive Sequences over Z/(p d).