1. Record Nr. UNISA996466076203316

Titolo	Arithmetic of Finite Fields [[electronic resource]] : Second International Workshop, WAIFI 2008, Siena, Italy, July 6-9, 2008, Proceedings / / edited by Joachim von zur Gathen, José Luis Imana, Cetin Kaya Koc
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
ISBN	3-540-69499-4
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (X, 205 p.)
Collana	Theoretical Computer Science and General Issues, , 2512-2029 ; ; 5130
Disciplina	003.54
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 -- Interpolation of the Double Discrete Logarithm -- Finite Dedekind Sums -- Transitive q-Ary Functions over Finite Fields or Finite Sets: Counts, Properties and Applications -- Efficient Finite Field Arithmetic -- Fast Point Multiplication on Elliptic Curves without Precomputation -- Optimal Extension Field Inversion in the Frequency Domain -- Efficient Finite Fields in the Maxima Computer Algebra System -- Efficient Implementation and Architectures -- Modular Reduction in GF(2 n) without Pre-computational Phase -- Subquadratic Space Complexity Multiplication over Binary Fields with Dickson Polynomial Representation -- Digit-Serial Structures for the Shifted Polynomial Basis Multiplication over

Binary Extension Fields -- Classification and Construction of Mappings over Finite Fields -- Some Theorems on Planar Mappings -- Classifying 8-Bit to 8-Bit S-Boxes Based on Power Mappings from the Point of DDT and LAT Distributions -- EA and CCZ Equivalence of Functions over GF (2 n) -- Codes and Cryptography -- On the Number of Two-Weight Cyclic Codes with Composite Parity-Check Polynomials -- On Field Size and Success Probability in Network Coding -- Montgomery Ladder for All Genus 2 Curves in Characteristic 2 -- On Cryptographically Significant Mappings over GF(2 n).

Sommario/riassunto

This book constitutes the refereed proceedings of the Second International Workshop on the Arithmetic of Finite Fields, WAIFI 2008, held in Siena, Italy, in July 2008. The 16 revised full papers presented were carefully reviewed and selected from 34 submissions. The papers are organized in topical sections on structures in finite fields, efficient finite field arithmetic, efficient implementation and architectures, classification and construction of mappings over finite fields, and codes and cryptography.