1. Record Nr. UNISA996465667103316

Titolo	Arithmetic of Finite Fields [[electronic resource]] : Third International Workshop, WAIFI 2010, Istanbul, Turkey, June 27-30, 2010, Proceedings / / edited by M. Anwar Hasan, Tor Helleseth
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	1-280-38738-6 9786613565303 3-642-13797-0
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (280 p. 41 illus.)
Collana	Theoretical Computer Science and General Issues, , 2512-2029 ; ; 6087
Disciplina	512.32
Soggetti	Computer programming Computer science—Mathematics Discrete mathematics Algorithms Cryptography Data encryption (Computer science) Computer networks Programming Techniques Symbolic and Algebraic Manipulation Discrete Mathematics in Computer Science Cryptology Computer Communication Networks
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	Invited Talk 1 -- Recursive Towers of Function Fields over Finite Fields -- Efficient Finite Field Arithmetic -- High-Performance Modular Multiplication on the Cell Processor -- A Modified Low Complexity Digit-Level Gaussian Normal Basis Multiplier -- Type-II Optimal Polynomial Bases -- Pseudo-random Numbers and Sequences -- Pseudorandom Vector Sequences Derived from Triangular Polynomial Systems with Constant Multipliers -- Structure of Pseudorandom

Numbers Derived from Fermat Quotients -- Boolean Functions -- Distribution of Boolean Functions According to the Second-Order Nonlinearity -- Hyper-bent Boolean Functions with Multiple Trace Terms -- Invited Talk 2 -- On the Efficiency and Security of Pairing-Based Protocols in the Type 1 and Type 4 Settings -- Functions, Equations and Modular Multiplication -- Switching Construction of Planar Functions on Finite Fields -- Solving Equation Systems by Agreeing and Learning -- Speeding Up Bipartite Modular Multiplication -- Finite Field Arithmetic for Pairing Based Cryptography -- Constructing Tower Extensions of Finite Fields for Implementation of Pairing-Based Cryptography -- Delaying Mismatched Field Multiplications in Pairing Computations -- Invited Talk 3 -- Regenerating Codes for Distributed Storage Networks -- Finite Fields, Cryptography and Coding -- On Rationality of the Intersection Points of a Line with a Plane Quartic -- Reflections about a Single Checksum -- Efficient Time-Area Scalable ECC Processor Using ?-Coding Technique.