1.	Record Nr.	UNINA9910483746003321
	Titolo	Arithmetic of finite fields : Third International Workshop, WAIFI 2010, Istanbul, Turkey, June 27-30, 2010 : proceedings / / M. Anwar Hasan, Tor Helleseth (eds.)
	Pubbl/distr/stampa	New York, : Springer, 2010
	ISBN	1-280-38738-6 9786613565303 3-642-13797-0
	Edizione	[1st ed.]
	Descrizione fisica	1 online resource (280 p. 41 illus.)
	Collana	Lecture notes in computer science, , 0302-9743 ; ; 6087 LNCS sublibrary. SL 1, Theoretical computer science and general issues
	Altri autori (Persone)	HasanM. Anwar HellesethTor
	Disciplina	512.32
	Soggetti	Finite fields (Algebra) Mappings (Mathematics) Curves, Algebraic
	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.