

1. Record Nr.	UNINA9910813035403321
Autore	Frishman Rick
Titolo	Author 101 : the insider's guide to publishing from proposal to bestseller // Rick Frishman and Robyn Spizman ; with Mark Steisel & Justin Spizman
Pubbl/distr/stampa	New York, New York : , : Morgan James Publishing, , [2015] ©2015
ISBN	1-63047-376-6
Descrizione fisica	1 online resource (xxi, 203 pages)
Disciplina	070.52
Soggetti	Authorship - Marketing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr.	UNINA9910483746003321
Titolo	Arithmetic of Finite Fields : Third International Workshop, WAIFI 2010, Istanbul, Turkey, June 27-30, 2010, Proceedings / / edited by M. Anwar Hasan, Tor Helleseeth
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
Altri autori (Persone)	HasanM. Anwar HelleseethTor
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  $\mathbb{F}_2$ -Coding Technique.

## Sommario/riassunto

These are the proceedings of WAIFI 2010, the Third International Workshop on the Arithmetic of Finite Fields, held in Istanbul, Turkey, during June 27-30, 2010. The first workshop, WAIFI 2007, was held in Madrid, Spain, and then WAIFI 2008 was held in Siena, Italy. In 2008, the workshop series was made biannual and it is now being held every even year, bringing together mathematicians, computer scientists, engineers and physicists who are doing research on various aspects of finite field arithmetic. This year the workshop received 33 submissions, each of which was reviewed by at least three reviewers who were either members of the Program Committee of the workshop or external reviewers chosen by the members. Once the review phase was over, the Program Committee had online discussions over a period of several days. In the end, a total of 15 papers representing both theoretical and practical aspects of finite field arithmetic were accepted for presentation. These accepted papers are part of these proceedings. In addition to the presentations of these papers, we were fortunate to have three invited talks given by P. Vijay Kumar, Alfred Menezes and Henning Stichtenoth. The papers, which the invited talks were based on, are also part of the proceedings. We are very grateful to the members of the Program Committee for their dedication, professionalism and careful work with the review and selection process. We also sincerely thank the external reviewers who contributed with their special expertise to review papers for this workshop.