1. Record Nr. UNISA996198863003316

Titolo	Arithmetic of Finite Fields [[electronic resource]] : 5th International Workshop, WAIFI 2014, Gebze, Turkey, September 27-28, 2014. Revised Selected Papers / / edited by Çetin Kaya Koç, Sihem Mesnager, Erkay Sava
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-16277-2
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (X, 213 p. 18 illus.)
Collana	Theoretical Computer Science and General Issues, , 2512-2029 ; ; 9061
Disciplina	512.74
Soggetti	Computer science—Mathematics Discrete mathematics Algorithms Cryptography Data encryption (Computer science) Computer networks Coding theory Information theory Symbolic and Algebraic Manipulation Discrete Mathematics in Computer Science Cryptology Computer Communication Networks Coding and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	First Invited talk -- Computing Discrete Logarithms in F36•137 and F36•163 using Magma -- Finite Field Arithmetic -- Accelerating Iterative SpMV for the Discrete Logarithm Problem using GPUs -- Finding Optimal Chudnovsky-Chudnovsky Multiplication Algorithms -- Reducing the Complexity of Normal Basis Multiplication -- O -- Second Invited talk -- Open Questions on Nonlinearity and on APN functions -- Boolean and Vectorial Functions -- Some Results on Difference

Balanced Functions -- Affine Equivalency and Nonlinearity Preserving Bijective Mappings over F2 -- On Verification of Restricted Extended Affine Equivalence of Vectorial Boolean Functions -- On o-Equivalence of Niho Bent Functions -- Third Invited Talk -- L-polynomials of the curve yqn y = xqh+1 _ over Fqm -- Coding Theory and Code-based Cryptography -- Efficient Software Implementations of Code-based Hash Functions -- Quadratic residue codes over Fp + vFp + v2F.p.

Sommario/riassunto

This book constitutes the refereed proceedings of the 5th International Workshop on the Arithmetic of Finite Field, WAIFI 2014, held in Gebze, Turkey, in September 2014. The 9 revised full papers and 43 invited talks presented were carefully reviewed and selected from 27 submissions. This workshop is a forum of mathematicians, computer scientists, engineers and physicists performing research on finite field arithmetic, interested in communicating the advances in the theory, applications, and implementations of finite fields. The workshop will help to bridge the gap between the mathematical theory of finite fields and their hardware/software implementations and technical applications.