1. Record Nr. UNINA9910820221703321

Titolo	Topics in finite fields : 11th International Conference on Finite Fields and Their Applications, July 22--26, 2013, Magdeburg, Germany / / Gohar Kyureghyan, Gary L. Mullen, Alexander Pott, editors
Pubbl/distr/stampa	Providence, Rhode Island : , : American Mathematical Society, , 2015 ©2015
ISBN	1-4704-2220-4
Descrizione fisica	1 online resource (371 p.)
Collana	Contemporary Mathematics, , 1098-3627 ; ; 632
Classificazione	05Bxx11Txx11Gxx12Exx12Fxx12Yxx20Cxx51Exx94Axx94Bxx
Disciplina	512/.3
Soggetti	Group theory Finite fields (Algebra) Commutative rings Combinatorial analysis Arithmetical algebraic geometry
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references at the end of each chapters.
Nota di contenuto	""Cover""; ""Title page""; ""Contents""; ""Preface""; ""New recursive construction of normal polynomials over finite fields""; ""1. Introduction""; ""2. Preliminaries""; ""3. Irreducibility of Polynomial Compositions""; ""4. Some construction of N-polynomials""; ""References""; ""Collineation groups strongly irreducible on an oval in a projective plane of odd order""; ""1. Introduction""; ""2. Preliminary results""; ""3. Proof of Theorem 1.1""; ""4. Proof of Theorem 1.2""; ""References""; ""On the solvability of certain equations over finite fields""; ""1. Introduction"" ""2. Preliminary Lemmas""""3. Main Results""; ""4. Applications""; ""Acknowledgement""; ""References""; ""On automorphism groups of binary linear codes""; ""1. Background and notations""; ""2. Cyclic group of order (an odd prime)""; ""3. Cyclic group of order 2 (an odd prime)""; ""4. Dihedral group of order 2 (an odd prime)""; ""5. Interaction between fixed codes""; ""6. The automorphism group of an extremal self-dual code of length 72""; ""References""; ""Extended differential properties of cryptographic functions""; ""1. Introduction"";

""2. Block cipher basics""

""3. Differential cryptanalysis""""""4. New bounds on the maximum probability of two-round differentials""; ""5. Sboxes with multiplication-invariant derivatives""; ""6. Conclusions""; ""Acknowledgements""; ""References""; ""A divisibility criterion for exceptional APN functions""; ""1. Introduction""; ""2. The state of the art""; ""3. New Results""; ""4. Preliminary lemmata""; ""5. Proof of theorem 3.1""; ""6. Some applications""; ""References""; ""Non weakly regular bent polynomials from vectorial quadratic functions""; ""1. Introduction""; ""2. Fourier coefficients for quadratic functions""

""An upper bound for the number of Galois points for a plane curve""""""1. Introduction""; ""2. Preliminaries""; ""3. Proof""; ""References""; ""A generalization of the nonlinear combination generator""; ""1. Introduction""; ""2. Preliminaries""; ""3. Results on linear recurring sequences""; ""4. Sequences of the form a?? a??+\dotsb+ _{ } _{ }""; ""5. Multiplication strong feedback shift registers""; ""References""; ""Dedekind sums with a parameter in function fields""; ""1. Introduction""; ""2. Review of higher-dimensional Dedekind sums""

""3. Higher-dimensional Dedekind sums with a parameter""