Contents

Preface vii

Construction of new toric quantum codes
Clarice Dias Albuquerque, Reginaldo Palazzo, Jr., and Eduardo Brandani Silva 1

On the calculation of the linear complexity of periodic sequences
Hassan Aly, Radwa Marzouk, and Wilfried Meidl 11

A few more functions that are not APN infinitely often
Yves Aubry, Gary McGuire, and François Rodier 23

An APN permutation in dimension six
K.A. Browning, J.F. Dillon, M.T. McQuistan, and A.J. Wolfe 33

CCZ-equivalence of single and multi output Boolean functions
Lilya Budaghyan and Claude Carlet 43

Structural weaknesses of permutations with a low differential uniformity and generalized crooked functions
Anne Canteaut and María Naya-Plasencia 55

Solvability of systems of polynomial equations with some prescribed monomials
Francis N. Castro and Ivelisse M. Rubio 73

Character sums in finite fields
Mei-Chu Chang 83

Monomial functions with linear structure and permutation polynomials
Pascale Charpin and Gohar M. Kyureghyan 99

Primitive elements on lines in extensions of finite fields
Stephen D. Cohen 113

Commutative semifields of order 243 and 3125
Robert S. Coulter and Pamela Kosick 129

Normal elliptic bases and torus-based cryptography
Clément Dunand and Reynald Lercier 137

Unitary superperfect binary polynomials
Luis H. Gallardo and Olivier Rahavandrainy 155

Shift-invariant polynomials and Ritts Second Theorem
Joachim von zur Gathen 161

Waring's problem in finite fields with Dickson polynomials
Domingo Gomez and Arne Winterhof 185

Jacobi sums and irreducible polynomials with prescribed trace and restricted norm
S. Gurak 193

A family of binary sequences from interleaved construction and their cryptographic properties
Jing Jane He, Daniel Panario, and Qiang Wang 209

Sziklai's conjecture on the number of points of a plane curve over a finite field II
Masaaki Homma and Seon Jeong Kim 225

Folded algebraic-geometric codes from Galois extensions
Ming-Deh Huang and Anand Kumar Narayanan 235

A multilinear generalization of the Tate pairing
Ming-Deh Huang and Wayne Raskind 255

The merit factor of binary sequence families constructed from m-sequences
Jonathan Jedwab and Kai-Uwe Schmidt 265

Intractable problems in cryptography
Neal Koblitz and Alfred Menezes 279

Modular curves and coding theory: A survey
Wen-Ching W. Li 301

Minimal generating sets of Weierstrass semigroups of certain m-tuples on the norm-trace function field
Gretchen L. Matthews and Justin D. Peachey 315

On the zeta functions of an optimal tower of function fields over $\mathbb{F}_4$
Gary McGuire and Alexey Zaytsev 327

The asymptotic theory of algebraic-geometry codes
Harald Niederreiter 339

A spectrum result on maximal partial ovoids of the generalized quadrangle $\mathcal{Q}(4, q)$, q odd
Valentina Pepe, Cornelia Rössing, and Leo Storme 349

Cyclic codes aspects of bent functions
J. Wolfmann 363