

Contents

Preface	vii
Analysis and optimization of elliptic-curve single-scalar multiplication DANIEL J. BERNSTEIN AND TANJA LANGE	1
On influences of Boolean variables and their computation SERDAR BOZTAŞ	21
Subsequences of Sidelnikov sequences NINA BRANDSTÄTTER AND ARNE WINTERHOF	33
A multi-level blocking distinct-degree factorization algorithm RICHARD P. BRENT AND PAUL ZIMMERMANN	47
New bounds on some parameters in the Waring problem for polynomials over a finite field MIREILLE CAR	59
Dickson polynomial permutations MIHAI CIPU AND STEPHEN D. COHEN	79
Ring theoretic study of linear codes using additive polynomials VINAY DEOLALIKAR	91
Toward a complete twin primes theorem for polynomials over finite fields GOVE EFFINGER	103
On the distribution of the elliptic curve power generator EDWIN EL-MAHASSNI AND IGOR E. SHPARLINSKI	111
Discrete logarithms in curves over finite fields ANDREAS ENGE	119
Some remarks on the Hasse-Arf theorem ARNALDO GARCIA AND HENNING STICHTENOTH	141
Character sums for sequences of iterations of Dickson polynomials DOMINGO GOMEZ AND ARNE WINTERHOF	147
What can be used instead of a Barker sequence? JONATHAN JEDWAB	153
Order dividing extension fields and the root computation problem ANNA M. JOHNSTON	179

Kasami bent functions are not equivalent to their duals PHILIPPE LANGEVIN, GREGOR LEANDER, AND GARY MCGUIRE	187
Equidistribution of roots of L -function of Gold exponential sum V. KUMAR MURTY AND KENNETH W. SHUM	199
Reduced linear modular systems EDUSMILDO OROZCO	205
Cocyclic Butson Hadamard matrices and codes over \mathbb{Z}_n via the trace map N. PINNAWALA AND A. RAO	213
Dickson permutation polynomials that decompose in cycles of the same length IVELISSE M. RUBIO, GARY L. MULLEN, CARLOS CORRADA, AND FRANCIS N. CASTRO	229
The simplex code over Galois rings H. TAPIA-RECILLAS	241
Finite fields and Galois geometries J. A. THAS	251