Table of Contents

Modifications of the Rao-Nam Cryptosystem 1
Ángela I. Barbero and Øyvind Ytrehus

Efficient Reduction on the Jacobian Variety of Picard Curves 13
Ernesto Reinaldo Barreiro, Jorge Estrada Sarlabous, and Jean-Pierre Cherdieu

Continued Fractions in Hyperelliptic Function Fields 29
T.G. Berry

Discrete Logarithms: Recent Progress 42
Johannes Buchmann and Damian Weber

One-weight $\mathbf{Z}_4$-linear Codes 57
Claude Carlet

Efficient Algorithms for the Jacobian Variety of Hyperelliptic Curves $y^2 = x^p - x + 1$ Over a Finite Field of Odd Characteristic p 73
Iwan Duursma and Kouichi Sakurai

On Weierstrass Semigroups and One-point Algebraic Geometry Codes 90
J.I. Farrán

On the Undetected Error Probability of m-out-of-n Codes on the Binary Symmetric Channel 102
Fang-Wei Fu, Torleiv Kløve, and Shu-Tao Xia

Skew Pyramids of Function Fields Are Asymptotically Bad 111
Arnaldo Garcia and Henning Stichtenoth

A Public Key Cryptosystem Based on Sparse Polynomials 114
D. Grant, K. Krastev, D. Lieman, and I. Shparlinski

Higher Weights of Grassmann Codes 122
Sudhir R. Ghorpade and Gilles Lachaud

Toric Surfaces and Error-correcting Codes 132
Johan P. Hansen

Decoding Spherical Codes Generated by Binary Partitions of Symmetric Pointsets 143
John K. Karlof and Guodong Liu

Worst-Case Analysis of an Algorithm for Computing the Greatest Common Divisor of n Inputs 156
Charles Lam, Jeffrey Shallit, and Scott Vanstone

Zeta Functions of Curves over Finite Fields with Many Rational Points . . . 167
Kristin Lauter

Codes on Drinfeld Modular Curves 175
Bartolomé López and Ignacio Luengo

Elliptic Curves, Pythagorean Triples and Applications 184
J. Miret, J. Tena, and M. Valls

Exponential Sums and Stationary Phase (I) 195
Carlos Julio Moreno

Exponential Sums in Several Variables over Finite Fields 209
Oscar Moreno, Francis N. Castro, and Alberto Cáceres

Decoding Reed-Solomon Codes Beyond Half the Minimum Distance 221
R. Refslund Nielsen and T. Høholdt

Reed-Muller Type Codes on the Veronese Variety over Finite Fields 237
C. Rentería and H. Tapia-Recillas

Cryptography Primitives Based on a Cellular Automaton 244
Jesús Urías

Factoring the Semigroup Determinant
of a Finite Commutative Chain Ring 249
Jay A. Wood