

Table of Contents

Modifications of the Rao-Nam Cryptosystem	1
<i>Ángela I. Barbero and Øyvind Ytrehus</i>	
Efficient Reduction on the Jacobian Variety of Picard Curves	13
<i>Ernesto Reinaldo Barreiro, Jorge Estrada Sarlabous, and Jean-Pierre Cherdieu</i>	
Continued Fractions in Hyperelliptic Function Fields	29
<i>T.G. Berry</i>	
Discrete Logarithms: Recent Progress.....	42
<i>Johannes Buchmann and Damian Weber</i>	
One-weight \mathbf{Z}_4 -linear Codes	57
<i>Claude Carlet</i>	
Efficient Algorithms for the Jacobian Variety of Hyperelliptic Curves $y^2 = x^p - x + 1$ Over a Finite Field of Odd Characteristic p	73
<i>Iwan Duursma and Kouichi Sakurai</i>	
On Weierstrass Semigroups and One-point Algebraic Geometry Codes	90
<i>J.I. Farrán</i>	
On the Undetected Error Probability of m -out-of- n Codes on the Binary Symmetric Channel	102
<i>Fang-Wei Fu, Torleiv Kløve, and Shu-Tao Xia</i>	
Skew Pyramids of Function Fields Are Asymptotically Bad.....	111
<i>Arnaldo Garcia and Henning Stichtenoth</i>	
A Public Key Cryptosystem Based on Sparse Polynomials.....	114
<i>D. Grant, K. Krastev, D. Lieman, and I. Shparlinski</i>	
Higher Weights of Grassmann Codes	122
<i>Sudhir R. Ghorpade and Gilles Lachaud</i>	
Toric Surfaces and Error-correcting Codes.....	132
<i>Johan P. Hansen</i>	
Decoding Spherical Codes Generated by Binary Partitions of Symmetric Pointsets	143
<i>John K. Karlof and Guodong Liu</i>	
Worst-Case Analysis of an Algorithm for Computing the Greatest Common Divisor of n Inputs.....	156
<i>Charles Lam, Jeffrey Shallit, and Scott Vanstone</i>	

VIII Table of Contents

Zeta Functions of Curves over Finite Fields with Many Rational Points . . .	167
<i>Kristin Lauter</i>	
Codes on Drinfeld Modular Curves	175
<i>Bartolomé López and Ignacio Luengo</i>	
Elliptic Curves, Pythagorean Triples and Applications	184
<i>J. Miret, J. Tena, and M. Valls</i>	
Exponential Sums and Stationary Phase (I)	195
<i>Carlos Julio Moreno</i>	
Exponential Sums in Several Variables over Finite Fields	209
<i>Oscar Moreno, Francis N. Castro, and Alberto C��ceres</i>	
Decoding Reed-Solomon Codes Beyond Half the Minimum Distance	221
<i>R. Refslund Nielsen and T. H��holdt</i>	
Reed-Muller Type Codes on the Veronese Variety over Finite Fields	237
<i>C. Renter��a and H. Tapia-Recillas</i>	
Cryptography Primitives Based on a Cellular Automaton	244
<i>Jes��s Ur��as</i>	
Factoring the Semigroup Determinant of a Finite Commutative Chain Ring	249
<i>Jay A. Wood</i>	

Coding Theory, Cryptography and Related Areas
Proceedings of an International Conference on Coding
Theory, Cryptography and Related Areas, held in
Guanajuato, Mexico, in April 1998
Buchmann, J.; Hoeholdt, T.; Stichtenoth, H.;
Tapia-Recillas, H. (Eds.)
2000, VIII, 260 p., Softcover
ISBN: 978-3-540-66248-8