

## Sommaire

- Modifications of the Rao-Nam Cryptosystem
- Efficient Reduction on the Jacobian Variety of Picard Curves
- Continued Fractions in Hyperelliptic Function Fields
- Discrete Logarithms: Recent Progress
- One-weight  $Z_4$ -linear Codes
- Efficient Algorithms for the Jacobian Variety of Hyperelliptic Curves  $y^2 = x^p - x + 1$  Over a Finite Field of Odd Characteristic
- On Weierstrass Semigroups and One-point Algebraic Geometry Codes
- On the Undetected Error Probability of  $m$ -out-of- $n$  Codes on the Binary Symmetric Channel
- Skew Pyramids of Function Fields Are Asymptotically Bad
- A Public Key Cryptosystem Based on Sparse Polynomials
- Higher Weights of Grassmann Codes
- Toric Surfaces and Error-correcting Codes
- Decoding Spherical Codes Generated by Binary Partitions of Symmetric Pointsets
- Worst-Case Analysis of an Algorithm for Computing the Greatest Common Divisor of  $n$  Inputs
- Zeta Functions of Curves over Finite Fields with Many Rational Points
- Codes on Drinfeld Modular Curves
- Elliptic Curves, Pythagorean Triples and Applications
- Exponential Sums and Stationary Phase (I)
- Exponential Sums in Several Variables over Finite Fields
- Decoding Reed-Solomon Codes Beyond Half the Minimum Distance
- Reed-Muller Type Codes on the Veronese Variety over Finite Fields
- Cryptography Primitives Based on a Cellular Automaton
- Factoring the Semigroup Determinant of a Finite Commutative Chain Ring