

Table of Contents

| | |
|---|-----|
| Cryptography and the Methodology of Provable Security | 1 |
| <i>Jacques Stern</i> | |
| Dynamical Systems Generated by Rational Functions | 6 |
| <i>Harald Niederreiter, Igor E. Shparlinski</i> | |
| Homotopy Methods for Equations over Finite Fields | 18 |
| <i>Alan G.B. Lauder</i> | |
| Three Constructions of Authentication/Secrecy Codes | 24 |
| <i>Cunsheng Ding, Arto Salomaa, Patrick Solé, Xiaojian Tian</i> | |
| The Jacobi Model of an Elliptic Curve and Side-Channel Analysis | 34 |
| <i>Olivier Billet, Marc Joye</i> | |
| Fast Point Multiplication on Elliptic Curves through Isogenies | 43 |
| <i>Eric Brier, Marc Joye</i> | |
| Interpolation of the Elliptic Curve Diffie–Hellman Mapping | 51 |
| <i>Tanja Lange, Arne Winterhof</i> | |
| An Optimized Algebraic Method for Higher Order Differential Attack . . . | 61 |
| <i>Yasuo Hatano, Hidema Tanaka, Toshinobu Kaneko</i> | |
| Fighting Two Pirates | 71 |
| <i>Hans Georg Schaathun</i> | |
| Copyright Control and Separating Systems | 79 |
| <i>Sylvia Encheva, Gérard Cohen</i> | |
| Unconditionally Secure Homomorphic Pre-distributed Commitments | 87 |
| <i>Anderson C.A. Nascimento, Akira Otsuka, Hideki Imai, Joern Mueller-Quade</i> | |
| A Class of Low-Density Parity-Check Codes Constructed Based on Reed–Solomon Codes with Two Information Symbols | 98 |
| <i>Ivana Djurdjevic, Jun Xu, Khaled Abdel-Ghaffar, Shu Lin</i> | |
| Relative Duality in MacWilliams Identity | 108 |
| <i>L.S. Kazarin, V.M. Sidelnikov, Igor B. Gashkov</i> | |
| Good Expander Graphs and Expander Codes: Parameters and Decoding . | 119 |
| <i>H. Janwa</i> | |
| On the Covering Radius of Certain Cyclic Codes | 129 |
| <i>Oscar Moreno, Francis N. Castro</i> | |

| | |
|---|-----|
| Unitary Error Bases: Constructions, Equivalence, and Applications | 139 |
| <i>Andreas Klappenecker, Martin Rötteler</i> | |
| Differentially 2-Uniform Cocycles – The Binary Case | 150 |
| <i>K.J. Horadam</i> | |
| The Second and Third Generalized Hamming Weights of Algebraic Geometry Codes | 158 |
| <i>Domingo Ramirez-Alzola</i> | |
| Error Correcting Codes over Algebraic Surfaces | 169 |
| <i>Thanasis Bouganis</i> | |
| A Geometric View of Decoding AG Codes | 180 |
| <i>Thanasis Bouganis, Drue Coles</i> | |
| Performance Analysis of M-PSK Signal Constellations in Riemannian Varieties | 191 |
| <i>Rodrigo Gusmão Cavalcante, Reginaldo Palazzo Jr.</i> | |
| Improvements to Evaluation Codes and New Characterizations of Arf Semigroups | 204 |
| <i>Maria Bras-Amorós</i> | |
| Optimal 2-Dimensional 3-Dispersion Lattices | 216 |
| <i>Moshe Schwartz, Tuvi Etzion</i> | |
| On g -th MDS Codes and Matroids | 226 |
| <i>Keisuke Shiromoto</i> | |
| On the Minimum Distance of Some Families of \mathbb{Z}_{2^k} -Linear Codes | 235 |
| <i>Fabien Galand</i> | |
| Quasicyclic Codes of Index ℓ over F_q Viewed as $F_q[x]$ -Submodules of $F_{q^\ell}[x]/\langle x^m - 1 \rangle$ | 244 |
| <i>Kristine Lally</i> | |
| Fast Decomposition of Polynomials with Known Galois Group | 254 |
| <i>Andreas Enge, François Morain</i> | |
| Author Index | 265 |