

CONTENTS

To Gilles Lachaud on the occasion of his 60th birthday <i>R. Rolland, M. Tsfasman</i>	v
Preface <i>J.-M. Goursaud</i>	vii
Organizing Committees	xi
Fast addition on non-hyperelliptic genus 3 curves <i>S. Flon, R. Oyono, C. Ritzenthaler</i>	1
Computing endomorphism rings of Jacobians of genus 2 curves over finite fields <i>D. Freeman, K.Lauter</i>	29
Complex multiplication and canonical lifts <i>D. Kohel</i>	67
Two letters to Jaap Top <i>J.-P. Serre</i>	84
On some questions of Serre on abelian threefolds <i>G. Lachaud, C. Ritzenthaler</i>	88
Pseudorandom Points on Elliptic Curves over Finite Fields <i>I. Shparlinski</i>	116
Symmetric Cryptography and Algebraic Curves <i>F. Voloch</i>	135

xiv *Contents*

Galois invariant smoothness basis <i>J.-M. Couveignes, R. Lercier</i>	142
Fuzzy Pairings-Based CL-PKC <i>M. Kiviharju</i>	168
Trace Zero Varieties over Fields of Characteristic 2 for Cryptographic Applications <i>R. Avanzi, E. Cesena</i>	188
Group Law Algorithms For Jacobian Varieties Of Curves Over Finite Fields <i>R. Cohen</i>	216
Discrete Logarithms, Duality, and Arithmetic in Brauer Groups <i>G. Frey</i>	241
On generators of the group $\widehat{H}^{-1}(\text{Gal}(L/K), E_L)$ in some abelian p -extension L/K <i>E. Hallouin, M. Perret</i>	273
On the semiprimitivity of cyclic codes <i>Y. Aubry, P. Langevin</i>	284
Decoding of scroll codes <i>G.H. Hitching, T. Johnsen</i>	294
List decoding using syndromes <i>P. Beelen, T. Høholdt</i>	315
A note on the tensor rank of the multiplication in certain finite fields <i>S. Ballet</i>	332
Multiplication in small finite fields using elliptic curves <i>J. Chaumine</i>	343
An optimal unramified tower of function fields <i>K. Brander</i>	351

Partial covering sequences: a method for designing classes of cryptographic functions <i>C. Carlet</i>	366
Non linéarité des fonctions booléennes données par des traces de polynômes de degré binaire 3 <i>E. Féraud, F. Rodier</i>	388
On Exponents with highly divisible Fourier Coefficients and Conjectures of Niho and Dobbertin <i>G. Leander, P. Langevin</i>	410
On the number of resilient Boolean functions <i>S. Mesnager</i>	419
On Quadratic Extensions of Cyclic Projective Planes <i>H. F. Law, P. P. W. Wong</i>	434
Some integral representations of finite groups and their arithmetic applications <i>D. A. Malinin</i>	467
Number of points of non-absolutely irreducible hypersurfaces <i>R. Rolland</i>	481
Neuberg cubics over finite fields <i>N. J. Wildberger</i>	488
Partitions of Vector Spaces over Finite Fields <i>Y. Zelenyuk</i>	505
Author Index	513