

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

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