

Contents

Preface	vii
Differentially 4-uniform functions YVES AUBRY AND FRANÇOIS RODIER	1
Computing Hironaka's invariants: Ridge and directrix JÉRÉMY BERTHOMIEU, PASCAL HIVERT AND HUSSEIN MOURTADA	9
Nondegenerate curves of low genus over small finite fields WOUTER CASTRYCK AND JOHN VOIGHT	21
Faster side-channel resistant elliptic curve scalar multiplication ALEXANDRE VENELLI AND FRANÇOIS DASSANCE	29
Non linéarité des fonctions booléennes données par des polynômes de degré binaire 3 définies sur \mathbb{F}_{2^m} avec m pair ERIC FÉRARD AND FRANÇOIS RODIER	41
A note on a maximal curve ARNALDO GARCIA AND HENNING STICHTENOTH	55
Computing Humbert surfaces and applications DAVID GRUENEWALD	59
Genus 3 curves with many involutions and application to maximal curves in characteristic 2 ENRIC NART AND CHRISTOPHE RITZENTHALER	71
Uniqueness of low genus optimal curves over \mathbb{F}_2 ALESSANDRA RIGATO	87
Group order formulas for reductions of CM elliptic curves ALICE SILVERBERG	107
Families of explicit isogenies of hyperelliptic Jacobians BENJAMIN SMITH	121
Computing congruences of modular forms and Galois representations modulo prime powers XAVIER TAIXÉS I VENTOSA AND GABOR WIESE	145