

Contents

Chapter 1. An Overview of Algebraic Curves and Cryptography	
V. KUMAR MURTY	1
1.1. Introduction	1
1.2. The basic paradigm	1
1.3. The Diffie-Hellman decision problem	2
1.4. Constraints on the group	2
1.5. Abelian varieties over finite fields	3
1.6. Elliptic curves	4
1.7. Statistical results	4
1.8. Abelian varieties of higher dimension	6
1.9. Outline of contents	7
Chapter 2. Schoof's Point Counting Algorithm	
NICOLAS THÉRIAULT	11
2.1. Preliminaries	11
2.2. Division polynomials	16
2.3. Schoof's algorithm	23
2.4. Implementation	30
2.5. Improvements by Atkin and Elkies	38
2.6. Computing the modular equations	45
2.7. Computing p_1 , \tilde{a} and \tilde{b}	52
2.8. Computing the factor of f_ℓ	58
2.9. Parallelization	61
Chapter 3. Report on the Denef-Vercauteren/Kedlaya Algorithm	
ZUBAIR ASHRAF, ALI JUMA, AND PRAMATHANATH SASTRY	65
3.1. Background	65
3.2. Generalities	66
3.3. Main strategy	68
3.4. Monsky-Washnitzer cohomology	69
3.5. Hyperelliptic curves	72
3.6. Data structures	76
3.7. Algorithm for lifting the curve to characteristic zero	77
3.8. Inversion	78
3.9. The 2-power Frobenius on K	78
3.10. The characteristic polynomial of Frobenius	79
3.11. Multiplication	79
3.12. Running times	80
3.13. Parallelization	81

Chapter 4. An Introduction to Gröbner Bases	
MOHAMMED RADI-BENJELLOUN	83
4.1. Introduction	83
4.2. Gröbner bases	88
Chapter 5. C_{ab} Curves and Arithmetic on Their Jacobians	
FARZALI IZADI	99
5.1. Introduction	99
5.2. Preliminaries	99
5.3. The C_{ab} curves	108
5.4. Addition algorithm for Jacobian group in divisor representation	110
5.5. Addition algorithm for Jacobian group in ideal representation	112
Chapter 6. The Zeta Functions of Two Garcia-Stichtenoth Towers	
KENNETH W. SHUM	119
6.1. Introduction	119
6.2. Background on zeta functions	119
6.3. The first Garcia-Stichtenoth tower	121
6.4. The second Garcia-Stichtenoth tower	123
6.5. Conclusion	126
Appendix: Counting points over P_0 in GS1	126
Bibliography	129
Index	133