Contents

Foreword ix

Preface xi

1 Introduction to Public Key Cryptography 1

1.1 Private Key Cryptography 1

1.2 Diffie-Hellman Key Exchange 3

1.3 Public Key Cryptography 4

1.4 Trapdoor One-Way Functions Based on Groups 5

1.4.1 Group Order as a TOF 6

1.4.2 RSA Cryptosystem 6

1.4.3 Exponentiation as a TOF 7

1.5 NIST Digital Signature Standard 10

1.6 Elliptic Curve Cryptosystems 13

1.7 Notes 14

2 Introduction to Elliptic Curves 15

2.1 Definitions 15

2.2 Group Law 17

2.3 The Discriminant and j-Invariant 19

2.4 Curves over K, $\mathrm{char}(K) \neq 2, 3$ 20

2.5 Curves over K, $\mathrm{char}(K) = 2$ 21

2.6 Group Structure 23

2.7 Divisor Theory 28

2.8 Elliptic Curves over $\mathbb{Z}_n$ 32

2.9 Notes 34

3 Isomorphism Classes of Elliptic Curves over Finite Fields 35

3.1 Introduction 35

3.2 Isomorphism Classes of Curves over F_q, char$(F_q) \neq 2, 3$. 37

3.3 Isomorphism Classes of Non-Supersingular Curves over F_{2^m} 39

3.4 Isomorphism Classes of Supersingular Curves over F_{2^m}, m odd 40

3.5 Isomorphism Classes of Supersingular Curves over F_{2^m}, m even 41

3.6 Number of Points 46

3.7 Notes 48

4 The Discrete Logarithm Problem 49

4.1 Algorithms 49

4.1.1 Square Root Methods 50

4.1.2 Pohlig-Hellman Method 51

4.1.3 Index Calculus Method 52

4.1.4 Index Calculus Method for Elliptic Curves 54

4.2 Reducing Some Logarithm Problems to Logarithms in a Finite Field 54

4.2.1 Singular Elliptic Curves 55

4.2.2 Another Class of Genus 0 Curves 57

4.3 Notes 59

5 The Elliptic Curve Logarithm Problem 61

5.1 The Weil Pairing 61

5.1.1 Definition 62

5.1.2 Computing the Function of a Principal Divisor . 63

5.1.3 Computing the Weil Pairing 66

5.2 Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field 68

5.2.1 The Reduction 69

5.2.2 Supersingular Curves 72

5.2.3 Non-Supersingular Curves 77

5.3 Cryptographic Implications 77

5.4 Finding the Group Structure 79

5.5 Notes 81

6 Implementation of Elliptic Curve Cryptosystems 83

6.1 Field Arithmetic in F_{2^m} 83

6.2 Selecting a Curve and Field K 86

6.3 Projective Coordinates 90

6.4 ElGamal Cryptosystem 91

6.5 Performance 92

6.6 Using Supersingular Curves 93

6.7 Elliptic Curve Cryptosystems over $\mathbb{Z}_n$ 97

6.8 Implementations 98

6.9 Notes 99

7 Counting Points on Elliptic Curves Over F_{2^m} 101

7.1 Some Basics 102

7.2 Outline of Schoof's Algorithm 103

7.3 Some Heuristics 104

7.3.1 Finding an Eigenvalue of ϕ, if One Exists 105

7.3.2 Schoof's Algorithm 106

7.3.3 Determining t modulo $l = 2^c$ 107

7.3.4 Baby-step Giant-step Algorithm 109

7.3.5 Checking Results 110

7.4 Implementation and Results 111

7.5 Recent Work 115

7.6 Notes 116

Bibliography 117

Index 127