

# Contents

|  |      |
|--|------|
| Preface  | xi   |
| Abbreviations and Standard Notation                      | xiii |
| Chapter I. Introduction                                  | 1    |
| I.1. Cryptography Based on Groups                        | 2    |
| I.2. What Types of Group are Used                        | 6    |
| I.3. What it Means in Practice                           | 8    |
| Chapter II. Finite Field Arithmetic                      | 11   |
| II.1. Fields of Odd Characteristic                       | 11   |
| II.2. Fields of Characteristic Two                       | 19   |
| Chapter III. Arithmetic on an Elliptic Curve             | 29   |
| III.1. General Elliptic Curves                           | 30   |
| III.2. The Group Law                                     | 31   |
| III.3. Elliptic Curves over Finite Fields                | 34   |
| III.4. The Division Polynomials                          | 39   |
| III.5. The Weil Pairing                                  | 42   |
| III.6. Isogenies, Endomorphisms and Torsion              | 44   |
| III.7. Various Functions and $q$ -Expansions             | 46   |
| III.8. Modular Polynomials and Variants                  | 50   |
| Chapter IV. Efficient Implementation of Elliptic Curves  | 57   |
| IV.1. Point Addition                                     | 57   |
| IV.2. Point Multiplication                               | 62   |
| IV.3. Frobenius Expansions                               | 73   |
| IV.4. Point Compression                                  | 76   |
| Chapter V. The Elliptic Curve Discrete Logarithm Problem | 79   |
| V.1. The Simplification of Pohlig and Hellman            | 80   |
| V.2. The MOV Attack                                      | 82   |
| V.3. The Anomalous Attack                                | 88   |
| V.4. Baby Step/Giant Step                                | 91   |
| V.5. Methods based on Random Walks                       | 93   |
| V.6. Index Calculus Methods                              | 97   |
| V.7. Summary   | 98   |



|   |     |
|---|-----|
| Chapter VI. Determining the Group Order   | 101 |
| VI.1. Main Approaches   | 101 |
| VI.2. Checking the Group Order  | 103 |
| VI.3. The Method of Shanks and Mestre   | 104 |
| VI.4. Subfield Curves   | 104 |
| VI.5. Searching for Good Curves   | 106 |
| Chapter VII. Schoof's Algorithm and Extensions  | 109 |
| VII.1. Schoof's Algorithm   | 109 |
| VII.2. Beyond Schoof  | 114 |
| VII.3. More on the Modular Polynomials  | 118 |
| VII.4. Finding Factors of Division Polynomials<br>through Isogenies: Odd Characteristic | 122 |
| VII.5. Finding Factors of Division Polynomials<br>through Isogenies: Characteristic Two | 133 |
| VII.6. Determining the Trace Modulo a Prime Power                                       | 138 |
| VII.7. The Elkies Procedure   | 139 |
| VII.8. The Atkin Procedure  | 140 |
| VII.9. Combining the Information from Elkies and Atkin Primes                           | 142 |
| VII.10. Examples  | 144 |
| VII.11. Further Discussion  | 147 |
| Chapter VIII. Generating Curves using Complex Multiplication                            | 149 |
| VIII.1. The Theory of Complex Multiplication  | 149 |
| VIII.2. Generating Curves over Large Prime Fields using CM                              | 151 |
| VIII.3. Weber Polynomials   | 155 |
| VIII.4. Further Discussion  | 157 |
| Chapter IX. Other Applications of Elliptic Curves                                       | 159 |
| IX.1. Factoring Using Elliptic Curves   | 159 |
| IX.2. The Pocklington-Lehmer Primality Test   | 162 |
| IX.3. The ECPP Algorithm  | 164 |
| IX.4. Equivalence between DLP and DHP   | 166 |
| Chapter X. Hyperelliptic Cryptosystems  | 171 |
| X.1. Arithmetic of Hyperelliptic Curves   | 171 |
| X.2. Generating Suitable Curves   | 173 |
| X.3. The Hyperelliptic Discrete Logarithm Problem                                       | 176 |
| Appendix A. Curve Examples  | 181 |
| A.1. Odd Characteristic   | 181 |
| A.2. Characteristic Two   | 186 |
| Bibliography  | 191 |
| Author Index  | 199 |



|   |     |
|---|-----|
| Chapter VI. Determining the Group Order   | 101 |
| VI.1. Main Approaches   | 101 |
| VI.2. Checking the Group Order  | 103 |
| VI.3. The Method of Shanks and Mestre   | 104 |
| VI.4. Subfield Curves   | 104 |
| VI.5. Searching for Good Curves   | 106 |
| Chapter VII. Schoof's Algorithm and Extensions  | 109 |
| VII.1. Schoof's Algorithm   | 109 |
| VII.2. Beyond Schoof  | 114 |
| VII.3. More on the Modular Polynomials  | 118 |
| VII.4. Finding Factors of Division Polynomials<br>through Isogenies: Odd Characteristic | 122 |
| VII.5. Finding Factors of Division Polynomials<br>through Isogenies: Characteristic Two | 133 |
| VII.6. Determining the Trace Modulo a Prime Power                                       | 138 |
| VII.7. The Elkies Procedure   | 139 |
| VII.8. The Atkin Procedure  | 140 |
| VII.9. Combining the Information from Elkies and Atkin Primes                           | 142 |
| VII.10. Examples  | 144 |
| VII.11. Further Discussion  | 147 |
| Chapter VIII. Generating Curves using Complex Multiplication                            | 149 |
| VIII.1. The Theory of Complex Multiplication  | 149 |
| VIII.2. Generating Curves over Large Prime Fields using CM                              | 151 |
| VIII.3. Weber Polynomials   | 155 |
| VIII.4. Further Discussion  | 157 |
| Chapter IX. Other Applications of Elliptic Curves                                       | 159 |
| IX.1. Factoring Using Elliptic Curves   | 159 |
| IX.2. The Pocklington-Lehmer Primality Test   | 162 |
| IX.3. The ECPP Algorithm  | 164 |
| IX.4. Equivalence between DLP and DHP   | 166 |
| Chapter X. Hyperelliptic Cryptosystems  | 171 |
| X.1. Arithmetic of Hyperelliptic Curves   | 171 |
| X.2. Generating Suitable Curves   | 173 |
| X.3. The Hyperelliptic Discrete Logarithm Problem                                       | 176 |
| Appendix A. Curve Examples  | 181 |
| A.1. Odd Characteristic   | 181 |
| A.2. Characteristic Two   | 186 |
| Bibliography  | 191 |
| Author Index  | 199 |