

contents

preface xii

author online and source code xiii

acknowledgments xiv

1 Introduction 1

1.1 Some initial comments 2

1.2 Why elliptic curves? 4

1.3 Orders of magnitude 4

1.4 About this book 7

1.5 Why C? 11

1.6 Comments on style 12

1.7 References 12

2 Basics of number theory 13

2.1 Large integer math header 14

2.2 Large integer math routines 19
Multiplication 21, Division 23

2.3 Large integer code example 27

2.4 Back to number theory 29

2.5 Greatest common factor 30

2.6 Modular arithmetic 37

2.7 Fermat's Theorem 39

2.8	Finite fields	40
2.9	Generators	43
2.10	References	44
3	Polynomial math over finite fields	47
3.1	Introduction to polynomials	48
3.2	All structures are polynomials	52
	Polynomial addition	54,
	Polynomial multiplication	55,
	Polynomial division	58
3.3	Modular polynomial arithmetic	64
3.4	Inversion over prime polynomials	66
3.5	Polynomial greatest common divisor	67
3.6	Prime polynomials	68
3.7	Summary	72
3.8	References	72
4	Normal basis mathematics	75
4.1	What is a normal basis?	76
4.2	Squaring normal basis numbers	78
4.3	Multiplication in theory	78
4.4	Type I optimal normal basis	80
4.5	Type II optimal normal basis	85
4.6	Multiplication in practice	92
4.7	Inversion over optimal normal basis	97
4.8	References	102
5	Elliptic curves	103
5.1	Mathematics of elliptic curves over real numbers	104
5.2	Mathematics of elliptic curves over prime fields	108
5.3	Mathematics of elliptic curves over Galois Fields	109
5.4	Polynomial basis elliptic curve subroutines	114
5.5	Optimal normal basis elliptic curve subroutines	118

5.6	Multiplication over elliptic curves	120
5.7	Balanced integer conversion code	122
5.8	Following the balanced representation	125
5.9	References	126
6	Cryptography	129
6.1	Fundamentals of elliptic curve cryptography	131
6.2	Choosing an elliptic curve	132
6.3	Nonsupersingular curves	133
6.4	Embedding data on a curve	136
6.5	Solving quadratic equations in binary fields	137
6.6	The Trace function	138
6.7	Solving quadratic equations in normal basis	141
6.8	Solving quadratic equations in polynomial basis	148
6.9	Quadratic polynomials: the code	149
6.10	Using the T matrix	158
6.11	Embedding data using polynomial basis	161
6.12	Summary of quadratic solving	162
6.13	References	163
7	Simple protocols	165
7.1	Introduction	166
7.2	Random bit generator	168
7.3	Choosing random curves	171
7.4	Protocols	174
	Diffie-Hellman	174,
	ElGamal Protocol	180,
	Menezes-Qu-Vanston	key agreement scheme 188
7.5	References	197
8	Elliptic curve encryption	199
8.1	Introduction to ECES	200
8.2	Mask generation function	202
8.3	Hash function SHA-1	203

- 8.4 Mask generation: the code 210
- 8.5 ECES: the code 212
 - Polynomial basis 212, Normal basis 216
- 8.6 References 219

9 Advanced protocols, key exchange 221

- 9.1 Preliminaries for key exchange 222
- 9.2 Polynomial solution to $\gamma^3 = \gamma + 1$ 226
- 9.3 Massey-Omura protocol 234
 - Massey-Omura: the code 236
- 9.4 MQV: the standard 244
 - MQV: normal basis version 246, MQV: polynomial basis version 250
- 9.5 References 254

Advanced protocols, signatures 255

- 10.1 Introduction to digital signatures 256
- 10.2 Message hash 259
- 10.3 Nyberg-Rueppel signature scheme 260
 - Nyberg-Rueppel signature: normal basis 261, Nyberg-Rueppel: polynomial basis 267
- 10.4 Digital Signature Algorithm (DSA) 271
 - DSA in normal basis 273, DSA: polynomial basis 278
- 10.5 Signatures: a summary 282
- 10.6 References 282

The bleeding edge 283

- 11.1 High-speed inversion for ONB 284
- 11.2 Faster inversion, preliminary subroutines 288
 - Faster inversion, the code 292
- 11.3 Security from cryptography 297
- 11.4 Counting points 298
- 11.5 Polynomials: base p 299

- 11.6 Hyperelliptic curves 299

- 11.7 References 300

12 A simple application 301

- 12.1 Personal security example 302
- 12.2 Security analysis 305
- 12.3 Putting it all together 305
- 12.4 References 307

index 309