

# Contents

<b>List of Algorithms</b>	<b>ix</b>
<b>List of Tables</b>	<b>xiv</b>
<b>List of Figures</b>	<b>xvi</b>
<b>Acronyms</b>	<b>xvii</b>
<b>Preface</b>	<b>xix</b>
<b>1 Introduction and Overview</b>	<b>1</b>
1.1 Cryptography basics . . . . .	2
1.2 Public-key cryptography . . . . .	6
1.2.1 RSA systems . . . . .	6
1.2.2 Discrete logarithm systems . . . . .	8
1.2.3 Elliptic curve systems . . . . .	11
1.3 Why elliptic curve cryptography? . . . . .	15
1.4 Roadmap . . . . .	19
1.5 Notes and further references . . . . .	21
<b>2 Finite Field Arithmetic</b>	<b>25</b>
2.1 Introduction to finite fields . . . . .	25
2.2 Prime field arithmetic . . . . .	29
2.2.1 Addition and subtraction . . . . .	30
2.2.2 Integer multiplication . . . . .	31
2.2.3 Integer squaring . . . . .	34
2.2.4 Reduction . . . . .	35
2.2.5 Inversion . . . . .	39
2.2.6 NIST primes . . . . .	44

2.3	Binary field arithmetic . . . . .	47
2.3.1	Addition . . . . .	47
2.3.2	Multiplication . . . . .	48
2.3.3	Polynomial multiplication . . . . .	48
2.3.4	Polynomial squaring . . . . .	52
2.3.5	Reduction . . . . .	53
2.3.6	Inversion and division . . . . .	57
2.4	Optimal extension field arithmetic . . . . .	62
2.4.1	Addition and subtraction . . . . .	63
2.4.2	Multiplication and reduction . . . . .	63
2.4.3	Inversion . . . . .	67
2.5	Notes and further references . . . . .	69
<b>3</b>	<b>Elliptic Curve Arithmetic</b> . . . . .	<b>75</b>
3.1	Introduction to elliptic curves . . . . .	76
3.1.1	Simplified Weierstrass equations . . . . .	78
3.1.2	Group law . . . . .	79
3.1.3	Group order . . . . .	82
3.1.4	Group structure . . . . .	83
3.1.5	Isomorphism classes . . . . .	84
3.2	Point representation and the group law . . . . .	86
3.2.1	Projective coordinates . . . . .	86
3.2.2	The elliptic curve $y^2 = x^3 + ax + b$ . . . . .	89
3.2.3	The elliptic curve $y^2 + xy = x^3 + ax^2 + b$ . . . . .	93
3.3	Point multiplication . . . . .	95
3.3.1	Unknown point . . . . .	96
3.3.2	Fixed point . . . . .	103
3.3.3	Multiple point multiplication . . . . .	109
3.4	Koblitz curves . . . . .	114
3.4.1	The Frobenius map and the ring $\mathbb{Z}[\tau]$ . . . . .	114
3.4.2	Point multiplication . . . . .	119
3.5	Curves with efficiently computable endomorphisms . . . . .	123
3.6	Point multiplication using halving . . . . .	129
3.6.1	Point halving . . . . .	130
3.6.2	Performing point halving efficiently . . . . .	132
3.6.3	Point multiplication . . . . .	137
3.7	Point multiplication costs . . . . .	141
3.8	Notes and further references . . . . .	147

<b>4</b>	<b>Cryptographic Protocols</b>	<b>153</b>
4.1	The elliptic curve discrete logarithm problem . . . . .	153
4.1.1	Pohlig-Hellman attack . . . . .	155
4.1.2	Pollard’s rho attack . . . . .	157
4.1.3	Index-calculus attacks . . . . .	165
4.1.4	Isomorphism attacks . . . . .	168
4.1.5	Related problems . . . . .	171
4.2	Domain parameters . . . . .	172
4.2.1	Domain parameter generation and validation . . . . .	173
4.2.2	Generating elliptic curves verifiably at random . . . . .	175
4.2.3	Determining the number of points on an elliptic curve . . . . .	179
4.3	Key pairs . . . . .	180
4.4	Signature schemes . . . . .	183
4.4.1	ECDSA . . . . .	184
4.4.2	EC-KCDSA . . . . .	186
4.5	Public-key encryption . . . . .	188
4.5.1	ECIES . . . . .	189
4.5.2	PSEC . . . . .	191
4.6	Key establishment . . . . .	192
4.6.1	Station-to-station . . . . .	193
4.6.2	ECMQV . . . . .	195
4.7	Notes and further references . . . . .	196
<b>5</b>	<b>Implementation Issues</b>	<b>205</b>
5.1	Software implementation . . . . .	206
5.1.1	Integer arithmetic . . . . .	206
5.1.2	Floating-point arithmetic . . . . .	209
5.1.3	SIMD and field arithmetic . . . . .	213
5.1.4	Platform miscellany . . . . .	215
5.1.5	Timings . . . . .	219
5.2	Hardware implementation . . . . .	224
5.2.1	Design criteria . . . . .	226
5.2.2	Field arithmetic processors . . . . .	229
5.3	Secure implementation . . . . .	238
5.3.1	Power analysis attacks . . . . .	239
5.3.2	Electromagnetic analysis attacks . . . . .	244
5.3.3	Error message analysis . . . . .	244
5.3.4	Fault analysis attacks . . . . .	248
5.3.5	Timing attacks . . . . .	250
5.4	Notes and further references . . . . .	250

<b>A</b>	<b>Sample Parameters</b>	<b>257</b>
A.1	Irreducible polynomials . . . . .	257
A.2	Elliptic curves . . . . .	261
A.2.1	Random elliptic curves over $\mathbb{F}_p$ . . . . .	261
A.2.2	Random elliptic curves over $\mathbb{F}_{2^m}$ . . . . .	263
A.2.3	Koblitz elliptic curves over $\mathbb{F}_{2^m}$ . . . . .	263
<b>B</b>	<b>ECC Standards</b>	<b>267</b>
<b>C</b>	<b>Software Tools</b>	<b>271</b>
C.1	General-purpose tools . . . . .	271
C.2	Libraries . . . . .	273
	<b>Bibliography</b>	<b>277</b>
	<b>Index</b>	<b>305</b>



<http://www.springer.com/978-0-387-95273-4>

Guide to Elliptic Curve Cryptography  
Hankerson, D.; Menezes, A.J.; Vanstone, S.  
2004, XX, 312 p., Hardcover  
ISBN: 978-0-387-95273-4