

AREHCC Project

IST - 2001 - 32613

**Advanced Research on
Elliptic and Hyperelliptic Curve Cryptography**

WP1 - State of the Art

Elliptic and Hyperelliptic Curve Cryptography

Version 25-06-2002

Contents

- Introduction** 1
 - Problems assumed to be hard 2
 - Structure of the report 3
 - Contributions of partners 4

- 1 Discrete Logarithm Systems** 5
 - 1.1 Why discrete logarithms? 5
 - 1.2 Why groups? 6

- 2 Integer Arithmetic** 9
 - 2.1 Multiprecision integers 9
 - 2.2 Addition and subtraction 10
 - 2.3 Multiplication 12
 - 2.3.1 Schoolbook multiplication 12
 - 2.3.2 Karatsuba multiplication 13
 - 2.3.3 Recursive middle product 14
 - 2.3.4 Squaring 15
 - 2.4 Division 16
 - 2.4.1 Short division 16
 - 2.4.2 Schoolbook division 17
 - 2.4.3 Recursive division 19
 - 2.4.4 Multiplication by the inverse 20
 - 2.4.5 Recursive Middle Product division 21
 - 2.4.6 Exact division 23

- 3 Exponentiation** 27
 - 3.1 Generic methods 27
 - 3.1.1 Binary methods 27
 - 3.1.2 Left-to-right 2^k -ary algorithm 29
 - 3.1.3 Sliding window method 30

3.1.4	Signed–digit recoding	31
3.1.5	Simultaneous exponentiation	32
3.2	Specific methods	33
3.2.1	Fixed exponent	33
3.2.1.a	Exponentiation with addition chains	34
3.2.1.b	Addition chain search	36
3.2.1.c	Addition–subtraction chain search	37
3.2.1.d	Addition sequences and vectorial addition chains search	39
3.2.2	Fixed base point	41
3.2.2.a	BGMW method	41
3.2.2.b	Euclidean method	42
3.2.2.c	Lim–Lee method	43
4	Finite Field Arithmetic	45
4.1	Overview of finite fields	45
4.2	Arithmetic over \mathbb{F}_p	46
4.2.1	Reduction and representations	46
4.2.1.a	Barrett and Montgomery methods	46
4.2.1.b	Special moduli	48
4.2.2	Addition and subtraction	48
4.2.3	Multiplication	49
4.2.3.a	Ordinary multiplication	49
4.2.3.b	Barrett and Quisquater multiplications	50
4.2.3.c	Montgomery multiplication	52
4.2.3.d	Modular squaring	53
4.2.4	Inversion and division	53
4.2.4.a	Euclid extended gcd	54
4.2.4.b	Lehmer extended gcd	55
4.2.4.c	Binary extended gcd	57
4.2.4.d	Montgomery inversion and division	59
4.2.5	Exponentiation	60
4.2.5.a	Ordinary exponentiation	60
4.2.5.b	Montgomery exponentiation	60
4.3	Arithmetic over \mathbb{F}_{2^d}	61
4.3.1	Representations	61
4.3.1.a	Polynomial representation	62
4.3.1.b	Normal basis	62
4.3.2	Addition	63

4.3.3	Multiplication	63
4.3.3.a	Ordinary multiplication	63
4.3.3.b	Optimal normal basis	64
4.3.3.c	Normal bases generated by Gauß periods	65
4.3.4	Inversion and division	67
4.3.4.a	Euclid extended gcd	67
4.3.4.b	Inversion based on Fermat's theorem	68
4.3.5	Exponentiation	69
4.3.5.a	Modular composition and Shoup's algorithm	69
4.3.5.b	Normal basis representation and q -th powers	71
5	Generic Attacks	73
5.1	Exponential time methods (square-root algorithms)	73
5.1.1	Brute force (exhaustive search)	74
5.1.2	Chinese remaindering	74
5.1.3	Baby-steps, giant-steps	75
5.1.3.a	Changing the giant step width dynamically	75
5.1.3.b	Smaller intervals and parallelization	76
5.1.4	Pollard's rho methods	76
5.1.4.a	Detecting cycles	77
5.1.4.b	Application to DLs	78
5.1.4.c	Better random walks and group orders	79
5.1.4.d	Parallelization	79
5.1.4.e	Inverse-point strategy	80
5.1.5	Catching kangaroos	80
5.1.5.a	Parallelization	81
5.2	Index calculus	83
5.2.1	Arithmetical formations	84
5.2.2	Examples of formations	85
5.2.3	The algorithm	85
5.2.4	An important example: finite fields	87
6	Elliptic Curves	89
6.1	Mathematical background	89
6.1.1	Elliptic functions, lattices and elliptic curves	89
6.1.2	Isomorphisms	90
6.1.3	Group law	91
6.1.4	Isogenies	93

6.1.5	Endomorphisms	95
6.1.6	Cardinality	96
6.2	Arithmetic of elliptic curves defined over \mathbb{F}_p	97
6.2.1	Choice of the coordinates	97
6.2.1.a	Affine coordinates	98
6.2.1.b	Projective coordinates	98
6.2.1.c	Jacobian and Chudnovsky Jacobian coordinates	98
6.2.1.d	Modified Jacobian coordinates	99
6.2.2	Efficient multiplication using mixed coordinates	99
6.2.3	Montgomery form	100
6.3	Arithmetic of elliptic curves defined over \mathbb{F}_{2^d}	102
6.3.1	Generic curves	102
6.3.1.a	Direct formulae for $2^j P$	102
6.3.1.b	Montgomery scalar multiplication	103
6.3.2	Koblitz curves	103
7	Hyperelliptic Curves	107
7.1	Mathematical background	107
7.1.1	Definition	108
7.1.2	Ideal class group	108
7.1.3	Divisor class group	109
7.1.4	Jacobian variety and Frobenius endomorphism	110
7.2	Arithmetic in the ideal class group	111
7.2.1	Arithmetic	111
7.2.2	Compression	112
7.2.3	Fast computation of scalar multiples on special curves	113
7.2.3.a	Computing τ -adic expansions	114
7.2.3.b	Density of the expansion	117
7.2.3.c	Comparison	118
7.2.3.d	Alternative set-up	119
7.2.4	Appendix: Explicit addition formula	120
8	Counting Points on Arbitrary Curves	125
8.1	The Schoof–Elkies–Atkin algorithm	126
8.1.1	Schoof’s algorithm	126
8.1.2	Elkies and Atkin primes	127
8.1.3	Complete SEA-algorithm	128
8.1.4	Larger genus	129

8.2	Satoh's algorithm	129
8.2.1	Computations in the ring \mathbb{Z}_q	129
8.2.2	Canonical lift and Satoh's idea	130
8.2.3	Improvements	132
8.3	AGM method	134
8.4	Subfield curves	136
8.4.1	Computing $P(T)$	137
8.4.2	Group order over extension fields	137
8.5	Kedlaya's algorithm and extensions	138
8.5.1	Monsky-Washnitzer cohomology	139
8.5.2	Overview of Kedlaya's construction	140
8.5.3	Cohomology of hyperelliptic curves over \mathbb{F}_{2^n}	141
9	Complex Multiplication	149
9.1	CM for elliptic curves	149
9.1.1	Complex multiplication and class field theory	149
9.1.1.a	Computation of class polynomials	150
9.1.1.b	Other computational aspects	151
9.1.2	Computation of the number of points over prime fields	151
9.1.3	Experimental results	153
9.2	CM for curves of genus ≥ 2	153
9.2.1	Principally polarized abelian varieties over \mathbb{C}	155
9.2.2	Abelian varieties with complex multiplication	156
9.2.3	Computation of the number of points over prime fields	158
9.2.4	Computing the curve	158
10	Transfers via Galois Action	161
10.1	Tate duality of abelian varieties	161
10.1.1	The additive case	162
10.1.2	The multiplicative case	162
10.1.2.a	Application to Jacobian varieties over finite fields	163
10.1.3	Computation of the duality pairing	164
10.1.3.a	The additive pairing	165
10.1.3.b	The multiplicative pairing	165
10.2	Transfer by Weil descent	166

11 Security of Elliptic Curve Cryptosystems	169
11.1 Singular curves	169
11.2 Review of the transfers to a finite field	169
11.2.1 The additive case	170
11.2.2 The multiplicative case	170
11.3 Transfer by Weil descent	172
11.3.1 The genus of \mathcal{C} in the GHS attack.	174
11.3.2 Effectiveness	176
11.3.2.a The case where n is prime.	176
11.3.2.b The case where n is composite.	176
11.4 Failure of index and Xedni calculus	177
11.4.1 Index calculus	177
11.4.2 Xedni calculus	178
11.5 Automorphisms of the group	180
11.6 Conclusions	182
12 Security of Hyperelliptic Curve Cryptosystems	185
12.1 Transfers to a finite field	185
12.2 Weil descent	185
12.3 Index calculus	186
12.4 Automorphisms of the group	187
12.4.1 Speeding-up Pollard's methods	187
12.4.2 Speeding-up the index calculus	188
12.5 Conclusions	189
13 Smart Cards Presentation	191
13.1 History	191
13.2 Smart Card Specifications	192
13.2.1 Definition and properties	192
13.2.2 Physical properties	192
13.2.3 The chip module and its embedding	194
13.2.4 Contact and contactless	196
13.2.5 Memory only cards (also called synchronous cards)	197
13.2.6 Microprocessor cards (also called asynchronous cards)	198
13.3 Products and future	199

14 Microprocessor Cards And Software	201
14.1 Microprocessor types	201
14.1.1 Generalities	201
14.1.2 Intel 8051 derivatives	202
14.1.3 Motorola 6805 derivative	204
14.1.4 RISC architectures	205
14.1.5 Coprocessors necessity	206
14.2 Cryptology and smart cards.	206
14.2.1 Cryptology	206
14.2.2 Symmetric algorithms	207
14.2.3 Asymmetric algorithms.	208
14.2.4 Hash algorithms	213
14.3 Environment and softwares	214
14.3.1 The Operating System (OS)	214
14.3.2 The Java Card	216
14.3.3 Development of cryptographic libraries	217
15 Attacks On Smart Cards	219
15.1 Invasive attacks	219
15.2 Non Invasive attacks	220
15.2.1 Timing attacks	220
15.2.2 Power consumption attacks	222
15.2.3 Electromagnetic radiation attacks	225
15.2.4 DFA attacks	225
16 Memory	227
16.1 Read-only Memory (ROM)	227
16.2 Random Access Memory (RAM)	228
16.3 Programmable Read-only Memory (PROM)	228
16.4 Erasable Programmable Read-only Memory (EPROM)	228
16.5 Electrically Erasable Programmable Read-only Memory (EEPROM)	230
16.6 Flash Electrically Erasable Programmable Read-only Memory (Flash EEPROM)	231
16.7 Ferroelectric Random-access Memory (FRAM)	231
16.7.1 Writing Data to a FRAM Cell	234
16.7.2 Reading Data from a FRAM Cell.	234

17 Electrical properties	237
17.1 Connections	237
17.2 Supply Voltage	238
17.3 Supply Current	238
17.4 External Clock	241
17.5 Activation and De-activation Sequences	241
18 Transmission Protocols	243
18.1 The Open System Interconnection (OSI) Reference Model	244
18.2 $T = 0$	244
18.3 $T = 1$	247
18.3.1 Prologue field (mandatory)	247
18.3.2 Information field (optional)	248
18.3.3 Epilogue field (mandatory)	248
18.3.4 Character Waiting Time (CWT)	248
18.3.5 Block Waiting Time (BWT) and Block Guardtime (BGT)	248
18.3.6 Information Field Size (IFS)	249
18.3.7 Error Detection Code (EDC)	249
18.3.8 Chaining	250
18.4 $T = CL$	250
18.4.1 Prologue field (mandatory)	251
18.4.2 Information field (optional)	251
18.4.3 Epilogue field (mandatory)	251
18.4.4 Frame Waiting Time (FWT)	251
18.4.5 Chaining	252
19 Supplementary Hardware	253
19.1 Memory management unit	253
19.2 Interfaces	257
19.2.1 UART	257
19.2.2 USB	260
19.2.3 Contactless smart card	262
20 Fast Arithmetic in Hardware	267
20.1 Introduction	267
20.2 Complement Representations of Signed Numbers	268
20.3 The Operation $X \times Y + Z$	269
20.3.1 Multiplication Using Left Shifts	270
20.3.2 Multiplication Using Right Shifts	270

20.4	Reducing the Number of Partial Products	272
20.4.1	Booth Encoding	272
20.4.1.a	Radix-4 Signed Digit Recoding	273
20.4.1.b	Radix-8 Recoding	274
20.4.2	Canonical Encoding	275
20.4.2.a	Some Comparisons	275
20.5	Accumulation of Partial Products	277
20.5.1	Full Adders	277
20.5.2	Faster Carry Propagation	278
20.5.2.a	Carry-look-ahead Adders	278
20.5.2.b	Carry-Look-ahead Adders Arranged in Groups	279
20.5.2.c	Conditional-Sum-Adders and Carry-Select Adders	280
20.5.2.d	Carry-Skip Adders	280
20.5.3	Analysis of Carry Propagation	281
20.5.4	Multi Operand Operations	283
20.5.4.a	Carry-Save-Adders	283
20.5.4.b	Accumulation of Partial Products Using Carry-Save-Adders	284
20.5.5	Array Multipliers	288
20.5.6	Pipelining	290
20.6	Modular Arithmetic over $GF(p)$ in Hardware	292
20.6.1	Design Considerations	292
20.6.2	Implementational Considerations for the Wordwise Approach	293
20.6.3	Barret and Quisquater Modular Multiplication	293
20.6.4	Montgomery Modular Multiplication	295
20.7	Fields of Characteristic 2	297
20.7.1	Bit Serial Multipliers	298
20.7.1.a	Polynomial Basis	298
20.7.1.b	Normal Basis	300
20.7.2	Hybrid Multipliers	301
20.8	Unified Multipliers	302
21	Cryptographic Coprocessors	305
22	Implementation of ECC and HEC in Hardware	307
22.1	Efficient Implementations of ECC	307
22.1.1	Implementations in Software	307
22.1.1.a	Implementations over Prime Fields	307
22.1.1.b	Implementations over Binary Fields	309

22.1.2	Implementations in Hardware Without Coprocessor	310
22.1.2.a	Implementations on 8-bit platforms	310
22.1.2.b	Implementations on 16- and 32-bit platforms	315
22.1.3	Implementations in Hardware Using Coprocessors	317
22.1.3.a	Implementations Using Special Fields	317
22.1.3.b	Implementations Using Finite Fields of General Type	318
22.2	Implementations of HEC	318
22.2.1	Implementation in Software	318
22.2.2	Implementations in Hardware	320
23	ECC Standards	323
23.1	Generalities	323
23.1.1	Mathematical objects	323
23.2	SEC 1	324
23.2.1	Domain parameters and Primitives	324
23.2.2	Schemes	326
23.3	SEC 2	328
23.4	IEEE Std 1363-2000	329
23.4.1	Mathematical Conventions	330
23.4.2	Auxiliary Functions	332
23.4.3	Message-encoding Methods	333
23.4.4	Elliptic Curve Primitives	334
23.4.5	Other Primitives	336
23.4.6	Key Agreement Schemes	338
23.4.7	Signature Schemes	339
23.4.8	Encryption Schemes	340
23.5	IEEE P1363a, Draft	341
23.5.1	Mathematical Conventions	341
23.5.2	Auxiliary Functions	342
23.5.3	Message-encoding methods	343
23.5.4	Elliptic Curve Primitives	344
23.5.5	Other Primitives	345
23.5.6	Key agreement schemes	346
23.5.7	Signature schemes	346
23.5.8	Encryption schemes	347
23.6	The ANSI X9.62 and X9.63 Standards	348
23.6.1	Mathematical Ingredients	348
23.6.2	Elliptic Curve Domain Parameters	349

23.6.3 Key pairs	351
23.7 ANSI X9.62	351
23.8 ANSI X9.63	353
23.8.1 Primitives	353
23.8.2 Key Agreement Schemes	356
23.8.3 Key Transport Schemes	363
24 Legal Aspects of Cryptography	365
24.1 Introduction	365
24.2 The Wassenaar Arrangement	365
24.3 European Union Regulation	367
24.4 Summary of the different foreign regulations	367
24.5 A few details on each country	371
Bibliography	377