

This is the Table of Contents of the Handbook of Elliptic and Hyperelliptic Curve Cryptography, Henri Cohen, Christophe Doche, and Gerhard Frey, Editors, CRC Press 2006.

CRC Press has granted the following specific permissions for the electronic version of this book: Permission is granted to retrieve a copy of this chapter for personal use. This permission does not extend to binding multiple chapters of the book, photocopying or producing copies for other than personal use of the person creating the copy, or making electronic copies available for retrieval by others without prior permission in writing from CRC Press.

The standard copyright notice from CRC Press applies to this electronic version: Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, without prior permission in writing from the publisher.

The consent of CRC Press does not extend to copying for general distribution, for promotion, for creating new works, or for resale. Specific permission must be obtained in writing from CRC Press for such copying.

© 2006 by CRC Press, LLC.

Table of Contents

| | |
|--|--------------|
| List of Algorithms | xxiii |
| Preface | xxix |
| 1 Introduction to Public-Key Cryptography | 1 |
| 1.1 Cryptography | 2 |
| 1.2 Complexity | 2 |
| 1.3 Public-key cryptography | 5 |
| 1.4 Factorization and primality | 6 |
| 1.4.1 Primality | 6 |
| 1.4.2 Complexity of factoring | 6 |
| 1.4.3 RSA | 7 |
| 1.5 Discrete logarithm systems | 8 |
| 1.5.1 Generic discrete logarithm systems | 8 |
| 1.5.2 Discrete logarithm systems with bilinear structure | 9 |
| 1.6 Protocols | 9 |
| 1.6.1 Diffie–Hellman key exchange | 10 |
| 1.6.2 Asymmetric Diffie–Hellman and ElGamal encryption | 10 |
| 1.6.3 Signature scheme of ElGamal-type | 12 |
| 1.6.4 Tripartite key exchange | 13 |
| 1.7 Other problems | 14 |

I Mathematical Background

| | |
|--|-----------|
| 2 Algebraic Background | 19 |
| 2.1 Elementary algebraic structures | 19 |
| 2.1.1 Groups | 19 |
| 2.1.2 Rings | 21 |
| 2.1.3 Fields | 23 |
| 2.1.4 Vector spaces | 24 |
| 2.2 Introduction to number theory | 24 |
| 2.2.1 Extension of fields | 25 |
| 2.2.2 Algebraic closure | 27 |
| 2.2.3 Galois theory | 27 |
| 2.2.4 Number fields | 29 |
| 2.3 Finite fields | 31 |
| 2.3.1 First properties | 31 |
| 2.3.2 Algebraic extensions of a finite field | 32 |
| 2.3.3 Finite field representations | 33 |
| 2.3.4 Finite field characters | 35 |

| | | |
|----------|---|-----------|
| 3 | Background on p-adic Numbers | 39 |
| 3.1 | Definition of \mathbb{Q}_p and first properties | 39 |
| 3.2 | Complete discrete valuation rings and fields | 41 |
| 3.2.1 | First properties | 41 |
| 3.2.2 | Lifting a solution of a polynomial equation | 42 |
| 3.3 | The field \mathbb{Q}_p and its extensions | 43 |
| 3.3.1 | Unramified extensions | 43 |
| 3.3.2 | Totally ramified extensions | 43 |
| 3.3.3 | Multiplicative system of representatives | 44 |
| 3.3.4 | Witt vectors | 44 |
| 4 | Background on Curves and Jacobians | 45 |
| 4.1 | Algebraic varieties | 45 |
| 4.1.1 | Affine and projective varieties | 46 |
| 4.2 | Function fields | 51 |
| 4.2.1 | Morphisms of affine varieties | 52 |
| 4.2.2 | Rational maps of affine varieties | 53 |
| 4.2.3 | Regular functions | 54 |
| 4.2.4 | Generalization to projective varieties | 55 |
| 4.3 | Abelian varieties | 55 |
| 4.3.1 | Algebraic groups | 55 |
| 4.3.2 | Birational group laws | 56 |
| 4.3.3 | Homomorphisms of abelian varieties | 57 |
| 4.3.4 | Isomorphisms and isogenies | 58 |
| 4.3.5 | Points of finite order and Tate modules | 60 |
| 4.3.6 | Background on ℓ -adic representations | 61 |
| 4.3.7 | Complex multiplication | 63 |
| 4.4 | Arithmetic of curves | 64 |
| 4.4.1 | Local rings and smoothness | 64 |
| 4.4.2 | Genus and Riemann–Roch theorem | 66 |
| 4.4.3 | Divisor class group | 76 |
| 4.4.4 | The Jacobian variety of curves | 77 |
| 4.4.5 | Jacobian variety of elliptic curves and group law | 79 |
| 4.4.6 | Ideal class group | 81 |
| 4.4.7 | Class groups of hyperelliptic curves | 83 |
| 5 | Varieties over Special Fields | 87 |
| 5.1 | Varieties over the field of complex numbers | 87 |
| 5.1.1 | Analytic varieties | 87 |
| 5.1.2 | Curves over \mathbb{C} | 89 |
| 5.1.3 | Complex tori and abelian varieties | 92 |
| 5.1.4 | Isogenies of abelian varieties over \mathbb{C} | 94 |
| 5.1.5 | Elliptic curves over \mathbb{C} | 95 |
| 5.1.6 | Hyperelliptic curves over \mathbb{C} | 100 |
| 5.2 | Varieties over finite fields | 108 |
| 5.2.1 | The Frobenius morphism | 109 |
| 5.2.2 | The characteristic polynomial of the Frobenius endomorphism | 109 |
| 5.2.3 | The theorem of Hasse–Weil for Jacobians | 110 |
| 5.2.4 | Tate’s isogeny theorem | 112 |

| | | |
|----------|---|------------|
| 6 | Background on Pairings | 115 |
| 6.1 | General duality results | 115 |
| 6.2 | The Tate pairing | 116 |
| 6.3 | Pairings over local fields | 117 |
| 6.3.1 | The local Tate pairing | 118 |
| 6.3.2 | The Lichtenbaum pairing on Jacobian varieties | 119 |
| 6.4 | An explicit pairing | 122 |
| 6.4.1 | The Tate–Lichtenbaum pairing | 122 |
| 6.4.2 | Size of the embedding degree | 123 |
| 7 | Background on Weil Descent | 125 |
| 7.1 | Affine Weil descent | 125 |
| 7.2 | The projective Weil descent | 127 |
| 7.3 | Descent by Galois theory | 128 |
| 7.4 | Zariski closed subsets inside of the Weil descent | 129 |
| 7.4.1 | Hyperplane sections | 129 |
| 7.4.2 | Trace zero varieties | 130 |
| 7.4.3 | Covers of curves | 131 |
| 7.4.4 | The GHS approach | 131 |
| 8 | Cohomological Background on Point Counting | 133 |
| 8.1 | General principle | 133 |
| 8.1.1 | Zeta function and the Weil conjectures | 134 |
| 8.1.2 | Cohomology and Lefschetz fixed point formula | 135 |
| 8.2 | Overview of ℓ -adic methods | 137 |
| 8.3 | Overview of p -adic methods | 138 |
| 8.3.1 | Serre–Tate canonical lift | 138 |
| 8.3.2 | Monsky–Washnitzer cohomology | 139 |

II Elementary Arithmetic

| | | |
|----------|--------------------------------------|------------|
| 9 | Exponentiation | 145 |
| 9.1 | Generic methods | 146 |
| 9.1.1 | Binary methods | 146 |
| 9.1.2 | Left-to-right 2^k -ary algorithm | 148 |
| 9.1.3 | Sliding window method | 149 |
| 9.1.4 | Signed-digit recoding | 150 |
| 9.1.5 | Multi-exponentiation | 154 |
| 9.2 | Fixed exponent | 157 |
| 9.2.1 | Introduction to addition chains | 157 |
| 9.2.2 | Short addition chains search | 160 |
| 9.2.3 | Exponentiation using addition chains | 163 |
| 9.3 | Fixed base point | 164 |
| 9.3.1 | Yao’s method | 165 |
| 9.3.2 | Euclidean method | 166 |
| 9.3.3 | Fixed-base comb method | 166 |

| | |
|--|------------|
| 10 Integer Arithmetic | 169 |
| 10.1 Multiprecision integers. | 170 |
| 10.1.1 Introduction. | 170 |
| 10.1.2 Internal representation | 171 |
| 10.1.3 Elementary operations. | 172 |
| 10.2 Addition and subtraction | 172 |
| 10.3 Multiplication | 174 |
| 10.3.1 Schoolbook multiplication | 174 |
| 10.3.2 Karatsuba multiplication | 176 |
| 10.3.3 Squaring | 177 |
| 10.4 Modular reduction | 178 |
| 10.4.1 Barrett method. | 178 |
| 10.4.2 Montgomery reduction. | 180 |
| 10.4.3 Special moduli. | 182 |
| 10.4.4 Reduction modulo several primes | 184 |
| 10.5 Division | 184 |
| 10.5.1 Schoolbook division | 185 |
| 10.5.2 Recursive division | 187 |
| 10.5.3 Exact division | 189 |
| 10.6 Greatest common divisor | 190 |
| 10.6.1 Euclid extended gcd | 191 |
| 10.6.2 Lehmer extended gcd | 192 |
| 10.6.3 Binary extended gcd | 194 |
| 10.6.4 Chinese remainder theorem | 196 |
| 10.7 Square root | 197 |
| 10.7.1 Integer square root | 197 |
| 10.7.2 Perfect square detection | 198 |
| 11 Finite Field Arithmetic | 201 |
| 11.1 Prime fields of odd characteristic. | 201 |
| 11.1.1 Representations and reductions | 202 |
| 11.1.2 Multiplication | 202 |
| 11.1.3 Inversion and division | 205 |
| 11.1.4 Exponentiation. | 209 |
| 11.1.5 Squares and square roots | 210 |
| 11.2 Finite fields of characteristic 2 | 213 |
| 11.2.1 Representation | 213 |
| 11.2.2 Multiplication | 218 |
| 11.2.3 Squaring | 221 |
| 11.2.4 Inversion and division | 222 |
| 11.2.5 Exponentiation | 225 |
| 11.2.6 Square roots and quadratic equations | 228 |
| 11.3 Optimal extension fields | 229 |
| 11.3.1 Introduction | 229 |
| 11.3.2 Multiplication | 231 |
| 11.3.3 Exponentiation. | 231 |
| 11.3.4 Inversion | 233 |
| 11.3.5 Squares and square roots | 234 |
| 11.3.6 Specific improvements for degrees 3 and 5 | 235 |

| | |
|---|------------|
| 12 Arithmetic of p-adic Numbers | 239 |
| 12.1 Representation | 239 |
| 12.1.1 Introduction | 239 |
| 12.1.2 Computing the Teichmüller modulus | 240 |
| 12.2 Modular arithmetic | 244 |
| 12.2.1 Modular multiplication | 244 |
| 12.2.2 Fast division with remainder | 244 |
| 12.3 Newton lifting | 246 |
| 12.3.1 Inverse | 247 |
| 12.3.2 Inverse square root | 248 |
| 12.3.3 Square root | 249 |
| 12.4 Hensel lifting | 249 |
| 12.5 Frobenius substitution | 250 |
| 12.5.1 Sparse modulus | 251 |
| 12.5.2 Teichmüller modulus | 252 |
| 12.5.3 Gaussian normal basis | 252 |
| 12.6 Artin–Schreier equations | 252 |
| 12.6.1 Lercier–Lubicz algorithm | 253 |
| 12.6.2 Harley’s algorithm | 254 |
| 12.7 Generalized Newton lifting | 256 |
| 12.8 Applications | 257 |
| 12.8.1 Teichmüller lift | 257 |
| 12.8.2 Logarithm | 258 |
| 12.8.3 Exponential | 259 |
| 12.8.4 Trace | 260 |
| 12.8.5 Norm | 261 |

III Arithmetic of Curves

| | |
|--|------------|
| 13 Arithmetic of Elliptic Curves | 267 |
| 13.1 Summary of background on elliptic curves | 268 |
| 13.1.1 First properties and group law | 268 |
| 13.1.2 Scalar multiplication | 271 |
| 13.1.3 Rational points | 272 |
| 13.1.4 Torsion points | 273 |
| 13.1.5 Isomorphisms | 273 |
| 13.1.6 Isogenies | 277 |
| 13.1.7 Endomorphisms | 277 |
| 13.1.8 Cardinality | 278 |
| 13.2 Arithmetic of elliptic curves defined over \mathbb{F}_p | 280 |
| 13.2.1 Choice of the coordinates | 280 |
| 13.2.2 Mixed coordinates | 283 |
| 13.2.3 Montgomery scalar multiplication | 285 |
| 13.2.4 Parallel implementations | 288 |
| 13.2.5 Compression of points | 288 |
| 13.3 Arithmetic of elliptic curves defined over \mathbb{F}_{2^d} | 289 |
| 13.3.1 Choice of the coordinates | 291 |
| 13.3.2 Faster doublings in affine coordinates | 295 |

| | | |
|-----------|--|------------|
| 13.3.3 | Mixed coordinates | 296 |
| 13.3.4 | Montgomery scalar multiplication | 298 |
| 13.3.5 | Point halving and applications | 299 |
| 13.3.6 | Parallel implementation | 302 |
| 13.3.7 | Compression of points. | 302 |
| 14 | Arithmetic of Hyperelliptic Curves | 303 |
| 14.1 | Summary of background on hyperelliptic curves | 304 |
| 14.1.1 | Group law for hyperelliptic curves | 304 |
| 14.1.2 | Divisor class group and ideal class group | 306 |
| 14.1.3 | Isomorphisms and isogenies | 308 |
| 14.1.4 | Torsion elements | 309 |
| 14.1.5 | Endomorphisms | 310 |
| 14.1.6 | Cardinality | 310 |
| 14.2 | Compression techniques. | 311 |
| 14.2.1 | Compression in odd characteristic | 311 |
| 14.2.2 | Compression in even characteristic | 313 |
| 14.3 | Arithmetic on genus 2 curves over arbitrary characteristic | 313 |
| 14.3.1 | Different cases | 314 |
| 14.3.2 | Addition and doubling in affine coordinates | 316 |
| 14.4 | Arithmetic on genus 2 curves in odd characteristic | 320 |
| 14.4.1 | Projective coordinates | 321 |
| 14.4.2 | New coordinates in odd characteristic | 323 |
| 14.4.3 | Different sets of coordinates in odd characteristic | 325 |
| 14.4.4 | Montgomery arithmetic for genus 2 curves in odd characteristic | 328 |
| 14.5 | Arithmetic on genus 2 curves in even characteristic | 334 |
| 14.5.1 | Classification of genus 2 curves in even characteristic. | 334 |
| 14.5.2 | Explicit formulas in even characteristic in affine coordinates | 336 |
| 14.5.3 | Inversion-free systems for even characteristic when $h_2 \neq 0$. | 341 |
| 14.5.4 | Projective coordinates | 341 |
| 14.5.5 | Inversion-free systems for even characteristic when $h_2 = 0$. | 345 |
| 14.6 | Arithmetic on genus 3 curves | 348 |
| 14.6.1 | Addition in most common case | 348 |
| 14.6.2 | Doubling in most common case | 349 |
| 14.6.3 | Doubling on genus 3 curves for even characteristic when $h(x) = 1$ | 351 |
| 14.7 | Other curves and comparison | 352 |
| 15 | Arithmetic of Special Curves | 355 |
| 15.1 | Koblitz curves | 355 |
| 15.1.1 | Elliptic binary Koblitz curves | 356 |
| 15.1.2 | Generalized Koblitz curves | 367 |
| 15.1.3 | Alternative setup | 375 |
| 15.2 | Scalar multiplication using endomorphisms | 376 |
| 15.2.1 | GLV method | 377 |
| 15.2.2 | Generalizations | 380 |
| 15.2.3 | Combination of GLV and Koblitz curve strategies | 381 |
| 15.2.4 | Curves with endomorphisms for identity-based parameters. | 382 |
| 15.3 | Trace zero varieties | 383 |
| 15.3.1 | Background on trace zero varieties | 384 |
| 15.3.2 | Arithmetic in G . | 385 |

| | |
|--|------------|
| 16 Implementation of Pairings | 389 |
| 16.1 The basic algorithm. | 389 |
| 16.1.1 The setting | 390 |
| 16.1.2 Preparation | 391 |
| 16.1.3 The pairing computation algorithm | 391 |
| 16.1.4 The case of nontrivial embedding degree k | 393 |
| 16.1.5 Comparison with the Weil pairing | 395 |
| 16.2 Elliptic curves | 396 |
| 16.2.1 The basic step | 396 |
| 16.2.2 The representation | 396 |
| 16.2.3 The pairing algorithm | 397 |
| 16.2.4 Example | 397 |
| 16.3 Hyperelliptic curves of genus 2 | 398 |
| 16.3.1 The basic step | 399 |
| 16.3.2 Representation for $k > 2$ | 399 |
| 16.4 Improving the pairing algorithm | 400 |
| 16.4.1 Elimination of divisions | 400 |
| 16.4.2 Choice of the representation | 400 |
| 16.4.3 Precomputations | 400 |
| 16.5 Specific improvements for elliptic curves | 400 |
| 16.5.1 Systems of coordinates | 401 |
| 16.5.2 Subfield computations | 401 |
| 16.5.3 Even embedding degree | 402 |
| 16.5.4 Example | 403 |

IV Point Counting

| | |
|---|------------|
| 17 Point Counting on Elliptic and Hyperelliptic Curves | 407 |
| 17.1 Elementary methods | 407 |
| 17.1.1 Enumeration | 407 |
| 17.1.2 Subfield curves | 409 |
| 17.1.3 Square root algorithms | 410 |
| 17.1.4 Cartier–Manin operator | 411 |
| 17.2 Overview of ℓ -adic methods | 413 |
| 17.2.1 Schoof's algorithm | 413 |
| 17.2.2 Schoof–Elkies–Atkin's algorithm | 414 |
| 17.2.3 Modular polynomials | 416 |
| 17.2.4 Computing separable isogenies in finite fields of large characteristic | 419 |
| 17.2.5 Complete SEA algorithm | 421 |
| 17.3 Overview of p -adic methods | 422 |
| 17.3.1 Satoh's algorithm | 423 |
| 17.3.2 Arithmetic–Geometric–Mean algorithm | 434 |
| 17.3.3 Kedlaya's algorithm | 449 |

| | |
|--|------------|
| 18 Complex Multiplication | 455 |
| 18.1 CM for elliptic curves | 456 |
| 18.1.1 Summary of background | 456 |
| 18.1.2 Outline of the algorithm | 456 |
| 18.1.3 Computation of class polynomials | 457 |
| 18.1.4 Computation of norms | 458 |
| 18.1.5 The algorithm | 459 |
| 18.1.6 Experimental results | 459 |
| 18.2 CM for curves of genus 2 | 460 |
| 18.2.1 Summary of background | 462 |
| 18.2.2 Outline of the algorithm | 462 |
| 18.2.3 CM-types and period matrices | 463 |
| 18.2.4 Computation of the class polynomials | 465 |
| 18.2.5 Finding a curve | 467 |
| 18.2.6 The algorithm | 469 |
| 18.3 CM for larger genera | 470 |
| 18.3.1 Strategy and difficulties in the general case | 470 |
| 18.3.2 Hyperelliptic curves with automorphisms | 471 |
| 18.3.3 The case of genus 3 | 472 |

V Computation of Discrete Logarithms

| | |
|--|------------|
| 19 Generic Algorithms for Computing Discrete Logarithms | 477 |
| 19.1 Introduction | 478 |
| 19.2 Brute force | 479 |
| 19.3 Chinese remaindering | 479 |
| 19.4 Baby-step giant-step | 480 |
| 19.4.1 Adaptive giant-step width | 481 |
| 19.4.2 Search in intervals and parallelization | 482 |
| 19.4.3 Congruence classes | 483 |
| 19.5 Pollard's rho method | 483 |
| 19.5.1 Cycle detection | 484 |
| 19.5.2 Application to DL | 488 |
| 19.5.3 More on random walks | 489 |
| 19.5.4 Parallelization | 489 |
| 19.5.5 Automorphisms of the group | 490 |
| 19.6 Pollard's kangaroo method | 491 |
| 19.6.1 The lambda method | 492 |
| 19.6.2 Parallelization | 493 |
| 19.6.3 Automorphisms of the group | 494 |
| 20 Index Calculus | 495 |
| 20.1 Introduction | 495 |
| 20.2 Arithmetical formations | 496 |
| 20.2.1 Examples of formations | 497 |
| 20.3 The algorithm | 498 |
| 20.3.1 On the relation search | 499 |
| 20.3.2 Parallelization of the relation search | 500 |

| | | |
|-----------|--|------------|
| 20.3.3 | On the linear algebra | 500 |
| 20.3.4 | Filtering | 503 |
| 20.3.5 | Automorphisms of the group | 505 |
| 20.4 | An important example: finite fields | 506 |
| 20.5 | Large primes | 507 |
| 20.5.1 | One large prime | 507 |
| 20.5.2 | Two large primes | 508 |
| 20.5.3 | More large primes | 509 |
| 21 | Index Calculus for Hyperelliptic Curves | 511 |
| 21.1 | General algorithm | 511 |
| 21.1.1 | Hyperelliptic involution | 512 |
| 21.1.2 | Adleman–DeMarrais–Huang | 512 |
| 21.1.3 | Enge–Gaudry | 516 |
| 21.2 | Curves of small genus | 516 |
| 21.2.1 | Gaudry’s algorithm | 517 |
| 21.2.2 | Refined factor base | 517 |
| 21.2.3 | Harvesting | 518 |
| 21.3 | Large prime methods | 519 |
| 21.3.1 | Single large prime | 520 |
| 21.3.2 | Double large primes | 521 |
| 22 | Transfer of Discrete Logarithms | 529 |
| 22.1 | Transfer of discrete logarithms to \mathbb{F}_q -vector spaces | 529 |
| 22.2 | Transfer of discrete logarithms by pairings | 530 |
| 22.3 | Transfer of discrete logarithms by Weil descent | 530 |
| 22.3.1 | Summary of background | 531 |
| 22.3.2 | The GHS algorithm | 531 |
| 22.3.3 | Odd characteristic | 536 |
| 22.3.4 | Transfer via covers | 538 |
| 22.3.5 | Index calculus method via hyperplane sections | 541 |

VI Applications

| | | |
|-----------|---|------------|
| 23 | Algebraic Realizations of DL Systems | 547 |
| 23.1 | Candidates for secure DL systems | 547 |
| 23.1.1 | Groups with numeration and the DLP | 548 |
| 23.1.2 | Ideal class groups and divisor class groups | 548 |
| 23.1.3 | Examples: elliptic and hyperelliptic curves | 551 |
| 23.1.4 | Conclusion | 553 |
| 23.2 | Security of systems based on Pic_C^0 | 554 |
| 23.2.1 | Security under index calculus attacks | 554 |
| 23.2.2 | Transfers by Galois theory | 555 |
| 23.3 | Efficient systems | 557 |
| 23.3.1 | Choice of the finite field | 558 |
| 23.3.2 | Choice of genus and curve equation | 560 |
| 23.3.3 | Special choices of curves and scalar multiplication | 563 |
| 23.4 | Construction of systems | 564 |

| | | |
|-----------|--|------------|
| 23.4.1 | Heuristics of class group orders | 564 |
| 23.4.2 | Finding groups of suitable size | 565 |
| 23.5 | Protocols | 569 |
| 23.5.1 | System parameters | 569 |
| 23.5.2 | Protocols on Pic_C^0 | 570 |
| 23.6 | Summary | 571 |
| 24 | Pairing-Based Cryptography | 573 |
| 24.1 | Protocols | 573 |
| 24.1.1 | Multiparty key exchange | 574 |
| 24.1.2 | Identity-based cryptography | 576 |
| 24.1.3 | Short signatures | 578 |
| 24.2 | Realization | 579 |
| 24.2.1 | Supersingular elliptic curves | 580 |
| 24.2.2 | Supersingular hyperelliptic curves | 584 |
| 24.2.3 | Ordinary curves with small embedding degree | 586 |
| 24.2.4 | Performance | 589 |
| 24.2.5 | Hash functions on the Jacobian | 590 |
| 25 | Compositeness and Primality Testing – Factoring | 591 |
| 25.1 | Compositeness tests | 592 |
| 25.1.1 | Trial division | 592 |
| 25.1.2 | Fermat tests | 593 |
| 25.1.3 | Rabin–Miller test | 594 |
| 25.1.4 | Lucas pseudoprime tests | 595 |
| 25.1.5 | BPSW tests | 596 |
| 25.2 | Primality tests | 596 |
| 25.2.1 | Introduction | 596 |
| 25.2.2 | Atkin–Morain ECPP test | 597 |
| 25.2.3 | APRCL Jacobi sum test | 599 |
| 25.2.4 | Theoretical considerations and the AKS test | 600 |
| 25.3 | Factoring | 601 |
| 25.3.1 | Pollard's rho method | 601 |
| 25.3.2 | Pollard's $p - 1$ method | 603 |
| 25.3.3 | Factoring with elliptic curves | 604 |
| 25.3.4 | Fermat–Morrison–Brillhart approach | 607 |

VII Realization of Discrete Logarithm Systems

| | | |
|-----------|--|------------|
| 26 | Fast Arithmetic in Hardware | 617 |
| 26.1 | Design of cryptographic coprocessors | 618 |
| 26.1.1 | Design criteria | 618 |
| 26.2 | Complement representations of signed numbers | 620 |
| 26.3 | The operation $XY + Z$ | 622 |
| 26.3.1 | Multiplication using left shifts | 623 |
| 26.3.2 | Multiplication using right shifts | 624 |
| 26.4 | Reducing the number of partial products | 625 |
| 26.4.1 | Booth or signed digit encoding | 625 |

| | | |
|-----------|--|------------|
| 26.4.2 | Advanced recoding techniques | 626 |
| 26.5 | Accumulation of partial products | 627 |
| 26.5.1 | Full adders | 627 |
| 26.5.2 | Faster carry propagation | 628 |
| 26.5.3 | Analysis of carry propagation | 631 |
| 26.5.4 | Multi-operand operations | 633 |
| 26.6 | Modular reduction in hardware | 638 |
| 26.7 | Finite fields of characteristic 2 | 641 |
| 26.7.1 | Polynomial basis | 642 |
| 26.7.2 | Normal basis | 643 |
| 26.8 | Unified multipliers | 644 |
| 26.9 | Modular inversion in hardware | 645 |
| 27 | Smart Cards | 647 |
| 27.1 | History | 647 |
| 27.2 | Smart card properties | 648 |
| 27.2.1 | Physical properties | 648 |
| 27.2.2 | Electrical properties | 650 |
| 27.2.3 | Memory | 651 |
| 27.2.4 | Environment and software | 656 |
| 27.3 | Smart card interfaces | 659 |
| 27.3.1 | Transmission protocols | 659 |
| 27.3.2 | Physical interfaces | 663 |
| 27.4 | Types of smart cards | 664 |
| 27.4.1 | Memory only cards (synchronous cards) | 664 |
| 27.4.2 | Microprocessor cards (asynchronous cards) | 665 |
| 28 | Practical Attacks on Smart Cards | 669 |
| 28.1 | Introduction | 669 |
| 28.2 | Invasive attacks | 670 |
| 28.2.1 | Gaining access to the chip | 670 |
| 28.2.2 | Reconstitution of the layers | 670 |
| 28.2.3 | Reading the memories | 671 |
| 28.2.4 | Probing | 671 |
| 28.2.5 | FIB and test engineers scheme flaws | 672 |
| 28.3 | Non-invasive attacks | 673 |
| 28.3.1 | Timing attacks | 673 |
| 28.3.2 | Power consumption analysis | 675 |
| 28.3.3 | Electromagnetic radiation attacks | 682 |
| 28.3.4 | Differential fault analysis (DFA) and fault injection attacks | 683 |
| 29 | Mathematical Countermeasures against Side-Channel Attacks | 687 |
| 29.1 | Countermeasures against simple SCA | 688 |
| 29.1.1 | Dummy arithmetic instructions | 689 |
| 29.1.2 | Unified addition formulas | 694 |
| 29.1.3 | Montgomery arithmetic | 696 |
| 29.2 | Countermeasures against differential SCA | 697 |
| 29.2.1 | Implementation of DSCA | 698 |
| 29.2.2 | Scalar randomization | 699 |
| 29.2.3 | Randomization of group elements | 700 |

| | | |
|-----------|---|------------|
| 29.2.4 | Randomization of the curve equation | 700 |
| 29.3 | Countermeasures against Goubin type attacks | 703 |
| 29.4 | Countermeasures against higher order differential SCA | 704 |
| 29.5 | Countermeasures against timing attacks | 705 |
| 29.6 | Countermeasures against fault attacks | 705 |
| 29.6.1 | Countermeasures against simple fault analysis | 706 |
| 29.6.2 | Countermeasures against differential fault analysis | 706 |
| 29.6.3 | Conclusion on fault induction | 708 |
| 29.7 | Countermeasures for special curves | 709 |
| 29.7.1 | Countermeasures against SSCA on Koblitz curves | 709 |
| 29.7.2 | Countermeasures against DSCA on Koblitz curves | 711 |
| 29.7.3 | Countermeasures for GLV curves | 713 |
| 30 | Random Numbers – Generation and Testing | 715 |
| 30.1 | Definition of a random sequence | 715 |
| 30.2 | Random number generators | 717 |
| 30.2.1 | History | 717 |
| 30.2.2 | Properties of random number generators | 718 |
| 30.2.3 | Types of random number generators | 718 |
| 30.2.4 | Popular random number generators | 720 |
| 30.3 | Testing of random number generators | 722 |
| 30.4 | Testing a device | 722 |
| 30.5 | Statistical (empirical) tests | 723 |
| 30.6 | Some examples of statistical models on Σ^n | 725 |
| 30.7 | Hypothesis testings and random sequences | 726 |
| 30.8 | Empirical test examples for binary sequences | 727 |
| 30.8.1 | Random walk | 727 |
| 30.8.2 | Runs | 728 |
| 30.8.3 | Autocorrelation | 728 |
| 30.9 | Pseudorandom number generators | 729 |
| 30.9.1 | Relevant measures | 730 |
| 30.9.2 | Pseudorandom number generators from curves | 732 |
| 30.9.3 | Other applications | 735 |
| | References | 737 |
| | Notation Index | 777 |
| | General Index | 785 |