

Contents

| | | |
|--|------|-----------|
| <i>Preface</i> | page | xiii |
| <i>Acknowledgements</i> | | xiv |
| 1 Introduction | | 1 |
| 1.1 Public key cryptography | | 2 |
| 1.2 The textbook RSA cryptosystem | | 2 |
| 1.3 Formal definition of public key cryptography | | 4 |
| PART I BACKGROUND | | 11 |
| 2 Basic algorithmic number theory | | 13 |
| 2.1 Algorithms and complexity | | 13 |
| 2.2 Integer operations | | 21 |
| 2.3 Euclid's algorithm | | 24 |
| 2.4 Computing Legendre and Jacobi symbols | | 27 |
| 2.5 Modular arithmetic | | 29 |
| 2.6 Chinese remainder theorem | | 31 |
| 2.7 Linear algebra | | 32 |
| 2.8 Modular exponentiation | | 33 |
| 2.9 Square roots modulo p | | 36 |
| 2.10 Polynomial arithmetic | | 38 |
| 2.11 Arithmetic in finite fields | | 39 |
| 2.12 Factoring polynomials over finite fields | | 40 |
| 2.13 Hensel lifting | | 43 |
| 2.14 Algorithms in finite fields | | 43 |
| 2.15 Computing orders of elements and primitive roots | | 47 |
| 2.16 Fast evaluation of polynomials at multiple points | | 51 |
| 2.17 Pseudorandom generation | | 53 |
| 2.18 Summary | | 53 |
| 3 Hash functions and MACs | | 54 |
| 3.1 Security properties of hash functions | | 54 |
| 3.2 Birthday attack | | 55 |

| | | | | | |
|--|---------------------------------|-----------|---|--|-----|
| 3.3 | Message authentication codes | 56 | 8.3 | Maps on divisor classes | 126 |
| 3.4 | Constructions of hash functions | 56 | 8.4 | Riemann–Roch spaces | 129 |
| 3.5 | Number-theoretic hash functions | 57 | 8.5 | Derivations and differentials | 130 |
| 3.6 | Full domain hash | 57 | 8.6 | Genus zero curves | 136 |
| 3.7 | Random oracle model | 58 | 8.7 | Riemann–Roch theorem and Hurwitz genus formula | 137 |
| PART II ALGEBRAIC GROUPS | | 59 | 9 Elliptic curves | 138 | |
| 4 Preliminary remarks on algebraic groups | 61 | | 9.1 Group law | 138 | |
| 4.1 Informal definition of an algebraic group | 61 | | 9.2 Morphisms between elliptic curves | 140 | |
| 4.2 Examples of algebraic groups | 62 | | 9.3 Isomorphisms of elliptic curves | 142 | |
| 4.3 Algebraic group quotients | 63 | | 9.4 Automorphisms | 143 | |
| 4.4 Algebraic groups over rings | 64 | | 9.5 Twists | 144 | |
| 5 Varieties | 66 | | 9.6 Isogenies | 146 | |
| 5.1 Affine algebraic sets | 66 | | 9.7 The invariant differential | 153 | |
| 5.2 Projective algebraic sets | 69 | | 9.8 Multiplication by n and division polynomials | 155 | |
| 5.3 Irreducibility | 74 | | 9.9 Endomorphism structure | 156 | |
| 5.4 Function fields | 76 | | 9.10 Frobenius map | 158 | |
| 5.5 Rational maps and morphisms | 79 | | 9.11 Supersingular elliptic curves | 164 | |
| 5.6 Dimension | 83 | | 9.12 Alternative models for elliptic curves | 168 | |
| 5.7 Weil restriction of scalars | 84 | | 9.13 Statistical properties of elliptic curves over finite fields | 175 | |
| 6 Tori, LUC and XTR | 86 | | 9.14 Elliptic curves over rings | 177 | |
| 6.1 Cyclotomic subgroups of finite fields | 86 | | 10 Hyperelliptic curves | 178 | |
| 6.2 Algebraic tori | 88 | | 10.1 Non-singular models for hyperelliptic curves | 179 | |
| 6.3 The group $G_{q,2}$ | 89 | | 10.2 Isomorphisms, automorphisms and twists | 186 | |
| 6.4 The group $G_{q,6}$ | 94 | | 10.3 Effective affine divisors on hyperelliptic curves | 188 | |
| 6.5 Further remarks | 99 | | 10.4 Addition in the divisor class group | 196 | |
| 6.6 Algebraic tori over rings | 99 | | 10.5 Jacobians, Abelian varieties and isogenies | 204 | |
| 7 Curves and divisor class groups | 101 | | 10.6 Elements of order n | 206 | |
| 7.1 Non-singular varieties | 101 | | 10.7 Hyperelliptic curves over finite fields | 206 | |
| 7.2 Weierstrass equations | 105 | | 10.8 Supersingular curves | 209 | |
| 7.3 Uniformisers on curves | 106 | | PART III EXPONENTIATION, FACTORING AND DISCRETE LOGARITHMS | 213 | |
| 7.4 Valuation at a point on a curve | 108 | | 11 Basic algorithms for algebraic groups | 215 | |
| 7.5 Valuations and points on curves | 110 | | 11.1 Efficient exponentiation using signed exponents | 215 | |
| 7.6 Divisors | 110 | | 11.2 Multi-exponentiation | 219 | |
| 7.7 Principal divisors | 111 | | 11.3 Efficient exponentiation in specific algebraic groups | 221 | |
| 7.8 Divisor class group | 112 | | 11.4 Sampling from algebraic groups | 231 | |
| 7.9 Elliptic curves | 114 | | 11.5 Determining group structure and computing generators for elliptic curves | 235 | |
| Rational maps on curves and divisors | 121 | | 11.6 Testing subgroup membership | 236 | |
| 8.1 Rational maps of curves and the degree | 121 | | | | |
| 8.2 Extensions of valuations | 123 | | | | |

| | |
|--|------------|
| 12 Primality testing and integer factorisation using algebraic groups | 238 |
| 12.1 Primality testing | 238 |
| 12.2 Generating random primes | 240 |
| 12.3 The $p - 1$ factoring method | 242 |
| 12.4 Elliptic curve method | 244 |
| 12.5 Pollard–Strassen method | 245 |
| 13 Basic discrete logarithm algorithms | 246 |
| 13.1 Exhaustive search | 247 |
| 13.2 The Pohlig–Hellman method | 247 |
| 13.3 Baby-step–giant-step (BSGS) method | 250 |
| 13.4 Lower bound on complexity of generic algorithms for the DLP | 253 |
| 13.5 Generalised discrete logarithm problems | 256 |
| 13.6 Low Hamming weight DLP | 258 |
| 13.7 Low Hamming weight product exponents | 260 |
| 14 Factoring and discrete logarithms using pseudorandom walks | 262 |
| 14.1 Birthday paradox | 262 |
| 14.2 The Pollard rho method | 264 |
| 14.3 Distributed Pollard rho | 273 |
| 14.4 Speeding up the rho algorithm using equivalence classes | 276 |
| 14.5 The kangaroo method | 280 |
| 14.6 Distributed kangaroo algorithm | 287 |
| 14.7 The Gaudry–Schoot algorithm | 292 |
| 14.8 Parallel collision search in other contexts | 296 |
| 14.9 Pollard rho factoring method | 297 |
| 15 Factoring and discrete logarithms in subexponential time | 301 |
| 15.1 Smooth integers | 301 |
| 15.2 Factoring using random squares | 303 |
| 15.3 Elliptic curve method revisited | 310 |
| 15.4 The number field sieve | 312 |
| 15.5 Index calculus in finite fields | 313 |
| 15.6 Discrete logarithms on hyperelliptic curves | 324 |
| 15.7 Weil descent | 328 |
| 15.8 Discrete logarithms on elliptic curves over extension fields | 329 |
| 15.9 Further results | 332 |
| PART IV LATTICES | 335 |
| 16 Lattices | 337 |
| 16.1 Basic notions on lattices | 338 |
| 16.2 The Hermite and Minkowski bounds | 343 |
| 16.3 Computational problems in lattices | 345 |

| | |
|---|------------|
| 17 Lattice basis reduction | 347 |
| 17.1 Lattice basis reduction in two dimensions | 347 |
| 17.2 LLL-reduced lattice bases | 352 |
| 17.3 The Gram–Schmidt algorithm | 356 |
| 17.4 The LLL algorithm | 358 |
| 17.5 Complexity of LLL | 362 |
| 17.6 Variants of the LLL algorithm | 365 |
| 18 Algorithms for the closest and shortest vector problems | 366 |
| 18.1 Babai’s nearest plane method | 366 |
| 18.2 Babai’s rounding technique | 371 |
| 18.3 The embedding technique | 373 |
| 18.4 Enumerating all short vectors | 375 |
| 18.5 Korkine–Zolotarev bases | 379 |
| 19 Coppersmith’s method and related applications | 380 |
| 19.1 Coppersmith’s method for modular univariate polynomials | 380 |
| 19.2 Multivariate modular polynomial equations | 387 |
| 19.3 Bivariate integer polynomials | 387 |
| 19.4 Some applications of Coppersmith’s method | 390 |
| 19.5 Simultaneous Diophantine approximation | 397 |
| 19.6 Approximate integer greatest common divisors | 398 |
| 19.7 Learning with errors | 400 |
| 19.8 Further applications of lattice reduction | 402 |
| PART V CRYPTOGRAPHY RELATED TO DISCRETE LOGARITHMS | 403 |
| 20 The Diffie–Hellman problem and cryptographic applications | 405 |
| 20.1 The discrete logarithm assumption | 405 |
| 20.2 Key exchange | 405 |
| 20.3 Textbook Elgamal encryption | 408 |
| 20.4 Security of textbook Elgamal encryption | 410 |
| 20.5 Security of Diffie–Hellman key exchange | 414 |
| 20.6 Efficiency considerations for discrete logarithm cryptography | 416 |
| 21 The Diffie–Hellman problem | 418 |
| 21.1 Variants of the Diffie–Hellman problem | 418 |
| 21.2 Lower bound on the complexity of CDH for generic algorithms | 422 |
| 21.3 Random self-reducibility and self-correction of CDH | 423 |
| 21.4 The den Boer and Maurer reductions | 426 |
| 21.5 Algorithms for static Diffie–Hellman | 435 |
| 21.6 Hard bits of discrete logarithms | 439 |
| 21.7 Bit security of Diffie–Hellman | 443 |

| | | |
|------------|---|-----|
| x | Contents | |
| 22 | Digital signatures based on discrete logarithms | 452 |
| 22.1 | Schnorr signatures | 452 |
| 22.2 | Other public key signature schemes | 459 |
| 22.3 | Lattice attacks on signatures | 466 |
| 22.4 | Other signature functionalities | 467 |
| 23 | Public key encryption based on discrete logarithms | 469 |
| 23.1 | CCA secure Elgamal encryption | 469 |
| 23.2 | Cramer–Shoup encryption | 474 |
| 23.3 | Other encryption functionalities | 478 |
| PART VI | CRYPTOGRAPHY RELATED TO INTEGER FACTORISATION | 483 |
| 24 | The RSA and Rabin cryptosystems | 485 |
| 24.1 | The textbook RSA cryptosystem | 485 |
| 24.2 | The textbook Rabin cryptosystem | 491 |
| 24.3 | Homomorphic encryption | 498 |
| 24.4 | Algebraic attacks on textbook RSA and Rabin | 499 |
| 24.5 | Attacks on RSA parameters | 504 |
| 24.6 | Digital signatures based on RSA and Rabin | 507 |
| 24.7 | Public key encryption based on RSA and Rabin | 511 |
| PART VII | ADVANCED TOPICS IN ELLIPTIC AND HYPERELLIPTIC CURVES | 513 |
| 25 | Isogenies of elliptic curves | 515 |
| 25.1 | Isogenies and kernels | 515 |
| 25.2 | Isogenies from j -invariants | 523 |
| 25.3 | Isogeny graphs of elliptic curves over finite fields | 529 |
| 25.4 | The structure of the ordinary isogeny graph | 535 |
| 25.5 | Constructing isogenies between elliptic curves | 540 |
| 25.6 | Relating the discrete logarithm problem on isogenous curves | 543 |
| 26 | Pairings on elliptic curves | 545 |
| 26.1 | Weil reciprocity | 545 |
| 26.2 | The Weil pairing | 546 |
| 26.3 | The Tate–Lichtenbaum pairing | 548 |
| 26.4 | Reduction of ECDLP to finite fields | 557 |
| 26.5 | Computational problems | 559 |
| 26.6 | Pairing-friendly elliptic curves | 561 |
| Appendix A | Background mathematics | 564 |
| A.1 | Basic notation | 564 |
| A.2 | Groups | 564 |

| | | |
|---------------|----------------------------------|-----|
| | Contents | xi |
| A.3 | Rings | 565 |
| A.4 | Modules | 565 |
| A.5 | Polynomials | 566 |
| A.6 | Field extensions | 567 |
| A.7 | Galois theory | 569 |
| A.8 | Finite fields | 570 |
| A.9 | Ideals | 571 |
| A.10 | Vector spaces and linear algebra | 572 |
| A.11 | Hermite normal form | 575 |
| A.12 | Orders in quadratic fields | 575 |
| A.13 | Binary strings | 576 |
| A.14 | Probability and combinatorics | 576 |
| References | | 579 |
| Author index | | 603 |
| Subject index | | 608 |

References 579
Author index 603
Subject index 608

The book is designed to be used as a textbook for a course in mathematics, or as a reference for self-study. However, it is not intended to be read from cover to cover. Instead, we encourage anyone to start at Part I, Chapter 1, and then move on to the chapters of interest. The book is divided into four parts: Part I (Chapters 1–4) covers the basics of number theory, Part II (Chapters 5–8) covers the basics of cryptography, Part III (Chapters 9–14) covers advanced topics in cryptography, and Part IV (Chapters 15–16) covers advanced topics in algebra. For an introduction to the book, see the Preface. For an introduction to the book, see the Preface. For an introduction to the book, see the Preface.

Exercises are distributed throughout the book, and are intended to be used as a guide for self-study. Some exercises are more difficult than others, and are marked with a star. Some exercises are more difficult than others, and are marked with a star. Some exercises are more difficult than others, and are marked with a star. Some exercises are more difficult than others, and are marked with a star.

Despite our best efforts, it is inevitable that the book will contain errors and misleading statements. Errors will be listed on the author's webpage for the book at www.math.auckland.ac.nz/~sga010/crypto-book/cryptobook.html. Readers are encouraged to bring any errors to the attention of the author.

I would like to thank Royal Holloway, University of London and the University of Auckland, each of which in turn has supported me a substantial time while I was writing the book. I also thank the LRSRC, who supported my research with an advanced fellowship for the first few years of writing the book.

The book is dedicated to Siobhán and Eve, both of whom tolerated my obsession with writing for the last four years.

Steven Galbraith
Auckland