MATHEMATICS OF PUBLIC KEY CRYPTOGRAPHY

Public key cryptography is a major interdisciplinary subject with many real-world applications, such as digital signatures. A strong background in the mathematics underlying public key cryptography is essential for a deep understanding of the subject, and this book provides exactly that for students and researchers in mathematics, computer science and electrical engineering.

Carefully written to communicate the major ideas and techniques of public key cryptography to a wide readership, this text is enlivened throughout with historical remarks and insightful perspectives on the development of the subject. Numerous examples, proofs and exercises make it suitable as a textbook for an advanced course, as well as for self-study. For more experienced researchers, it serves as a convenient reference for many important topics: the Pollard algorithms, Maurer reduction, isogenies, algebraic tori, hyperelliptic curves, lattices and many more.

Steven D. Galbraith is a leading international authority on the mathematics of public key cryptography. He is an Associate Professor in the Department of Mathematics at the University of Auckland.
# Contents

<table>
<thead>
<tr>
<th>Preface</th>
<th>xiii</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgements</td>
<td>xiv</td>
</tr>
</tbody>
</table>

## 1 Introduction

1.1 Public key cryptography
1.2 The textbook RSA cryptosystem
1.3 Formal definition of public key cryptography

## PART I BACKGROUND

### 2 Basic algorithmic number theory

2.1 Algorithms and complexity
2.2 Integer operations
2.3 Euclid’s algorithm
2.4 Computing Legendre and Jacobi symbols
2.5 Modular arithmetic
2.6 Chinese remainder theorem
2.7 Linear algebra
2.8 Modular exponentiation
2.9 Square roots modulo $p$
2.10 Polynomial arithmetic
2.11 Arithmetic in finite fields
2.12 Factoring polynomials over finite fields
2.13 Hensel lifting
2.14 Algorithms in finite fields
2.15 Computing orders of elements and primitive roots
2.16 Fast evaluation of polynomials at multiple points
2.17 Pseudorandom generation
2.18 Summary

### 3 Hash functions and MACs

3.1 Security properties of hash functions
3.2 Birthday attack

© in this web service Cambridge University Press
Contents

3.3 Message authentication codes 56
3.4 Constructions of hash functions 56
3.5 Number-theoretic hash functions 57
3.6 Full domain hash 57
3.7 Random oracle model 58

PART II ALGEBRAIC GROUPS 59

4 Preliminary remarks on algebraic groups 61
4.1 Informal definition of an algebraic group 61
4.2 Examples of algebraic groups 62
4.3 Algebraic group quotients 63
4.4 Algebraic groups over rings 64

5 Varieties 66
5.1 Affine algebraic sets 66
5.2 Projective algebraic sets 69
5.3 Irreducibility 74
5.4 Function fields 76
5.5 Rational maps and morphisms 79
5.6 Dimension 83
5.7 Weil restriction of scalars 84

6 Tori, LUC and XTR 86
6.1 Cyclotomic subgroups of finite fields 86
6.2 Algebraic tori 88
6.3 The group $G_{q,2}$ 89
6.4 The group $G_{q,6}$ 94
6.5 Further remarks 99
6.6 Algebraic tori over rings 99

7 Curves and divisor class groups 101
7.1 Non-singular varieties 101
7.2 Weierstrass equations 105
7.3 Uniformisers on curves 106
7.4 Valuation at a point on a curve 108
7.5 Valuations and points on curves 110
7.6 Divisors 111
7.7 Principal divisors 112
7.8 Divisor class group 114
7.9 Elliptic curves 116

8 Rational maps on curves and divisors 121
8.1 Rational maps of curves and the degree 121
8.2 Extensions of valuations 123
# Contents

8.3 Maps on divisor classes 126  
8.4 Riemann–Roch spaces 129  
8.5 Derivations and differentials 130  
8.6 Genus zero curves 136  
8.7 Riemann–Roch theorem and Hurwitz genus formula 137

9 Elliptic curves 138  
9.1 Group law 138  
9.2 Morphisms between elliptic curves 140  
9.3 Isomorphisms of elliptic curves 142  
9.4 Automorphisms 143  
9.5 Twists 144  
9.6 Isogenies 146  
9.7 The invariant differential 153  
9.8 Multiplication by \( n \) and division polynomials 155  
9.9 Endomorphism structure 156  
9.10 Frobenius map 158  
9.11 Supersingular elliptic curves 164  
9.12 Alternative models for elliptic curves 168  
9.13 Statistical properties of elliptic curves over finite fields 175  
9.14 Elliptic curves over rings 177

10 Hyperelliptic curves 178  
10.1 Non-singular models for hyperelliptic curves 179  
10.2 Isomorphisms, automorphisms and twists 186  
10.3 Effective affine divisors on hyperelliptic curves 188  
10.4 Addition in the divisor class group 196  
10.5 Jacobians, Abelian varieties and isogenies 204  
10.6 Elements of order \( n \) 206  
10.7 Hyperelliptic curves over finite fields 206  
10.8 Supersingular curves 209

PART III EXPONENTIATION, FACTORING AND DISCRETE LOGARITHMS 213

11 Basic algorithms for algebraic groups 215  
11.1 Efficient exponentiation using signed exponents 215  
11.2 Multi-exponentiation 219  
11.3 Efficient exponentiation in specific algebraic groups 221  
11.4 Sampling from algebraic groups 231  
11.5 Determining group structure and computing generators for elliptic curves 235  
11.6 Testing subgroup membership 236
# Contents

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–Schost 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
## Contents

### 17 Lattice basis reduction
- 17.1 Lattice basis reduction in two dimensions
- 17.2 LLL-reduced lattice bases
- 17.3 The Gram–Schmidt algorithm
- 17.4 The LLL algorithm
- 17.5 Complexity of LLL
- 17.6 Variants of the LLL algorithm

### 18 Algorithms for the closest and shortest vector problems
- 18.1 Babai’s nearest plane method
- 18.2 Babai’s rounding technique
- 18.3 The embedding technique
- 18.4 Enumerating all short vectors
- 18.5 Korkine–Zolotarev bases

### 19 Coppersmith’s method and related applications
- 19.1 Coppersmith’s method for modular univariate polynomials
- 19.2 Multivariate modular polynomial equations
- 19.3 Bivariate integer polynomials
- 19.4 Some applications of Coppersmith’s method
- 19.5 Simultaneous Diophantine approximation
- 19.6 Approximate integer greatest common divisors
- 19.7 Learning with errors
- 19.8 Further applications of lattice reduction

### PART V CRYPTOGRAPHY RELATED TO DISCRETE LOGARITHMS

#### 20 The Diffie–Hellman problem and cryptographic applications
- 20.1 The discrete logarithm assumption
- 20.2 Key exchange
- 20.3 Textbook Elgamal encryption
- 20.4 Security of textbook Elgamal encryption
- 20.5 Security of Diffie–Hellman key exchange
- 20.6 Efficiency considerations for discrete logarithm cryptography

#### 21 The Diffie–Hellman problem
- 21.1 Variants of the Diffie–Hellman problem
- 21.2 Lower bound on the complexity of CDH for generic algorithms
- 21.3 Random self-reducibility and self-correction of CDH
- 21.4 The den Boer and Maurer reductions
- 21.5 Algorithms for static Diffie–Hellman
- 21.6 Hard bits of discrete logarithms
- 21.7 Bit security of Diffie–Hellman
## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Digital signatures based on discrete logarithms</td>
<td>452</td>
</tr>
<tr>
<td>22.1</td>
<td>Schnorr signatures</td>
<td>452</td>
</tr>
<tr>
<td>22.2</td>
<td>Other public key signature schemes</td>
<td>459</td>
</tr>
<tr>
<td>22.3</td>
<td>Lattice attacks on signatures</td>
<td>466</td>
</tr>
<tr>
<td>22.4</td>
<td>Other signature functionalities</td>
<td>467</td>
</tr>
<tr>
<td>23</td>
<td>Public key encryption based on discrete logarithms</td>
<td>469</td>
</tr>
<tr>
<td>23.1</td>
<td>CCA secure Elgamal encryption</td>
<td>469</td>
</tr>
<tr>
<td>23.2</td>
<td>Cramer–Shoup encryption</td>
<td>474</td>
</tr>
<tr>
<td>23.3</td>
<td>Other encryption functionalities</td>
<td>478</td>
</tr>
<tr>
<td>24</td>
<td>The RSA and Rabin cryptosystems</td>
<td>485</td>
</tr>
<tr>
<td>24.1</td>
<td>The textbook RSA cryptosystem</td>
<td>485</td>
</tr>
<tr>
<td>24.2</td>
<td>The textbook Rabin cryptosystem</td>
<td>491</td>
</tr>
<tr>
<td>24.3</td>
<td>Homomorphic encryption</td>
<td>498</td>
</tr>
<tr>
<td>24.4</td>
<td>Algebraic attacks on textbook RSA and Rabin</td>
<td>499</td>
</tr>
<tr>
<td>24.5</td>
<td>Attacks on RSA parameters</td>
<td>504</td>
</tr>
<tr>
<td>24.6</td>
<td>Digital signatures based on RSA and Rabin</td>
<td>507</td>
</tr>
<tr>
<td>24.7</td>
<td>Public key encryption based on RSA and Rabin</td>
<td>511</td>
</tr>
<tr>
<td>25</td>
<td>Isogenies of elliptic curves</td>
<td>515</td>
</tr>
<tr>
<td>25.1</td>
<td>Isogenies and kernels</td>
<td>515</td>
</tr>
<tr>
<td>25.2</td>
<td>Isogenies from ( j )-invariants</td>
<td>523</td>
</tr>
<tr>
<td>25.3</td>
<td>Isogeny graphs of elliptic curves over finite fields</td>
<td>529</td>
</tr>
<tr>
<td>25.4</td>
<td>The structure of the ordinary isogeny graph</td>
<td>535</td>
</tr>
<tr>
<td>25.5</td>
<td>Constructing isogenies between elliptic curves</td>
<td>540</td>
</tr>
<tr>
<td>25.6</td>
<td>Relating the discrete logarithm problem on isogenous curves</td>
<td>543</td>
</tr>
<tr>
<td>26</td>
<td>Pairings on elliptic curves</td>
<td>545</td>
</tr>
<tr>
<td>26.1</td>
<td>Weil reciprocity</td>
<td>545</td>
</tr>
<tr>
<td>26.2</td>
<td>The Weil pairing</td>
<td>546</td>
</tr>
<tr>
<td>26.3</td>
<td>The Tate–Lichtenbaum pairing</td>
<td>548</td>
</tr>
<tr>
<td>26.4</td>
<td>Reduction of ECDLP to finite fields</td>
<td>557</td>
</tr>
<tr>
<td>26.5</td>
<td>Computational problems</td>
<td>559</td>
</tr>
<tr>
<td>26.6</td>
<td>Pairing-friendly elliptic curves</td>
<td>561</td>
</tr>
</tbody>
</table>

**PART VII  ADVANCED TOPICS IN ELLIPTIC AND HYPERELLIPTIC CURVES**  513

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>Isogenies of elliptic curves</td>
<td>515</td>
</tr>
<tr>
<td>25.1</td>
<td>Isogenies and kernels</td>
<td>515</td>
</tr>
<tr>
<td>25.2</td>
<td>Isogenies from ( j )-invariants</td>
<td>523</td>
</tr>
<tr>
<td>25.3</td>
<td>Isogeny graphs of elliptic curves over finite fields</td>
<td>529</td>
</tr>
<tr>
<td>25.4</td>
<td>The structure of the ordinary isogeny graph</td>
<td>535</td>
</tr>
<tr>
<td>25.5</td>
<td>Constructing isogenies between elliptic curves</td>
<td>540</td>
</tr>
<tr>
<td>25.6</td>
<td>Relating the discrete logarithm problem on isogenous curves</td>
<td>543</td>
</tr>
<tr>
<td>26</td>
<td>Pairings on elliptic curves</td>
<td>545</td>
</tr>
<tr>
<td>26.1</td>
<td>Weil reciprocity</td>
<td>545</td>
</tr>
<tr>
<td>26.2</td>
<td>The Weil pairing</td>
<td>546</td>
</tr>
<tr>
<td>26.3</td>
<td>The Tate–Lichtenbaum pairing</td>
<td>548</td>
</tr>
<tr>
<td>26.4</td>
<td>Reduction of ECDLP to finite fields</td>
<td>557</td>
</tr>
<tr>
<td>26.5</td>
<td>Computational problems</td>
<td>559</td>
</tr>
<tr>
<td>26.6</td>
<td>Pairing-friendly elliptic curves</td>
<td>561</td>
</tr>
</tbody>
</table>

**Appendix A  Background mathematics**  564

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.1</td>
<td>Basic notation</td>
<td>564</td>
</tr>
<tr>
<td>A.2</td>
<td>Groups</td>
<td>564</td>
</tr>
</tbody>
</table>
Contents

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
Preface

The book has grown from lecture notes of a Master’s level course in mathematics, for students who have already attended a cryptography course along the lines of Stinson’s or Smart’s books. The book is therefore suitable as a teaching tool or for self-study. However, it is not expected that the book will be read linearly. Indeed, we discourage anyone to start reading with either Part I, Part II or Part III. The best place to start, for an understanding of mathematical cryptography, is probably Part V (replacing all references to “algebraic group $G$” by $\mathbb{F}_p^\times$). For an introduction to RSA and Rabin one could start reading at Part VI and ignore most references to the earlier parts.

Exercises are distributed throughout the book so that the reader performing self-study can do them at precisely the right point in their learning. Readers may find exercises denoted by ★ somewhat more difficult than the others, but it would be dangerous to assume that everyone’s experience of the exercises will be the same.

Despite our best efforts, it is inevitable that the book will contain errors and misleading statements. Errata will be listed on the author’s webpage for the book at www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.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 was my employer for a substantial time while I was writing the book. I also thank the EPSRC, who supported my research with an advanced fellowship for the first few years of writing the book.

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

Steven Galbraith
Auckland
Acknowledgements

The book grew out of my lecture notes from the Master’s course “Public key cryptography” at Royal Holloway. I thank the students who took that course for asking questions and doing their homework in unexpected ways.

The staff at Cambridge University Press have been very helpful during the preparation of this book.

I also thank the following people for answering my questions, pointing out errors in drafts of the book, helping with LaTeX, examples, proofs, exercises, etc: José de Jesús Angel Angel, Olivier Bernard, Nicolas Bonifas, Nils Bruin, Ilya Chevyrev, Bart Coppens, Alex Dent, Claus Diem, Marion Duporté, Andreas Enge, Victor Flynn, David Freeman, Pierrick Gaudry, Takuya Hayashi, Nadia Heninger, Florian Hess, Mark Holmes, Everett Howe, David Jao, Jonathan Katz, Eike Kiltz, Kitae Kim, David Kohel, Cong Ling, Alexander May, Esmaeil Mehrabi, Ciaran Mullan, Mats Näslund, Francisco Monteiro, James McKee, James Nelson, Samuel Neves, Phong Nguyen, TaeHun Oh, Chris Peikert, Michael Phillips, John Pollard, Francesco Pretto, Oded Regev, Christophe Ritzenthaler, Karl Rubin, Raminder Ruprai, Takakazu Satoh, Leanne Scheepers, Davide Schipani, Michael Schneider, Peter Schwabe, Reza Sepahi, Victor Shoup, Igor Shparlinski, Andrew Shallue, Francesco Sica, Alice Silverberg, Benjamin Smith, Martijn Stam, Damien Stehlé, Anton Stolbunov, Drew Sutherland, Garry Tee, Emmanuel Thomé, Frederik Vercauteren, Timothy Vogel, Anastasia Zaytseva, Chang-An Zhao, Paul Zimmermann.

Any remaining errors and omissions are the author’s responsibility.