

Cambridge University Press  
978-1-107-01392-6 - Mathematics of Public Key Cryptography  
Steven D. Galbraith  
Frontmatter  
[More information](#)

---

## 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.

Cambridge University Press  
978-1-107-01392-6 - Mathematics of Public Key Cryptography  
Steven D. Galbraith  
Frontmatter  
[More information](#)

---

Cambridge University Press  
978-1-107-01392-6 - Mathematics of Public Key Cryptography  
Steven D. Galbraith  
Frontmatter  
[More information](#)

---

# MATHEMATICS OF PUBLIC KEY CRYPTOGRAPHY

STEVEN D. GALBRAITH

*University of Auckland*



Cambridge University Press  
978-1-107-01392-6 - Mathematics of Public Key Cryptography  
Steven D. Galbraith  
Frontmatter  
[More information](#)

CAMBRIDGE UNIVERSITY PRESS  
Cambridge, New York, Melbourne, Madrid, Cape Town,  
Singapore, São Paulo, Delhi, Mexico City

Cambridge University Press  
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

[www.cambridge.org](http://www.cambridge.org)  
Information on this title: [www.cambridge.org/9781107013926](http://www.cambridge.org/9781107013926)

© S. D. Galbraith 2012

This publication is in copyright. Subject to statutory exception  
and to the provisions of relevant collective licensing agreements,  
no reproduction of any part may take place without the written  
permission of Cambridge University Press.

First published 2012

Printed in the United Kingdom at the University Press, Cambridge

*A catalogue record for this publication is available from the British Library*

*Library of Congress Cataloguing in Publication data*

Galbraith, Steven D.

Mathematics of public key cryptography / Steven D. Galbraith.  
p. cm.

Includes bibliographical references and index.

ISBN 978-1-107-01392-6 (hardback)

1. Coding theory. 2. Cryptography – Mathematics. I. Title.

QA268.G35 2012

003'.54 – dc23 2011042606

ISBN 978-1-107-01392-6 Hardback

Additional resources for this publication at  
[www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html](http://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html)

---

Cambridge University Press has no responsibility for the persistence or  
accuracy of URLs for external or third-party internet websites referred to in  
this publication, and does not guarantee that any content on such websites is,  
or will remain, accurate or appropriate.

---

## Contents

|  |                  |
|--|------------------|
| <i>Preface</i>   | <i>page</i> xiii |
| <i>Acknowledgements</i>                                | xiv              |
| <b>1 Introduction</b>                                  | <b>1</b>         |
| 1.1 Public key cryptography                            | 2                |
| 1.2 The textbook RSA cryptosystem                      | 2                |
| 1.3 Formal definition of public key cryptography       | 4                |
| <b>PART I BACKGROUND</b>                               | <b>11</b>        |
| <b>2 Basic algorithmic number theory</b>               | <b>13</b>        |
| 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               |
| <b>3 Hash functions and MACs</b>                       | <b>54</b>        |
| 3.1 Security properties of hash functions              | 54               |
| 3.2 Birthday attack                                    | 55               |

|                |  |            |
|----------------|--|------------|
| vi             | <i>Contents</i>                                |            |
| 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         |
| <b>PART II</b> | <b>ALGEBRAIC GROUPS</b>                        | <b>59</b>  |
| <b>4</b>       | <b>Preliminary remarks on algebraic groups</b> | <b>61</b>  |
| 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         |
| <b>5</b>       | <b>Varieties</b>                               | <b>66</b>  |
| 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         |
| <b>6</b>       | <b>Tori, LUC and XTR</b>                       | <b>86</b>  |
| 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         |
| <b>7</b>       | <b>Curves and divisor class groups</b>         | <b>101</b> |
| 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        |
| <b>8</b>       | <b>Rational maps on curves and divisors</b>    | <b>121</b> |
| 8.1            | Rational maps of curves and the degree         | 121        |
| 8.2            | Extensions of valuations                       | 123        |

*Contents*

vii

|   |  |            |
|---|--|------------|
| 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        |
| <b>9</b>  | <b>Elliptic curves</b>   | <b>138</b> |
| 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        |
| <b>10</b>   | <b>Hyperelliptic curves</b>  | <b>178</b> |
| 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        |
| <b>PART III EXPONENTIATION, FACTORING AND DISCRETE LOGARITHMS</b> |  | <b>213</b> |
| <b>11</b>   | <b>Basic algorithms for algebraic groups</b>                             | <b>215</b> |
| 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        |

|                |   |            |
|----------------|---|------------|
| <b>12</b>      | <b>Primality testing and integer factorisation using algebraic groups</b> | <b>238</b> |
| 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        |
| <b>13</b>      | <b>Basic discrete logarithm algorithms</b>                                | <b>246</b> |
| 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        |
| <b>14</b>      | <b>Factoring and discrete logarithms using pseudorandom walks</b>         | <b>262</b> |
| 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        |
| <b>15</b>      | <b>Factoring and discrete logarithms in subexponential time</b>           | <b>301</b> |
| 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        |
| <b>PART IV</b> | <b>LATTICES</b>   | <b>335</b> |
| <b>16</b>      | <b>Lattices</b>   | <b>337</b> |
| 16.1           | Basic notions on lattices   | 338        |
| 16.2           | The Hermite and Minkowski bounds  | 343        |
| 16.3           | Computational problems in lattices  | 345        |



|               |  |            |
|---------------|--|------------|
| <b>17</b>     | <b>Lattice basis reduction</b>                                   | <b>347</b> |
| 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        |
| <b>18</b>     | <b>Algorithms for the closest and shortest vector problems</b>   | <b>366</b> |
| 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        |
| <b>19</b>     | <b>Coppersmith’s method and related applications</b>             | <b>380</b> |
| 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        |
| <b>PART V</b> | <b>CRYPTOGRAPHY RELATED TO DISCRETE LOGARITHMS</b>               | <b>403</b> |
| <b>20</b>     | <b>The Diffie–Hellman problem and cryptographic applications</b> | <b>405</b> |
| 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        |
| <b>21</b>     | <b>The Diffie–Hellman problem</b>                                | <b>418</b> |
| 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        |

|  |   |            |
|--|---|------------|
| <b>22</b>  | <b>Digital signatures based on discrete logarithms</b>      | <b>452</b> |
| 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        |
| <b>23</b>  | <b>Public key encryption based on discrete logarithms</b>   | <b>469</b> |
| 23.1   | CCA secure Elgamal encryption                               | 469        |
| 23.2   | Cramer–Shoup encryption                                     | 474        |
| 23.3   | Other encryption functionalities                            | 478        |
| <b>PART VI CRYPTOGRAPHY RELATED TO INTEGER FACTORISATION</b>         |   | <b>483</b> |
| <b>24</b>  | <b>The RSA and Rabin cryptosystems</b>                      | <b>485</b> |
| 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        |
| <b>PART VII ADVANCED TOPICS IN ELLIPTIC AND HYPERELLIPTIC CURVES</b> |   | <b>513</b> |
| <b>25</b>  | <b>Isogenies of elliptic curves</b>                         | <b>515</b> |
| 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        |
| <b>26</b>  | <b>Pairings on elliptic curves</b>                          | <b>545</b> |
| 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        |
| <b>Appendix A Background mathematics</b>                             |   | <b>564</b> |
| A.1  | Basic notation  | 564        |
| A.2  | Groups  | 564        |

|      | <i>Contents</i>                  | 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 |
|      | <i>References</i>                | 579 |
|      | <i>Author index</i>              | 603 |
|      | <i>Subject index</i>             | 608 |

Cambridge University Press  
978-1-107-01392-6 - Mathematics of Public Key Cryptography  
Steven D. Galbraith  
Frontmatter  
[More information](#)

---

## 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  $\mathbb{F}_p^*$ ). 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](http://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.