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.

MATHEMATICS OF PUBLIC KEY CRYPTOGRAPHY

STEVEN D. GALBRAITH
University of Auckland

CAMBRIDGE
UNIVERSITY PRESS

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
Information on this title: www.cambridge.org/9781107013926

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

Contents

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. 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.