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