

Cambridge University Press  
978-1-107-01392-6 - Mathematics of Public Key Cryptography  
Steven D. Galbraith  
Copyright Information  
[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  
Copyright Information  
[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.

---