

CAMBRIDGE  
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom  
One Liberty Plaza, 20th Floor, New York, NY 10006, USA  
477 Williamstown Road, Port Melbourne, VIC 3207, Australia  
314-321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi - 110025, India  
103 Penang Road, #05-06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of the University of Cambridge.  
It furthers the University's mission by disseminating knowledge in the pursuit of  
education, learning and research at the highest international levels of excellence.

[www.cambridge.org](http://www.cambridge.org)  
Information on this title: [www.cambridge.org/9781108795937](http://www.cambridge.org/9781108795937)  
DOI: 10.1017/9781108854207

© Cambridge University Press 2021

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 2021

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

*Library of Congress Cataloging in Publication data*

Names: Bos, Joppe W., editor. | Stam, Martijn, editor.

Title: Computational cryptography : algorithmic aspects of cryptology /  
edited by Joppe W. Bos, NXP Semiconductors, Belgium, Martijn Stam,  
Simula UiB, Norway.

Description: Cambridge, United Kingdom ; New York, NY, USA : Cambridge  
University Press, 2021. | Series: London mathematical society lecture  
note series | Includes bibliographical references and index.

Identifiers: LCCN 2021012303 (print) | LCCN 2021012304 (ebook) |  
ISBN 9781108795937 (paperback) | ISBN 9781108854207 (epub)

Subjects: LCSH: Cryptography. | BISAC: MATHEMATICS / Number Theory |  
MATHEMATICS / Number Theory

Classification: LCC QA268 .C693 2021 (print) | LCC QA268 (ebook) |  
DDC 005.8/24—dc23

LC record available at <https://lcn.loc.gov/2021012303>

LC ebook record available at <https://lcn.loc.gov/2021012304>

ISBN 978-1-108-79593-7 Paperback

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.