

Cambridge University Press

978-1-107-04305-3 - Secure Multiparty Computation and Secret Sharing

Ronald Cramer, Ivan Bjerre Damgård and Jesper Buus Nielsen

Copyright Information

[More information](#)

# Secure Multiparty Computation and Secret Sharing

Ronald Cramer

*CWI & Leiden University*

Ivan Bjerre Damgård

*Aarhus University*

Jesper Buus Nielsen

*Aarhus University*



CAMBRIDGE  
UNIVERSITY PRESS

Cambridge University Press  
 978-1-107-04305-3 - Secure Multiparty Computation and Secret Sharing  
 Ronald Cramer, Ivan Bjerre Damgård and Jesper Buus Nielsen  
 Copyright Information  
[More information](#)

**CAMBRIDGE**  
 UNIVERSITY PRESS

32 Avenue of the Americas, New York, NY 10013-2473, USA

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/9781107043053](http://www.cambridge.org/9781107043053)

© Ronald Cramer, Ivan Bjerre Damgård, Jesper Buus Nielsen 2015

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 2015

Printed in the United States of America

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

*Library of Congress Cataloging in Publication Data*

Cramer, Ronald, 1968–

Secure multiparty computation and secret sharing / Ronald Cramer,  
 CWI & Leiden University, Ivan Damgård, Aarhus University, Jesper Buus Nielsen,  
 Aarhus University.

pages cm

Includes bibliographical references and index.

ISBN 978-1-107-04305-3 (hardback)

1. Computer networks—Security measures. 2. Computer security. 3. Computer network protocols.  
 4. Information theory. I. Damgaard, Ivan, 1956– II. Nielsen, Jesper Buus, 1973– III. Title.

TK5105.59.C685 2015

005.8—dc23 2015002282

ISBN 978-1-107-04305-3 Hardback

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.