Secure Multiparty Computation and Secret Sharing

In a data-driven society, individuals and companies encounter numerous situations where private information is an important resource. How can parties handle confidential data if they do not trust everyone involved? This text is the first to present a comprehensive treatment of unconditionally secure techniques for multiparty computation (MPC) and secret sharing. In a secure MPC, each party possesses some private data, whereas secret sharing provides a way for one party to spread information on a secret such that all parties together hold full information, yet no single party has all the information. The authors present basic feasibility results from the last thirty years, generalizations to arbitrary access structures using linear secret sharing, some recent techniques for efficiency improvements, and a general treatment of the theory of secret sharing, focusing on asymptotic results with interesting applications related to MPC.

RONALD CRAMER leads the Cryptology Group at CWI Amsterdam, the national research institute for mathematics and computer science in the Netherlands, and is Professor at the Mathematical Institute, Leiden University. He is Fellow of the International Association for Cryptologic Research and Member of the Royal Netherlands Academy of Arts and Sciences.

IVAN BJERRE DAMGÅRD leads the Cryptology Group in the Department of Computer Science, Aarhus University, and is a professor in the same department. He is a Fellow of the International Association for Cryptologic Research, and he received the RSA conference 2015 award for outstanding achievements in mathematics. He is a co-founder of the companies Cryptomathic and Partisia.

JESPER BUUS NIELSEN is an associate professor in the Department of Computer Science, Aarhus University. He is a co-founder of the company Partisia.

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

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
Information on this title: www.cambridge.org/9781107043053

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

Contents

Preface

This is a book on information theoretically secure multiparty computation (MPC) and secret sharing and about the intimate and fascinating relationship between the two notions. We decided to write this book because we felt that a comprehensive treatment of unconditionally secure techniques for MPC was missing in the literature. In particular, because some of the first general protocols were found before appropriate definitions of security had crystallized, proofs of those basic solutions have been missing so far.

We present the basic feasibility results for unconditionally secure MPC from the late 1980s, generalizations to arbitrary access structures using linear secret sharing, and a selection of more recent techniques for efficiency improvements. We also present our own simplified variant of the Universally Composable (UC) framework in order to be able to give complete and modular proofs for the protocols we present.

We also present a general treatment of the theory of secret sharing, in particular, secret-sharing schemes with additional algebraic properties, which is also a subject missing in textbooks. One of the things we focus on is asymptotic results for multiplicative secret sharing, which has various interesting applications that we present in the MPC part.

Our ambition has been to create a book that will be of interest to both computer scientists and mathematicians and can be used for teaching at several different levels. We have therefore tried to make Parts I and II self-contained units, even if this implies some overlap between the parts. This means that there are several different ways to read this book; we give a few suggestions in the following paragraphs. In particular, the concept of secret sharing, of course, appears prominently in both parts. In Part I, on MPC, however, it is introduced only as a tool on a "need-to-know" basis. In Part II, we reintroduce the notion, but as a general concept that is interesting in its own right and with a comprehensive treatment of the mathematical background.

This book is intended to be self-contained enough to be read by advanced undergraduate students, and the authors have used large parts of the material in the book for teaching courses at this level. By covering a selection of more advanced material, the book can also be used for a graduate course.

How to Use This Book

For a course on the advanced undergrad level for computer science students, we recommend covering Chapters 1 through 5. This will include the basic feasibility results for unconditionally secure MPC and the UC model. For some extra perspective, it may also

be a good idea to cover Chapter 7, which is basically a survey of cryptographically secure solutions.

For a graduate-level computer science course, we recommend including also Chapters 8 and 9 because they contain several recent techniques and survey some open problems.

For a course in mathematics on secret sharing and applications, we recommend covering Chapters 1, 3, and 6 first. This will provide an intuition for what secret sharing is and how it is used in MPC. Then Part II should be covered to present the general theory of algebraic secret sharing. Finally, the last part of Chapter 9 can be used to present some of the more advanced applications.

Acknowledgments

We thank Alp Bassa, Morten D. Bech, Wieb Bosma, Ignacio Cascudo, Iwan Duursma, Morten Dahl Jørgensen, Serge Fehr, Helene Flyvholm Haagh, Irene Giacomelli, Lingfei Jin, Michiel Kosters, Carolin Lunemann, Antonio Macedone, Diego Mirandola, Carles Padró, Gabriele Spini, Anders Vinther, Chaoping Xing, and Sarah Zakarias for doing an enormous amount of work in proofreading and commenting. We also thank Sarah Zakarias for writing some of the simulation proofs and helping us to avoid many more mistakes than are present now.

RC would like to warmly thank the School of Mathematical Sciences at Nanyang Technological University in Singapore for its excellent hospitality during his frequent visits throughout the years for research and work on parts of this book.