SpringerBriefs in Computer Science

More information about this series at http://www.springer.com/series/10028

Niklas Büscher • Stefan Katzenbeisser

Compilation for Secure Multi-party Computation

Springer

Niklas Büscher
Security Engineering Group
Technische Universität Darmstadt
Darmstadt, Germany

Stefan Katzenbeisser
Security Engineering Group
Technische Universität Darmstadt
Darmstadt, Germany

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-3-319-67521-3 ISBN 978-3-319-67522-0 (eBook)
https://doi.org/10.1007/978-3-319-67522-0

Library of Congress Control Number: 2017954354

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

In memory of Helmut Veith.

Preface

An ever-growing amount of data is processed by online services every day. Unfortunately, data owners are at risk to lose control over their possibly sensitive data once it is deployed at an untrusted third party. A solution to this dilemma is Secure Multi-party Computation (MPC), which has emerged as a generic approach to realize Privacy-Enhancing Technology in a cryptographically sound manner, as it allows to perform arbitrary computations between two or more parties over encrypted data. In recent years, numerous protocols and optimizations have made MPC practical for relevant real world scenarios. This development has led to a significant improvement in the performance and size of applications that can be realized with MPC.

A major obstacle in the past was to generate MPC applications by hand. Recently special compilers have been developed to build all kinds of applications. In this book, we summarize our research on the compiler CBMC-GC for MPC over Boolean circuits. We show and explain how efficient MPC applications can be created automatically from ANSI-C, which bridges the areas of cryptography, compilation and hardware synthesis. Moreover, we give an insight into the requirements for creating efficient applications for MPC, and thus we hope that this work can be of interest not only to researchers in the area of MPC but also developers realizing practical applications with MPC.

The authors wish to thank Andreas Holzer, Martin Franz and Helmut Veith, with whom we started the research on compilers for MPC. Moreover, we wish to thank our students Alina Weber and David Kretzmer who contributed ideas and implementations to the later parts of this book. This work has been co-funded by the DFG as part of project S5 within the CRC 1119 “CROSSING” and by the DFG within the RTG 2050 “Privacy and Trust for Mobile Users”.

Darmstadt, Germany
August 2017

Niklas Büscher
Stefan Katzenbeisser

Contents