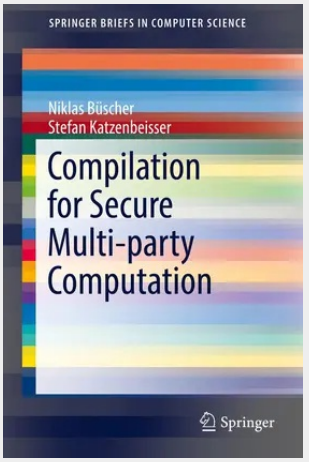
Büscher / Katzenbeisser

Compilation for Secure Multi-party Computation



This book presents a holistic view on compiler assisted practical secure multi-party computation (MPC) over Boolean circuits. It discusses that two or more parties jointly evaluate a function over their inputs in such a way that each party keeps its input unknown to the other parties in MPC. MPC provides a generic way to construct Privacy-Enhancing Technologies, which protect sensitive data during processing steps in untrusted environments. 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.

This book also explains in detail how efficient MPC applications can be created automatically from ANSI-C, thus, bridging the areas of cryptography, compilation and hardware synthesis. It also gives an insight into the requirements for creating efficient applications for MPC and is hence of interest to not only researchers in the area of MPC but also developers realizing practical applications with MPC. For a better understanding of the complete compile chain from ANSI-C to circuits, which is the ‘machine code’ of MPC, the authors first give the necessary background information on MPC protocols, Boolean logic, and logic synthesis. Then the authors describe the various compilation steps required to translate any code into an adequate circuit description. Afterwards, the authors introduce a variety of optimization techniques for two classes of MPC protocols, namely techniques that improve the runtime of applications in constant- and multi-round MPC protocols. The authors also illustrate how efficient parallelization of MPC protocols can be achieved using the assistance of compilers. It presents the effectiveness of the proposed techniques by giving a detailed evaluation on benchmarking applications. Most of the aforementioned techniques are implemented in our open source compiler that is accompanying this book and allows to study compilation for MPC in practice.Researchers who are interested in practical secure multi-party computation (MPC), and developers who are interested in realizing MPC applications in practice will find this book useful as a reference, as well as advanced-level students in computer science.

This book presents a holistic view on compiler assisted practical secure multi-party computation (MPC) over Boolean circuits. It discusses that two or more parties jointly evaluate a function over their inputs in such a way that each party keeps its input unknown to the other parties in MPC. MPC provides a generic way to construct Privacy-Enhancing Technologies, which protect sensitive data during processing steps in untrusted environments. 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. This book also explains in detail how efficient MPC applications can be created automatically from ANSI-C, thus, bridging the areas of cryptography, compilation and hardware synthesis. It also gives an insight into the requirements for creating efficient applications for MPC and is hence of interest to not only researchers in the area of MPC but also developers realizing practical applications with MPC. For a better understanding of the complete compile chain from ANSI-C to circuits, which is the ‘machine code’ of MPC, the authors first give the necessary background information on MPC protocols, Boolean logic, and logic synthesis. Then the authors describe the various compilation steps required to translate any code into an adequate circuit description. Afterwards, the authors introduce a variety of optimization techniques for two classes of MPC protocols, namely techniques that improve the runtime of applications in constant- and multi-round MPC protocols. The authors also illustrate how efficient parallelization of MPC protocols can be achieved using the assistance of compilers. It presents the effectiveness of the proposed techniques by giving a detailed evaluation on benchmarking applications. Most of the aforementioned techniques are implemented in our open source compiler that is accompanying this book and allows to study compilation for MPC in practice.Researchers who are interested in practical secure multi-party computation (MPC), and developers who are interested in realizing MPC applications in practice will find this book useful as a reference, as well as advanced-level students in

64,19 €
59,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783319675213
Medium: Buch
ISBN: 978-3-319-67521-3
Verlag: Springer
Erscheinungstermin: 27.11.2017
Sprache(n): Englisch
Auflage: 1. Auflage 2017
Serie: SpringerBriefs in Computer Science
Produktform: Kartoniert
Gewicht: 1708 g
Seiten: 93
Format (B x H): 155 x 235 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)