

Preface

Secure two-party computation, called Secure Function Evaluation (SFE), enables two mutually mistrusting parties (client & server) to evaluate an arbitrary function f on their respective private inputs x, y while revealing nothing but the result $z = f(x; y)$. Since its invention by Andrew Chi-Chih Yao in the 1980s, SFE has gained the attention of many researchers in cryptography, but was widely believed to be too inefficient for practical privacy-preserving applications. In recent years, the rapidly growing speed of computers and communication networks, algorithmic improvements, automatic generation, and optimizations of SFE protocols have made them usable in many practical application scenarios.

Engineering such efficient SFE protocols for practical privacy-preserving applications is a rapidly emerging topic in many top conferences on information security and applied cryptography and several research projects are working on this subject, e.g., the EU funded project “Computer Aided Cryptography Engineering” (CACE) or the U.S. funded project “Programming on Encrypted Data” (PROCEED). Also, for the first time companies are adapting SFE technology for their products.

In contrast to previous books, we cover the practical aspects of SFE protocols, in particular their systems and implementation aspects. Hence, this book is an ideal counterpart to Hazay and Lindell’s book “Efficient Secure Two-Party Protocols: Techniques and Constructions” (Springer 2010) which focuses on the underlying security definitions, general constructions for different adversary models, and constructions for specific two-party functionalities. While Hazay and Lindell consider the (theoretical) efficiency of protocols and stronger covert and malicious adversaries, we concentrate on today’s best performing constructions for the semi-honest adversaries setting.

We present advanced state-of-the-art techniques in the design, optimization, and applications of (practically) efficient SFE protocols. This makes the book essential for researchers, students, and practitioners in the area of applied cryptography and information security who aim to construct practical cryptographic protocols for privacy-preserving real-world applications.

Outline. This book contains the following main parts:

- *Basics of Practically Efficient Secure Function Evaluation.* We give a detailed overview on state-of-the-art techniques and optimizations for efficient Secure Function Evaluation (SFE) with special focus on their practicability. In particular, we are concerned with their performance and possibilities for pre-computations.
- *Circuit Optimizations and Constructions.* The complexity of today's most efficient SFE protocols depends linearly on the size of the Boolean circuit representation of the evaluated function. Further, recent techniques for SFE based on so-called improved Garbled Circuits (GCs) allow for very efficient secure evaluation of XOR gates. We give transformations that substantially reduce the size of Boolean circuits if the costs for evaluating XOR gates are much lower than for other types of gates. Our optimizations provide more efficient circuits for standard functionalities such as integer comparison, finding minima/maxima, and fast multiplication. Example applications that benefit from our improvements include secure first-price auctions.
- *Hardware-Assisted GC Protocols.* We improve the deployability of SFE protocols by using tamper-proof Hardware (HW) tokens. In particular, GCs can be generated by a tamper-proof HW token which is provided by the server to a client but not trusted by the client. The presented HW-assisted SFE protocol makes the communication between client and server independent of the size of the evaluated function. Further, we show how GCs can be evaluated in HW in a leakage resilient way, so-called One-Time Programs. As an application we show how the combination of GCs and tamper-proof HW allows one to securely outsource data to an untrusted cloud service provider such that arbitrary functions can be computed securely on the data with low latency.
- *Modular Design of Efficient SFE Protocols.* Automatic generation of SFE protocols from high-level specifications makes SFE usable for application programmers and yields less-error-prone implementations. We present a framework which enables one to modularly design efficient SFE protocols as a sequence of operations on encrypted data. In our framework, efficient SFE protocols based on Homomorphic Encryption and GCs can be combined while abstracting from the underlying cryptographic details. Our corresponding language and tool, called Tool for Automating Secure Two-party Computations (TASTY), allow one to describe, automatically generate, execute, and benchmark such modular and efficient SFE protocols. As an application example we consider privacy-preserving face recognition.

Comments and Errata. Your feedback on the book or any errors you may find are highly appreciated. Please e-mail your comments and errata to thomaschneider@gmail.com. A list of known errata will be maintained at <http://thomaschneider.de/engineeringSFEbook>.

Engineering Secure Two-Party Computation Protocols
Design, Optimization, and Applications of Efficient
Secure Function Evaluation

Schneider, Th.

2012, XVI, 138 p. 35 illus., Softcover

ISBN: 978-3-642-30041-7