Review of the book

"Efficient Secure Two-Party Protocols"
by Carmit Hazay, Yehuda Lindell
Springer, 2010

ISBN: 978-3-642-14303-8

Maria Cristina Onete
CASED (TU Darmstadt)

1 What the book is about

This book provides a rigorous introduction to a smaller example of general secure multiparty computation (SMC), namely the case of two-party protocols. The approach is structured somewhat top-down: the authors first explain notions of security and security definitions for their chosen scenario, namely that of two-party protocols, with a static adversary, in the stand-alone model; then they look closer into a generic way of constructing SMC for any functionality (based on garbled circuits), explaining how the construction must be altered in order to provide for stronger adversaries; and finally they look at some concrete types of protocols, such as Sigma protocols, a limited type of oblivious transfer, and private list searching.

This book is not meant for those in search of a compiled list of constructions for secure multiparty computation – or even of known two-party protocols. The focus of the book is not so much the constructions themselves (though these constructions are fundamental and should be studied in detail) as *how* to construct new protocols for given security requirements, *what* security guarantees one may hope to achieve, and finally *how* to prove protocols secure in one of various models. Though technical, the book is not overwhelming in density and is a good way of learning a way to look at cryptography in general, i.e. from the point of view of provable security.

The book could be divided in three parts, as described also in the Preface. These parts can be summarily described as follows:

① **Part I: Introduction and Definitions.** This part consists of two chapters: *Introduction* and resp. *Definitions.* I recommend going through the introductory chapter before starting to read the book, whether the reader is already somewhat-versed in multiparty computation or not. Far from giving a shallow description of the remainder of the book, the introduction is meant to explore the significance of secure multiparty computation and the importance of security models towards achieving security in many applications. In this chapter, the reader becomes acquainted with terms such as semi-honest, malicious, and covert adversaries, and in particular some subtleties of modelling are explained and explored. The introduction is a good point to decide whether you are interested in the book or not, since the style in which it is written, and the general topics it presents will also carry through in the remainder of the book. A particular positive point in this chapter is the structured discussion of how the security of SMC is generally defined, starting from the security goal continuing with the attack model, comprising: (1) types of corruption strategies (static vs. dynamic); (2) type of adversary (semi-honest, malicious, or an intermediate adversary between the two); and (3) attack complexity (polynomial time vs. unbounded).

The second chapter, *Definitions* offers a good treatment of the two-party stand-alone model with static corruptions. This is in many ways the most technical part of the book, and it has quite a few definitions. However, a positive point is that most of the definitions are also intuitively explained, and the structure of the book is such that reading through the entire chapter provides a cohesive, and quite complete story. The definitions start from the easier case of a semi-honest adversary, where the authors explain more technical concepts, such as functionalities, party view and output, and protocol security. More technical insight is also given into how to write the definition, i.e. real/ideal world definitions vs. simulation-based security, where a part's view must be simulated (in polynomial time) given just its input and output. From the semi-honest case, the model is then extended towards malicious behaviour, where an adversary can also: abort protocol executions, send correct inputs, or send other inputs. Intermediate flavours are also considered, such as: (i) augmented semi-honest behaviour, (ii) covert behaviour, where adversaries may cheat, but if so, they are caught cheating. For the reader who is not familiar with provable security, this chapter will be somewhat difficult to stomach, as it presents quite a few subtle differences in modelling, which are hard to grasp even with the aid of several well-placed remarks in the text. However, *without* this chapter, the book will lose a great deal of its value. In my opinion, the strength of this book, and its main goal, is to build a structured comprehension of SMC, and this cannot be done without understanding basic approaches and terminology in provably security. In this sense, Part I of the book is its core.

② **Part II: General Constructions.** This part consists of three chapters, namely *Semi-honest Adversaries*, resp. *Malicious Adversaries*, and *Covert Adversaries.* The core topic of this part is Yao's garbled circuit construction, presented in more detail in sections 3.3 and 3.4. The full construction is introduced step-by-step in Chapter 3 and then discussed more technically in Chapter 4 and 5. The transition between adversary models is gradual, and the modifications to the constructions are explained in a constructive way, such that the reader can learn to extrapolate the same kind of reasoning to other types of e.g. functionalities or attack models. The pinnacle of this gradual analysis is the case of covert adversaries, where the protocol needs to provide for cheating adversaries. The chapter on *Covert Adversaries* can serve both as instructional reading and as an exercise. Indeed, Chapters 3 and 4 serve to introduce the protocol and then to explain how constructions need to be adapted when the model changes; having the model for covert adversaries presented in Chapter 2, the reader can try to adjust the construction first on their own, and then read Chapter 5. Alternatively, one can simply follow the constructive reasoning from Chapter 3 and 4 into Chapter 5.

These three chapters are quite technical, in the sense that they present formal security proofs. These proofs are nevertheless well structured and aired; a reader could also, as an exercise, follow a part of the proof and then try to duplicate the reasoning in order to prove a following step. At the end of Chapter 4 there is a list of suggestions for further reading, which could be a building point for the reader who is already quite familiar with the topic. Another important feature, worth mentioning, is that each construction comes with an analysis of its efficiency; this allows for a comparative study of how much complexity is added e.g. when stronger adversaries are considered.

③ **Part III: Specific Constructions.** This part consists of four chapters, each introducing a different type of functionality, i.e. *Sigma Protocols and Efficient Zero-Knowledge*, resp. *Oblivious Transfer and Applications*, *The k-th Ranked Element*, and *Search Problems*. Though these functionalities are by no means the only ones existing in the literature, they are representative in that they usually involve very different constructions and security requirements. The first of these chapters, namely Chapter 6, is quite technical, and it focuses chiefly on zero-knowledge. The focus is not so much on where such protocols are used in bigger constructions; rather, the idea is to present proofs of knowledge as a particular type of 2-party functionality, and to show how to construct it efficiently. The build-up starts from Sigma protocols, and how they can be used for zero-knowledge proofs of knowledge, and the final part of the chapter shows how to construct commitment schemes from proofs of knowledge. I found Chapter 7 much more interesting than Chapter 6, in that it shows not just a general view of Oblivious Transfer, but several aspects of it, from constructions (five protocols are given), to analysis, to special properties: privacy-only, fully-simulatable, batch oblivious transfer, etc. A very interesting follow-up of the oblivious transfer protocols is the private pseudo-random function evaluation functionality; the interest here lies particularly in the fact that pseudo-random functions are such fundamental cryptographic primitives.

Chapters 8 and 9 are somewhat related, concerning data sets. The former chapter looks at the k-th ranked element in the *union* of two sorted data sets (each subset corresponding to one party). In particular, an application of this problem is computing a measure of location for these sets, such as the median. In fact, the strategy in this chapter is to reduce the computation of the k-th ranked element to computing the median. The authors also discuss the modifications in an underlying greater-than functionality, which are necessary in order to move from the semi-honest to the malicious adversary model. Chapter 9 takes the issue of private data sets one step further, considering now database search. This last chapter contains more protocols than most of the previous ones, and it includes general full database searches, but also more specialised searches, such as document searches. A very interesting part of the last chapter is a brief introduction to resource-constrained devices, specifically smart-cards, where the authors show why they are useful, how they are deployed, and the characteristics that protocols must have in order to be implemented on such devices. A particularly popular application of database searches is text search and pattern matching, topics which are briefly covered in the last sections of the book.

2 What is the book like (style)?

This is a rather technical book, following approaches of provable security. That being said, it is not too dense, and its structure is constructive, in the sense that it strives to construct a basic knowledge of provable security in two-party protocols. The core of the book, and a definite must-read, is Part I, which consists of two chapters, an introduction and a chapter on definitions and security models. This is a good way to learn whether the book is useful for you or not: if the content of the first chapter appeals to you and you can read the technical part in Chapter 2, then you will probably like this book.

Though technical and sometimes highly formal, the book also includes a lot of informal insight into definitions, proof strategies, protocols, and aspects of modelling. The syntax is not overly formal: whenever it is not absolutely necessary the authors skip formalism. For readers wondering why it is even relevant to be so precise in modelling, the authors often draw parallels between attack models and what we call “real-life”, also discussing advantages and disadvantages of model formalisation. A very good example of the instructional build-up of this book is the way Chapter 2 builds towards a meaningful definition for a covert adversary, where the authors also discuss why we need formalism to reflect reality. In particular, the book shows the tricky points in writing a good definition, and where the modelling might get rough. Similarly, the build-up towards Chapter 5 (which handles generic constructions for covert adversaries) is made gradually, by first presenting a basic construction for semi-honest adversaries, modifying it, with a security proof, for malicious adversaries, and finally adjusting it again for covert adversaries.

The book does *not* focus on constructions, though several constructions are given and analyzed. I consider the book more of a guide to how one can analyze and build new constructions than a compendium of existing work. Indeed, apart from the general GMW construction, there are precious few other constructions, all presented in Part III. However, each construction is very rigorously treated and its applications are also discussed.

3 Would you recommend this book?

I would heartily recommend this book to anyone who is interested in provable security and secure multiparty computation, especially students just starting on the topic of cryptography. More than the topics themselves, the book tries to teach a way of learning and analysing cryptography, which is expressed through formalisms, but not centred around them. The top-down approach ensures that the learning process goes smoothly, and terms used in earlier chapters are re-used so that they may be learned.

However, I would *not* recommend this book for the reader purely interested in recent protocols and applications of two-party protocols. The book is not intended as a collection of existing protocols, but rather as teaching material to those who are interested in the intricacies of provable security. In order to best learn from this book, I would also recommend that the reader tries to extrapolate the knowledge gathered throughout the book in order to write proofs of their own (either for constructions within the book, or for different protocols); furthermore, the reader must be aware of the fact that this is an introductory book, which focuses on a limited scenario for multiparty protocols. In order to be efficient, this book should also be followed-up by more extensive reading in the topics of security for more than 2 parties, dynamic corruptions, and sequential protocol composition.

The reviewer is a Ph.D. student at the Center for Advanced Security Research Darmstadt (CASED).