Preface

Scope

The global economy and sustainability issues are driving suppliers to new operating modes. Smart grids and their smart metering systems can yield sustainable and profitable operating modes. Thus, smart grids are important enablers of economic development. However, along with benefits, smart grids bring drawbacks. Similar to other interconnected technologies, security and privacy are crucial to smart grids. Neglecting security concerns might eventually compromise, for instance, the supply of electricity, water, or gas. Neglecting privacy concerns might cause the violation of the right to privacy of customers, enable surveillance, and permit manipulation of all customers. Indeed, smart meters are becoming ubiquitous, and smart grids face unprecedented threats. Public infrastructures might be jeopardized, and citizens might be manipulated. Luckily, Privacy-Preserving Protocols (PPPs) can solve this impasse.

Audience

This book is intended to researchers and students who are interested in the area of security and privacy. Indeed, this book's focus is smart grids. However, the techniques presented in this book can be used in several application areas, for instance, electronic voting, reputation systems, sensor networks, electronic money, mobile sensing, multiparty computation, and image processing.

Recommended Background

This book covers the topics necessary to understand the bases of security and privacy. However, the background required to have a better understanding of some equations in Chap. 6 is knowledge of cryptography and an undergraduate degree in computer science or mathematics.

Content

This work advances state-of-the-art PPPs with the development of several protocols that preserve customers' privacy and security in smart grid scenarios. Four of them are revisited and improved in this book. Such development culminated in the concept of Asymmetric DC-Nets (ADC-Nets)—from "Dining Cryptographers"—which are generalizations of additive homomorphic encryption primitives. In addition, we can use such primitives to construct ADC-Nets, which are cryptographic primitives for encryption, aggregation, and decryption of aggregated data. ADC-Nets underlie secure, verifiable, efficient, and scalable protocols with low communication overhead, which are independent of trusted parties and resistant to collusion. Furthermore, smart meters can send the minimum number of required messages directly to their supplier. Thus, they can sign their messages, and as consequence, the protocols can ensure non-repudiation and fault tolerance. The former ensures that customers cannot deny the messages of their smart meters if these were transmitted. The latter ensures that their supplier can detect smart meters with failure—in themselves or in the communication channel—and can run the protocols without the compromised smart meters. Moreover, ADC-Nets can enforce customers' privacy.

Besides the concept and results of ADC-Nets, this book presents other contributions listed as follows:

- This book contextualizes smart metering systems in smart grids around the world and points out the needed models to have security and privacy in smart grid scenarios. Furthermore, it reviews the state of the art of privacy-enhancing technologies for smart metering systems.
- This book presents three scenarios, which require remote and frequent measurements. In addition, it assesses the minimum requirements for PPPs. Moreover, it is shown how computations can be done over encrypted measurements.
- An algebraic and a probabilistic analysis show that PPPs cannot keep customers' privacy secure using data aggregation with a small number of customers. Counterintuitively, when the number of measurements increases, the effectiveness of PPPs also increases. The optimal effectiveness is achieved when the sum of measurements and the number of smart meters are equal. These results are independent of PPPs.

- The four selected PPPs have different interesting properties. The first protocol leads to the conjecture that it has the fastest encryption algorithm, because it requires only a "one-way function." The second is based on elliptic curves, and further, the encryption algorithm uses only two scalar multiplications that lead to a fast protocol. The third uses an ADC-Net and inherits its benefits. When the level of security is increased, the second and the third protocol become increasingly faster than typical solutions. The fourth follows the laws of quantum mechanics, which surprisingly implies that the smart meters do not need to store a key, but they can send messages directly to their supplier without compromising privacy.
- To compare the protocols' performance, this book presents simulations with millions of real-world measurements that validate the theoretical results. It is shown that the raw dataset has inconsistencies, which reinforce the necessity to verify the truthfulness of the transactions. Encrypted measurements are necessary and sufficient to determine whether the computations and the measurements are correct.

Besides smart grids, several application areas can use the results of this book. ADC-Nets can be used to create several protocols provided with security, privacy, verifiability, scalability, reliability, efficiency, etc.

More important than efficiency, PPPs should enforce the security of customers' privacy by means of cryptography. Considering smart grids, PPPs are paramount for suppliers, for customers, and for the proper development of society.

Highlights

The following results of this book can be highlighted:

- This book presents limitations for all PPPs with data aggregations.
- This work introduces the concept of ADC-Nets.
- ADC-Nets have interesting properties including verification.
- This book presents an efficient ADC-Net.
- ADC-Nets are generalizations of additive homomorphic encryption.
- This work can be transferred to several other applications.

Acknowledgments

Many people have influenced my life for me to publish this book.

I'm thankful for all of them. Thank you very much!

Some people participated more intensively in this journey. Special thanks to my family and my Doktorvater.

I thank Prof. Max Mühlhäuser and Prof. Fengjun Li for the inspiration, talks, and corrections. I thank Renata and Lawrence Hamtil for proofreading.

I thank all my coauthors, especially those whose papers are references of this work. Thank you: Prof. Max Mühlhäuser, Prof. Leonardo Martucci, Prof. Renato Portugal, Prof. Johannes Buchmann, Prof. Franklin Marquezino, Prof. Nadia Nedjah, Prof. Pedro Lara, Dr. Raqueline Santos, Dr. Florian Volk, Dr. Filipe Beato, Dr. Denise Demirel, Dr. Albrecht Petzoldt, and Leon Böck. I also thank our editors and anonymous reviewers for their helpful comments.

I thank Prof. Neal Koblitz for interesting discussions about algebra, number theory, and cryptography.

Many friends of mine have made my life better. I thank all of them. In particular, three of them have been closer during this work. I thank Leonardo Martucci, Gino Brunetti, and Gerald Heinig.

Petrópolis, Brazil Fábio Borges de Oliveira
February 2015

http://www.springer.com/978-3-319-40717-3

On Privacy-Preserving Protocols for Smart Metering Systems
Security and Privacy in Smart Grids
Borges de Oliveira, F.
2017, XXVII, 143 p. 41 illus., 37 illus. in color., Hardcover
ISBN: 978-3-319-40717-3