Preface

Power system safety has been drawing increasing public attention, and there have been extensive efforts in both industry and academia to mitigate the impacts of power system failures. Recent advances in information and communications technology and smart grid evolution bring promising new ways to facilitate power system security and mitigate system failure rate.

The concept of smart grid has been proposed with expectation to provide a coordinated, efficient, reliable, robust, and secure power generation, transmission, and distribution. Precisely, smart grid is comprised of three main parts: smart infrastructure system, smart communication system, and smart management system. The smart infrastructure system is the physical power infrastructure integrated with intelligent electronic devices underlying the smart grid. It supports not only the two-way flow of electricity but also the integration of renewable power resources. The smart communication system is grounded on the wide-area measurement architecture that collects the real-time status across the widespread power system. The smart management system is the most critical subsystem in smart grid, which provides advanced real-time data analysis, operation management, and control services based on the aforementioned two subsystems. Effective and efficient coordination of the three partitions is expected to achieve promising objectives.

However, without strong security and privacy-preserving mechanisms in place, the smart grid will not only inherit the massive existing vulnerabilities of the legacy power grid but also introduce new potential class of vulnerabilities with the integration of various novel technologies. Many security threats (like worms, malwares, insider attacks, etc.) have been reported for the existing power system till now, which result from both physical space and cyber space.

Particularly, secure and privacy-preserving data aggregation is one of the main challenges in smart grid communications. Smart grid is characterized by the real-time data analysis, monitoring, and control, which means massive measurement data of the system status and the customer's detailed electricity usage will be collected and reported to the system control center. This feature will cause considerable communication burden toward the whole network. As a result, an efficient data aggregation scheme is expected to effectively reduce such communication burden

in smart grid communications. In addition, the detailed electricity usage data will inevitably expose the customers' personal privacy once they are leaked to unauthorized parties. Therefore, preservation of customer privacy has also been considered as a critical issue in smart grid communications.

In this monograph, we focus on the secure data aggregation and customer privacy issues in smart grid communications. We first provide an overview of security and privacy issues in smart grid communications, as well as the challenges in addressing these issues, and then introduce several privacy-enhancing aggregation techniques for smart grid communications. Note that these privacy-enhancing aggregation techniques naturally can also be applied in other Internet of Things (IoT) scenarios.

There are total eight chapters in *Privacy-Enhancing Aggregation Techniques for Smart Grid Communications*. These are organized as follows:

Chapter 1 introduces the background of smart grid system and identifies its security and privacy challenges, particularly focusing on the data aggregation techniques in smart grid communications.

Chapter 2 discusses two popular homomorphic public key encryption (PKE) techniques, i.e., Paillier PKE and Boneh-Goh-Nissim (BGN) PKE, which serve as the preliminary for building most privacy-enhancing aggregation techniques in the rest of the chapters of this monograph. In addition, the Java source codes of the two homomorphic PKEs are also provided for the interested readers to better understand and implement them.

Chapter 3 presents the first privacy-enhancing aggregation technique in this monograph, i.e., a privacy-preserving multidimensional data aggregation (PPMDA) scheme, which utilizes the unique data characteristics, i.e., nearly real-time data collection and small-size individual data in smart grid, to provide a much efficient data aggregation for smart grid communications.

Chapter 4 proposes another flexible and fine-grained privacy-preserving subset data aggregation (PPSDA) scheme for secure smart grid communications, and the Java source code is also provided at the end of the chapter.

Chapter 5 introduces a multifunctional data aggregation scheme, named MuDA, for privacy-preserving smart grid communications, achieving privacy-preserving aggregation of multiple functions such as average, variance, one-way ANOVA, etc.

Chapter 6 presents a privacy-preserving data aggregation scheme with fault tolerance, named PDAFT, for smart grid communications. Because PDAFT supports the fault-tolerant feature, even when some user failure or server malfunction occurs, PDAFT can still work well.

Chapter 7 discusses a new secure data aggregation scheme, named DPAFT, for secure smart grid communications, which can not only support fault tolerance but also resist against the differential privacy attacks in smart grid communications.

Chapter 8 proposes another secure data aggregation scheme to achieve privacy preservation and data integrity with differential privacy and fault tolerance, obtaining a good tradeoff of accuracy and security of differential privacy for arbitrary number of malfunctioning smart meters.

Finally, I hope this monograph can provide the interested readers with some valuable insights on the design and deployment of future privacy-preserving data aggregation techniques in IoT scenarios in general and smart grid communications in particular.

Singapore, Singapore Rongxing Lu
January 2016

http://www.springer.com/978-3-319-32897-3

Privacy-Enhancing Aggregation Techniques for Smart Grid Communications

Lu, R.

2016, XVI, 177 p. 28 illus., Hardcover
ISBN: 978-3-319-32897-3