

Preface

A smart grid has emerged as a promising solution to the next generation power grid system. It utilizes information and communications technology to gather and act on information, such as the behavior of suppliers and consumers, in an automated fashion to improve the reliability, efficiency, economics, and sustainability of the generation and distribution of electricity. However, security and privacy issues still present practical concerns to the deployment of smart grids. In this book, we investigate three schemes for secure and privacy-preserving smart grid communications.

In Chap. 2, we present an efficient privacy-preserving demand response scheme which employs a homomorphic encryption to achieve privacy-preserving demand aggregation and efficient response. In addition, an adaptive key evolution technique is further investigated to ensure the users' session keys to be forward secure. In Chap. 3, we introduce an efficient authentication scheme which utilizes the Merkle hash tree technique to secure smart grid communication. Specifically, the proposed authentication scheme considers the smart meters with computation-constrained resources and puts the minimum computation overhead on them. In Chap. 4, an efficient fine-grained keywords comparison scheme is proposed. Based on the homomorphic Paillier cryptosystem, we use two super-increasing sequences to aggregate multidimensional keywords. As a result, the comparison between the keywords of all sellers and those of one buyer can be achieved with only one calculation.

This book presents an overview of the state-of-the-art solutions to secure and privacy-preserving communications in smart grids. It not only reveals unique security and privacy characteristics but also offers effective solutions. Security analysis and performance evaluation demonstrate effectiveness and efficiency of three schemes. Last but not least, this book highlights promising future research directions to guide interested readers.

Sichuan, China

Hongwei Li



<http://www.springer.com/978-3-319-04944-1>

Enabling Secure and Privacy Preserving
Communications in Smart Grids

Li, H.

2014, XI, 62 p. 20 illus., Softcover

ISBN: 978-3-319-04944-1