

# Preface

How to query over encrypted data is an important and challenging problem for the smart grid, especially when encryption is required to protect data privacy for decision making. Though querying encrypted data has been well researched in both cryptography and database communities, little attention has been paid to the multidimensional characteristics of metering data in the smart grid. Therefore, the existing query techniques cannot be directly applied to the smart grid. In this brief, we provide a comprehensive study of encrypted data query in the smart grid. Three kinds of queries are introduced, namely, equality query, conjunctive query and range query. Detailed security and performance analysis are also provided. Future research directions are suggested. We hope this brief could be a useful reference for graduate students and professionals who are interested in encrypted data query in smart grid.

In Chap. 1, we give an overview of the concept of the smart grid architecture and discuss the security challenges of the smart grid and the existing encrypted data query techniques. In Chap. 2, we present an efficient Searchable Encryption Scheme for Auction (SESA). Specifically, public key encryption with keyword search is used to enable the energy sellers to inquire potential winner from the auction server while preserving the privacy of the energy buyers. In addition, an extension of SESA is proposed to support detailed filtering of the bids. In Chap. 3, we address the conjunctive query problem in the smart grid. An Efficient Conjunctive Query (ECQ) scheme is proposed to support conjunctive keywords query on multiple dimensions. To resolve the data privacy problem in financial auditing for the smart grid, we introduce a novel privacy-preserving range query scheme over encrypted metering data, named PaRQ, in Chap. 4. Finally, we draw conclusions and outline future research directions in Chap. 5.

We would like to thank our BBCR colleagues for their valuable comments on the brief. We also would like to thank the Springer editors and staff for their great help in getting this brief published. This research work was supported by the National Natural Science Foundation of China under Grant No. 61373152, No. 61272437 and No. 61202369; NSERC, Canada; Innovation Program of Shanghai Municipal

Education Commission No. 13ZZ131, No. 14YZ129; Foundation Key Project of Shanghai Science and Technology Committee No. 12JC1404500, and Project of Shanghai Science and Technology Committee No. 12510500700.

Shanghai, China  
Nanyang, NH, Singapore  
Hanover, USA  
Shanghai, China  
Waterloo, ON, Canada

Mi Wen  
Rongxing Lu  
Xiaohui Liang  
Jingsheng Lei  
Xuemin (Sherman) Shen

Querying over Encrypted Data in Smart Grids

Wen, M.; Lu, R.; Liang, X.; Lei, J.; Shen, X.S.

2014, IX, 78 p. 22 illus., 17 illus. in color., Softcover

ISBN: 978-3-319-06354-6