

Contents

- 1 Introduction to Smart Grids** 1
 - 1.1 Smart Grids..... 1
 - 1.1.1 Communication Network Architecture 1
 - 1.1.2 Characteristics of Smart Grids 2
 - 1.2 Research Topics in Smart Grids 4
 - 1.3 Security Primitives 6
 - 1.3.1 Homomorphic Encryption..... 6
 - 1.3.2 Bilinear Pairing 7
 - 1.3.3 Identity-Based Signature 7
 - 1.3.4 Merkle Hash Tree..... 7
 - 1.4 Summary 8
 - References 9
- 2 Privacy-Preserving Demand Response in Smart Grids**..... 11
 - 2.1 Introduction 11
 - 2.2 Models and Design Goal..... 12
 - 2.2.1 Network Model 12
 - 2.2.2 Security Model 13
 - 2.2.3 Design Goal 14
 - 2.3 Methodologies 14
 - 2.3.1 System Initialization 14
 - 2.3.2 Demand Aggregation 15
 - 2.3.3 Demand Processing and Response 17
 - 2.3.4 Key Evolution 18
 - 2.4 Security Analysis..... 20
 - 2.4.1 Authenticity, Data Integrity and Confidentiality 20
 - 2.4.2 Privacy Preservation of Electricity Demand 21
 - 2.4.3 Forward Secrecy of Users’ Session Keys 22
 - 2.4.4 Evolution of Users’ Private Keys 24

2.5	Performance Evaluation	25
2.5.1	Communication Overhead.....	25
2.5.2	Computation Overhead	26
2.6	Related Works	27
2.7	Summary	29
	References	29
3	An Efficient Authentication Scheme in Smart Grids.....	31
3.1	Introduction	31
3.2	Models and Design Goal.....	33
3.2.1	Network Model	33
3.2.2	Threat Model.....	33
3.2.3	Design Goal	34
3.3	Methodologies	35
3.3.1	System Initialization	35
3.3.2	Reports Generation	37
3.3.3	Neighborhood Gateway Authentication	37
3.4	Security Analysis.....	39
3.4.1	Resist the Message Analysis Attack	39
3.4.2	Resist the Message Modification Attack.....	39
3.4.3	Resist the Replay Attack	40
3.4.4	Resist the Message Injection Attack	40
3.5	Performance Evaluation	41
3.5.1	Communication Overhead.....	41
3.5.2	Computation Complexity.....	42
3.6	Related Works	43
3.7	Summary	44
	References	45
4	An Efficient Fine-Grained Keywords Comparison Scheme in the Smart Grid Auction Market.....	47
4.1	Introduction	47
4.2	System Model, Security Requirements, and Design Goals	48
4.2.1	System Model.....	48
4.2.2	Security Requirements.....	49
4.2.3	Design Goals	49
4.3	Methodologies	50
4.3.1	System Initialization	50
4.3.2	Auction Message Creating	51
4.3.3	Filtering	52
4.4	Security Analysis.....	54
4.4.1	Secure Fine-Grained Keywords Comparison Between Tag and Trapdoor	55
4.4.2	Privacy Preservation of Auction Messages	55
4.4.3	Encrypted Messages' Authentication and Data Integrity	55

- 4.4.4 Private Messages’ Authentication, Data Integrity
and Confidentiality 56
 - 4.5 Performance Evaluation 56
 - 4.5.1 Computation Overhead 56
 - 4.5.2 Communication Overhead..... 58
 - 4.6 Related Works 59
 - 4.7 Summary 59
 - References 59
- 5 Conclusions and Future Directions 61**
 - 5.1 Research Conclusions..... 61
 - 5.2 Future Extensions 62



<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