

Contents

- 1 Introduction 1**
 - 1.1 Background..... 1
 - 1.2 Smart Grid 2
 - 1.2.1 Smart Infrastructure System..... 2
 - 1.2.2 Smart Communication System 3
 - 1.2.3 Smart Management System 3
 - 1.3 Security and Privacy Threats 4
 - 1.3.1 Security Threats..... 4
 - 1.3.2 Privacy Threats..... 5
 - 1.4 Security and Privacy Requirements 6
 - 1.5 Challenges 7
 - 1.5.1 User Privacy..... 7
 - 1.5.2 Secure Data Aggregation 8
 - 1.6 Related Activities 9
 - 1.7 Outline of the Book 10
 - References 10
- 2 Homomorphic Public Key Encryption Techniques 13**
 - 2.1 Paillier Public Key Encryption 13
 - 2.1.1 Mathematical Background 14
 - 2.1.2 Description of Paillier PKE 16
 - 2.2 Boneh-Goh-Nissim (BGN) Public Key Encryption 17
 - 2.2.1 Bilinear Pairing Techniques 17
 - 2.2.2 Description of BGN PKE 21
 - 2.3 Summary 22
 - References 39
- 3 Privacy-Preserving Multidimensional Data Aggregation 41**
 - 3.1 Introduction 41
 - 3.2 System Model, Security Requirements and Design Goal 44
 - 3.2.1 System Model..... 44

3.2.2	Security Requirements	45
3.2.3	Design Goal	46
3.3	Proposed PPMDA Scheme	46
3.3.1	System Initialization	47
3.3.2	User Report Generation	48
3.3.3	Privacy-Preserving Report Aggregation	48
3.3.4	Secure Report Reading and Response	49
3.4	Security Analysis	51
3.5	Performance Evaluation	54
3.5.1	Computation Complexity	54
3.5.2	Communication Overhead	56
3.6	Related Work	57
3.7	Summary	58
	References	59
4	Privacy-Preserving Subset Data Aggregation	61
4.1	Introduction	61
4.2	Models and Design Goal	63
4.2.1	System Model	63
4.2.2	Security Model	64
4.2.3	Design Goal	64
4.3	Proposed PPSDA Scheme	65
4.3.1	Hard Problems in Group with Composite Order	65
4.3.2	Description of The Proposed Scheme	65
4.4	Security Analysis	69
4.5	Performance Evaluation	72
4.6	Related Work	73
4.7	Summary	74
	References	84
5	Privacy-Preserving Multifunctional Data Aggregation	85
5.1	Introduction	85
5.2	Problem Formalization	87
5.2.1	System Model	88
5.2.2	Security Model	89
5.2.3	Design Goal	90
5.3	The Basic MuDA Scheme	90
5.3.1	System Initialization	91
5.3.2	User Report Generation	91
5.3.3	Privacy-Preserving Report Aggregation	91
5.3.4	Secure Report Reading	94
5.4	The Enhanced MuDA Version	97
5.4.1	Differential Privacy	97
5.4.2	Description of the Enhanced Version	98

5.5	Security and Utility Analysis	100
5.5.1	Security Analysis	101
5.5.2	Utility Analysis	102
5.6	Performance Evaluation	103
5.6.1	Computational Optimization of Basic Scheme	104
5.6.2	Computation Complexity	105
5.6.3	Communication Overhead Comparison	106
5.7	Related Work	107
5.8	Summary	109
	References	109
6	Privacy-Preserving Data Aggregation with Fault Tolerance	111
6.1	Introduction	111
6.2	Problem Formalization	113
6.2.1	System Model	114
6.2.2	Adversary Model	115
6.2.3	Security Requirements	115
6.2.4	Design Goal	116
6.3	Proposed PDRAFT Scheme	116
6.3.1	System Initialization	117
6.3.2	User Report Generation	117
6.3.3	Privacy-Preserving Report Aggregation	118
6.3.4	Secure Report Reading	118
6.3.5	Fault Tolerance Handling	119
6.4	Security Analysis	120
6.5	Performance Evaluation	122
6.5.1	Extension to Support Temporal Aggregation	122
6.5.2	Extension to Support Dynamic Users	123
6.5.3	Communication Overhead Comparison	124
6.6	Related Work	125
6.7	Summary	126
	References	127
7	Differentially Private Data Aggregation with Fault Tolerance	129
7.1	Introduction	129
7.2	Problem Formalization	132
7.2.1	System Model	132
7.2.2	Attack Model	133
7.2.3	Design Goal	134
7.3	Preliminary	135
7.3.1	Differential Privacy	135
7.4	Proposed Basic DPRAFT	136
7.4.1	System Initialization	136
7.4.2	Data Aggregation Request	136
7.4.3	Data Aggregation Request Relay	137

7.4.4	User Report Generation	137
7.4.5	Privacy-Preserving Report Aggregation	137
7.4.6	Secure Report Reading	138
7.5	The Enhanced DPAFT	139
7.5.1	User Report Generation	139
7.5.2	Privacy-Preserving Report Aggregation	139
7.5.3	Secure Report Reading	140
7.6	Security Analysis.....	141
7.6.1	Secure Against Eavesdropping Attack.....	141
7.6.2	Secure Against Malwares Attack	142
7.6.3	Secure in Honest-but-Curious Model.....	142
7.6.4	Secure and Reliable with Fault-Tolerance	143
7.6.5	Secure Against Differential Attack	143
7.7	Performance Evaluation	143
7.7.1	Storage Cost.....	144
7.7.2	Computation Complexity.....	144
7.7.3	Utility of Differential Privacy	145
7.7.4	Robustness of Fault Tolerance	147
7.7.5	Efficiency of User Addition and Removal.....	148
7.8	Related Work	148
7.9	Summary	150
	References	150
8	Privacy-Preserving Data Aggregation with Data Integrity and Fault Tolerance	153
8.1	Introduction	153
8.2	Problem Formalization.....	156
8.2.1	System Model.....	157
8.2.2	Attack Model.....	158
8.2.3	Design Goal	159
8.3	Preliminary	159
8.3.1	Differential Privacy	159
8.3.2	Differential Privacy via Symmetric Geometric Noise.....	160
8.4	Our Proposed Scheme	160
8.4.1	System Initialization	160
8.4.2	Data Aggregation Request	161
8.4.3	Data Aggregation Request Relay	161
8.4.4	User Report Generation	161
8.4.5	Secure Report Aggregation.....	162
8.4.6	Secure Report Reading	164
8.5	Security Analysis.....	164
8.6	Performance Evaluation	167
8.7	Related Work	174
8.8	Summary	175
	References	176

Privacy-Enhancing Aggregation Techniques for Smart
Grid Communications

Lu, R.

2016, XVI, 177 p. 28 illus., Hardcover

ISBN: 978-3-319-32897-3