

Contents

Part I Foundations

1 Introduction	3
1.1 Motivation	5
1.2 Research Questions	6
1.3 Contributions	7
1.3.1 High Level Explanation of the Selected PPPs	8
1.3.2 Summary of the Results	9
1.4 Outline	9
References	11
2 Background and Models	13
2.1 Smart Grids Around the World	13
2.2 Security and Privacy Models	17
2.2.1 Terminology in PPPs	17
2.2.2 Security Model	18
2.2.3 Privacy Model	21
References	23
3 A Selective Review	25
3.1 Solutions with Restrictive Result	25
3.1.1 Data Obfuscation by Means of Storage Banks	25
3.1.2 Anonymization Via Pseudonymous	26
3.1.3 Data Obfuscation by Means of Noise Injection	26
3.2 Solutions Addressed in This Book: Anonymization Via Cryptographic Protocols	27
3.2.1 Protocols Based on Homomorphic Encryption	28
3.2.2 Protocols Based on DC-Nets	30
3.2.3 Protocols Based on Commitment	32
References	34

Part II Contributions

4	Reasons to Measure Frequently and Their Requirements	39
4.1	Reasons for Frequent Measurements	40
4.1.1	Fraud and Energy Loss	40
4.1.2	Virtualization of the Supplier Commodity Network	41
4.1.3	Fair Distribution	43
4.2	Requirements	44
	References	46
5	Quantifying the Aggregation Size	49
5.1	Algebraic Properties	50
5.2	Probabilistic Properties	56
	References	59
6	Selected Privacy-Preserving Protocols	61
6.1	Monetary Value	62
6.2	PPP1 The Fastest	63
6.2.1	Security Analysis	65
6.2.2	Privacy Analysis	65
6.2.3	Performance Analysis	66
6.3	PPP2 Based on Commitments and ECC	66
6.3.1	Cryptographic Primitives	67
6.3.2	Proposed Protocol	71
6.3.3	Security Analysis	76
6.3.4	Privacy Analysis	77
6.3.5	Performance Analysis	78
6.4	PPP3 Based on Asymmetric DC-Nets	79
6.4.1	Cryptographic Primitives	80
6.4.2	Attacker Model	84
6.4.3	Proposed Protocol	85
6.4.4	Verification Property	86
6.4.5	Security Analysis	90
6.4.6	Privacy Analysis	90
6.4.7	Performance Analysis	91
6.5	PPP4 Based on Quantum Mechanics	92
6.5.1	Cryptographic Primitives	92
6.5.2	Proposed Protocol	93
6.5.3	Security Analysis	96
6.5.4	Privacy Analysis	97
	References	97
7	Analytical Comparison	101
7.1	Security	102
7.2	Privacy	103
7.3	Requirements	104
7.4	Verification Property	105

- 7.5 Performance 105
- 7.6 Summary 107
- References 108
- 8 Simulation and Validation 111**
 - 8.1 Dataset 111
 - 8.1.1 Anomalies 112
 - 8.1.2 Sanitized Dataset 113
 - 8.1.3 Dataset Characteristics 114
 - 8.2 Implementation of the Core Algorithms 118
 - 8.3 Simulation Parameters 118
 - 8.4 Simulation Results 119
 - 8.4.1 Encryption Algorithms 120
 - 8.4.2 Aggregation Algorithms 121
 - 8.4.3 Decryption Algorithms 123
 - 8.4.4 Overall Performance 124
 - References 126
- 9 Concluding Remarks 127**
 - 9.1 Recapitulation 127
 - 9.2 Main Results 128
 - 9.3 Outlook 128
 - 9.4 Final Remarks 129
- A Algorithms 131**
- B Parameters for ECC 133**
- C Mean Measurement by Meter 135**
- Glossary 137**
- Index 139**



<http://www.springer.com/978-3-319-40717-3>

On Privacy-Preserving Protocols for Smart Metering
Systems

Security and Privacy in Smart Grids

Borges de Oliveira, F.

2017, XXVII, 143 p. 41 illus., 37 illus. in color., Hardcover

ISBN: 978-3-319-40717-3