

Contents

Acknowledgements	i
Abstract	iii
Contents	v
List of Figures	ix
List of Tables	xiii
List of Algorithms	xiii
List of Acronyms	xv
Nomenclature	xvii
1 Introduction	1
2 Problem Statement	3
2.1 Key Aspects of Distributed Energy Management	3
2.2 Privacy Definition	6
2.3 Thesis Goal	8
2.4 Evaluation Criteria	9
3 Background and Related Work	11
3.1 Distributed Energy Management in Smart Grids	11
3.1.1 Smart Grid	11
3.1.2 Energy Management	13
3.1.3 Summary and Conclusions	17
3.2 Privacy in Distributed Energy Management	18
3.2.1 Smart Meter Data Aggregation	18
3.2.2 Demand Response	20
3.2.3 Summary and Conclusions	21
3.3 Privacy in Distributed Systems	21
3.3.1 Communication Security	22
3.3.2 Threat Models	24
3.3.3 Secret Sharing	25

3.3.4	Zero-Knowledge	25
3.3.5	Differential Privacy	26
3.3.6	Homomorphic Encryption	27
3.3.7	Summary and Conclusions	31
3.4	Scheduling	32
3.4.1	FIFO	33
3.4.2	Max-Min Fairness	33
3.4.3	Summary and Conclusions	34
3.5	Simulation of Distributed Energy Management	34
3.5.1	Scenario-Specific Simulators	35
3.5.2	Co-Simulation	36
3.5.3	Simulation Frameworks	38
3.5.4	Summary and Conclusions	39
4	Research Questions	41
5	Approaches to Privacy in DEM	43
5.1	Selection of Methods	43
5.2	Energy Management	46
5.2.1	Load Shifting	47
5.2.2	Load Adaption	50
5.2.3	Load Switching	52
5.3	Distributing the Energy Management	54
5.4	Privacy Threats	56
5.5	Basic Privacy Measures	59
5.6	Approach 1: Bucket Encryption Scheme – Privacy-Friendly Algorithm	61
5.6.1	Bucket Encryption Scheme	61
5.6.2	Remaining Privacy Threats	64
5.7	Approach 2: Homomorphic Encryption Scheme – PrivADE	64
5.7.1	Homomorphic Encryption Scheme	65
5.7.2	PrivADE ⁺	68
5.8	Clustering	70
5.9	Summary and Conclusions	72
6	SiENA – Smart Grid Simulator	75
6.1	Scope	75
6.2	Selection of Methods	77
6.3	Architecture	77
6.3.1	Modules and Scalability	78

6.3.2	Data-Basis	80
6.3.3	Households and Other Participants	83
6.3.4	Controllable Devices	84
6.3.5	Communication Network	86
6.3.6	Power Distribution Grid	86
6.3.7	Statistics	87
6.4	Simulation Showcase	88
7	Evaluation	93
7.1	Comparative Algorithms	93
7.1.1	COHDA	93
7.1.2	PowerMatcher	96
7.2	Scenario	99
7.3	Energy Management Quality	103
7.4	Privacy	107
7.5	Communicational Cost	113
7.6	Computational Cost	128
7.7	Scalability	131
7.8	Discussion of Evaluation Results	134
8	PrivADE⁺ Beyond This Thesis	137
8.1	Privacy-Preserving PowerMatcher	137
8.2	Voltage Control	139
8.3	Employee Appraisal and Bonus Payments	141
8.4	Summary and Conclusions	142
9	Conclusions and Outlook	143
9.1	Summary of Contributions and Findings	143
9.2	Future Work Directions	147
	Bibliography	149
	Contributions by Author	149
	References	150
	Appendix A Communicational Scaling	161
A.1	Data Volume	161
A.2	Convergence Time	164
	Appendix B Sample Calculation for the Paillier Cryptosystem	167