

Contents

1	Introduction	1
1.1	Smart Grid Architecture	1
1.1.1	Power System Layer	3
1.1.2	Communications Layer	3
1.2	Security Challenges in SGCN	4
1.2.1	Security Objectives in SGCN	5
1.2.2	Attacks in SGCN	5
1.2.3	Coutermeasures in SGCN	7
1.3	Existing Techniques for Encrypted Data Query	9
1.3.1	Order-Preserving Encryption	10
1.3.2	Searchable Encryption Techniques	10
1.3.3	Special Data Structure Traversal	11
1.3.4	Data Partitioning Problems	11
1.4	Security Primitives	12
1.4.1	Bilinear Pairing	12
1.4.2	PKE with Keyword Search	12
1.4.3	HEV Based Query Predicate	13
	References	15
2	Equality Query for Auction in Emerging Smart Grid Marketing	19
2.1	Introduction	19
2.2	System Model and Design Goal	20
2.2.1	Smart Grid Marketing Architecture	21
2.2.2	Security Requirements	22
2.2.3	Design Goal	22
2.3	SESA Scheme	23
2.3.1	Registration Phase	23
2.3.2	Bidding Phase	24
2.3.3	Pre-filtering Phase	24
2.3.4	Decision-of-Winner Phase	25

2.4	Extended SESA with Conjunctive Keywords Search	25
2.4.1	Registration Phase	25
2.4.2	Information Encryption	26
2.4.3	Pre-filtering Phase	27
2.5	Security Analysis	28
2.6	Performance Analysis	29
2.6.1	SESA vs. EPPKS	29
2.6.2	Extended SESA vs. EPPKS	31
2.7	Related Works	33
2.8	Summary	34
	References	34
3	Conjunctive Query over Encrypted Multidimensional Data	37
3.1	Introduction	37
3.2	System Model, Security Requirements and Design Goal	38
3.2.1	System Model	39
3.2.2	Security Requirements	39
3.2.3	Design Goal	40
3.3	The ECQ Scheme	41
3.3.1	Registration Phase	41
3.3.2	Data and Tags Encryption Phase	41
3.3.3	Conjunctive Query Phase	42
3.3.4	Data Recovery Phase	43
3.4	Performance Analysis	44
3.4.1	Security Analysis	44
3.4.2	Performance Evaluation	45
3.5	Related Works	48
3.6	Summary	49
	References	50
4	Range Query over Encrypted Metering Data for Financial Audit	51
4.1	Introduction	51
4.2	System Model, Security Requirements and Design Goal	53
4.2.1	System Model	53
4.2.2	Security Requirements	54
4.2.3	Designing Goal	55
4.3	The PaRQ Scheme	56
4.3.1	Construction of the Range Query Predicate	56
4.3.2	The Encrypted Data Deposit Phase	57
4.3.3	Range Query Phase	60
4.3.4	Enhancement with Collusion Resilience	63
4.4	Security Analysis	63
4.5	Performance Evaluation	66
4.5.1	Communication Overhead	66
4.5.2	Computation Overhead	68
4.5.3	Response Time	69

- 4.6 Related Works 72
 - 4.6.1 Security and Privacy in Smart Grid 72
 - 4.6.2 Range Query 73
- 4.7 Summary 74
- References 74
- 5 Conclusions and Future Works**..... 77
 - 5.1 Conclusions 77
 - 5.2 Future Research Directions 78

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