

Contents

1	Introduction	1
1.1	Background	1
1.2	Overview	2
1.3	Summary of Contributions	4
	References	6
2	Related Work	7
2.1	Privacy Preservation	7
2.2	Side-Channel Attacks	9
2.3	Side-Channel Leaks in Data Publishing	9
2.4	Side-Channel Leaks in Web Applications	11
2.5	Side-Channel Leaks in Smart Metering	11
	References	12
3	Data Publishing: Trading Off Privacy with Utility Through the k-Jump Strategy	17
3.1	Overview	17
3.2	The Model	21
3.2.1	The Algorithms a_{naive} and a_{safe}	22
3.3	k -Jump Strategy	24
3.3.1	The Algorithm Family $a_{jump}(\mathbf{k})$	24
3.3.2	Properties of $a_{jump}(\mathbf{k})$	26
3.4	Data Utility Comparison	28
3.4.1	Data Utility of k -Jump Algorithms	28
3.4.2	Reusing Generalization Functions	33
3.4.3	The Relationships of a_{safe} and $a_{jump}(1)$	35
3.5	Computational Complexity	37
3.6	Making Secret Choices of Algorithms	39
3.6.1	Secret-Choice Strategy	39
3.6.2	Subset Approach	41
3.7	Summary	44
	References	44

4 Data Publishing: A Two-Stage Approach to Improving Algorithm Efficiency	45
4.1 Overview	45
4.1.1 Motivating Example	47
4.2 The Model	49
4.2.1 The Basic Model	49
4.2.2 l -Candidate and Self-Contained Property	51
4.2.3 Main Results	53
4.3 The Algorithms	56
4.3.1 The RIA Algorithm (Random and Independent)	57
4.3.2 The RDA Algorithm (Random and Dependent)	59
4.3.3 The GDA Algorithm (Guided and Dependent)	61
4.3.4 The Construction of SGSS	63
4.4 Experiments	63
4.4.1 Computation Overhead	64
4.4.2 Data Utility	65
4.5 Discussion	67
4.6 Summary	69
References	69
5 Web Applications: k-Indistinguishable Traffic Padding	71
5.1 Overview	71
5.2 The Model	75
5.2.1 Basic Model	75
5.2.2 Privacy and Cost Model	76
5.3 PPTP Problem Formulation	78
5.3.1 SVSD and SVM D	79
5.3.2 MVMD	80
5.4 The Algorithms	82
5.5 Extension to l -Diversity	84
5.5.1 The Model and Problem Formulation	84
5.5.2 The Algorithms	86
5.6 Evaluation	89
5.6.1 Implementation and Experimental Settings	89
5.6.2 Communication Overhead	90
5.6.3 Computational Overhead	92
5.6.4 Processing Overhead	95
5.7 Summary	95
References	96
6 Web Applications: Background-Knowledge Resistant Random Padding	99
6.1 Overview	99
6.1.1 Motivating Example	101
6.2 The Model	102
6.2.1 Traffic Padding	103

6.2.2	Privacy Properties	103
6.2.3	Padding Method	105
6.2.4	Cost Metrics	106
6.3	The Algorithms	107
6.3.1	The Random Ceiling Padding Scheme	107
6.3.2	Instantiations of the Scheme	108
6.4	The Analysis	110
6.4.1	Analysis of Privacy Preservation	110
6.4.2	Analysis of Costs	113
6.4.3	Analysis of Computational Complexity	116
6.5	Experiment	116
6.5.1	Experimental Setting	116
6.5.2	Uncertainty and Cost vs k	117
6.5.3	Randomness Drawn from Bounded Uniform Distribution ...	117
6.5.4	Randomness Drawn from Normal Distribution	118
6.6	Summary	121
	References	123
7	Smart Metering: Inferences of Appliance Status from Fine-Grained Readings	125
7.1	Overview	125
7.2	Motivating Example	126
7.3	The Model	128
7.3.1	Adversary Model	129
7.3.2	Privacy Property	129
7.3.3	Cost Metrics	131
7.4	Summary	132
	References	132
8	The Big Picture: A Generic Model of Side-Channel Leaks	133
8.1	A General Framework for Side Channel Leaks	133
8.1.1	Application Model	133
8.1.2	Privacy Properties	135
8.1.3	Cost Metrics	136
8.1.4	Obfuscating Mechanisms	137
8.2	Instantiations of the General Model	137
8.2.1	Privacy-Preserving Data Publishing	138
8.2.2	Privacy-Preserving Traffic Padding	139
8.2.3	Privacy-Preserving Smart Metering	140
8.2.4	Others	140
8.3	Conclusion	141
8.4	Future Work	142

<http://www.springer.com/978-3-319-42642-6>

Preserving Privacy Against Side-Channel Leaks
From Data Publishing to Web Applications

Liu, W.M.; Wang, L.

2016, XIII, 142 p. 19 illus., 1 illus. in color., Hardcover

ISBN: 978-3-319-42642-6