

Foundations and Trends® in
Theoretical Computer Science
Vol. 9, Nos. 3–4 (2014) 211–407
© 2014 C. Dwork and A. Roth
DOI: 10.1561/04000000042



The Algorithmic Foundations of Differential Privacy

Cynthia Dwork
Microsoft Research, USA
dwork@microsoft.com

Aaron Roth
University of Pennsylvania, USA
aaroht@cis.upenn.edu

Contents

Preface	3
1 The Promise of Differential Privacy	5
1.1 Privacy-preserving data analysis	6
1.2 Bibliographic notes	10
2 Basic Terms	11
2.1 The model of computation	11
2.2 Towards defining private data analysis	12
2.3 Formalizing differential privacy	15
2.4 Bibliographic notes	26
3 Basic Techniques and Composition Theorems	28
3.1 Useful probabilistic tools	28
3.2 Randomized response	29
3.3 The laplace mechanism	30
3.4 The exponential mechanism	37
3.5 Composition theorems	41
3.6 The sparse vector technique	55
3.7 Bibliographic notes	64

4	Releasing Linear Queries with Correlated Error	66
4.1	An offline algorithm: SmallDB	70
4.2	An online mechanism: private multiplicative weights	76
4.3	Bibliographical notes	86
5	Generalizations	88
5.1	Mechanisms via α -nets	89
5.2	The iterative construction mechanism	91
5.3	Connections	109
5.4	Bibliographical notes	115
6	Boosting for Queries	117
6.1	The boosting for queries algorithm	119
6.2	Base synopsis generators	130
6.3	Bibliographical notes	139
7	When Worst-Case Sensitivity is Atypical	140
7.1	Subsample and aggregate	140
7.2	Propose-test-Release	143
7.3	Stability and privacy	150
8	Lower Bounds and Separation Results	158
8.1	Reconstruction attacks	159
8.2	Lower bounds for differential privacy	164
8.3	Bibliographic notes	170
9	Differential Privacy and Computational Complexity	172
9.1	Polynomial time curators	174
9.2	Some hard-to-Synthesize distributions	177
9.3	Polynomial time adversaries	185
9.4	Bibliographic notes	187
10	Differential Privacy and Mechanism Design	189
10.1	Differential privacy as a solution concept	191
10.2	Differential privacy as a tool in mechanism design	193
10.3	Mechanism design for privacy aware agents	204
10.4	Bibliographical notes	213

11 Differential Privacy and Machine Learning	216
11.1 The sample complexity of differentially private machine learning	219
11.2 Differentially private online learning	222
11.3 Empirical risk minimization	227
11.4 Bibliographical notes	230
12 Additional Models	231
12.1 The local model	232
12.2 Pan-private streaming model	237
12.3 Continual observation	240
12.4 Average case error for query release	248
12.5 Bibliographical notes	252
13 Reflections	254
13.1 Toward practicing privacy	254
13.2 The differential privacy lens	258
Appendices	260
A The Gaussian Mechanism	261
A.1 Bibliographic notes	266
B Composition Theorems for (ϵ, δ)-DP	267
B.1 Extension of Theorem 3.16	267
Acknowledgments	269
References	270

Abstract

The problem of privacy-preserving data analysis has a long history spanning multiple disciplines. As electronic data about individuals becomes increasingly detailed, and as technology enables ever more powerful collection and curation of these data, the need increases for a robust, meaningful, and mathematically rigorous definition of privacy, together with a computationally rich class of algorithms that satisfy this definition. Differential Privacy is such a definition.

After motivating and discussing the meaning of differential privacy, the preponderance of this monograph is devoted to fundamental techniques for achieving differential privacy, and application of these techniques in creative combinations, using the query-release problem as an ongoing example. A key point is that, by rethinking the computational goal, one can often obtain far better results than would be achieved by methodically replacing each step of a non-private computation with a differentially private implementation. Despite some astonishingly powerful computational results, there are still fundamental limitations — not just on what can be achieved with differential privacy but on what can be achieved with any method that protects against a complete breakdown in privacy. Virtually all the algorithms discussed herein maintain differential privacy against adversaries of arbitrary computational power. Certain algorithms are computationally intensive, others are efficient. Computational complexity for the adversary and the algorithm are both discussed.

We then turn from fundamentals to applications other than query-release, discussing differentially private methods for mechanism design and machine learning. The vast majority of the literature on differentially private algorithms considers a single, static, database that is subject to many analyses. Differential privacy in other models, including distributed databases and computations on data streams is discussed.

Finally, we note that this work is meant as a thorough introduction to the problems and techniques of differential privacy, but is not intended to be an exhaustive survey — there is by now a vast amount of work in differential privacy, and we can cover only a small portion of it.

Preface

The problem of privacy-preserving data analysis has a long history spanning multiple disciplines. As electronic data about individuals becomes increasingly detailed, and as technology enables ever more powerful collection and curation of these data, the need increases for a robust, meaningful, and mathematically rigorous definition of privacy, together with a computationally rich class of algorithms that satisfy this definition. *Differential Privacy* is such a definition.

After motivating and discussing the meaning of differential privacy, the preponderance of the book is devoted to fundamental techniques for achieving differential privacy, and application of these techniques in creative combinations (Sections 3–7), using the *query-release* problem as an ongoing example. A key point is that, by rethinking the computational goal, one can often obtain far better results than would be achieved by methodically replacing each step of a non-private computation with a differentially private implementation.

Despite some astonishingly powerful computational results, there are still fundamental limitations — not just on what can be achieved with differential privacy but on what can be achieved with *any* method that protects against a complete breakdown in privacy (Section 8).

Virtually all the algorithms discussed in this book maintain differential privacy against adversaries of arbitrary computational power. Certain algorithms are computationally intensive, others are

efficient. Computational complexity for the adversary and the algorithm are both discussed in Section 9.

In Sections 10 and 11 we turn from fundamentals to applications other than query-release, discussing differentially private methods for mechanism design and machine learning. The vast majority of the literature on differentially private algorithms considers a single, static, database that is subject to many analyses. Differential privacy in other models, including distributed databases and computations on data streams is discussed in Section 12.

Finally, we note that this book is meant as a thorough introduction to the problems and techniques of differential privacy, but is not intended to be an exhaustive survey — there is by now a vast amount of work in differential privacy, and we can cover only a small portion of it.