Local Differential Privacy: Refined Mechanism Design and Utility Analysis

by

Ye Zheng

A proposal submitted in partial fulfillment of the
requirements for the degree of Doctor of Philosophy
in Computing and Information Sciences

B. Thomas Golisano College of Computing and Information Sciences
Rochester Institute of Technology

[Month and year of Dissertation Acceptance was signed]

GCCIS Ph.D. PROGRAM IN COMPUTING AND INFORMAITON SCIENCES
ROCHESTER INSTITUTE OF TECHNOLOGY
ROCHESTER, NEW YORK

CERTIFICATE OF APPROVAL

Ph.D. DEGREE PROPOSAL

The Ph.D. Degree Proposal of Ye Zheng
has been examined and approved by the
proposal committee as satisfactory for the
proposal required for the
Ph.D. degree in Computing and Information Sciences

Ph.D. Program Director Date

Yidan Hu, Proposal Advisor Date

[External Chair's name], External Chair Date

[Committee member's name] Date

[Committee member's name] Date

Local Differential Privacy: Refined Mechanism Design and Utility Analysis

by

Ye Zheng

Submitted to the
B. Thomas Golisano College of Computing and Information Sciences Ph.D. Program in Computing and Information Sciences
in partial fulfillment of the requirements for the
Doctor of Philosophy Degree
at the Rochester Institute of Technology

Abstract

Local Differential Privacy (LDP) is a privacy model that enables users to perturb their data locally before sharing it with untrusted data collectors for analysis. This privacy model provides provable privacy guarantees for each individual user. Owing to these guarantees, it has been widely deployed by major technology companies, inducing Apple, Google, and Microsoft, to protect user privacy while still enabling the collection of data for analytics and machine learning tasks. However, a fundamental challenge of LDP is the trade-off between privacy and data utility: stronger privacy guarantees for users typically result in lower data utility for data collectors. Addressing this challenge, a central direction of theoretical LDP research is to design mechanisms that provide better data utility under the same privacy guarantee. This dissertation focuses on the central direction, aiming to advance both the design of LDP mechanisms and the analysis of data utility under LDP.

This dissertation makes four main contributions: (i) It introduces correlated perturbation of multiple attributes to improve data utility under LDP, generalizing existing independent-perturbation mechanisms; (ii) it establishes the optimality of piecewise-based mechanisms, a state-of-the-art category of LDP mechanisms for collecting bounded numerical data; (iii) building on piecewise-based mechanisms, it proposes two mechanisms for collecting individual trajectory data, which achieve higher efficiency and data utility by operating in continuous space instead of previously studied discrete space; (iv) it provides a quantification framework for theoretically analyzing data utility of classifiers under LDP-perturbed inputs, making a first step towards connecting LDP mechanisms with robustness.

Acknowledgments

This is the acknowledgements text

To the three cold, sober years I lived in Rochester,
whose quiet shaped me and whose memory I shall always carry.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Local differential privacy (LDP) mechanisms protect individual users' data privacy against untrusted data collectors by allowing each user to locally perturb their data before sharing it [2, 3]. Though the data collector receives only perturbed data, they can still learn valuable statistics while being unable to infer much about any individual user's true data, with privacy guarantees quantified by the privacy parameter ε. Due to these provable privacy guarantees, LDP mechanisms have been widely adopted by major technology companies, including Apple's operating systems [6], Google Chrome [4], and Microsoft Office [7] for collecting user statistics on-device. Furthermore, LDP is a key privacy-enhancing component in federated learning, a decentralized machine learning paradigm where users collaboratively train a global model without sharing sensitive data with a central server [1, 5].

Figure 1 illustrates the LDP model. Each user perturbs their true data using a randomized algorithm (the LDP mechanism) before sending it to the data collector.

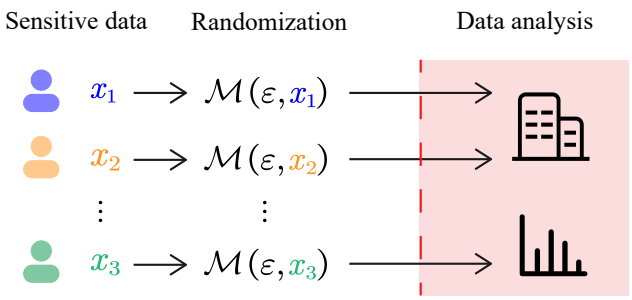

Figure 1.1: Local Differential Privacy Model. Each user perturbs their true data using an LDP mechanism before sending it to the data collector. The data collector aggregates the perturbed data to learn useful statistics while preserving individual privacy.

Table 1.1: Comparison of typical privacy-enhancing techniques.

Threat Model	Technique	Privacy Strength	Complexity	Data Utility
Trusted Collector	k-anonymity	Syntactic	Medium	High
	Central DP	Semantic (ε-DP)	Simple	ε-dependent
Untrusted Collector[a]	HE[b]	Semantic (IND-CPA)	Complex	High
	MPC[c]	Semantic (Real/Ideal)	Complex	High
	LDP	Semantic (ε-LDP)	Simple	ε-dependent

[a] For correct service functionality, an untrusted data collector is often modeled as honest-but-curious.

[b] Homomorphic Encryption (HE) typically requires that the service functionality be expressible using operations supported by the encryption scheme.

[c] Secure Multi-Party Computation (MPC) usually assumes that only a subset of parties may be malicious.

Advantages over other privacy-enhancing techniques.

can be honest-but-curious or malicious.

Compared with central DP, LDP removes trust by moving randomness to the user.

MPC's privacy is grounded in cryptographic simulation security: the formal guarantee that any adversary's view in the protocol can be simulated using only its own input and the output, implying no additional information is learned beyond what the output inherently reveals.

Challenges and research directions.

Contributions of this dissertation.

1.1 Correlated Perturbation for LDP

Chapter 3 presents a novel LDP mechanism that leverages correlation among multiple attributes

And now, here is an example paper citation [**?**], and a forward reference to Chapter 2.

If you use labels to refer to figures and document sections, then LaTeX will automatically re-number them when you move them around in a document.

This template also uses the `cite` package, which is configured to automatically sorts citations when provided in a list, even if the order does not match the order of appearance in the bibliography. For example, let's cite our papers in the reverse order they appear in the bibliography, and let

LaTeX automatically sort the citation list: [?, ?, ?].

1.2 Optimal Piecewise-based Mechanism

Some more text here

1.3 Trajectory Collection in Continuous Space under LDP

Some more text here

1.4 Quantification of Classifier Utility under LDP

Chapter 2

Background

threat model

Here is some text. And some more text. And some more text. And some more text. And some more text. And some more text. And some more text. And some more text. And some more text. And some more text. And some more text. And some more text. And some more text.

2.1 And Now, Figures

Figure 2.1: A picture of the GCCIS atrium, with mascot Ritchie. Figure captions are often at the bottom, and table captions at the top

Table 2.1: This is a table caption. Note that the third row contains a value that spans two columns. Small caps (sc) is a fun font, but isn't always used for table captions

	C1	C2
V1	120	52
V2	105	66
v3	2-col-value	

2.2 Using Tables

Above is an example of a table. While a matter of taste, it is often a good idea to place figures at the top or bottom of a page, so that they do not interrupt the main text.

Also, here are references to Chapter 1 and Section **??**, the earlier Figure (Figure 2.1), and table above (Table 2.1).

Bibliography

[1] Martín Abadi, Andy Chu, Ian J. Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 308–318. ACM, 2016.

[2] John C. Duchi, Michael I. Jordan, and Martin J. Wainwright. Local privacy and statistical minimax rates. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, Berkeley, CA, USA, October, 26-29, 2013*, pages 429–438. IEEE Computer Society, 2013.

[3] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3-4):211–407, 2014.

[4] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. RAPPOR: randomized aggregatable privacy-preserving ordinal response. In Gail-Joon Ahn, Moti Yung, and Ninghui Li, editors, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014*, pages 1054–1067. ACM, 2014.

[5] Muah Kim, Onur Günlü, and Rafael F. Schaefer. Federated learning with local differential privacy: Trade-offs between privacy, utility, and communication. In *IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2021, Toronto, ON, Canada, June 6-11, 2021*, pages 2650–2654. IEEE, 2021.

[6] Apple Machine Learning Research. Learning with privacy at scale, 2017.

[7] Sharmistha Chatterjee Sapient, Senior Manager Data Sciences at Publicis. A guide to differential privacy at scale, December 2020.

Appendices

Appendix A

Proofs

This is an appendix.

A.1 First Appendix Section

A.1.1 First Appendix Subsection

Appendix B

Complimentary Materials

This is an appendix.

B.1 First Appendix Section

B.1.1 First Appendix Subsection