

# Privacy-preserving Bandits Algorithm and Post-bandit Inference in High Dimension

Jiheng Zhang

December 6, 2024

## Contents

Abstract	ii
Objectives	iii
Pathways to Impact Statement	1
1 Background of Research	1
2 Research Plan and Methodology	1
Graphs	1
Gantt Chart	i
Education Plan	ii

## Abstract

## Objectives

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.

# Pathways to Impact Statement

- 1 Background of Research
- 2 Research Plan and Methodology

## Graphs

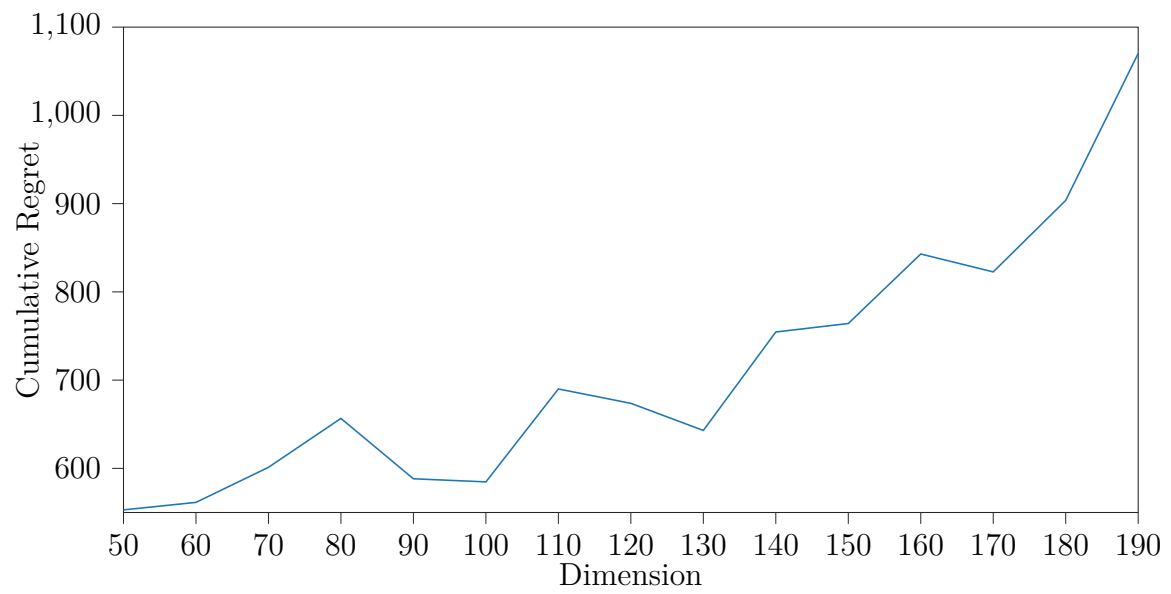
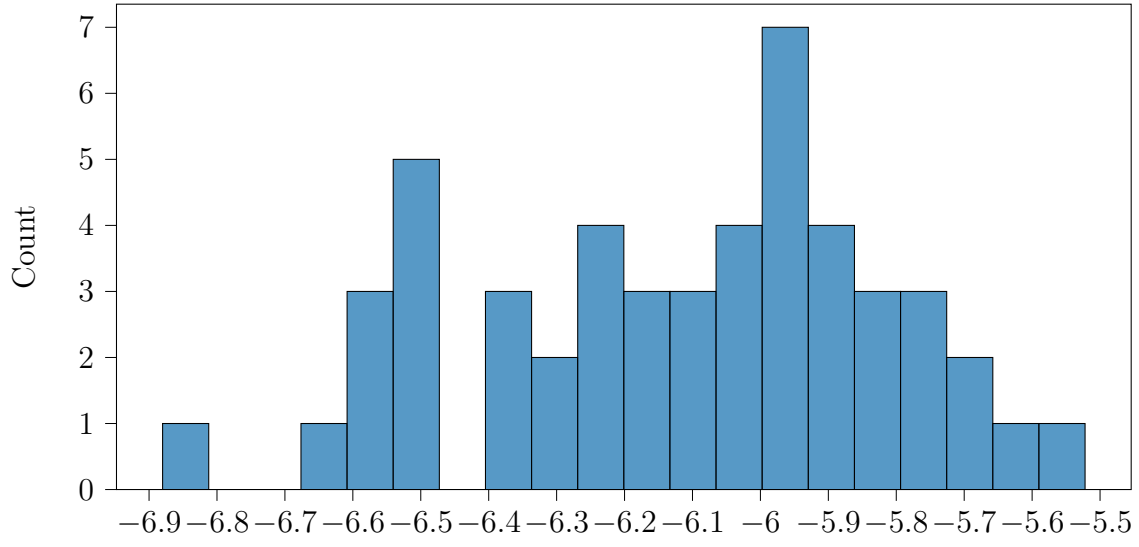
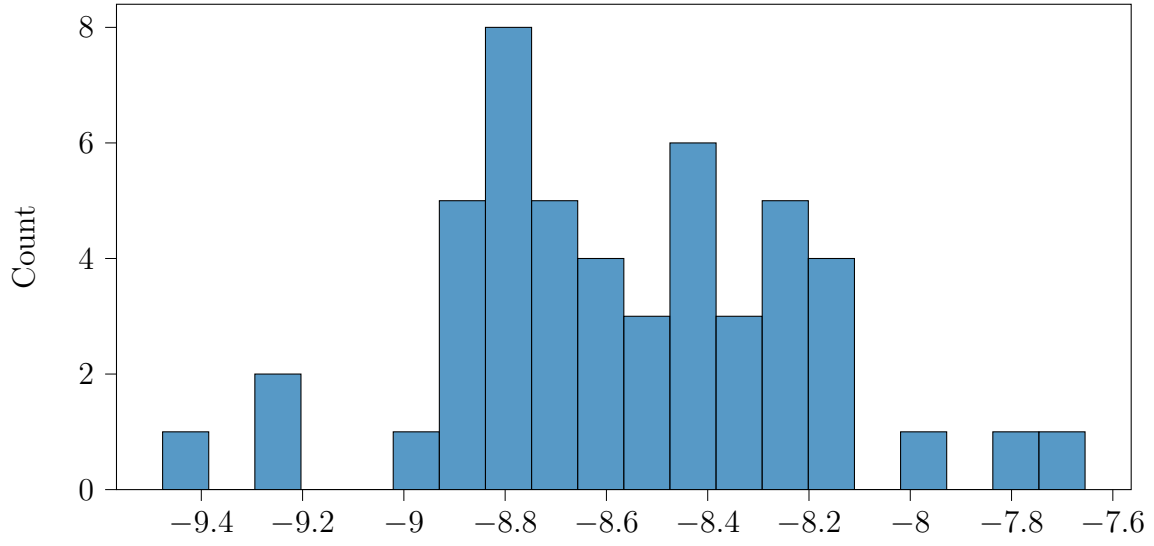


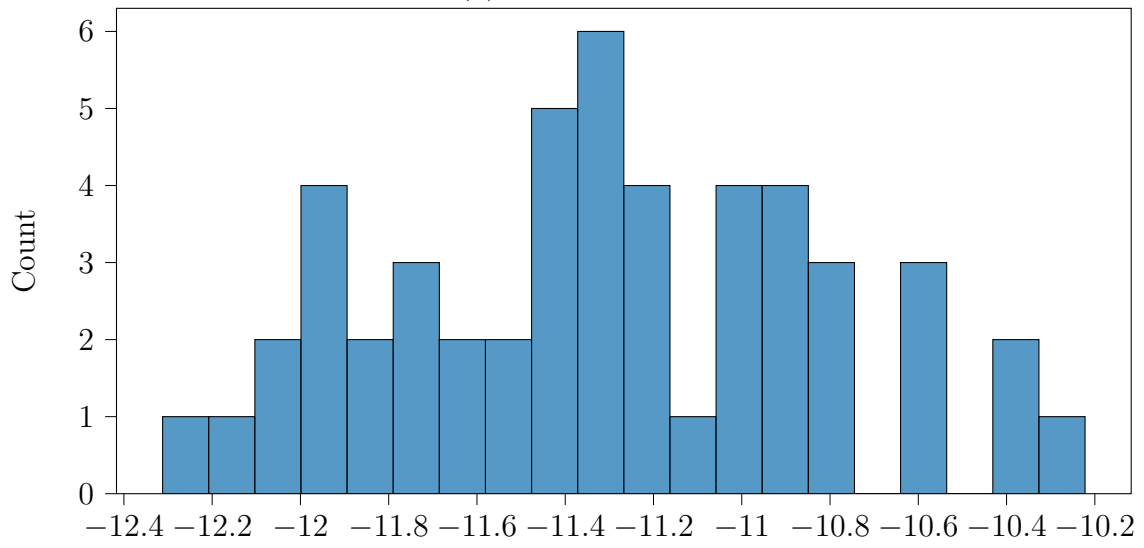
Figure 1: Gaussian Mechanism + Lasso Bandits



(a) Dimension  $d = 50$



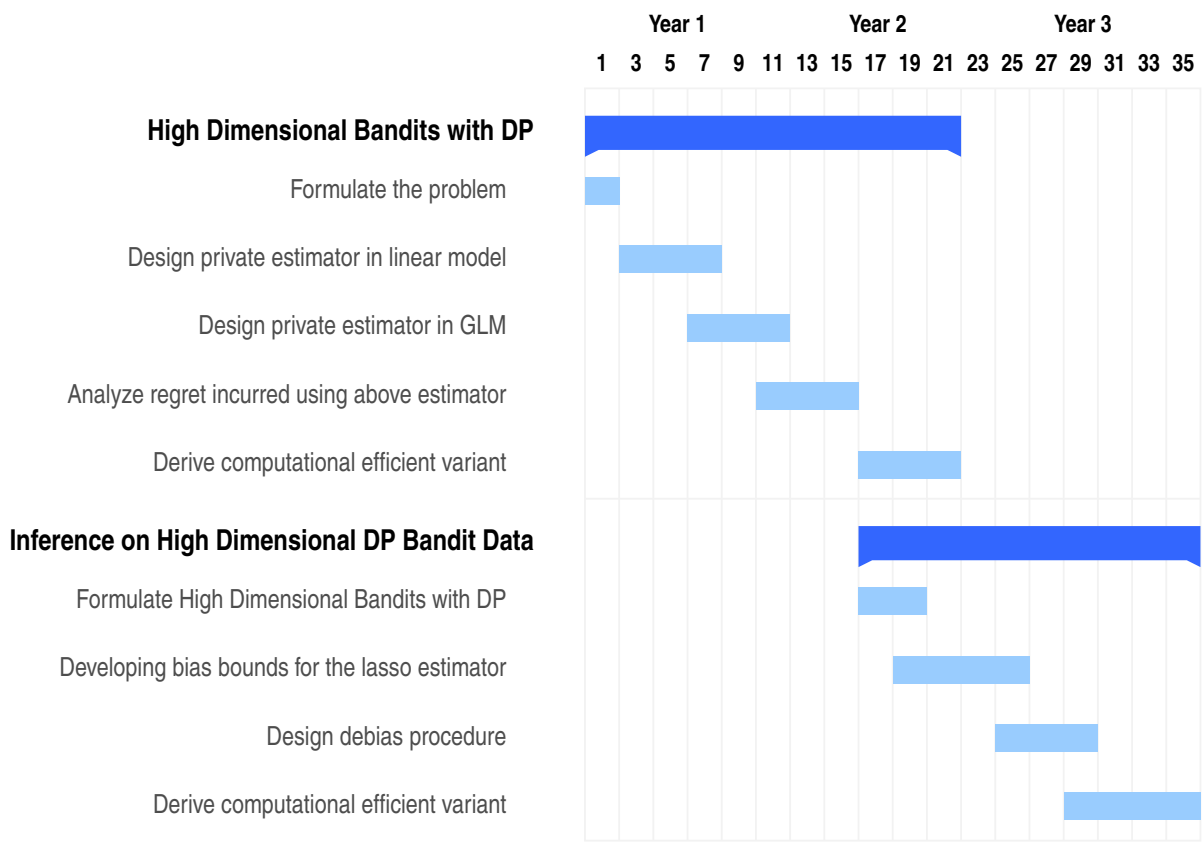
(b) Dimension  $d = 100$



(c) Dimension  $d = 200$

Figure 2: Simulation Study for Bandit Inference

# Gantt Chart





# Education Plan

This research project will generate new insights, both quantitatively and qualitatively, into the design and implementation of novel machine learning algorithms on data privacy in high dimensional decision-making setting. Despite the increasing use and importance of these issues in machine learning and data technology, few courses currently focus on this emerging area. We plan to turn the insights and domain knowledge gained from this project into relevant course materials for undergraduate, graduate, and professional education. The material generated from this project can be taught with different focuses at various levels.

At my university, I have developed a series of courses, *IEDA 2520 Probability*, *IEDA 2540 Statistics* and *IEDA 3650 predictive analytics*, which has been well received by students. In particular, *IEDA 3650* focuses on various machine learning algorithms. Based on some of the resulting outcomes, we plan to involve the course into incorporate privacy and bandit algorithms. Since our proposed research comes from practical applications, some of the results will become perfect material for the case study of the proposed new course. For teaching undergraduate students, the key is to make the basic elements clear and illustrate a few simplified models without losing the essence, such as the fundamental principle of privacy protection. By contrast, Ph.D. level courses will focus on the theoretical analysis of various privacy mechanisms and the related algorithms. In addition to developing undergraduate courses, I also plan to incorporate some methodologies developed in this research into the course *IEDA 6000E Advanced Methods in Machine Learning* targeted for Ph.D. students in our field by focusing more on the theoretical aspects. It is also possible to contribute to the department core Ph.D. course *IEDA 5270 Engineering Statistics and Data Analytics*. The purpose is to strengthen the training of students (both undergraduate and postgraduate) by improving students' analytical and logical thinking ability, and problem-solving skills for real-world applications.

In addition to fostering the integration of research and education by developing course materials, this research will also involve research students (both undergraduate and Ph.D. students with strong mathematical and programming skills) in numerical experiments because code implementation and simulation are an integral part of the project. The proposed research has the potential to be rich enough to cover several Ph.D. dissertations. In fact, we have already involved two Ph.D. students in a preliminary study, including a literature review and basic model analysis. Students who participate in this research will gain valuable insight into the intricacies underlying mathematics. This research project will help grow future academic and industry leaders.