Introduction to Differential Privacy: Theory, Algorithms and Applications

DSC291 Fall 2024

First lecture: Monday, September 30, 2024

Instructor: Prof. Yu-Xiang Wang (Email: yuxiangw@ucsd.edu)

TA: Dan Qiao (Email: d2qiao@ucsd.edu)

Lectures: CENTR 205 MWF 1:00p - 1:50p

Office Hours: To be announced on the course website.

Piazza: `https://piazza.com/ucsd/fall2024/dsc291/home`
(We use Piazza for Q&A, discussion, and most announcement!)

Gradescope: `https://www.gradescope.com/courses/879296`
(We use gradescope for submitting your assignments!)

Canvas: The Canvas is active, but it is only reserved for communications that are restricted to people who are officially registered.

1 Overview

Differential privacy (DP) is one of the most promising approaches towards addressing the privacy challenges in the era of artificial intelligence and big data. It represents a gold standard and is a key enabler in many applications including medical research, data sharing, training machine learning models with users' private data and their federated learning extensions. This course is a gentle introduction of differential privacy to graduate students in computer science, statistics and various data-driven engineering disciplines. The focus is for students to develop sufficient theoretical and algorithmic foundation so as to effectively and correctly apply differential privacy to various applications, to design new differentially private algorithms using basic building blocks, as well as to understand the key challenges and limitations of differential privacy so as to be able to choose applications where DP algorithms could result in sufficient utility.

Different from various existing offering of DP courses (from other institutes), a big part of the course will devoted to differentially private machine learning and students will receive hands-on practices in working on actual datasets with runnable code while understanding the empirical aspects of various DP algorithms.

2 What you will learn?

1. Privacy risks, privacy attacks and motivations of differential privacy.
2. The definition of differential privacy and its interpretations.

3. Understanding the promise of DP: what does it protects and what not?
4. Fundamental building blocks of DP algorithms.
5. Modern methods in differential privacy: Renyi DP, Privacy profiles, tradeoff functions
6. How to use [autodp] for privacy accounting and privacy calibration.
7. Differentially private (linear) machine learning
8. Differentially private deep learning under various models
9. Data-adaptive differentially private algorithms.

3 Prerequisites

As this is a graduate level course, there is no hard pre-requisite, but students entering the class are expected of the following.

- Students are expected to be able to follow rigorous mathematical arguments and perform derivation and proofs using notations, definitions and theorems from calculus, linear algebra, probability and statistics.
- Students are expected to have working knowledge of basic algorithms and data structures, and could write simple code in Python / Numpy.
- If you have taken a course in graduate-level mathematical statistics, statistical machine learning, linear / convex optimization, or are familiar with topics such that concentration inequalities, then you are very well-prepared to enjoy the course.

4 Textbooks

We will be relying on two reference books.

1. "The Algorithmic Foundations of Differential Privacy" by Dwork and Roth [Link]
2. "The Complexity of Differential Privacy" by Salil Vadhan [Link]

However, for more recent materials we will also draw from research papers and other sources. Students taking this course are expected to help with putting together scribed notes for a subset of the lectures.

5 Assignments and Grades

The grades will be based on the following breakdowns.

- 30% Homework assignments.
- 20% Midterm In-Class Quiz
- 40% Course project
- 10% Lecture attendance and participation.

6 Course project Project

The course project will be in teams of maximum size 3. Individual projects are fine, but it is usually more fun to have someone to talk to. The scope of the project depends on your own interest and bandwidth, and is intended to be flexible (beyond a required part). For example, you could leverage your ongoing research work if it is related.

Required part of the project:

Differentially Private Data Analysis Practicum Pick up one of the data analysis tasks that the instructor provides. Come up with your own way of *privatizing* it using what we learned in the class or otherwise. Implements the algorithm (using AutoDP for privacy accounting whenever needed), then document the privacy-utility tradeoff.

Flexible part of the project:

DP Theory Read one (or a few) papers on one theoretical aspect of differential privacy; understand the results and the proof.

DP applications Implement one (or a few) existing DP algorithms and apply to a synthetic / real-life dataset. Conduct benchmarking experiments.

Opensource contribution Contribute code to AutoDP. It could be a new "Mechanism", a new "Transformer", a new example or tutorials, or even new test cases for the unit test.

DP + X research project Develop new differentially private algorithms for a new problem or a new application.

In all three cases, you will need to submit: a short proposal, a midterm report, and a final report; as well as to present your project to the class towards the end of the quarter. For group projects, each student need to contribute and a section should be included in the midterm and final report on the contribution from each group member.

7 Logistics

Attendance policy: The instruction will be in-person. The attendance to lectures is required. It is part of the course evaluation to attend the lectures. Send PM on Piazza if you will have to miss lectures due to personal businesses.

Late homework policy: Late submissions are allowed, but if you are late more than one full week then there will be a 20% penalty.

8 Policy on Academic Integrity

Please read this section carefully.

The university, the department, and this instructor all take the issue of academic integrity **very** seriously. A university requires an atmosphere of mutual trust and respect. While collaboration is an integral part of many scholarly activities, it is not always appropriate in a course, and it is never appropriate unless due credit is given to all participants in the collaboration.

Here are some examples:

- Allowed: Discussion of lecture and textbook materials
- Allowed: Discussion of how to approach assignments, what techniques to consider, what textbook or lecture material is relevant

- Allowed: Collaboration on homeworks. You need to declare your collaborators, and describe what you get from the person who helped you, and each student still needs to write their own report / code independently.
- Allowed: Refer to online resources, but you need to cite the exact references.
- Not allowed: Turning in someone else's work as your own, even with that person's permission.
- Not allowed: Allowing someone else to turn in your work as his or her own.
- Not allowed: Turning in work without proper acknowledgment of the sources of the content (including ideas) contained within the work.

For some views on academic integrity at UCSD see the Academic Integrity (AI) Office.

Summary: Academic integrity is absolutely required - dishonesty (cheating, plagiarism, etc.) benefits no one and hurts everyone. Violations of these honor codes on academic integrity will be reported to the Office of Student Conduct. If you find yourself in such a situation, please contact the instructor. If you are not sure whether or not something is appropriate, please ask the instructor.

9 Code of conduct

The University of California, Dandiego has a general code of conduct for all students published here: `https://sage.ucsd.edu/l`

The University's commitment to Diversity, Equity and Inclusion is published here: `https://ucsd.edu/about/principles.html`.

10 Students with Disabilities

If you are a student with a disability and would like to discuss special academic accommodations, please contact the instructor. In addition, students with temporary or permanent disabilities are referred to the Office of Students with Disabilities (OSD) at UCSD. OSD will arrange for special services when appropriate (e.g., facilitation of access, note takers, readers, sign language interpreters). Please note that it is the student's responsibility to communicate his or her special needs to the instructor, along with a letter of verification from OSD.

11 Copyright of course materials

My lectures and course materials, including presentations slides, written notes, homework assignments and similar materials, are protected by U.S. copyright law and by University policy. I am the exclusive owner of the copyright in those materials I create. You may take notes and make copies of course materials for your own use. You may also share those materials with another student who is enrolled in or auditing this course. You may not reproduce, distribute or display (post/upload) lecture notes or recordings or course materials in any other way — whether or not a fee is charged — without my express prior written consent. You also may not allow others to do so.

If you do so, you may be subject to student conduct proceedings under the UCSD Student Code of Conduct.