Introduction to Differential Privacy: Theory, Algorithms and Applications

CS291A Fall 2021

Instructor: Prof. Yu-Xiang Wang

Lectures: Harold Frank Hall 1132[1] and also on Zoom. Monday and Wednesday 1:00 - 2:50

Piazza: `https://piazza.com/ucsb/fall2021/cs291/home`
(We use Piazza for Q&A, discussion, and most announcement!)

Gradescope: `https://www.gradescope.com/courses/318956`
(We will be using the gradescope for submitting homeworks and project reports.)

Gauchospace: The Gauchospace 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.

[1] Notice that it was previously Phelps 3526 in the system by mistake!

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.

- 45% Homework assignments.
- 40% Course project.
- 10% Scribing.
- 5% 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. For example, you could leverage your ongoing research work if it is related.

Three typical types of projects are

DP Theory Read one (or a few) recent papers on a 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.

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

The instruction will be primarily in-person. But to accommodate to students who has to attend from remotely, lectures will be live-casted on Zoom and recorded.

Zoom lectures: Unless the instructor approves otherwise, only registered students are given access to the real-time lectures over Zoom. You have been emailed instructions on how to connect to the lecture. If you are having trouble, please contact the instructor. The live Zoom sessions will be recorded for students who may not be able to attend synchronous. By default, your microphone and camera will be muted when you join the session. If you do not want to be included in the recording, simply keep your camera and microphone off. You may ask questions in the chat window. Please refer to the "copyright" section for more details.

Zoom office hours: Office hours will be by appointment, by zoom if needed.

Attendance policy: 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 other personal businesses. If you are in a different timezone which makes attendance of the live lectures infeasible, please alert the instructor.

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 UCSB see the Academic Integrity page of the Office of Judicial Affairs.

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, Santa Barbara has a general code of conduct for all students published here: `http://www.sa.ucsb.edu/docs/default-source/student-conduct/conductofcode2017.pdf?sfvrsn=d3c07d4f_2`

The computer science department's commitment to Diversity, Equity and Inclusion is published here: `https://cs.ucsb.edu/content/diversity-equity-and-inclusion`.

As a department, we holds students, staff, and faculty to the following standards:

- Treat all members of the academic community (students, staff, and faculty) with respect regardless of their experiences and background, including (but not limited to) their cultural backgrounds, socioeconomic status, disabilities, age, religion, sexual orientation, neuro(a)typicality, and gender identity.
- Physical or mental harm, sexual harassment, aggression, and derogatory language is not acceptable in any form.
- Respect the personal property of others and University resources. Unauthorized access, use, vandalism, or theft of equipment, computer servers, labs / offices / classrooms, etc. is prohibited.
- The exchange and challenge of ideas are done in a thoughtful, respectful and constructive manner.
- Disruption of departmental activities such as special events, talks, lectures, and meetings is not acceptable.

- Any violation of the given standards should be reported to the Computer Science chair and/or the CS diversity committee (`diversity@cs.ucsb.edu`). Consequences may include a formal warning, suspension, or expulsion from the University.

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 Disabled Students Program (DSP) at UCSB. DSP 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 DSP.

11 Copyright of course materials

My lectures and course materials, including presentations slides, written notes, recorded lectures, 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 UC Santa Barbara Student Code of Conduct.

Similarly, you own the copyright in your original papers and exam essays. If I am interested in posting your answers or papers on the course web site, I will ask for your written permission.

The live Zoom session will be recorded for students who may not be able to attend at this time. By default, your microphone and camera will be muted when you join the session. If you do not want to be included in the recording, simply keep your camera and microphone off. You may ask questions in the chat window.