JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

Computer Science 601.438/638
Algorithmic Foundations of Differential Privacy
Spring, 2025
(3 credits, EQ, CS-THEORY)

Instructor
Professor Michael Dinitz, mdinitz@cs.jhu.edu, `http://www.cs.jhu.edu/~mdinitz/`
Office: Malone 217
Office hours: By appointment

Teaching Assistant
Shruthi Prusty, sprusty1@jhu.edu

Meetings
T Th 9 – 10:15am, Hodson Hall

Textbook

- Cynthia Dwork and Aaron Roth (2014), "The Algorithmic Foundations of Differential Privacy", Foundations and Trends® in Theoretical Computer Science: Vol. 9: No. 3–4, pp 211-407. `http://dx.doi.org/10.1561/0400000042`

Online Resources
Course webpage: `https://www.cs.jhu.edu/~mdinitz/classes/DP-class/Spring2025/`
Online Discussion: Courselore. Invite link: `https://courselore.org/courses/5350835276/invitations/7395827440`
Homework submission and grading: Gradescope

Course Information

- This course provides an introduction to differential privacy, with a focus on algorithmic aspects (rather than statistical or engineering aspects). Specific topics we will cover include:
  - Motivation for differential privacy, and different versions of differential privacy (pure, approximate, Rényi, and zero-concentrated in particular).
  - Basic mechanisms (Laplace, Gaussian, Discrete Gaussian, and Exponential)
  - Composition theorems
  - Basic algorithmic techniques (sparse vector technique, private multiplicative weights, private selection)
  - Beyond global sensitivity: local sensitivity, propose-test-release, subsampling
  - Differentially private graph algorithms
  - Lower bounds
- **Prerequisites**
  Introduction to Algorithms (601.433/633)
- **Required, Elective or Selective Elective:** Elective

Course Goals
Specific Outcomes for this course are that:

- Students will learn the basic definitions of differential privacy.
- Students will learn how to design and analyze differentially private algorithms using state-of-the-art techniques.
- Students will learn how to prove limitations on differential privacy (lower bounds).

This course will address the following ABET Student Outcomes:

- SO1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.

Course Topics

- Differential privacy definitions
- Basic private mechanisms
- Composition theorems
- Foundational algorithms using basic mechanisms
- Differentially private graph algorithms
- Lower bounds for differential privacy

Course Expectations & Grading
There will be homework assignments approximately every other week and a final project. Class participation is also required.

Homeworks: 50%
Final Project: 30%
Participation: 20%

You are free to work on the homework in groups of up to 3, but you must write up your solutions entirely on your own. That is, collaboration is limited to discussing the problem, and does not include writing down the solution. Please list the members of your group on your submission.

Assignments & Readings
These will be posted on the course webpage.

Ethics
The strength of the university depends on academic and personal integrity. In this course, you must be honest and truthful, abiding by the *Computer Science Academic Integrity Policy*:

> Cheating is wrong. Cheating hurts our community by undermining academic integrity, creating mistrust, and fostering unfair competition. The university will punish cheaters with failure on an assignment, failure in a course, permanent transcript notation, suspension, and/or expulsion. Offenses may be reported to medical, law or other professional or graduate schools when a cheater applies.
>
> Violations can include cheating on exams, plagiarism, reuse of assignments without permission, improper use of the Internet and electronic devices, unauthorized collaboration, alteration of graded assignments, forgery and falsification, lying, facilitating academic dishonesty, and unfair competition. Ignorance of these rules is not an excuse.
>
> Academic honesty is required in all work you submit to be graded. Except where the instructor specifies group work, you must solve all homework and programming assignments without the help of others. For example, you must not look at anyone else.s solutions (including program code) to your homework problems. However, you may discuss assignment specifications (not solutions) with others to be sure you understand what is required by the assignment.

If your instructor permits using fragments of source code from outside sources, such as your textbook or on-line resources, you must properly cite the source. Not citing it constitutes plagiarism. Similarly, your group projects must list everyone who participated.

Falsifying program output or results is prohibited.

Your instructor is free to override parts of this policy for particular assignments. To protect yourself: (1) Ask the instructor if you are not sure what is permissible. (2) Seek help from the instructor, TA or CAs, as you are always encouraged to do, rather than from other students. (3) Cite any questionable sources of help you may have received.

On every exam, you will sign the following pledge: "I agree to complete this exam without unauthorized assistance from any person, materials or device. [Signed and dated]". Your course instructors will let you know where to find copies of old exams, if they are available.

In addition, the specific ethics guidelines for this course are:

(1) Homeworks may be done in groups of up to three, but you must list your group members on the first page of your submission.
(2) On all assignments each person should hand-in their own writeup. That is, collaboration should be limited to talking about the problems, so that your writeup is written entirely by you and not copied from your partner. In addition, list all members of your group.
(3) While you are allowed to use outside resources to help your understanding and knowledge of course material, you *must not* go looking for outside resources to get answers for homework questions. That is, you can look up concepts that you do not understand, but you cannot simply go looking for solutions.
(4) Moreover, you are not allowed to upload, download, or access solutions to homework or exam questions, including through "backtest" websites, Chegg, Course Hero, etc.

Report any violations you witness to the instructor.
You can find more information about university misconduct policies on the web at these sites:

- Undergraduates: `https://studentaffairs.jhu.edu/policies-guidelines/undergrad-ethics/`
- Graduate students: `http://e-catalog.jhu.edu/grad-students/graduate-specific-policies/#misconduct`

Students with Disabilities

Any student with a disability who may need accommodations in this class must obtain an accommodation letter from Student Disability Services, 385 Garland, (410) 516–4720, `studentdisabilityservices@jhu.edu`.