JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

Computer Science EN.601.438/638
Theory of Differential Privacy
Fall, 2026 (3 credits, EQ, CSCI-THRY)

Instructor
Professor Lydia Zakynthinou, lzakynthinou@jhu.edu,
https://www.cs.jhu.edu/faculty/lydia-zakynthinou/
Office hours: TBD
Office hours location: TBD

Teaching Assistant
TBD, tbd@ece.jhu.edu
Office hours: TBD
Office hours location: TBD

Meetings
TBD

Textbook
Recommended: Cynthia Dwork and Aaron Roth, *The Algorithmic Foundations of Differential Privacy*, Foundations and Trends® in Theoretical Computer Science, Volume 9, Issue 3-4, Pages 211 – 407, https://doi.org/10.1561/0400000042J (2014).

Online Resources
Relevant resources will accompany each lecture on the course webpage.

Course Information

- This course is an introduction to differential privacy as a foundational framework for reasoning about privacy in data analysis. Students will develop a principled understanding of why privacy risks arise when privacy is not an explicit design objective and how differential privacy enables formal, provable guarantees. In this course, we will build on the algorithmic toolkit and statistical techniques for designing and analyzing differentially private methods, and study fundamental tradeoffs and lower bounds that characterize the limits of privacy.
- **Prerequisites**
  Students should be comfortable writing mathematical proofs involving algorithms, probability, and linear algebra.
  Introduction to Algorithms (601.433/633) satisfies this requirement; comparable theory coursework may be accepted with instructor approval.
- **Elective**

Course Goals

Specific Outcomes for this course are that students will:

- Understand why privacy risks arise when privacy is not treated as an explicit design objective.
- Understand the core definitions of differential privacy and formally reason about privacy risks using the differential privacy framework.
- Design and analyze differentially private algorithms using state-of-the-art techniques.
- Understand the fundamental tradeoffs and limitations of differential privacy, including when strong privacy guarantees are provably impossible.

This course will address the following CSAB ABET Criterion 3 Student Outcomes

Graduates of the program will have an ability to:

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

Course Topics

- Privacy attacks; motivation for provable privacy
- Differential privacy: definitions, variants, composition
- Core mechanisms and algorithmic techniques (Laplace, Gaussian, Exponential, Binary Tree)
- Differentially private optimization and machine learning (DP-SGD, Amplification by Subsampling, Factorization Mechanisms)
- Techniques beyond global sensitivity (Local Sensitivity, Propose-Test-Release)
- Fundamental limits and lower bounds (Fingerprinting and Packing Lower Bounds)
- Advanced topics may include: differentially private approaches for graphs, high-dimensional statistics, or PAC learning, as well as connections between differential privacy and other trustworthy machine learning desiderata.

Topics Schedule:

Lecture	Topic
1	Introduction, Attacks
	DP Fundamentals
2	Definition of DP, Randomized Response, Laplace Mechanism
3	Report Noisy Max, Sparse Vector Technique
4	Exponential Mechanism and Inverse Sensitivity
5	Group privacy, Post-processing, Composition
6	Approximate DP, Gaussian Mechanism

7	Advanced Composition
	Linear Queries
8	SmallDB (synthetic data v1)
9	Private MWU (synthetic data v2)
10	Binary Tree Mechanism
11	Factorization and Projection
	Optimization
12	Other notions: Rényi DP and zCDP
13	DP-SGD and Amplification by Subsampling
14	DP-FTRL
15	Amplification by Iteration
	Private Statistical Estimation Beyond Global Sensitivity
16	Local sensitivity, Propose-Test-Release
17	Stable Histograms, Smooth Sensitivity
18	FriendlyCore
19	Stable Estimators
20	Robustness to Privacy Transformation
21	Fingerprinting lower bounds
	Additional special topics
22	Local and shuffle model
23	Private PAC learning
24	DP and Generalization/Adaptive Data Analysis
25	Project Presentations
26	Project Presentations

Course Expectations & Grading
In-class participation is required. There will be 3-4 homework assignments and a final project. The final grade will be computed based on the following weights:
Homeworks - 50%
Final Project - 30%
Participation - 20%

Late assignments: Each student has 4 late days to use on homework assignments (not projects) over the course of the semester, no questions asked. Each late day extends the deadline by 24 hours, and you may use your late days however you like, including stacking multiple days on a single assignment. Once your late days are used up,

additional late submissions will not be accepted. If something serious comes up, please contact me as soon as possible so we can discuss options.

Assignments & Readings
These will be 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. **Collaboration**
   You are encouraged to discuss homework assignments and projects with classmates at a high level. However, all written solutions must be produced independently and reflect your own understanding. You are solely responsible for the content of what you submit.

   As a rule of thumb, after any discussion you should be able to set aside all notes, return home, and write the solution from scratch entirely on your own. Please list the classmates you collaborated with on your submission. You may not consult written solutions, online resources, or materials from past offerings of this or similar courses.

2. **Use of AI**
   Generative AI tools (such as ChatGPT) can be helpful for learning when used appropriately. In this course, you're welcome to use AI tools to clarify concepts, work through points of confusion, or think through high-level ideas—much like you would in a conversation with a classmate, TA, or instructor.

   That said, AI tools should not be used to generate solutions for homework assignments or projects. Please don't paste problem statements into an AI system and ask for an answer or an outline. The value of the assignments comes from you doing the intellectual work yourself.

   A good rule of thumb is the same one we use for collaboration: after using an AI tool, you should be able to close your laptop, put everything away, and later write the solution entirely on your own, without notes. You also shouldn't have your assignment open while interacting with the AI.

   If you use an AI tool, please list which tool you used and briefly how you used it. Remember, you're responsible for everything you submit, including any mistakes or inaccuracies that may come from AI-assisted learning.

Report any violations you witness to the instructor.

You can find more information about university misconduct policies on the web at these sites:

- For undergraduates: https://studentaffairs.jhu.edu/policies-guidelines/undergrad-ethics/
- For graduate students: http://e-catalog.jhu.edu/grad-students/graduate-specific-policies/

Mental Health Statement
Many students struggle at times with stress and mental health concerns. Johns Hopkins University Mental Health Services has a range of services to support students with their

mental health. Beyond clinical services, JHU also has many resources available to support overall student well-being.

For 24/7 behavioral health support, The Johns Hopkins University Behavioral Health Crisis Support Team (BHCST) pairs experienced, compassionate crisis clinicians with specially trained public safety officers on every shift on and around the Homewood campus, seven days a week. The BHCST will provide immediate assistance to those who need it and link individuals in crisis to ongoing support services in the days and weeks that follow. BHCST can be reached directly at 410-516-9355 or by calling Public Safety, 410-516-4600 or 7777, and asking to be connected to a BHCST clinician.

If you have concerns about yourself or another student, please contact:

- For emergencies (threat to self or others): Public Safety 410-516-7777 or 911
- For 24/7 mental health support (mobile, access line and virtual): BHCST at 410-516-9355
- For undergraduate students who may benefit from Case Management services (1:1 support, coordination and connection to relevant campus resources): Student Outreach & Support at 410-516-7857 or studentoutreach@jhu.edu
- For KSAS Graduate Students: Renee Eastwood, Assistant Dean for Graduate and Postdoctoral Academic and Student Affairs
- For WSE Graduate Students: Megan Barrett, Assistant Dean for Engineering Student Affairs

Students with Disabilities – Accommodations and Accessibility

Johns Hopkins University is committed to providing welcoming, equitable, and accessible educational experiences for all students. If disability accommodations are needed for this course, students should request accommodations through Student Disability Services (SDS) as early as possible to provide time for effective communication and arrangements.

For further information about this process, please refer to the SDS Website.

Inclusivity

Johns Hopkins University is committed to creating a classroom environment that values the diversity of experiences and perspectives that each student brings. Everyone deserves to be treated with dignity and respect. Fostering an inclusive climate is important because research and experience show that students who interact with peers who are different from themselves learn new things and experience tangible educational outcomes. We invite you to help create a welcoming, vibrant and intellectually engaging classroom climate. Note that you should expect to be challenged intellectually by the instructor, the TAs, and your peers, and at times this may feel uncomfortable. Indeed, growth often requires being pushed beyond your comfort zone. However, at no time in this learning process should someone be singled out or treated unequally based on any aspect of their identity (visible or invisible).

If you ever have concerns in this course about harassment, discrimination, or any unequal treatment, or if you seek accommodations or resources, please reach out to your instructor or the TAs, who will take your communication seriously and seek mutually acceptable resolutions and accommodations. Reporting will never impact your course grade. You may also share concerns with the department chair, the Director of Undergraduate Studies [link to heads/DUS document], the WSE Associate Dean of Outreach and Belonging (Darlene Saporu, dsaporu@jhu.edu), the KSAS Assistant Dean for Diversity and Inclusion (Araceli Frias, afrias3@jhu.edu) or the Office of Institutional Equity (oie@jhu.edu).

In handling reports, people will protect your privacy as much as possible, but faculty and staff are required to officially report information for some cases (e.g., sexual harassment).