

Theory of Differential Privacy

EN.601.438/638, Fall 2026

Project guidelines

100 points • 30% of course grade • Due: December 17, 23:59.

Overview. The course project is worth **30% of the course grade**. The project grade will be based entirely on the final report; the proposal and presentation are required milestones intended to help you develop and communicate a great project.

The goal is to investigate a focused question in differential privacy more deeply than we can in class. A successful project does not need to prove a new theorem or beat a benchmark. A careful analysis, a well-designed experiment, a negative result, or a deep synthesis of the literature on a particular topic can all make for an excellent project.

Possible project types

You may choose a project in any of these styles:

- **Small research project.** Investigate whether an assumption in a result is necessary, change a parameter regime, seek a counterexample, or extend a technique from class to a nearby problem.
- **Empirical or implementation project.** Reproduce, compare, or adapt private algorithms and explain the resulting privacy-utility tradeoffs.
- **Extensive survey.** Give a focused, critical survey of an area of the literature. A strong survey should compare models, assumptions, techniques, and open questions instead of summarizing papers one by one.

Deliverables

Deliverable	When	What to submit
Project proposal	November 11	Roughly half a page
Project presentation	Week of December 7	A 30-min presentation to the class followed by questions
Final report	December 17	A short scientific report

No late days are allowed for the above, in contrast to the problem sets.

Proposal

Your proposal should be about half a page and include:

- the central question or topic;
- why it is interesting;
- your tentative approach;
- the main papers, course results, data, or tools you expect to use; and
- the outcome you hope to produce.

The proposal is not a contract: research projects often change direction. Its purpose is to make sure the scope is feasible and to give you useful feedback early.

Presentation

During the week of December 7, you will present your project to the class. Explain the question, the relevant background, your approach, and your main findings or current conclusions. Aim for a presentation that classmates who know the course material can follow.

Final report

The final report should read like a short scientific paper. It should be written for your classmates: you may assume familiarity with course material, but include any additional background needed to understand the main idea.

A typical report will include:

- an abstract;
- an introduction and motivation;
- relevant background and related work;
- a precise problem statement or organizing question;
- methods, analysis, experiments, or survey synthesis;
- conclusions, limitations, and possible next steps; and
- references.

The report will be assessed for the quality and precision of the question, technical correctness and depth, use of relevant evidence or literature, interpretation of limitations, and clarity of exposition.

Possible project directions

The directions below are intentionally broad and are only suggestions. Start with a paper or sub-area, then use the proposal to identify a question that is both interesting and feasible. A project might explain and extend a proof, test the importance of particular assumptions, compare implementations, or develop a focused survey.

1. **Differentially private optimization and learning.** Explore how privacy-utility tradeoffs change under different loss functions, geometry or regularity assumptions, parameter regimes, clipping choices, use of public data, or nested objectives such as hyperparameter tuning. This includes convex and nonconvex optimization, generalized linear models, bilevel optimization, and private learning beyond standard ERM. Possible starting points include *Differentially Private Non-Convex Optimization under the KL Condition with Optimal Rates* (ALT 2024) and *Differentially Private Bilevel Optimization: Efficient Algorithms with Near-Optimal Rates* (NeurIPS 2025).
2. **Private fine-tuning, parameter-efficient learning, and LoRA.** Investigate how low-rank adaptation, adapter placement, rank, parameterization, clipping, noise, accounting, or model modality affect private fine-tuning. This could include language models, diffusion models, or federated learning, and could study both utility and memorization or inference attacks. LoRA alone is not a privacy guarantee; the project should make the DP mechanism and privacy model explicit. Possible starting points include *PRISM: Gauge-Invariant Tangent-Space Differentially Private LoRA* (ICML 2026) and *Differentially Private Fine-Tuning of Diffusion Models* (ICCV 2025).
3. **Differential privacy for combinatorial problems.** Explore how privacy changes a discrete optimization problem such as graph cuts, matchings, facility location, allocation, submodular optimization, or graph analysis. Interesting questions include the right adjacency or output model, approximation and lower-bound tradeoffs, and when structure in the problem improves private utility. Possible starting points include *Differentially Private Algorithms for Graph Cuts*

(SODA 2026) and *Streaming Submodular Maximization with Differential Privacy* (ICML 2023).

4. **Auditing, attacks, and privacy accounting.** Study the relationship between a formal DP guarantee and observable privacy leakage. Projects might audit an implementation, reproduce a controlled attack, investigate implementation pitfalls, or compare accountants and sampling assumptions for DP-SGD. An empirical audit can expose a violation or provide evidence about tightness, but it cannot by itself certify that a mechanism is differentially private. Possible starting points include *Privacy Auditing with One (1) Training Run* (NeurIPS 2023) and *Avoiding Pitfalls for Privacy Accounting of Subsampled Mechanisms Under Composition* (SaTML 2025).
5. **Privacy over time and interaction.** Explore continual observation, streaming algorithms, private data structures, online queries, or everlasting prediction. What changes when releases continue indefinitely, inputs or queries are adaptive, or the mechanism's internal state evolves? Possible starting points include *Lower Bounds for Differential Privacy Under Continual Observation and Online Threshold Queries* (COLT 2024) and *Private Truly-Everlasting Robust-Prediction* (ICML 2024).