Final Project Guidelines

CS208: Applied Privacy for Data Science, Spring 2019

The final projects in the course are meant to give you the opportunity to further explore an aspect of differential that interests you, give you the experience of formulating, carrying out, and presenting an interesting, short-term independent project that is similar to an experience you might have in a career as an applied data scientist confronting privacy issues and/or as a data privacy researcher.¹

Projects can be done individually or in pairs, with groups of three allowed for ambitious projects. Many different types of projects are possible:

- Implement and experimentally evaluate differentially private algorithms or attacks on real-life datasets. For example, identify a dataset that resembles a sensitive data use case and a type of statistical analysis that would be useful on such a dataset, implement and tune a differentially private algorithm for that analysis and evaluate the privacy-utility tradeoff.
- Critically evaluate an existing system for privacy protection, identify potential vulnerabilities and propose or demonstrate improvements using techniques from this class.
- Explore how the “noisy” results from differential privacy can be properly incorporated into usable scientific or consumer data products in a specific use case.
- Explore how differential privacy might be incorporated into a larger system design (with some particular application domain in mind).
- Seek new theoretical results on some aspect of differential privacy or related topics.
- Connect differential privacy to some other area of interest to you (whether in CS or outside).
- Model some new problem that might not be captured by the current literature
- Synthesize and write an exposition of several papers in the differential privacy research literature (beyond those covered in detail in class)
- And more... be creative!

Refer to the course syllabus, reading list, and other suggestions we provide as sources of inspiration.

The deadlines for various aspects of the project are as follows:

- **Topic Ideas (Tuesday 2/26, revised 3/12):** As part of PS1 (due 2/26), submit about a paragraph of discussion about 1-3 ideas you have for potential project topics. For each topic, you should include the general kind of problem or use case that you’d like to address in your project and the general methodology (e.g. is it a theory project or an experimental project or...). The point of these topic ideas is both to get you thinking about the project early on and to enable us to give you early feedback and suggestions, which we will provide by Monday March 4. After that, we will set up a forum for you all to seek

¹ We don’t expect you to produce publishable results during time you have this semester, but we do hope that some of the projects in the class can subsequently be developed into publishable research.
project partners with similar interests to yours, and your group should submit a revised, more detailed set of topic ideas, including an initial list of relevant papers, with Problem Set 2 on March 12.

- **Project Description (Tuesday 4/9):** Submit a couple of pages giving a detailed description of what your final project will look like. You should be able to clearly state your research questions, briefly articulate how your project relates to what has been done in the past, describe the approach you are taking, give your timeline for completing various aspects of the project, and *discuss your fallback plan in case you don't obtain the results that you're hoping to obtain.*

- **Written Paper (Reading Period):** Submit a paper (approx. 10 pages) describing your completed project. The paper should motivate your research questions and results, explain how the project fits into the context of previous work, justify the methodology, and present the results in a convincing manner. (Naturally, the form will differ depending on the type of project.)

- **Presentation (Exam Period, Dates TBD):** Every group will give an approx. 15 min presentation on their final project.

We encourage you to discuss your ideas with us throughout the process, at office hours or by email. We hope you enjoy the experience!