Course Introduction

CS 6501, Data Privacy, Spring 2022
Tianhao Wang

Instructors

Tianhao Wang

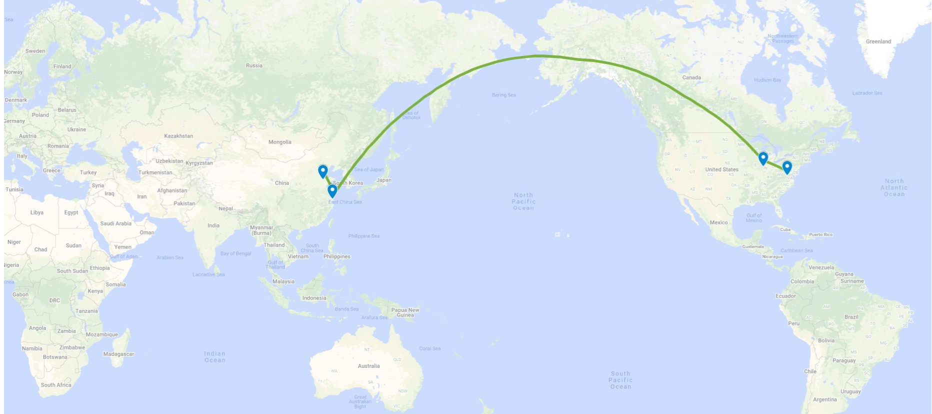
CS@UVA, SDS@UVA

1st year Assistant Professor, Prior PhD from Purdue and Postdoc from CMU

tianhao@virginia.edu

https://tianhao.wang/s22-dataprivacy/

Machine Learning Privacy and Differential Privacy



TA

Dung Nguyen ("Dzung When")

CS@UVA

dungn@virginia.edu

Differential Privacy on Graphs

Course Hours

Location: Zoom and Rice 032

Time: Monday and Wednesday 2:00PM - 3:15PM

Office Hour: Friday 2PM - 3PM and by appointment

Thursday 11AM-1PM and by appointment

Discussion: https://piazza.com/virginia/spring2022/cs6501

Due to covid, no attendance. But there is no recordings. Please read slides online and come to the class if you are not sick.

Course Expectation

This is a graduate-level seminar course

You are about to read and share a lot

We have weak (pre-)assumptions

- Math (Probability)
- Programming (Python)

Discuss fundamental problems and state-of-the-art solutions in sub-areas

Get hands-on experience by solving practical problems

Prepare for doing cutting-edge projects data privacy and related fields

Grading

- No exams
- Paper presentations (20%)
  - Student-led lectures
  - 35-minutes lecture-style presentations
  - Topics should be chosen from the instructor's suggested list
- Paper review (20%)
  - Each student selects 4 papers to review
- Participation (10%)
- Two assignments (10%) for theory (proofs) and practice (programming)
- Course project (40%) on research topics or review and evaluation
  - Last week of semester
  - Performed in individually or in groups of 2

Papers: Different areas of data privacy

- Privacy attacks against machine learning
    - Membership inference attacks
    - Property inference attacks
- Differential privacy with
    - machine learning (NLP, Hyperparameter Tuning, GAN, federated learning, etc)
    - theory (better utility/privacy bounds, positive/negative results, etc)
    - cryptography (1. accelerate crypto with DP, 2. improve DP with crypto)
    - systems (build efficient DP systems)
    - software engineering/programming languages (verify/check DP implementation, type systems, etc)

Presentations

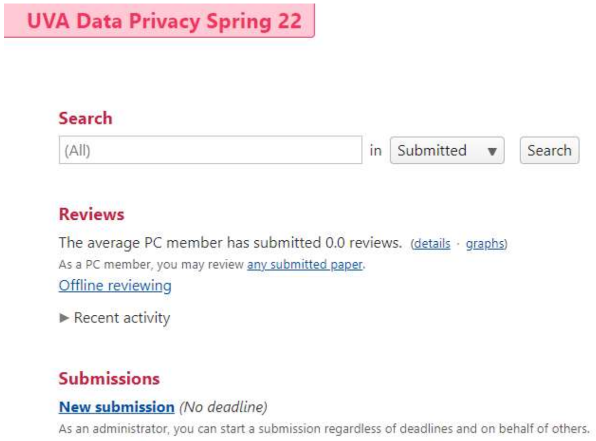
- 35min +- 5 mins
- Think about how you deliver the material to a large audience
  - 60% engineers
  - 30% researchers
  - 10% domain experts
  - Put more emphasis to motivation and background (unless those covered), and focus on intuition and give pointers and take-away messages
- It is okay to borrow ideas/materials from online resources
- Please ack what you used and how you changed them
- Send your slides to me or (better) come to my office hour one week before

Reviews

Before the presentation, submit a review (each student present a paper and submit 4 reviews, so each paper receives 4 reviews). Read others' reviews and discuss. Also raise the issue in class (to show your participation!).

Think critically but write professionally (guidelines at https://tianhao.wang/s22-dataprivacy/review.html).

- Turn:
  - This is not interesting.
  - The paper did not compare with x and y.
  - Writing is poorly.
- Into:
  - The paper can add discussions on a and b to address the wider audience.
  - X and y are closely related and applicable to the problem of this paper, if changing the methods.
  - Section a.b is confusing me. Notations are misused. Typos …



UVA Data Privacy Spring 22

Search

Reviews

The average PC member has submitted 0.0 reviews. (details · graphs)

As a PC member, you may review any submitted paper.

Offline reviewing

▶ Recent activity

Submissions

New submission (No deadline)

As an administrator, you can start a submission regardless of deadlines and on behalf of others.

Projects: Two flavors

- Research-oriented (for students who want to do/experience research)
  - Could be on data privacy, or the interaction of your research and privacy
  - Goal: a top-tier conference paper: proposal, related work, theory/empirical study
- Review-oriented (for demonstrations in industry)
  - A survey/review of existing tools/methods in some area
  - Implementation and empirical evaluation and comparison

Can work individually or form a group of 2

Encouraged to discuss with me or send me your draft/proposal for feedbacks

It cannot be the project you've already done

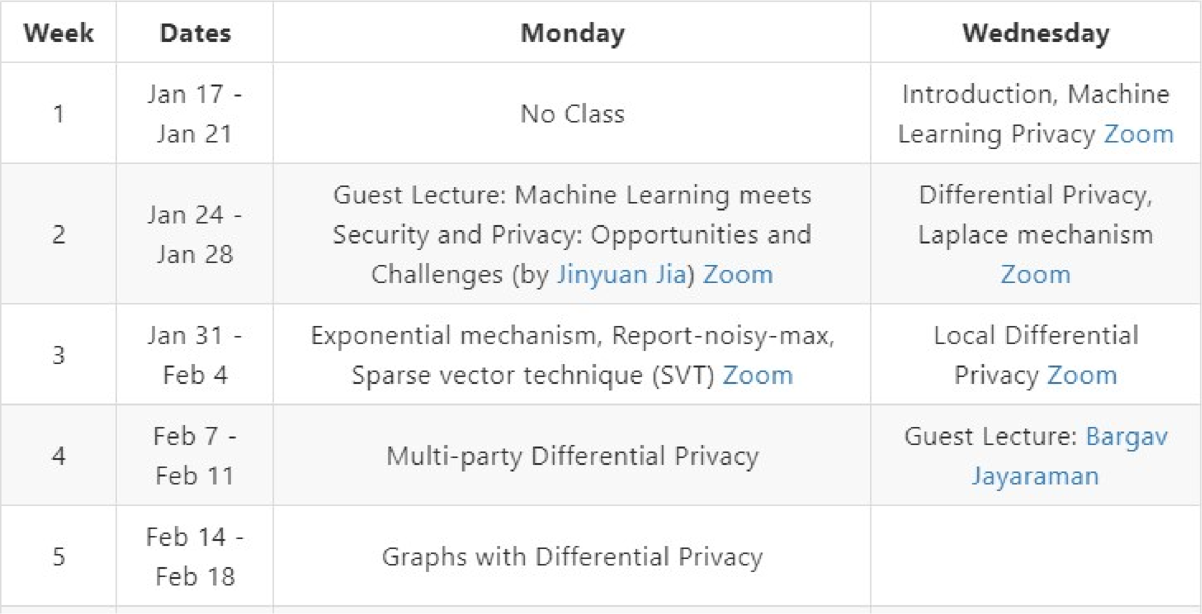
Schedule

Machine learning privacy attacks

Differential privacy and other privacy-enhancing technologies

Student presentations

Project presentations



Week	Dates	Monday	Wednesday
1	Jan 17 - Jan 21	No Class	Introduction, Machine Learning Privacy Zoom
2	Jan 24 - Jan 28	Guest Lecture: Machine Learning meets Security and Privacy: Opportunities and Challenges (by Jinyuan Jia) Zoom	Differential Privacy, Laplace mechanism Zoom
3	Jan 31 - Feb 4	Exponential mechanism, Report-noisy-max, Sparse vector technique (SVT) Zoom	Local Differential Privacy Zoom
4	Feb 7 - Feb 11	Multi-party Differential Privacy	Guest Lecture: Bargav Jayaraman
5	Feb 14 - Feb 18	Graphs with Differential Privacy	