# Yuqing Zhu

**yuqingzhu@ucsb.edu**
**https://jeremy43.github.io/**

## RESEARCH INTERESTS

My research interest is machine learning, including differential privacy [1-9] and domain adaptation [6, 8]. I am also the co-creator of AutoDP, an open-source library that allows researchers to use advanced mechanisms in differential privacy and obtain strong guarantees correctly.

## EDUCATION

**University of California, Santa Barbara** *2018.09– 2023.10 (expected)*
Ph.D. in Computer Science

**Nanjing University** *2014.09–2018.06*
B.S in Computer Science
National Elite Program

## AWARDS

2021 Google PhD Fellowship Recipient

## PUBLICATION AND PREPRINT

[1] Rachel Redberg, **Yuqing Zhu**, Yu-Xiang Wang. *Generalized PTR: User-Friendly Recipes for Data-Adaptive Algorithms with Differential Privacy.* In AISTATS-2023 (Oral presentation)

[2] **Yuqing Zhu**, Yu-Xiang Wang. *Adaptive Private-K-Selection with Adaptive K and Application to Multi-label PATE.* In AISTATS-2022.

[3] **Yuqing Zhu**, Jinshuo Dong, Yu-Xiang Wang. *Optimal Accounting of Differential Privacy via Characteristic Function.* In AISTATS-2022.

[4] Chong Liu, **Yuqing Zhu**, Kamalika Chaudhuri and Yu-Xiang Wang. *Revisiting Model-Agnostic Private Learning: Faster Rates and Active Learning.* In AISTATS-2021 and the Journal of Machine Learning Research-2021.

[5] **Yuqing Zhu** and Yu-Xiang Wang. *Improving Sparse Vector Technique with Renyi Differential Privacy.* In NeurIPS-2020.

[6] **Yuqing Zhu**, Xiang Yu, Manmohan Chandraker, Yu-Xiang Wang. *Private-kNN: Practical Differential Privacy for Computer Vision.* In CVPR-2020.

[7] **Yuqing Zhu** and Yu-Xiang Wang. *Poisson Subsampled Renyi Differential Privacy.* In ICML-2019.

[8] **Yuqing Zhu**, Chong Liu and Yu-Xiang Wang. *Model-Agnostic Private Learning with Domain Adaptation.* In CSS Theory and Practice of Differential Privacy Workshop ( TPDP-2020).

[9] **Yuqing Zhu**, Xiang Yu, Yi-Hsuan Tsai, Francesco Pittaluga, Masoud Faraki, Manmohan chandraker, Yu-Xiang Wang. *Voting-based Approaches For Differentially Private Federated Learning.* In International Workshop on Federated Learning (FL-NeurIPS-2022).

## RESEARCH EXPERIENCE

**Google Research NYC** 2022.06 - 2022.09
*Advisor: Matthew Joseph, Kareem Amin (Privacy team)* *New York*

- Investigated amplification by sampling in differentially private statistics release with c++ implementations in Google products.

**Google Research Seattle** 2021.06 - 2021.09
*Advisor: Shanshan Wu and Galen Andrew (Federated Learning Team)* *WFH*

- Investigated weighting approaches in differentially private federated learning.

**NEC Laboratories America** 2020.06 - 2020.09
*Advisor: Xiang Yu ( Media Analytics)* *San Jose, CA*

- **Differentially private federated learning**

  Proposed a voting-based solution for differentially private federated learning. See Publication [6, 9].

**Microsoft Research Asia** 2017.06 - 2017.11
*Advisor: Jifeng Dai (Visual Computing Group)* *MSRA, Beijing, China*

- **Video Instance-aware segmentation**

  Created an Official Implementation for Flow-Guided-Feature-Aggregation, and the git repo has already accumulated **500 stars**.github

**LAMDA Lab** 2016.05 - 2017.09
*Advisor: Prof .Wu-Jun LI, Prof. Zhi-Hua Zhou* *NJU,Nanjing,China*

- Proposed a deep discrete hybrid recommendation system for image & text recommendation.

## ACADEMIC SERVICE

Reviewer: NeurIPS-22, ICML-22, NeurIPS-21, AISTATS-21, ICLR-20, ICML-20, ICML-19, UAI-19, NeurIPS-19

## TECHNICAL SKILLS

| | |
|---|---|
| **Computer Languages** | Python, C++, Matlab |
| **Deep Learning Frameworks** | Pytorch/Tensorflow/MXNet/Caffee |