Yuqing Zhu

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

RESEARCH INTERESTS

My research interests is machine learning theory, e.g. differential privacy, off-policy reinforcement learning, deep learning theory. Recently, I am working on auto differential privacy project, which aims to help researchers build automating differential privacy computation and obtain tight DP guarantees. In addition to building practical tools with DP, I am also interested in establishing rigorous differential privacy guarantees to release large-scale real dataset (**Project Private Knowledge Transfer**) and how to privately expose the parameters of machine learning models that have been trained on sensitive dataset (**Project Poisson Subsampled Renyi Differential Privacy**).

EDUCATION

University of California, Santa Barbara *2018.09– now*
Ph.D. in Computer Science

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

PUBLICATION

Private-kNN: Practical Differential Privacy for Computer Vision
Yuqing Zhu, Xiang Yu, Manmohan Chandraker, Yu-Xiang Wang
Computer Vision and Pattern Recognition **(CVPR-2020)**.

Poisson Subsampled Renyi Differential Privacy

Yuqing Zhu and Yu-Xiang Wang
36th International Conference on Machine Learning **(ICML-2019)**.

Revisiting Model-Agnostic Private Learning: Faster Rates and Active Learning

Chong Liu, Yuqing Zhu, Kamalika Chaudhuri and Yu-Xiang Wang
To appear at CSS Theory and Practice of Differential Privacy Workshop (**TPDP-2020**) and ICML Federated Learning Workshop (**FC-ICML'20**).

Model-Agnostic Private Learning with Domain Adaptation *

Yuqing Zhu, Chong Liu and Yu-Xiang Wang
To appear at CSS Theory and Practice of Differential Privacy Workshop (**TPDP-2020**).

Improving Sparse Vector Technique with Renyi Differential Privacy *

Yuqing Zhu and Yu-Xiang Wang.

To appear at CSS Theory and Practice of Differential Privacy Workshop (**TPDP-2020**).

* under review at NeurIPS-2020.

RESEARCH EXPERIENCE

University of California, Santa Barbara 2018.9 - now
Advisor: Prof. Yu-Xiang Wang *UCSB, Santa Barbara, USA*

· · **Poisson Subsampled Renyi Differential Privacy** 2018.12 - 2019.3

- We consider the problem of "privacy-amplification by subsampling" under the Renyi Differential Privacy framework.
- Proved a nearly optimal upper bound of ”privacy amplification” of RDP via Poisson subsampling.

- Makes the moments accountant technique efficient and generally applicable for all Poisson-subsampled mechanisms.
- Appeared at **ICML 2019.**

Learning Privately from Your Neighbors 2019.08-2019.10

- Proposed a data-efficient scheme based on private release of k-nearest neighbor (kNN) queries, which altogether avoids splitting the training dataset.
- Present a new Renyi-differential privacy analisis to a "noisy screening" mechanism, together with " subsampling", allows our model to answer 10 times more quereis with even less privacy budget compared to state-of-the-art private knowledge transfer model.
- Achieved comparable or better accuracy than previous SOTA methods while reducing more than 90% of the privacy loss on MNIST, SVHN, CIFAR-10 and other realistic indentity relevant tasks.
- Appeared at **CVPR 2020.**

- **Autodp: Automating Differential Privacy Computation** 2018.09 - Now

- Autodp is a Renyi Differential Privacy based analytical Moment Accountant for automatical privacy computation.
- It generalizes the moments accounting technique for Gaussian mechanism, to any subsampled RDP mechanism, and could help researchers to correctly use advanced methods in differential privacy and obtain provable DP guarantees.
- Major contributor for implementing privacy amplification for generic Renyi DP algorithm for subsampling.
- https://github.com/yuxiangw/autodp github

Private Knowledge Transfer under Domain Adaptation 2019.03-now

- Considered two opposite targets of private knowledge transfer with a distribution shift between the private domain and the unlabeled public domain: training a model performs well on the public distribution or performs well on the private distribution.
- Derived a utility guarantee of the above two situations.
- Designed algorithms to privately estimate importance weight between shifted public data and private data under covariate shift or label shift assumption.

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

- **Video Instance-aware segmentation**

  Proposed a weakly-supervised solution to video instance-aware segmentation.
- Designed an algorithm leveraging color, texture and optical ow to tackle instance segmentation problem in videos with semi-supervised annotation.
- Created an **Official Implementation** for Flow-Guided-Feature-Aggregation, as the major contributor, reorganized and rewrote the code from an old internal Caffe version into a MXNet version, and the git repo has already accumulated **500 stars**.
- https://github.com/msracver/Flow-Guided-Feature-Aggregation 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.
- Constructed a model to learn hash codes of users and items give users feature and previous user-item rating matrix, signicantly reducing the storage cost by exploiting the efficient hamming distance based retrieval scheme.
- learned users code through deep neural network and encoded items by solving a discrete optimization problem based on user-item rating matrix.

ACADEMIC SERVICE

Reviewer :ICML-20, ICML-19, UAI-19, NeurIPS-19

TECHNICAL SKILLS

Computer Languages	C, C++, Java, Python, Matlab
Deep Learning Frameworks	Pytorch/Tensorflow/MXNet/Caffee