# Shuaiqi Wang

4720 Forbes Avenue, CIC 2225F – Pittsburgh, PA 15213 – USA
shuaiqiw@andrew.cmu.edu • wsqwsq.github.io

## Education

**Carnegie Mellon University** — **Pittsburgh, PA, USA**
*Jan. 2021 - Mar. 2026 (expected)*

- Ph.D. Student, Dept. of Electrical and Computer Engineering
- Advisor: Giulia Fanti

**Shanghai Jiao Tong University (SJTU)** — **Shanghai, China**
*Sep. 2016 - Jun. 2020*

- Bachelor of Engineering, Dept. of Computer Science
- Zhiyuan Honors Program of Engineering (Top 5%)

## Research Interests

Theoretical foundations of machine learning, and the applications in privacy and security, large language models, data synthesis and sharing, and federated learning.

## Experience

**Microsoft (Research Intern)** — **Pittsburgh, PA, USA**
*Sep. 2024 - Dec. 2024*

- Host: Zinan Lin, Pei Zhou
- Topic: differentially private data synthesis for structured datasets based on large language models

**Amazon (Research Intern)** — **San Diego, CA, USA**
*Jun. 2024 - Aug. 2024*

- Host: Alireza Mehrtash
- Topic: adversarial attack on vision language models

**JPMorgan Chase (AI Research Intern)** — **New York, NY, USA**
*Jun. 2023 - Aug. 2023*

- Host: Mohsen Ghassemi
- Topic: privacy protection across multiple summary statistical properties

## Publications

- **Shuaiqi Wang**, Vikas Raunak, Arturs Backur, Victor Reis, Pei Zhou, Sihao Chen, Longqi Yang, Zinan Lin, Sergey Yekhanin and Giulia Fanti. "Struct-Bench: A Benchmark for Differentially Private Structured Text Generation", in *arXiv*.
- **Shuaiqi Wang**, Sayali Deshpande, Rajesh Kudupudi, Alireza Mehrtash and Danial Sabri Dashti. "MASAN: Enhancing Attack Stealth and Efficacy on Vision-Language Models via Smart Noise", in ***ICLR 2025 BuildingTrust***.
- **Shuaiqi Wang**, Shuran Zheng, Zinan Lin, Giulia Fanti and Zhiwei Steven Wu. "Inferentially-Private Private Information", in ***WWW 2025***.
- Jiajun Gu, Yuhang Yao, **Shuaiqi Wang**, Carlee Joe-Wong. "Evaluating Selective Encryption Against Gradient Inversion Attacks ", in *arXiv*.
- Enshu Liu, Junyi Zhu, Zinan Lin, Xuefei Ning, **Shuaiqi Wang**, Matthew B Blaschko, Sergey Yekhanin, Shengen Yan, Guohao Dai, Huazhong Yang and Yu Wang. "Linear Combination of Saved Checkpoints Makes Consistency and Diffusion Models Better", in ***ICLR 2025***.
- **Shuaiqi Wang**, Zinan Lin and Giulia Fanti. "Statistic Maximal Leakage", in ***ISIT 2024***.
- **Shuaiqi Wang**, Rongzhe Wei, Mohsen Ghassemi, Eleonora Kreacic and Vamsi Potluru. "Guarding Multiple Secrets: Enhanced Summary Statistic Privacy for Data Sharing", in ***ICLR 2024 PML***.

- Xinyi Xu, **Shuaiqi Wang**, Chuan-Sheng Foo, Bryan Kian Hsiang Low and Giulia Fanti. "Data Distribution Valuation with Incentive Compatibility", in ***NeurIPS 2024***.
- **Shuaiqi Wang***, Zinan Lin*, Vyas Sekar and Giulia Fanti. "Summary Statistic Privacy in Data Sharing", in ***IEEE Journal on Selected Areas in Information Theory*** (***JSAIT***) (2024).

  * Equal contribution.
- Ronghao Ni, Zinan Lin, **Shuaiqi Wang** and Giulia Fanti. "Mixture-of-Linear-Experts for Long-term Time Series Forecasting", in ***AISTATS 2024***.
- **Shuaiqi Wang**, Jonathan Hayase, Giulia Fanti and Sewoong Oh. "Towards a Defense Against Federated Backdoor Attacks Under Continuous Training", in ***Transactions on Machine Learning Research*** (***TMLR***) (2023).
- Benjie Miao, **Shuaiqi Wang**, Luoyi Fu and Xiaojun Lin. "De-anonymizability of Social Network: Through the Lens of Symmetry", in ***MobiHoc 2020***.
- Luoyi Fu, Jiapeng Zhang, **Shuaiqi Wang**, Xinyu Wu, Xinbing Wang and Guihai Chen. "De-anonymizing social networks with overlapping community structure", in ***IEEE/ACM Transactions on Networking*** *28.1 (2020): 360-375.*
- Xudong Wu, Luoyi Fu, **Shuaiqi Wang**, Bo Jiang, Xinbing Wang and Guihai Chen. "Collective Influence Maximization in Mobile Social Networks" in ***IEEE Transactions on Mobile Computing*** (*2021*).

## Honors and Awards

- **Carnegie Institute of Technology Dean's Fellow** 2021
- **Zhiyuan Distinguish Scholarship** (Top 1%) 2020
- **Zhiyuan College Honors Scholarship** (Top 5%) 2017, 2018, 2019
- **Academic Excellence Scholarship** 2017, 2018, 2019
- **First Prize in China Undergraduate Computer Design Competition** (Top 5%) 2019

## Skills

**Programming Languages:** Python, C, C++, Java, MATLAB, Mathematica, LaTeX, HTML, bash, shell.
**Machine Learning Frameworks:** TensorFlow, PyTorch, Keras, Transformers, etc.

## Professional Services

**Conference Reviewer:** NeurIPS'21-25, ICLR'24-25, ICML'25, AISTATS'24-25, WWW'25.
**Journal Reviewer:** TMLR, IEEE/ACM Transactions on Networking, IEEE Transactions on Information Forensics and Security.
**Graduate Teaching Assistant:** CMU 18752 Estimation, Detection and Learning; CMU 18734 Foundations of Privacy.

## Talks and Interviews

Statistic Maximal Leakage

- GCoM Lab in Georgia Tech Oct. 2024
- SIAM Conference on Mathematics of Data Science (MDS 2024) Oct. 2024
- CMU CyLab Partners Conference 2024 Sep. 2024
- Interview by NiklasOPF [*talk video*] Aug. 2024
- IEEE International Symposium on Information Theory (ISIT 2024) Aug. 2024