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 - present

- 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%)
- GPA: 92.1/100

Research Interests

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

Publications and Manuscripts

- **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 Workshop***.
- Xinyi Xu, **Shuaiqi Wang**, Chuan-Sheng Foo, Bryan Kian Hsiang Low and Giulia Fanti. "Data Distribution Valuation with Incentive Compatibility", under submission.
- Zinan Lin*, **Shuaiqi Wang***, Vyas Sekar, and Giulia Fanti. "Summary Statistic Privacy in Data Sharing", in ***IEEE Journal on Selected Areas in Information Theory*** and ***NeurIPS 2022 SyntheticData4ML***.

  * 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*** (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*).

Research Experiences

Statistic Maximal Leakage in Trade Secret Privacy
Guide: Prof. Giulia Fanti *Mar. 2023 - present*

- Formalized trade secret privacy concerns by notion of maximal leakage
- Designed and analyzed operational privacy and utility metrics
- Proposed mechanisms that balance privacy-utility tradeoffs in data sharing applications

Summary Statistic Privacy for Data Sharing
Guide: Prof. Giulia Fanti, Prof. Vyas Sekar *Mar. 2022 - Mar. 2023*

- Formalized summary statistic privacy concerns in data sharing applications
- Derived fundamental limits on the tradeoff between privacy and distortion
- Proposed mechanisms that achieve order-optimal privacy-distortion tradeoffs under certain types of secrets

Towards a Defense against Backdoor Attacks in Continual Federated Learning
Guide: Prof. Giulia Fanti, Prof. Sewoong Oh *May. 2021 - May. 2022*

- Proposed a federated learning algorithm that is robust to backdoor attacks under continual learning
- Provided theoretical justifications for the proposed defense algorithm
- Achieved best defense results cross a wide range of adversarial corruption ratios and time-varying attacks

Group Testing with Inexact Reconstruction
Guide: Prof. Giulia Fanti *Sep. 2020 - Mar. 2021*

- Proved the lower bound on the sample complexity of group testing with reconstruction error
- Designed an algorithm that achieves order-optimal sample complexity
- Proved the robustness of the proposed algorithm to the sparsity estimation error

Reinforcement Learning for Safe Control
Guide: Prof. Yorie Nakahira *May. 2020 - Dec. 2020*

- Designed a safe control algorithm based on learning-based Model Predictive Control and model-free RL
- Quantified the model uncertainty and derived the safety guarantee of our algorithm in nonlinear systems
- Analyzed the conversion between model-driven and data- driven methods quantitatively

Distributed Steiner Tree Construction in Wireless Networks with Unreliable Links
Guide: Prof. Luoyi Fu, Prof. Xinbing Wang, Prof. Xiaojun Lin *Jul. 2019 - Mar. 2020*

- Proposed a protocol to search and communicate in wireless networks reliably and energy-efficiently
- Designed a distributed multicast tree construction algorithm with the lowest time and message complexity
- Achieved the approximate rate of 1.061 to the Steiner tree length

De-anonymizability of Social Network: Through the Lens of Symmetry
Guide: Prof. Luoyi Fu, Prof. Xinbing Wang, Prof. Xiaojun Lin *Mar. 2019 - Aug. 2019*

- Defined the symmetry of networks by automorphism and homomorphism
- Determined the de-anonymizability of given networks based on the symmetry level
- Designed an approximate algorithm to estimate de-anonymizability via sampling techniques

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

Teaching Assistant

CMU 18734: Foundations of Privacy **Pittsburgh, PA, USA**
Instructor: Steven Wu *Fall 2021*

CMU 18752: Estimation, Detection and Learning **Pittsburgh, PA, USA**
Instructor: Rohit Negi *Spring 2024*

Coding

C, C++, Python, Java, MATLAB, Mathematica, LaTeX, etc.