Curriculum Vitae

SHIMING WANG

my16wsm@sjtu.edu.cn | +86 18217356119

EDUCATION

Shanghai Jiao Tong University **Shanghai**

Ph.D Candidate in Computer Science, Department of Computer Science *Sept 2020 – Present*

Shanghai Jiao Tong University **Shanghai**

B.S in Electrical and Computer Engineering, UM-SJTU Joint Institute *Sept 2016 – Aug 2020*

PUBLICATION

Curator Attack: When Blackbox Differential Privacy Auditing Loses Its Power

Shiming Wang, Liyao Xiang, Bowei Cheng, Zhe Ji, Xinbing Wang.

In the ACM Conference on Computer and Communications Security, October 2024, **CCS 2024**.

Crafter: Facial Feature Crafting against Inversion-based Identity Theft on Deep Models

Shiming Wang, Zhe Ji, Liyao Xiang, Hao Zhang, Xinbing Wang, Chenghu Zhou, Bo Li.

In the Network and Distributed System Security Symposium, February 2024, **NDSS 2024**.

Privacy-Preserving Split Learning via Pareto Optimal Search

Xiyu, Liyao Xiang, **Shiming Wang**, Chengnian Long.

In the European Symposium on Research in Computer Security, September 2023, **ESORICS 2023**.

RESEARCH EXPERIENCE

Loophole Analysis on Black-box Differential Privacy Auditing Tools *Oct 2022 – Feb 2024*

Supervised by Prof. Liyao Xiang, John Hopcroft Center

This project focuses on evaluating the differential privacy level of data curators. I inspect existing black-box differential privacy auditing tools and conclude that they all exhibit a substantial flaw of failing to catch curators with overstated privacy guarantees. This discovery reveals that black-box auditors are widely unreliable in practice and the privacy of data owners requires protection from more robust auditing tools.

- Analyze existing black-box auditing tools for differential privacy and discover a shared loophole of failing to catch curators with overly strong differential privacy claims.
- Interpret the loophole as false positive errors through the lens of hypothesis testing, and devise an analysis pipeline applicable to general future auditors.
- Confirm the findings on various curator tasks including statistical analysis (eg. counting queries using SVT & crowdsourcing software statistics using RAPPOR) and machine learning (eg. next-word prediction using LLM & image classification using ResNet20).

Facial Feature Crafting against Identity Theft on Machine Learning Models *Sept 2020 – Oct 2022*

Supervised by Prof. Liyao Xiang, John Hopcroft Center

This project addresses the common concern of personal identity privacy in cloud machine learning tasks. I build a defense tool that allows users to modify their photos before sharing them with cloud service providers. It prevents unauthorized parties from reconstructing users' raw faces and inferring their private identities.

- Allow users to craft features of their images that are robust against unauthorized facial recognition programs.
- Design Crafter, a simple open-source tool for everyday users to safeguard their identity according to their preferences.
- Confirm the effectiveness of Crafter on open-source machine learning (eg. ResNet50 & VGG16) and public datasets (eg. CelebA & LFW).

PROFESSIONAL SKILLS

Programming: C, C++, Python

Language: Chinese (Native), English (**GRE 326+4.0, TOEFL 117**)