Weizhao Jin

weizhaoj@usc.edu | weizhaojin.netlify.app | www.linkedin.com/in/wzjin

Education

University of Southern California Aug. 2020 – May 2025 (Expected)
Ph.D. in Computer Science

University of Virginia Aug. 2018 – May 2020
Master of Engineering in Computer Engineering

Zhejiang University Sep. 2014 – June 2018
Bachelor of Engineering in Electrical Engineering and Automation

Experience

Applied Scientist Intern May 2023 – April 2024 (Extended)
Amazon *AWS Privacy Engineering*

- **AWS Differential Privacy Library**
  Built the key components including privacy budget accountant and private query execution history for the first (easy-to-use, hard-to-misuse) differential privacy library at Amazon to raise the privacy bar of Amazon services

Research Intern Oct. 2022 – Mar. 2023
FedML Inc. *Privacy-Preserving Federated Learning*

- **FedML with Homomorphic Encryption**
  Integrated homomorphic encryption to FedML's open-source library and MLOps services to facilitate the adoption of privacy enhancement for users

Graduate Research Assistant Aug. 2020 – Present
University of Southern California *Advisors: Srivatsan Ravi and Muhammad Naveed*

- **Efficient Homomorphic-Encryption-Based Privacy-Preserving Federated Learning System**
  Built an efficient homomorphic-encryption-based federated learning system by using selective encryption with parameter sensitivity
- **Privacy-Preserving Path Validation for 5G Network Slicing**
  Built a decentralized path validation protocol for 5G network slicing using NIZK, designing a privacy-preserving malicious path recovery integrated with VNE-CBS network embedding
- **Secure Publish-Process-Subscribe IoT System**
  Built a secure Publish-Process-Subscribe IoT system supporting functions like private set intersection and federated learning with Yao's Garbled Circuits, homomorphic encryption and proxy re-encryption atop MQTT protocol

Applied Scientist Intern May 2022 – Aug. 2022
Amazon *Buyer Risk Prevention*

- **Privacy-Preserving Federated Learning Using Fully Homomorphic Encryption**
  Built a privacy-preserving Federated Learning framework using homomorphic encryption for solving cross-region data restriction as well as facilitating cross-team collaboration on sensitive data; worked with the engineering team to design and implement an AWS-based FL system; integrated our framework with tabular neural networks like TabNet and Tab1DCNN

Student Research Assistant Oct. 2018 – May 2020
Security Lab, University of Virginia *Advisor: Yuan Tian*

- **Vulnerabilities of Autonomous Vehicle Sensor Fusion Algorithm**
  Composed adversarial examples against perception module; tested attacks on the sensor fusion algorithm of the autonomous vehicle platform Baidu Apollo
- **Vulnerabilities of Dedicated Short-Range Communication**
  Analyzed existing vulnerabilities in the current version of DSRC protocol for connected vehicles; designed several attacks on DSRC protocol on connected vehicle modules

Student Research Assistant Oct. 2017 – June 2018
USS Lab, Zhejiang University *Advisors: Wenyuan Xu and Xiaoyu Ji*

- **Security Research on Multi-factor Verification for Online Accounts**
  Built a SMS sniffing system with USRP and Osmocombb; designed a chain reaction attack mechanism which could possibly compromise most of the online service accounts with defective SMS-based multi-factor verification

Selected Publications (Full list)

- **FedML-HE: An Efficient Homomorphic-Encryption-Based Privacy-Preserving Federated Learning System**
  Weizhao Jin*, Yuhang Yao*, Shanshan Han, Carlee Joe-Wong, Srivatsan Ravi, Salman Avestimehr, Chaoyang He
  preprint (short version: NeurIPS 2023 Federated Learning Workshop), 2023
- **Homomorphic-Encryption-Based Privacy-Preserving Federated TabNet Learning**
  Weizhao Jin, Shahin Navardi, Gaoyuan Du, Daniel Cociorva, Hakan Brunzell, Xiaoyang Liu
  Amazon Machine Learning Conference (Oral), 2023
- **FedGCN: Convergence-Communication Tradeoffs in Federated Training of Graph Convolutional Networks**
  Yuhang Yao, Weizhao Jin, Srivatsan Ravi, Carlee Joe-Wong
  Thirty-seventh Conference on Neural Information Processing Systems (NeurIPS), 2023
- **Labeling without Seeing? Blind Annotation for Privacy-Preserving Entity Resolution**
  Yixiang Yao, Weizhao Jin, Srivatsan Ravi
  preprint, 2023
- **FedMLSecurity: A Benchmark for Attacks and Defenses in Federated Learning and Federated LLMs**
  Shanshan Han, Baturalp Buyukates, Zijian Hu, Han Jin, Weizhao Jin, Lichao Sun, Xiaoyang Wang, Chulin Xie, Yuhang Yao, Kai Zhang, Qifan Zhang, Yuhui Zhang, Chaoyang He, Salman Avestimehr
  preprint, 2023
- **Kick Bad Guys Out! Zero-Knowledge-Proof-Based Anomaly Detection in Federated Learning**
  Shanshan Han, Wenxuan Wu, Baturalp Buyukates, Weizhao Jin, Yuhang Yao, Qifan Zhang, Salman Avestimehr, Chaoyang He
  preprint, 2023
- **P3V: Privacy-Preserving Path Validation System for Multi-Authority Sliced Networks**
  Weizhao Jin, Erik Kline, TK Satish Kumar, Lincoln Thurlow, Srivatsan Ravi
  preprint, 2023
- **Secure Publish-Process-Subscribe System for Dispersed Computing**
  Weizhao Jin, Bhaskar Krishnamachari, Muhammad Naveed, Srivatsan Ravi, Kwame-Lante Wright
  41st International Symposium on Reliable Distributed Systems (SRDS), 2022
- **Decentralized Privacy-Preserving Path Validation for Multi-Slicing-Authority 5G Networks**
  Weizhao Jin, Srivatsan Ravi, Erik Kline
  IEEE Wireless Communications and Networking Conference (WCNC), 2022
- **SMS Goes Nuclear: Fortifying SMS-Based MFA in Online Account Ecosystem**
  Weizhao Jin*, Xiaoyu Ji*, Ruiwen He, Zhou Zhuang, Wenyuan Xu, Yuan Tian
  Workshop on Data-Centric Dependability and Security (co-located with the IEEE/IFIP International Conference on Dependable Systems and Networks), 2021

Miscellaneous

- Reviewer: Amazon Research Awards, IEEE Transactions on Network Science and Engineering, PeerJ Computer Science
- USC Graduate School Research Award (2022)
- Amazon BRP Trustworthy and Privacy ML Working Group Talk: Homomorphic Encryption and Privacy-Preserving Federated Learning (2022)
- USC ISI NCD Talk: Decentralized Privacy-Preserving Path Validation for Multi-Authority 5G Networks (2022)
- Graduate Teaching Assistant: USC CSCI 103 Introduction to Programming (C++), UVA APMA 3100 Probability

Skills

Languages: Chinese(native), English (proficient), German (European B1)
Technical: Python, Java, C/C++, PyTorch, AWS, Docker, MATLAB, JavaScript