Qingzhao Zhang

(+1) 734-881-5608 | qzzhang@umich.edu | Github: zqzqz |
Website: https://zqzqz.github.io/ | Google Scholar | LinkedIn

EDUCATION

University of Michigan *Sep 2019 – May 2025 (Expected)*
Ph.D. *candidate in Computer Science | Overall GPA: 3.98/4.0*

University of Michigan *Sep 2019 – Dec 2023*
M.S. *in Computer Science*

Shanghai Jiao Tong University *Sep 2015 – May 2019*
B.E. *in Computer Engineering | Overall GPA: 89.63/100*

RESEARCH INTERESTS

System security (e.g., cyber-physical systems, autonomous driving), software security (e.g., program analysis, formal verification), AI security (e.g., adversarial attacks, robustness).

EXPERIENCE

Research Assistant | University of Michigan *Sep 2019 - Present*
Advisor: Prof. Z. Morley Mao

- Research on software/system for cyber-physical system safety — *AVChecker*, the first traffic rule compliance checker on autonomous driving software; *SmtConf*, safety vetting of industrial control system configuration.
- Research on adversarial machine learning on cyber-physical systems — Adversarial attack and mitigation on trajectory prediction on autonomous driving; Analyzed data fabrication vulnerability on collaborative perception.
- Research on robustness of vehicular network — *RAO*, collaborative perception with asynchronous sensors.
- Research on robust perception algorithms of autonomous driving, and large language model security/efficiency.

Software Engineer Intern | Google *May 2023 - July 2023*

- Designed and implemented formal verification solutions to enhance the security properties of an embedded system kernel (based on open-sourced Tock OS), involving modular model checking and theorem proving.

Software Engineer Intern | Google *May 2022 - July 2022*

- Designed and implemented static analysis checks based on Android Lint for Google's Android tests, which was deployed to assist Google developers to write high-quality unit tests.

Software Engineer Intern | YITU Technology *May 2019 - July 2019*

- Implemented Web APIs for face recognition applications in the company's production.

Visiting Scholar | UIUC *Jul 2018 - Oct 2018*
Advisor: Prof. Tao Xie, Prof. Bo Li

- Designed blockchain-based decentralized advertising systems using public smart contracts.
- Research on vulnerability detection and automatic repair of Ethereum smart contracts.

Research Assistant | Shanghai Jiao Tong University *May 2017 - May 2019*
Advisor: Dr. Haining Lu, Dr. Ning Ding

- Research on vulnerability detection of smart contracts and privacy-preserving blockchain systems.

SELECTED PUBLICATIONS (*: co-primary)

Conference papers

- **[ICLR'25]** Minkyoung Cho, Yulong Cao, Jiachen Sun, **Qingzhao Zhang**, Marco Pavone, Jeong Joon Park, Heng Yang, Z. Morley Mao. "Cocoon: Robust Multi-Modal Perception with Uncertainty-Aware Sensor Fusion", *The 13th International Conference on Learning Representations*.
- **[Security'24] Qingzhao Zhang**, Shuowei Jin, Ruiyang Zhu, Jiachen Sun, Xumiao Zhang, Qi Alfred Chen, Z. Morley Mao. "On Data Fabrication in Collaborative Vehicular Perception: Attacks and Countermeasures", *The 33th USENIX Security Symposium*.
- **[ICLR'24]** Jiachen Sun, Haizhong Zheng, **Qingzhao Zhang**, Atul Prakash, Z. Morley Mao, Chaowei Xiao. "CALICO: Self-Supervised Camera-LiDAR Contrastive Pre-training for BEV Perception", *The 12th International Conference on Learning Representations*.
- **[Mobicom'23] Qingzhao Zhang***, Xumiao Zhang*, Ruiyang Zhu*, Fan Bai, Mohammad Naserian, Z. Morley Mao. "Robust Real-time Multi-vehicle Collaboration on Asynchronous Sensors", *The 29th International Conference on Mobile Computing and Networking*.
- **[CVPR'22] Qingzhao Zhang**, Shengtuo Hu, Jiachen Sun, Qi Alfred Chen, Z. Morley Mao. "On Adversarial Robustness of Trajectory Prediction for Autonomous Vehicles", *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*.
- **[RAID'22] Qingzhao Zhang**, Xiao Zhu, Mu Zhang, Z. Morley Mao. "Automated Runtime Mitigation for Timing-based Safety Hazards in Industrial Controllers", *The 25th International Symposium on Research in Attacks, Intrusions and Defenses*.
- **[AsiaCCS'22]** Shengtuo Hu, **Qingzhao Zhang**, André Weimerskirch, Z Morley Mao. "GateKeeper: A Gateway-based Broadcast Authentication Protocol for the In-vehicle Ethernet", *Proceedings of the ACM on Asia Conference on Computer and Communications Security*.
- **[IV'22]** Ze Zhang, Sanjay Sri Vallabh Singapuram, **Qingzhao Zhang**, David Ke Hong, Brandon Nguyen, Z Morley Mao, Scott Mahlke, Qi Alfred Chen. "AVMaestro: A Centralized Policy Enforcement Framework for Safe Autonomous-driving Environments", *IEEE Intelligent Vehicles Symposium*.
- **[SIGMETRICS'21] Qingzhao Zhang**, David Ke Hong, Ze Zhang, Qi Alfred Chen, Scott Mahlke, Z. Morley Mao. "A Systematic Framework for Checking Driving Rule Compliance in Autonomous Vehicle Software", *Proceedings of the ACM on Measurement and Analysis of Computing Systems*.
- **[SANER'20] Qingzhao Zhang***, Yizhuo Wang*, Juanru Li, Siqi Ma. "EthPloit: From Fuzzing to Efficient Exploit Generation against Smart Contracts", *IEEE 27th International Conference on Software Analysis, Evolution and Reengineering*.
- **[FC'20]** Yanxue Jia, Shi-Feng Sun, Yuncong Zhang, **Qingzhao Zhang**, Ning Ding, Zhiqiang Liu, Joseph K Liu, Dawu Gu. "Ringct 3.0 for blockchain confidential transaction: Shorter size and stronger security", *Financial Cryptography and Data Security: 24th International Conference*.

Journal papers

- **[TDSC]** Yanxue Jia, Shi-Feng Sun, Yuncong Zhang, **Qingzhao Zhang**, Ning Ding, Zhiqiang Liu, Joseph K Liu, Dawu Gu. "PBT: A New Privacy-Preserving Payment Protocol for Blockchain Transactions", *IEEE Transactions on Dependable and Secure Computing*.

Workshop papers

- **[CPSIoTSec'24] Qingzhao Zhang**, Z. Morley Mao. "Stealthy Data Fabrication in Collaborative Vehicular Perception", *The 6th Workshop on CPS and IoT Security*.
- **[SRML'22]** Jiachen Sun, **Qingzhao Zhang**, Bhavya Kailkhura, Zhiding Yu, Chaowei Xiao, Z Morley Mao. "ModelNet40-C: A Robustness Benchmark for 3D Point Cloud Recognition Under Corruption", *ICLR 2022 Workshop on Socially Responsible Machine Learning*.

- **[FEAST'20]** Ze Zhang, **Qingzhao Zhang**, Brandon Nguyen, Sanjay Sri Vallabh Singapuram, Z Morley Mao, Scott Mahlke. "Automatic Feature Isolation in Network Protocol Software Implementations", *ACM Workshop on Forming an Ecosystem Around Software Transformation*.

Preprints & In submission

- **Qingzhao Zhang**, Ziyang Xiong, Z. Morley Mao. "Safeguard is a Double-edged Sword: Denial-of-service Attack on Large Language Models".
- Shuowei Jin, Xueshen Liu, **Qingzhao Zhang**, Z. Morley Mao. "Compute Or Load KV Cache? Why Not Both?".
- Shuowei Jin, Yongji Wu, Haizhong Zheng, **Qingzhao Zhang**, Matthew Lentz, Z Morley Mao, Atul Prakash, Feng Qian, Danyang Zhuo. "Adaptive Skeleton Graph Decoding".
- Fangzhou Wu, **Qingzhao Zhang**, Ati Priya Bajaj, Tiffany Bao, Ning Zhang, Ruoyu Wang, Chaowei Xiao. "Exploring the Limits of ChatGPT in Software Security Applications".
- Spencer Hallyburton, **Qingzhao Zhang**, Z. Morley Mao, Miroslav Pajic. "Partial-Information, Longitudinal Cyber Attacks on LiDAR in Autonomous Vehicles".
- Jiachen Sun, **Qingzhao Zhang**, Bhavya Kailkhura, Zhiding Yu, Chaowei Xiao, Z. Morley Mao. "Benchmarking Robustness of 3d Point Cloud Recognition Against Common Corruptions".
- Anrin Chakraborti*, **Qingzhao Zhang***, Jingjia Peng, Z. Morley Mao, Michael K. Reiter. "StreetCred: A Privacy-Preserving Reputation System for Connected Autonomous Vehicles".
- Ruiyang Zhu, **Qingzhao Zhang**, Xumiao Zhang, Fan Bai, Mohammad Naserian, Z. Morley Mao. "RAO++: Realistic Real-time Multi-vehicle Collaboration on Asynchronous Sensors".

TEACHING AND MENTORSHIP

Supervisor of Undergraduate Research *2022*

- Multidisciplinary Design Program (MDP) at University of Michigan. Lead cybersecurity research and supervised a team of four students.

Research Mentorship *2020-2024*

- Research on program analysis, autonomous driving, adversarial machine learning.
- Mentees: Charles Ziegenbein Jr., Kevin Zhang, Andrew Wei, Xingyu Wang, Jingjia Peng, Ziyang Xiong.

SERVICES

- Conference Reviewer: ICLR 2025, ICRA 2025, ACM MM 2024, IV 2024, IV 2023
- Journal Reviewer: IEEE Internet of Things Journal, IEEE Intelligent Transportation Systems Magazine, 5G/6G Precise Positioning on C-ITS and CAV, Transactions on Dependable and Secure Computing
- Workshop Reviewer: Re-design Industrial Control Systems with Security (RICSS 2024)
- Artifact Reviewer: Usenix Security 2022
- Pre-review Task Force: NSDI 2025

TALKS

- Enhancing Security, Safety, and Reliability of Cyber-physical Systems

Presentation at Midwest Security Workshop *11/16/2024*

- Stealthy Data Fabrication in Collaborative Vehicular Perception

Presentation at 6th CPSIoTSec Workshop, co-located with CCS 2024 *10/18/2024*

Poster at Midwest Security Workshop *11/16/2024*

- On data fabrication in collaborative vehicular perception: attacks and countermeasures

Poster at Athena institute (NSF AI Institute) annual showcase (best poster award) *5/3/2023*

Presentation at USENIX Security 2024 *8/16/2024*

- Automated runtime mitigation for timing-based safety hazards in industrial controllers

Virtual presentation at RAID 2022 *10/27/2022*

- On adversarial robustness of trajectory prediction for autonomous vehicles

Poster at Athena institute (NSF AI Institute) annual showcase *8/18/2022*

Poster at CVPR 2022 *6/23/2022*

- Robustness of applications for autonomous vehicles

Presentation at Workshop on Future Automotive Research Datasets *11/19/2021*

- A systematic framework for checking driving rule compliance in autonomous vehicle software

Virtual presentation at SIGMETRICS 2021 *6/16/2021*

HONORS AND AWARDS

- Student Travel Grant, Usenix Security 2024, SIGMETRICS 2021, CCS 2021 *2019 – 2024*
- Rackham Student Fellowship, University of Michigan *2019*
- Academic Excellence Scholarship of SJTU (top 5%) *2016, 2017, 2018*