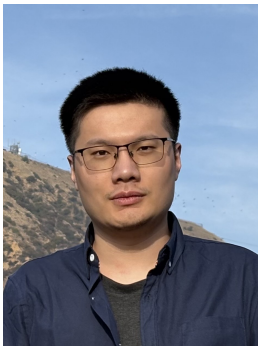
COLLEGE OF ENGINEERING
Electrical & Computer Engineering



# Qingzhao Zhang

*Incoming Tenure-Track Assistant Professor*
*Department of Electrical and Computer Engineering*
*University of Arizona (Starting Fall 2025)*

PhD, University of Michigan, advised by Dr. Z. Morley Mao

**Email:** qzzhang@umich.edu
**Website:** https://zqzqz.github.io

## About Me

My research lies at the intersection of system security, artificial intelligence, and cyber-physical systems (CPS). I develop techniques to secure AI components and networked software systems in real-world, safety-critical applications such as connected and autonomous vehicles. My work has been published in top-tier venues including Usenix Security, Mobicom, SIGMETRICS, and CVPR. I have mentored over a dozen undergraduate and graduate researchers and actively collaborate with experts across domains at leading universities. Beginning in Fall 2025, I will lead a research group in ECE@UA, focused on building secure, trustworthy, and intelligent systems.

## Research Focus

- **Trustworthy AI and Systems**: Investigating and mitigating security vulnerabilities in AI components, especially in cyber-physical systems like autonomous vehicles.
- **Security and Reliability of Networked Software Systems**: Applying program analysis and system design to improve the resilience of large-scale, connected CPS infrastructures.
- **Security and Safety of LLMs**: Enhancing the trustworthiness of large language models and exploring their safe integration in real-world CPS environments.

## Openings

I plan to recruit **fully funded PhD students** to join in **Fall 2026** as well as **research interns** who are welcome to start at any time. If you are interested in working on cutting-edge research in security and AI for CPS, please email me at `qzzhang@umich.edu` with your CV, transcript, and an optional research statement.

## Candidate Profile

Looking for self-motivated students with strong foundations in systems, AI, or security. Strong programming skills and interest in research are essential. A bachelor's or master's degree in computer science, computer engineering, or a related field is required. Prior research experience or academic publications in AI, cybersecurity, or CPS domains is a plus.