

# Chongzhou Fang

University of California, Davis  
Room 2346, 455 Crocker Ln, Davis, CA

czfang@ucdavis.edu  
<https://chongzhoufang.github.io>

## Higher Education

---

- **University of California, Davis** Davis, USA  
*PhD in Computer Engineering* Sep. 2020 - Jun. 2025 (Expected)  
– Advised by Prof. Houman Homayoun
- **Southeast University** Nanjing, China  
*BSc in Information Science* Aug. 2016 - Jun. 2020

## Research Interest

---

- Cloud Infrastructure
- Cloud Security
- LLM for System Security
- Serverless Cloud
- Side-Channel Attacks

## Industrial Research

---

- **Intel Programmable Solution Group (PSG)**  
*Project: Securing Intel's Heterogeneous Computing Platform.* Jun. 2022 - Sep. 2022  
– Develop new security features for Intel FPGAs.  
– Develop a library that handles secure communication and attestation protocols between CPU and peripheral FPGAs.

## Selected Publications

---

1. **Large Language Models for Code Analysis: Do LLMs Really Do Their Job?**  
*Chongzhou Fang, Ning Miao, Shaurya Srivastav, Jialin Liu, Ruoyu Zhang, Ruijie Fang, Asmita Asmita, Ryan Tsang, Najmeh Nazari, Han Wang and Houman Homayoun.*  
Usenix Security Symposium 2024.
2. **Forget and Rewire: Enhancing the Resilience of Transformer-based Models against Bit-Flip Attacks**  
*Najmeh Nazari, Hosein Mohammadi Makrani, Chongzhou Fang, Hossein Sayadi, Setareh Rafatirad, Khaled N. Khasawneh and Houman Homayoun.*  
Usenix Security Symposium 2024.
3. **Fuzzing BusyBox: Leveraging LLM and Crash Reuse for Embedded Bug Unearthing**  
*Asmita Asmita, Yaroslav Oliinyk, Michael Scott, Ryan Tsang, Chongzhou Fang and Houman Homayoun*  
Usenix Security Symposium 2024.
4. **LLM-FIN: Large Language Models Fingerprinting Attack on Edge Devices**  
*Najmeh Nazari, Furi Xiang, Chongzhou Fang, Hosein Mohammadi Makrani, Aditya Puri, Kartik Patwari, Hossein Sayadi, Setareh Rafatirad, Chen-Nee Chuah, Houman Homayoun*  
International Symposium on Quality Electronic Design (ISQED) 2024.

5. **SpecScope: Automating Discovery of Exploitable Spectre Gadgets on Black-Box Microarchitectures**  
*Najmeh Nazari, Behnam Omid, Chongzhou Fang, Hosein Mohammadi Makrani, Setareh Rafatirad, Avesta Sasan, Houman Homayoun, Khaled N Khasawneh*  
 Design, Automation & Test in Europe Conference & Exhibition (DATE) 2024.
6. **Gotcha! I Know What You are Doing on the FPGA Cloud: Fingerprinting Co-Located Cloud FPGA Accelerators via Measuring Communication Links**  
*Chongzhou Fang, Ning Miao, Han Wang, Jiacheng Zhou, Tyler Sheaves, John M Emmert, Avesta Sasan, Houman Homayoun*  
 ACM Conference on Computer and Communications Security (CCS) 2023.
7. **Side Channel-Assisted Inference Attacks on Machine Learning-Based ECG Classification**  
*Jialin Liu, Houman Homayoun, Chongzhou Fang, Ning Miao, Han Wang*  
 IEEE/ACM International Conference on Computer Aided Design (ICCAD) 2023.
8. **Adversarial Attacks Against Machine Learning-Based Resource Provisioning Systems**  
*Najmeh Nazari, Hosein Mohammadi Makrani, Chongzhou Fang, Behnam Omid, Setareh Rafatirad, Hossein Sayadi, Khaled N Khasawneh, Houman Homayoun*  
 IEEE Micro, 43(5), 35-44.
9. **HeteroScore: Evaluating and Mitigating Cloud Security Threats Brought by Heterogeneity**  
*Chongzhou Fang, Najmeh Nazari, Behnam Omid, Han Wang, Aditya Puri, Manish Arora, Setareh Rafatirad, Houman Homayoun, Khaled N Khasawneh*  
 Network and Distributed System Security Symposium (NDSS) 2023.
10. **Repttack: Exploiting Cloud Schedulers to Guide Co-Location Attacks**  
*Chongzhou Fang, Han Wang, Najmeh Nazari, Behnam Omid, Avesta Sasan, Khaled N Khasawneh, Setareh Rafatirad, Houman Homayoun*  
 Network and Distributed System Security Symposium (NDSS) 2022.

## Teaching and Mentoring

---

- **ECS 152A: Computer Networks** UC Davis  
*Teaching Assistant* Winter 2022 & Winter 2024  
 – Deliver a 50-min lecture every week and host office hour Q&A sessions.
- **EEC 170: Computer Architecture** UC Davis  
*Teaching Assistant* Fall 2023  
 – Provide lab assignment benchmarks and host office hour Q&A sessions.
- **EEC 172: Embedded Systems** UC Davis  
*Teaching Assistant* Winter 2021 & Spring 2021  
 – Teach lab sessions and hosting office hour Q&A sessions.
- **EEC 193B: Internet of Things Project** UC Davis  
*Teaching Assistant* Spring 2022  
 – Design lab projects and teach lab sessions.
- **EEC 001: Introduction To Electrical And Computer Engineering** UC Davis  
*Teaching Assistant* Fall 2021

- Teach lab sessions and host office hour Q&A sessions.

- **Research Mentorship:**

- Wei Shao, PhD Student at UC Davis, with Prof. Houman Homayoun
- Ning Miao, PhD Student at UC Davis, with Prof. Houman Homayoun
- Jialin Liu, PhD Student at Temple University, with Prof. Han Wang
- Farhad Alemi, MSc Student at UC Davis, with Prof. Houman Homayoun and Prof. Setareh Rafatirad
- Jiacheng Zhou, MSc Student at UC Davis, with Prof. Houman Homayoun
- Jiawei Liu, MSc Student at UC Davis, with Prof. Houman Homayoun
- Wenjun Tu, MSc Student at UC Davis, with Prof. Houman Homayoun
- Shaurya Srivastav, Undergraduate Student at UC Davis, with Prof. Houman Homayoun
- Jinsi Guo, Undergraduate Student at UC Davis, with Prof. Houman Homayoun

## **Presentations**

---

- **Large Language Models for Code Analysis: Do LLMs Really Do Their Job?**  
at Usenix Security Symposium, Philadelphia, PA, Aug. 14, 2024.
- **Gotcha! I Know What You are Doing on the FPGA Cloud: Fingerprinting Co-Located Cloud FPGA Accelerators via Measuring Communication Links**  
at ACM Conference on Computer and Communications Security (CCS), Copenhagen, Denmark, Nov. 28, 2023.
- **HeteroScore: Evaluating and Mitigating Cloud Security Threats Brought by Heterogeneity**  
at Network and Distributed System Security Symposium (NDSS), San Diego, CA, Mar. 2, 2023.
- **Repttack: Exploiting Cloud Schedulers to Guide Co-Location Attacks**  
at Network and Distributed System Security Symposium (NDSS), San Diego, CA, Apr. 26, 2022.

## **Awards and Grants**

---

- ACM CCS Student Travel Grant, 2023.

Grant Writing Experience:

- Google Cloud Research Credits, 2023.
- Fingerprinting FPGA Circuits Using Communication Interfaces, NSF CHEST, 2022.