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, CA, 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

- **System, System Security:** Cloud Security, Side-Channel Attacks, Serverless Computing
- **LLM for System Security**

Industrial Research Experience

- **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.

Publications

[UsenixSecurity'24a] **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.*

[UsenixSecurity'24b] **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.*

[UsenixSecurity'24c] **Fuzzing BusyBox: Leveraging LLM and Crash Reuse for Embedded Bug Unearthing**
Asmita Asmita, Yaroslav Oliinyk, Michael Scott, Ryan Tsang, ***Chongzhou Fang*** *and Houman Homayoun.*

[DAC'24] **Architectural Whispers: Unveiling Machine Learning Models with Frequency Throttling Side-Channel Fingerprinting**

*Najmeh Nazari, **Chongzhou Fang**, Hosein Mohammadi Makrani, Behnam Omidi, Setareh Rafatirad, Avesta Sasan, Hossein Sayadi, Houman Homayoun and Khaled N. Khasawneh*

[ISQED'24] **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 and Houman Homayoun.*

[ISCAS'24] **Securing On-Chip Learning: Navigating Vulnerabilities and Potential Safeguards in Spiking Neural Network Architectures**
*Najmeh Nazari, Kevin Immanuel Gubbi, Banafsheh Saber Latibari, Muhtasim Alam Chowdhury, **Chongzhou Fang**, Avesta Sasan, Setareh Rafatirad, Houman Homayoun and Soheil Salehi.*

[DATE'24] **SpecScope: Automating Discovery of Exploitable Spectre Gadgets on Black-Box Microarchitectures**
*Najmeh Nazari, Behnam Omidi, **Chongzhou Fang**, Hosein Mohammadi Makrani, Setareh Rafatirad, Avesta Sasan, Houman Homayoun and Khaled N. Khasawneh.*

[BIBM'23] **Introducing an Open-Source Python Toolkit for Machine Learning Research in Physiological Signal based Affective Computing**
*Ruijie Fang, Ruoyu Zhang, Elahe Hosseini, **Chongzhou Fang**, Setareh Rafatirad and Houman Homayoun.*

[CCS'23] **Gotcha! I Know What You are Doing on the FPGA Cloud: Fingerprinting Co-Located Cloud FPGA Accelerators via Measuring Communication Links**

(CSAW'24 ARC Tech Impact Award Runner-Up) *__Chongzhou Fang__, Ning Miao, Han Wang, Jiacheng Zhou, Tyler Sheaves, John M Emmert, Avesta Sasan and Houman Homayoun.*

[ICCAD'23] **Side Channel-Assisted Inference Attacks on Machine Learning-Based ECG Classification**
*Jialin Liu, Houman Homayoun, **Chongzhou Fang**, Ning Miao and Han Wang.*

[Ubicomp/ISWC'23 Adj.] **Privee: A Wearable for Real-Time Bladder Monitoring System**
*Ruoyu Zhang, Ruijie Fang, **Chongzhou Fang**, Houman Homayoun and Gozde Goncu Berk.*

[CODES+ISSS'23] **Special Session: Mitigating Side-channel Attacks through Circuit to Application Layer Approaches**
*Nima Kavand, Armin Darjani, Jens Trommer, Giulio Galderisi, Thomas Mikolajick, Nicolai Müller, Amir Moradi, **Chongzhou Fang**, Ning Miao, Han Wang, Sai Manoj Pudukotai Dinakarrao, Houman Homayoun, Benjamin Hettwer, Luca Parrini and Akash Kumar*

[DAC'23] **Don't Cross Me! Cross-Layer System Security**
*Najmeh Nazari, **Chongzhou Fang**, Sai Manoj PD, Houman Homayoun.*

[IEEE Micro] **Adversarial Attacks Against Machine Learning-Based Resource Provisioning Systems**

*Najmeh Nazari, Hosein Mohammadi Makrani, **Chongzhou Fang**, Behnam Omidi, Setareh Rafatirad, Hossein Sayadi, Khaled N. Khasawneh and Houman Homayoun.*

[NDSS'23] **HeteroScore: Evaluating and Mitigating Cloud Security Threats Brought by Heterogeneity**
Chongzhou Fang, *Najmeh Nazari, Behnam Omidi, Han Wang, Aditya Puri, Manish Arora, Setareh Rafatirad, Houman Homayoun and Khaled N. Khasawneh.*

[NDSS'22] **Repttack: Exploiting Cloud Schedulers to Guide Co-Location Attacks**
Chongzhou Fang, *Han Wang, Najmeh Nazari, Behnam Omidi, Avesta Sasan, Khaled N. Khasawneh, Setareh Rafatirad and Houman Homayoun.*

Teaching and Mentoring

- **ECS 152A: Computer Networks (∼180 Students)** UC Davis
  Teaching Assistant *Winter 2022 & 2024*
  - Deliver a 50-min lecture every week and host office hour Q&A sessions.
- **EEC 170: Computer Architecture (∼80 Students)** UC Davis
  Teaching Assistant *Fall 2023 & 2024*
  - Provide lab assignment benchmarks and host office hour Q&A sessions.
- **EEC 172: Embedded Systems (∼90 Students)** UC Davis
  Teaching Assistant *Winter & Spring 2021*
  - Teach lab sessions and hosting office hour Q&A sessions.
- **EEC 193B: Internet of Things Project (∼20 Students)** UC Davis
  Teaching Assistant *Spring 2022*
  - Design lab projects and teach lab sessions.
- **EEC 001: Introduction To Electrical And Computer Engineering (∼280 Students)** UC Davis
  Teaching Assistant *Fall 2021*
  - Teach lab sessions and host office hour Q&A sessions.
- **Graduate Student Mentor Under ECE Mentorship Program**
- **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

  - Aditya Puri, High School Student at Foothill High School (Pleasanton, CA), with Prof. Houman Homayoun and Dr. Manish Arora

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

- CSAW Applied Research Competition Finalist (15 out of 194 submissions) & Technical Impact Award Runner-Up, 2024.
- ACM CCS Student Travel Grant, 2023.

Grant Writing Experience

- *Collaborative Research: Frameworks: Advancing Computer Hardware and Systems' Research Capability, Reproducibility, and Sustainability with the gem5 Simulator Ecosystem*, NSF, 2023.
  - Award Amount: $2.6M
  - Contributed to proposing security support in gem5.
- Google Cloud Research Credits, 2023.
  - Award Amount: $10,000
  - Composed a proposal in utilizing Google Cloud for cloud reserach.
- *Collaborative Research: SaTC: CORE: Medium: Targeted Microarchitectural Attacks and Defenses in Cloud Infrastructure*, NSF, 2022
  - Award Amount: $1.2M
  - Contributed a section regarding cloud co-location attacks.
- *Fingerprinting FPGA Circuits Using Communication Interfaces*, NSF CHEST, 2022.
  - Award Amount: $100,000
  - Composed a proposal in cloud FPGA fingerprinting attack.
- *Hardware Watermark for Edge IoT TinyML Model Protection*, NSF CHEST, 2025.
  - Award Amount: $80,000
  - Composed a proposal in using physical side-channels as watermarks for edge TinyML model protection.