Yicheng Zhang

University of California, Irvine
+1 9492312128
Website: yichez.site
yzhan846@ucr.edu

Education

University of California, Riverside — Riverside, CA
P.h.D in Electrical Engineering, GPA: 4.00/4.00 — 2021.9–Current

- Advisors: Professor Nael Abu-Ghazaleh

University of California, Irvine — Irvine, CA
M.S. in Computer Engineering, GPA: 3.78/4.00 — 2018.9–2021.3

- Advisors: Professor Mohammad Abdullah Al Faruque and Professor Zhou Li
- Thesis: "Stealing Deep Learning Model Secret through Remote FPGA Side-channel Analysis."

Sichuan University — Chengdu, China
B.S. in Electrical Engineering and Automation, GPA: 3.53/4.00 — 2014.9–2018.6

- Thesis: "Fault detection in power transmission system using Machine Learning."

Experience

University of California, Riverside — Riverside, CA
Research Assistant in Secure and Efficient Architectures and Systems (SEAS) Lab — 2021.9–Current

- AR/VR Security, Computer Architecture Support for Security.
- I worked with my advisor Prof. Nael B. Abu-Ghazaleh on research topics including security in AR/VR systems and side-channel attack & defense on computer architecture.

University of California, Irvine — Irvine, CA
Research Assistant in Embedded & Cyber-Physical Systems Lab — 2018.9–2021.3

- Embedded and Cyber-Physical System Security, Computer Microarchitecture.
- I worked with Prof. Mohammad Abdullah Al Faruque on research topics including security in Embedded & Cyber-Physical Systems and side-channel attack & defense.

University of California, Irvine — Irvine, CA
Research Assistant in Data-driven Security and Privacy (DSP) Lab — 2018.9–2021.3

- Machine learning privacy and defense.
- I worked with Prof. Zhou Li on research topics including machine learning privacy attack and GPU security.

University of California, Irvine — Irvine, CA
Teaching Assistant in Department of Electrical Engineering and Computer Science — 2019.12–2021.3

- Assisted course instructors in course website design, grading, and lecturing.

Publications

1. Wei Junyi*, **Yicheng Zhang***, Zhe Zhou, Zhou Li, and Mohammad Abdullah Al Faruque, "Leaky DNN: Stealing Deep-Learning Model Secret with GPU Context-Switching Side-Channel.", *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (**DSN**), Valencia, Spain, June, 2020.*
*__Junyi Wei and Yicheng Zhang are both first author.__

2. **Yicheng Zhang**, Rozhin Yasaei, Hao Chen, Zhou Li and Mohammad Abdullah Al Faruque, "Poster : Stealing Neural Network Structure through Remote FPGA Side-channel Analysis", *In 29th ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (**FPGA**), February, 2021.*

3. **Yicheng Zhang**, Rozhin Yasaei, Hao Chen, Zhou Li and Mohammad Abdullah Al Faruque, "Stealing Neural Network Structure through Remote FPGA Side-channel Analysis", *In IEEE Transactions on Information Forensics and Security (**TIFS**), August, 2021.*

4. **Yicheng Zhang**, Jiasi Chen, Nael B. Abu-Ghazaleh, "It's all in your head(set): side-channel attacks on augmented reality systems", *To appear in **USENIX Security Symposium**, August, 2023.*

Teaching

- **Teaching Assistant** at University of California, Irvine — Winter 2019
  EECS 150 Continuous-Time Signals and Systems
- **Teaching Assistant** at University of California, Irvine — Spring 2020
  EECS 111 Sytem Software
- **Teaching Assistant** at University of California, Irvine — Fall 2020
  EECS 40 Object Oriented System Programming
- **Teaching Assistant** at University of California, Irvine — Winter 2021
  CS 125 Next Generation Search Systems
- **Teaching Assistant** at University of California, Irvine — Spring 2021
  EECS 112 Organization of Digital Computers

Computer Skills

- **Programming:** C/C++, CUDA C, Python, Verilog, Bash Script(Linux), Java
- **Assembly:** MIPS, 8051
- **CAD Tools:** Altera Quartus, Xilinx ISE, Vivado, Vivado HLS, Xilinx SDK
- **Softwares:** Matlab and Simulink, Arduino

Languages

- **English:** Fluent
  - **EXAM:** Score 102 for TOEFL iBT test
- **Chinese:** Native

Scholarships and Awards

- Student Travel Grant for ACM Conference on Computer and Communications Security — 2021
- Student Travel Grant for USENIX Security Symposium — 2021
- Student Travel Grant for IEEE Symposium on Security and Privacy — 2021,2022
- Dean's Distinguished Fellowship Award (UC Riverside) — 2021
- Sichuan University Scholarship (China) — 2014,2015,2016,2017
- Outstanding Students Leader of Sichuan University — 2016.10

Extracurricular Activities

- Member at University of California Irvine Cycling Club — 2018–Current
- Member at Chinese Students Scholars Association at UCI (UCI-CSSA) — 2018–Current
- Head of Practice Department of Sichuan University Cycling Club — 2014–2018
- Volunteers at 120th Anniversary of Sichuan University — 2016.9