Yicheng Zhang

University of California, Riverside
+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: Prof. Nael Abu-Ghazaleh

University of California, Irvine — Irvine, CA
M.S. in Computer Engineering, GPA: 3.78/4.00 — 2018.9–2021.6

- 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"

Professional 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
Teaching Assistant in Department of Electrical Engineering and Computer Science — 2018.9–2021.6

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

Peer-reviewed Publications

1. **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.*

2. **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.*

3. **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.*

4. 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.__

Teaching Experience

Teaching Assistant at University of California, Irvine — Spring 2021
Organization of Digital Computers (EECS112)

Teaching Assistant at University of California, Irvine — Winter 2021
Next Generation Search Systems (CS125)

Teaching Assistant at University of California, Irvine — Fall 2020
Object Oriented System & Programming (EECS40)

Teaching Assistant at University of California, Irvine — Spring 2020
Sytem Software (EECS111)

Teaching Assistant at University of California, Irvine — Winter 2019
Continuous-Time Signals and Systems (EECS150)

Presentations & Talks

1. "Poster: Stealing Neural Network Structure through Remote FPGA Side-channel Analysis" at FPGA'21, virtual, February 2021
2. "Leaky DNN: Stealing Deep-Learning Model Secret with GPU Context-Switching Side-Channel" at DSN'20, virtual, June 2020

Skills

- **Programming:** C/C++, Python, Java, Verilog/System Verilog, TensorFlow, PyTorch, Numpy, Assembly
- **Tools:** Altera Quartus, Xilinx Vivado/ISE, Vivado HLS, Jupyter Notebook
- **Softwares:** Matlab, Arduino, Unity, Unreal Engine

Professional Service

- Reviewer for ICPS' 20, CYBER' 21, CYBER' 22

Mentoring Experience

Undergraduate Students

Cheng Gu — UCR CSE, 2022-

Selected Honors & 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

Outreach Activities

- **Mentor** at UCR Graduate Student Mentorship Program — –2022-2023
- **Chair** of Practice Department of Sichuan University Cycling Club — 2015-2016
- **Volunteers** at 120th Anniversary of Sichuan University — 2016.9