

Education

- | | |
|--|---------------------------------|
| University of California, Riverside
P.h.D in Electrical Engineering, GPA: 4.00/4.00
– Advisors: Prof. Nael Abu-Ghazaleh | Riverside, CA
2021.9–Current |
| University of California, Irvine
M.S. in Computer Engineering, GPA: 3.78/4.00
– Thesis: “Stealing Deep Learning Model Secret through Remote FPGA Side-channel Analysis” | Irvine, CA
2018.9–2021.6 |
| Sichuan University
B.S. in Electrical Engineering and Automation, GPA: 3.53/4.00
– Thesis: “Fault detection in power transmission system using Machine Learning” | Chengdu, China
2014.9–2018.6 |

Professional Experience

- | | |
|---|---------------------------------|
| University of California, Riverside
Research Assistant in Secure and Efficient Architectures and Systems (SEAS) Lab
– 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 | Riverside, CA
2021.9–Current |
| University of California, Irvine
Teaching Assistant in Department of Electrical Engineering and Computer Science
– Assisted course instructors in course website design, grading, and lecturing | Irvine, CA
2018.9–2021.6 |

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
Organization of Digital Computers (EECS112) Spring 2021
- **Teaching Assistant** at University of California, Irvine
Next Generation Search Systems (CS125) Winter 2021
- **Teaching Assistant** at University of California, Irvine
Object Oriented System & Programming (EECS40) Fall 2020
- **Teaching Assistant** at University of California, Irvine
System Software (EECS111) Spring 2020
- **Teaching Assistant** at University of California, Irvine
Continuous-Time Signals and Systems (EECS150) Winter 2019

Presentations & Talks

- “Poster: Stealing Neural Network Structure through Remote FPGA Side-channel Analysis” at FPGA’21, virtual, February 2021
- “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, IEEE TIFS

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

Extracurricular Activities

- Member at University of California Irvine Cycling Club 2018–2021
- Member at Chinese Students & Scholars Association at UCI (UCI-CSSA) 2018–2021
- Head of Practice Department of Sichuan University Cycling Club 2014–2016
- Volunteers at 120th Anniversary of Sichuan University 2016.9