

## EDUCATION

---

- University of California, Irvine** Irvine, CA  
Ph.D./M.S. in Computer Engineering, Advisors: Mohammad Abdullah Al Faruque and Zhou Li 2018.9–Current
- Sichuan University** Chengdu, China  
B.S. in Electrical Engineering and Automation, GPA: 3.56/4.00 2014.9–2018.6  
– Thesis: “Fault detection in power transmission system using Machine Learning”

## EXPERIENCE

---

- University of California, Irvine** Irvine, CA  
Research Assistant in Embedded & Cyber-Physical Systems Lab 2018.9–Current  
– Embedded and Cyber-Physical System Security, Computer Microarchitecture  
– I worked with my advisor 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–Current  
– Machine learning privacy and defense  
– I worked with my advisor Prof. Zhou Li on research topics including machine learning privacy attack and hardware security.
- University of California, Irvine** Irvine, CA  
Teaching Assistant in Department of Electrical Engineering and Computer Science 2019.12–2020.6  
– I assisted the course instructors in course website design, grading, and lecturing.
- University of California, San Diego** San Diego, CA  
Visiting undergraduate researcher in Adaptive Computing and Embedded Systems (ACES) Lab 2017.9–2017.12  
– PUFs security  
– I worked with my advisor Prof. Farinaz Koushanfar on research topics related to security of PUFs.

## 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’2020)*, 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, “Stealing Neural Network Structure through Remote FPGA Side-channel Analysis”, *Submitted to the 29th ACM/SIGDA International Symposium on Field-Programmable Gate Arrays(Accepted as a poster in **FPGA’2021**)*

## TEACHING

---

- **Teaching Assistant** at University of California, Irvine  
*EECS 150 Continuous-Time Signals and Systems* Winter 2019
- **Teaching Assistant** at University of California, Irvine  
*EECS 111 Sytem Software* Spring 2020
- **Teaching Assistant** at University of California, Irvine  
*EECS 40 Object Oriented System Programming* Fall 2020

## COMPUTER SKILLS

---

- **Programming:** C/C++, CUDA C, Python, Verilog, HLS, 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:** TOEP 5.0
- **Chinese:** Native

## PROJECTS

---

### Machine Learning Model Stealing Attacks on GPU

- Developed a novel GPU side-channel based on context-switching penalties.
- Implementation of LSTM-based inference model to identify the structural secret.
- Extracted the fine-grained structural secret of VGG16/ZFNET/AlexNet/MLP.

### Remote Side-Channel Attack on FPGA to Steal Neural Network Structure

- Developed a novel FPGA power side-channel based attack on a Machine learning models.
- Implementation of VGG16, AlexNet, and MLP models on FPGA accelerator as victim models and a ring oscillator-based circuit to extract power side-channel of victim models.
- Used NearestNeighbors, GradientBoosting, DecisionTree, RandomForest, NeuralNetwork, NaiveBayes, AdaBoost, and XGB classifiers to recover hyper-parameters of victim model from side-channel signals.

## SCHOLARSHIPS AND AWARDS

---

- 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
- Volunteers at HIV Propaganda and Education 2015.10