# 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, 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

- 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...

#### TEACHING

Teaching Assistant at University of California, Irvine
 EECS 150 Continuous-Time Signals and Systems
 Teaching Assistant at University of California, Irvine
 EECS 111 Sytem Software
 Teaching Assistant at University of California, Irvine
 EECS 40 Object Oriented System Programming
 Teaching Assistant at University of California, Irvine
 CS 125 Next Generation Search Systems
 Teaching Assistant at University of California, Irvine
 Spring 2021

# Computer Skills

• **Programming:** C/C++, CUDA C, Python, Verilog, Bash Script(Linux), Java

EECS 112 Organization of Digital Computers

• 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

# 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.

#### Bayesian Memory-Deduplication based Rowhammer Attack on Industrial Control Systems

- Developed a new technique to duplicate the .bss section of the target control DLL file, which requires less memory and time compared to recent works.
- Created a Hardware-in-the-Loop (HIL) testbed with a scaleddown model of a practical engine cooling system of thermo-electric plants as an example of ICS.
- Used the Beremiz softPLC to create the automation platform and connect the softPLC to clouds using industry-standard cloud protocols.

# SCHOLARSHIPS AND AWARDS

• Student Travel Grant for 30th USENIX Security Symposium 2021

• Student Travel Grant for 42nd IEEE Symposium on Security and Privacy

2021

• Dean's Distinguished Fellowship Award (UC Riverside)

Outstanding Students Leader of Sichuan University

2014,2015,2016,2017

• Sichuan University Scholarship (China)

2016.10

2021

# 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      |