

## Education

---

### University of California, Riverside

P.h.D in Electrical Engineering, GPA: 3.71/4.00

- 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”
- Thesis Advisor: Prof. Abdullah Al Faruque and Prof. Zhou Li

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”
- Thesis Advisor: Prof. Yang Liu

Chengdu, China

2014.9–2018.6

## Professional Experience

---

### University of California, Riverside

Research Assistant in Secure and Efficient Architectures and Systems (SEAS) Lab

- Mentor: Prof. Nael B. Abu-Ghazaleh
- Topic: AR/VR Security, Computer Architecture Support for Security

Riverside, CA

2021.9–Current

### Pacific Northwest National Laboratory

Research Intern at the Center for Advanced Technology Evaluation (CENATE)

- Mentors: Dr. Kevin J. Barker, Dr. Andres Marquez, and Dr. Sankha Baran Dutta
- Topic: Microarchitecture Security in Multi-GPU Systems

Richland, WA

2023.6–2023.9

### University of California, Riverside

Graduate Student Mentor in UCR Graduate Student Mentorship Program (GMSP)

- Mentor: Prof. Philip Brisk
- I worked with Prof. Philip Brisk to help first-year graduate students transition from undergraduate programs or careers into graduate study

Riverside, CA

2022.9–2023.6

### 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

---

### Conference Papers

1. **Yicheng Zhang**, Dhroov Pandey, Di Wu, Turja Kundu, Ruopu Li and Tong Shu, “Accuracy-Constrained Throughput Optimization and Performance Profiling of CNN Inference for Detecting Drainage Crossing Locations”, *In Workshop on Software and Hardware Co-design of Deep Learning Systems on Accelerators (SHDA Workshop 2023 co-located with SC’ 23)*, Denver, CO, USA, November 2023.

2. Carter Slocum\*, **Yicheng Zhang**\*, Erfan Shayegani, Pedram Zaree, Nael B. Abu-Ghazaleh, and Jiasi Chen, “That Doesn’t Go There: Attacks on Shared State in Multi-User Augmented Reality Applications”, *In Proceedings of the 33rd USENIX Security Symposium (Under review), Philadelphia, PA, USA, August 2024.*  
\***Equal contribution.**
3. Carter Slocum, **Yicheng Zhang**, Jiasi Chen, and Nael B. Abu-Ghazaleh, “Going through the motions: AR/VR keylogging from user head motions”, *In Proceedings of the 32nd USENIX Security Symposium (USENIX Security), Anaheim, CA, USA, August 2023.*
4. **Yicheng Zhang**, Carter Slocum, Jiasi Chen, and Nael B. Abu-Ghazaleh, “It’s all in your head(set): side-channel attacks on augmented reality systems”, *In Proceedings of the 32nd USENIX Security Symposium (USENIX Security), Anaheim, CA, USA, August 2023.*
5. 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”, *In 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Valencia, Spain, June, 2020.*  
\***Equal contribution.**

## Journal Articles

1. **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.*

## Posters

1. **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.*

## Teaching Experience

---

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

## Presentations and Talks

---

1. “It’s all in your head(set): side-channel attacks on augmented reality systems” at USENIX Security’23, Anaheim, CA, USA, August, 2023
2. “Poster: Stealing Neural Network Structure through Remote FPGA Side-channel Analysis” at FPGA’21, virtual, February 2021
3. “Leaky DNN: Stealing Deep-Learning Model Secret with GPU Context-Switching Side-Channel” at DSN’20, virtual, June 2020

## Skills

---

- **Programming:** C/C++, CUDA C++, C#, Python, Java, Verilog, TensorFlow, PyTorch, Linux (Bash), Assembly
- **Tools:** Altera Quartus, Xilinx Vivado/ISE, Vivado HLS, Jupyter Notebook
- **Softwares:** Matlab, Arduino, Unity, Unreal Engine, Android Studio

## Professional Service

---

- Program Committee: EISA' 23
- Reviewer for Conference: ICPS' 20, CYBER' 21, CYBER' 22, ARES' 23, EAI SecureComm' 23
- Reviewer for Journal: JCS, IEEE TIFS, IEEE TC, IJACT, SCN, JSA
- Artifact Evaluation: Micro' 22

## Research Projects

---

### AR/VR typing inference using head motion tracking

- Developed a system, **TyPose**, that automatically infers words and characters typed by a user, including a Segmenter to divide a stream of sensor readings into the corresponding words/characters and a Classifier to infer the text corresponding to those segments.
- Collected user traces of AR/VR typing behavior and evaluated our attack on these traces. The results show that **TyPose** can detect segments and identify words with high accuracy.
- The related paper was accepted in Usenix Security 2023.

### Side-channel attacks on Mixed Reality systems via Rendering Performance Counters

- Presented a taxonomy of the potential targets and leakage sources of software-based side-channel attacks on AR/VR devices and applications.
- Demonstrated five end-to-end side-channel attacks that illustrate three types of targets: Inferring (1) user interactions (hand gesture inputs, voice commands, and virtual keyboard inputs); (2) information about concurrent applications (fingerprinting newly launched applications); and (3) information about the environment (detecting and ranging a person in the environment).
- The related paper was accepted by Usenix Security 2023 (First author).

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

- Developed a novel FPGA power side-channel-based attack on Machine learning models.
- Used NearestNeighbors, GradientBoosting, DecisionTree, RandomForest, NeuralNetwork, NaiveBayes, AdaBoost, and XGB classifiers to recover hyper-parameters of victim model from side-channel signals.
- The related paper was accepted by FPGA 2021 and IEEE TIFS (First author).

### Machine Learning Model Stealing Attacks via GPU Context-Switching Side-Channel

- Developed a novel GPU side-channel based on context-switching penalties.
- Implementation of LSTM-based inference model to identify the structural secret of VGG16, ZFNET, AlexNet and MLP.
- The related paper was accepted by IEEE DSN 2020 (First author).

## Academic Supervision and Mentorship

---

### Undergraduate Students

- |                           |                          |
|---------------------------|--------------------------|
| • Clarity Shimoniak       | UCR CSE, 2023–Current    |
| • Cheng Gu                | UCR CSE, 2022–Current    |
| • Xuchang Zhan            | UCI EECS, 2019-2020      |
| • Kendus Tisdale-Jeffries | Alabama A&M, 2019 summer |

## Graduate Students

- Sriraksha Srirangapatna Arun
- Yuxin Qiu
- Ziyang Men

UCR CSE, 2023–Current  
UCR CSE, 2022–2023  
UCR CSE, 2022–2023

## Media Coverage

---

### Side-channel attacks on AR/VR systems

- Reported by [UCR News](#), [ZME Science](#), [Tech Xplore](#), [Analytics Insight](#), [Gillett News](#), [Fagen Wasanni](#), [Analytics Insight](#), [Game Is Hard](#), [Knowridge](#), [Inside](#), 2023

## Honors and Awards

---

- Student Travel Grant for DL-GPU Workshop 2023
- International Peer Educator Training Program Certification (IPTPC) Level 1 2023
- UCR GSA Conference Travel Grant 2023
- Student Travel Grant for gem5 Boot Camp 2022
- Student Travel Grant for IEEE Symposium on Security and Privacy 2021,2022
- Student Travel Grant for ACM Conference on Computer and Communications Security 2021
- Student Travel Grant for USENIX Security Symposium 2021
- Dean's Distinguished Fellowship Award (UC Riverside) 2021
- Sichuan University Scholarship (China) 2014–2018

## Membership

---

IEEE Student Member, ACM Student Member.

## Volunteering, Diversity & Inclusion

---

- **Mentor** at UCR Graduate Student Mentorship Program (GSMP) 2022-2023
- **Mentor** at UCR International Student Peer Mentor Program (ISPMP) 2022-2023
- **Mentor** domestic and international undergraduate students in UCI 2019-2020
- **Volunteer** at 120th Anniversary of Sichuan University 2016.9