

# Yicheng Zhang

University of California, Riverside  
+1 9492312128  
Website: [yichez.site](http://yichez.site)  
Email: [yzhan846@ucr.edu](mailto:yzhan846@ucr.edu)

## Education

---

- |  |                                 |
|--|---------------------------------|
| <b>University of California, Riverside</b><br>P.h.D in Electrical Engineering, GPA: 3.71/4.00<br>– Advisor: Prof. Nael Abu-Ghazaleh  | Riverside, CA<br>2021.9–Current |
| <b>University of California, Irvine</b><br>M.S. in Computer Engineering, GPA: 3.78/4.00<br>– Thesis: “Stealing Deep Learning Model Secret through Remote FPGA Side-channel Analysis”<br>– Thesis Advisors: Prof. Abdullah Al Faruque and Prof. Zhou Li | Irvine, CA<br>2018.9–2021.6     |
| <b>Sichuan University</b><br>B.S. in Electrical Engineering and Automation, GPA: 3.53/4.00<br>– Thesis: “Fault detection in power transmission system using Machine Learning”<br>– Thesis Advisor: Prof. Yang Liu                                      | Chengdu, China<br>2014.9–2018.6 |

## Professional Experience

---

- |  |                                 |
|--|---------------------------------|
| <b>University of California, Riverside</b><br>Research Assistant in Secure and Efficient Architectures and Systems (SEAS) Lab<br>– Mentor: Prof. Nael B. Abu-Ghazaleh<br>– Topic: AR/VR Security, Computer Architecture Support for Security   | Riverside, CA<br>2021.9–Current |
| <b>Pacific Northwest National Laboratory</b><br>Research Intern at the Center for Advanced Technology Evaluation (CENATE)<br>– Mentors: Dr. Kevin J. Barker, Dr. Andres Marquez, and Dr. Sankha Baran Dutta<br>– Topic: Microarchitecture Security in Multi-GPU Systems                                  | Richland, WA<br>2023.6–2023.9   |
| <b>University of California, Riverside</b><br>Graduate Student Mentor in UCR Graduate Student Mentorship Program (GMSP)<br>– Mentor: Prof. Philip Brisk<br>– I worked with Prof. Philip Brisk to help first-year graduate students transition from undergraduate programs or careers into graduate study | Riverside, CA<br>2022.9–2023.6  |
| <b>University of California, Irvine</b><br>Teaching Assistant in Department of Electrical Engineering and Computer Science<br>– Assisted course instructors in course website design, grading, and lecturing   | Irvine, CA<br>2018.9–2021.6     |

## Peer-reviewed Publications

---

Full profile on Google Scholar: <https://scholar.google.com/citations?user=X3LwPLAAAAAJ&hl=en>

## Conference Papers

- C1. **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.
- C2. 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.
- C3. 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.
- C4. **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.
- C5. 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

- J1. **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 (IEEE TIFS)*, August, 2021.

## Posters

- P1. **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>System 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

## Service and Professional Activities

---

### Service to Profession - Program Committee

- TPC Member, International Conference on Emerging Information Security and Applications (EISA), 2023.
- TPC Member, International Workshop on Security (IWSEC), 2023.
- TPC Member, International Conference on Cyber-Technologies and Cyber-Systems (CYBER), 2021, 2022, 2023.

### Service to Profession - Conference and Journal Reviewer

- Reviewer, IEEE International Conference on Industrial Cyber-Physical Systems (ICPS), 2020.
- Reviewer, EAI International Conference on Sec. and Pri. in Communication Networks (EAI SecureComm), 2023.
- Reviewer, IEEE Transactions on Information Forensics and Security (IEEE TIFS), 2023.
- Reviewer, Journal of Computer Security (JCS), 2023.
- Reviewer, IEEE Transactions on Computers (IEEE TC), 2023.
- Reviewer, International Journal of Applied Cryptography (IJACT), 2023.
- Reviewer, Security and Communication Networks (SCN), 2023.
- Reviewer, Journal of Systems Architecture (JSA), 2023.

### Other Activities:

- Artifact Evaluation, IEEE/ACM International Symposium on Microarchitecture (MICRO), 2022.
- Student Volunteer, IEEE International Symposium on Secure and Private Exe. Env. Design (SEED), 2024.

## 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** [C3].

### 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) [C4].

### 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 papers were accepted by **FPGA 2021** [P1] (First author) and **IEEE TIFS** [J1] (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 CNN models.
- The related paper was accepted by **IEEE DSN 2020** [C5] (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, Now at VISA
- Kendus Tisdale-Jeffries Alabama A&M, 2019 summer

### Graduate Students

- Sriraksha Srirangapatna Arun UCR CSE, 2023–Current
- Yuxin Qiu UCR CSE, 2022–2023
- Ziyang Men 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

---

- **Volunteer** at IEEE International Symposium on Secure and Private Execution Environment Design (SEED) 2024
- **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