

Yicheng Zhang

Work Authorization: US Permanent Resident

University of California, Riverside

+1 9492312128

🌐 Home Page: yichez.site

✉ Email: yzhan846@ucr.edu

🌐 [linkedin.com/in/yichez16](https://www.linkedin.com/in/yichez16)

🌐 [Google Scholar](https://scholar.google.com/)

Education

University of California, Riverside

P.h.D candidate in Electrical Engineering

– Advisor: Prof. Nael Abu-Ghazaleh

Riverside, CA

09/2021 - 12/2025 (expected)

University of California, Irvine

M.S. in Computer Engineering

– Thesis: “Stealing Deep Learning Model Secret through Remote FPGA Side-channel Analysis”

– Thesis Advisors: Prof. Mohammad Abdullah Al Faruque and Prof. Zhou Li

Irvine, CA

09/2018 - 06/2021

Sichuan University

B.S. in Electrical Engineering and Automation

Chengdu, China

09/2014 - 06/2018

Professional Experience

University of California, Riverside

Associate Instructor at the Department of Computer Science and Engineering (CSE)

– Lead lecturer for the upper-division undergraduate course CS 153 – Design of Operating Systems

– Excellent student reviews: 4.55/5.00 (30 students)

Riverside, CA

06/2024 - 09/2024

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

06/2023 - 09/2023

University of California, Riverside

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

– Mentor: Prof. Philip Brisk

– Working with Prof. Philip Brisk to guide first-year graduate students in transitioning to graduate study.

Riverside, CA

09/2022 - 06/2023

University of California, Irvine

Teaching Assistant in Department of Electrical Engineering and Computer Science

– Teaching assistant for various undergraduate courses (5 semesters)

Irvine, CA

09/2018 - 06/2021

Peer-reviewed Publications

- My research interest lies in **Hardware Security, AR/VR, Side-channel Attacks, GPU Security, Rowhammer Attacks, and Machine Learning Security.**

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

- **10** peer-reviewed papers (6 papers as the 1st author), 2 papers in submission, **5** talks, **1** poster, **8** media coverages, **10** mentored students.
- Major publications: USENIX Security (4), IEEE S&P, IEEE TIFS, IEEE DSN, IEEE SEED, FPGA, ISMAR, SC.
- Students advised at UCR are marked with “#”. Co-first-authors are marked with “*”.

Conference Papers

- C7. Cheng Gu#, **Yicheng Zhang**, and Nael B. Abu-Ghazaleh, “I know What You Sync: Covert and Side Channel Attacks on File Systems via syncfs”, *In 46th IEEE Symposium on Security and Privacy (IEEE S&P)*, San Francisco, USA, May 2025.
- C6. Ravan Nazaraliyev#, **Yicheng Zhang**, Sankha Baran Dutta, Andres Marquez, Kevin Barker, and Nael Abu-Ghazaleh, “Not so Refreshing: Attacking GPUs using RFM Rowhammer Mitigation”, *In Proceedings of the 34th USENIX Security Symposium (USENIX Security)*, Seattle, USA, August 2025.
- C5. **Yicheng Zhang**, Ravan Nazaraliyev, Sankha Baran Dutta, Nael Abu-Ghazaleh, Andres Marquez and Kevin Barker, “Beyond the Bridge: Contention-Based Covert and Side Channel Attacks on Multi-GPU Interconnect”, *In Proceedings of the 2024 IEEE International Symposium on Secure and Private Execution Environment Design (SEED)*, Orlando, FL, USA, January 2024.
- C4. 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 (USENIX Security)*, Philadelphia, PA, USA, August 2024.
- C3. Carter Slocum, **Yicheng Zhang**, Jiasi Chen, and Nael B. Abu-Ghazaleh, “Going through the motions: AR/VR key-logging from user head motions”, *In Proceedings of the 32nd USENIX Security Symposium (USENIX Security)*, Anaheim, CA, USA, August 2023.
- C2. **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.
- C1. 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.

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.

Workshop Papers

- W2. Jiasi Chen, Carter Slocum, **Yicheng Zhang**, Erfan Shayegani, Pedram Zaree, and Nael B. Abu-Ghazaleh, “Securing Shared State in Multi-User Augmented Reality”, *In Proceedings of the 2024 IEEE International Symposium on Mixed and Augmented Reality Workshop (ISMAR’24 Workshop)*, Seattle, WA, USA, October 2024.
- W1. **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 Proceedings of the SC’23 Workshops of The International Conference on High Performance Computing, Network, Storage, and Analysis (SC’23 Workshop)*, Denver, CO, USA, November 2023.

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.

arXiv (In submission)

- A2. Zijian Huang, **Yicheng Zhang**, Sophie Chen, Nael Abu-Ghazaleh, and Jiasi Chen, “Siren Song: Manipulating Pose Estimation in XR Headsets Using Acoustic Attacks”, *arXiv, January 2025, Under review in In Proceedings of the 34th USENIX Security Symposium (USENIX Security)*, Seattle, USA, August 2025).
- A1. **Yicheng Zhang**, Ravan Nazaraliyev, Sankha Baran Dutta, Nael Abu-Ghazaleh, Andres Marquez, and Kevin Barker, “NVBleed: Covert and Side Channel Attacks on NVIDIA Multi-GPU Interconnect”, *arXiv, January 2025, Under review in 2025 International Symposium on Computer Architecture (ISCA)*

Teaching Experience

Associate Instructor at University of California, Riverside <i>Design of Operating Systems (CS 153)</i>	Summer 2024
<ul style="list-style-type: none">– Lead lecturer for the upper-division undergraduate course CS 153 – Design of Operating Systems– Excellent student reviews: 4.55/5.00 (30 students)	
Teaching Assistant at University of California, Irvine <i>Organization of Digital Computers (EECS 112)</i>	Spring 2021
Teaching Assistant at University of California, Irvine <i>Next Generation Search Systems (CS 125)</i>	Winter 2021
Teaching Assistant at University of California, Irvine <i>Object Oriented System & Programming (EECS 40)</i>	Fall 2020
Teaching Assistant at University of California, Irvine <i>System Software (EECS 111)</i>	Spring 2020
Teaching Assistant at University of California, Irvine <i>Continuous-Time Signals and Systems (EECS 150)</i>	Winter 2019

Presentations and Talks

1. “Beyond the Bridge: Contention-Based Covert and Side Channel Attacks on Multi-GPU Interconnect” at IEEE SEED 2024, Orlando, Florida, USA, May, 2024
2. “Accuracy-Constrained Efficiency Optimization and GPU Profiling of CNN Inference for Detecting Drainage Crossing Locations” at SC’23 Workshop, Denver, CO, USA, November, 2023
3. “It’s all in your head(set): side-channel attacks on augmented reality systems” at USENIX Security’23, Anaheim, CA, USA, August, 2023
4. “Poster: Stealing Neural Network Structure through Remote FPGA Side-channel Analysis” at FPGA’21, virtual, February 2021
5. “Leaky DNN: Stealing Deep-Learning Model Secret with GPU Context-Switching Side-Channel” at DSN’20, virtual, June 2020

Skills and Selected Courses

- **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
- **Selected Courses:** Autonomous Cyber-Physical Systems (A+), GPU Architecture & Parallel Programming (A), Advanced Operating Systems (A), Pattern Recognition (A), Advanced Computer Vision (A), Advanced System Security (A), Machine Learning & Artificial Intelligence (A)

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.
- TPC Member, International Conference on Edge Comp. and IoT: Sys., Mana. and Sec. (EAI ICECI), 2024.

Service to Profession - Conference and Journal Reviewer (Reviewed over 40 submissions)

- Reviewer, Journal of Network and Computer Applications (JNCA), 2024.
- Reviewer, IEEE Journal on Selected Areas in Communications (JSAC), 2024.
- Reviewer, Journal of Systems Architecture (JSA), 2023-2024.
- Reviewer, Security and Communication Networks (SCN), 2023-2024.
- Reviewer, Journal of Computer Security (JCS), 2023-2024.
- Reviewer, International Journal of Advanced Computer Technology (IJACT), 2023-2024.
- Reviewer, International Conference on Electrical, Computer and Energy Technologies (ICECET), 2024.
- Reviewer, EURASIP Journal on Information Security (EURASIP JINS), 2023-2024.
- 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, IEEE Transactions on Computers (IEEE TC), 2023.
- Reviewer, International Journal of Applied Cryptography (IJACT), 2023.
- Reviewer, International Conference on Cyber-Technologies and Cyber-Systems (CYBER), 2021-2023.
- Reviewer, IEEE International Conference on Industrial Cyber-Physical Systems (ICPS), 2020.

Other Activities:

- Student Volunteer, International Conference on Arch. Supp. for Prog. Lang. and Op. Sys. (ASPLOS), 2024.
- Student Volunteer, IEEE International Symposium on Secure and Private Exe. Env. Design (SEED), 2024.
- Artifact Evaluation, IEEE/ACM International Symposium on Microarchitecture (MICRO), 2022.

Academic Supervision and Mentorship

Undergraduate Students

- Cheng Gu UCR CSE, 2022–Current, related paper: [C7], incoming PhD at University of Rochester
- Gabriel Haresco UCR CSE, 2023–2024
- Clarity Shimoniak UCR CSE, 2023–2024
- Xuchang Zhan UCI EECS, 2019-2020, Now at VISA
- Kendus Tisdale-Jeffries Alabama A&M, 2019 Summer, Now at NextEra Energy

Graduate Students

- Ravan Nazaraliyev
- Sriraksha Srirangapatna Arun
- Yuxin Qiu
- Ziyang Men
- Ziliang Zhang

UCR CSE, 2023–Current, related paper: [A1, C6, C5]
 UCR CSE, 2023 Spring, Now at Intel
 UCR CSE, 2022–2023
 UCR CSE, 2022–2023
 UCR ECE, 2022–2023

Media Coverage

Side channel attacks on AR/VR headset via rendering performance counters

- Reported by [UCR News](#), [ZME Science](#), [Tech Xplore](#), [Analytics Insight](#), [Gillett News](#) , 2023

VR keylogging from user head motions

- Reported by [UCR 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, 2024
- 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

- **Challenge Course Judge** at Inland Empire Regional Seaperch Competition 2024
- **Volunteer** at ACM ASPLOS 2024 2024
- **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

List of References

- **Prof. Nael B. Abu-Ghazaleh**
Professor, Computer Science & Engineering
University of California, Riverside
Email: naelag@ucr.edu
Phone: (951) 827-2347
- **Prof. Mohammad Al Faruque**
Professor, Electrical Engineering and Computer Science
University of California, Irvine
Email: alfaruqu@uci.edu
Phone: (949) 824-1909
- **Prof. Philip Brisk**
Professor, Computer Science & Engineering Dept
University of California, Riverside
Email: philip.brisk@ucr.edu
Phone: (951) 827-5639
- **Prof. Jiasi Chen**
Associate Professor, Electrical Engineering and Computer Science
University of Michigan, Ann Arbor
Email: jiasi@umich.edu
Phone: (951) 827-5815
- **Prof. Zhou Li**
Assistant Professor, Electrical Engineering and Computer Science
University of California, Irvine
Email: zhou.li@uci.edu
Phone: (949) 824-9724
- **Prof. Rozhin Yasaei**
Assistant Professor, College of Applied Science and Technology
The University of Arizona
Email: yasaei@arizona.edu
Phone: (949) 537-6396
- **Dr. Kevin J. Barker**
Group Leader, High-Performance Computing Group
Pacific Northwest National Laboratory (PNNL)
Email: kevin.barker@pnnl.gov
Phone: (509) 375-6743
- **Dr. Andres Marquez**
Senior Computer Scientist, High-Performance Computing Group
Pacific Northwest National Laboratory (PNNL)
Email: andres.marquez@pnnl.gov
Phone: (509) 372-4457