

# YICHENG ZHANG

✉ [yzhan846@ucr.edu](mailto:yzhan846@ucr.edu) [/Linkedin](#) [/Github](#) [/Personal Page](#)

## EDUCATION

**Ph.D in Electrical Engineering** | University of California, Riverside 09/2021 - present  
**M.S. in Computer Engineering** | University of California, Irvine 09/2018 - 06/2021  
**B.S. in Electrical Engineering and Automation** | Sichuan University 09/2014 - 06/2018

## WORK EXPERIENCE

**Associate Instructor** | University of California, Riverside 06/2024 - 09/2024  
*Lecturing for upper-division undergraduate class CS 153 - Design of Operating Systems*  
**Research Intern** | Pacific Northwest National Laboratory 06/2023 - 09/2023  
*Research on micro-architecture security in multi-GPU systems*

## RESEARCH AREA

**Hardware security; AR/VR Security; Side-channel Attacks; Machine Learning; Computer Architecture**

## TECHNICAL SKILLS

**Programming Languages & Software:** C++, Python, CUDA, TensorFlow, MATLAB, PyTorch, Verilog, Xilinx Vivado, Unity, Unreal Engine

**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)

## SELECTED PROJECTS (FULL PUBLICATION LIST)

**Research Intern** | Pacific Northwest National Laboratory, Richland, WA 06/2023 - 09/2023  
*Covert and Side Channel Attacks on Multi-GPU Systems* ([SEED'24](#), under review in [ASPLOS'25](#))

- Identified a novel contention-based leakages vector on NVIDIA Multi-GPU's NVLink interconnect.
- Performed covert and side-channel attacks on the NVIDIA DGX system and Google Compute Platform.

*Accuracy-Constrained Efficiency Optimization for Detecting Drainage Crossing* ([SC Workshop'23](#))

- Demonstrated the efficacy of resource-aware Neural Architecture Search (NAS) in refining the hyper parameters of SPP-Net, leading to significant enhancements in inference efficiency.
- Performed comprehensive profiling of the drainage crossing detection models on GPU systems, pinpointing the performance bottlenecks unique to single GPU configurations.

**Research Assistant** | University of California, Riverside, Riverside, CA 09/2021 - present  
*Shared State Attacks in Multi-User Augmented Reality Applications* ([Usenix Security'24](#))

- Demonstrated a series of innovative and robust attacks on multiple AR frameworks with shared states, focusing on three publicly accessible frameworks from Meta and Google.
- Proposed several potential mitigation strategies that help enhance the security of multi-user AR applications.

*AR/VR typing inference using head motion tracking* ([Usenix Security'23](#))

- Developed a system named **TyPose** that autonomously deduces words and characters typed by users from their head motion sensor data.
- Collected tens of user traces depicting AR/VR typing behavior and conducted a thorough evaluation of our attack on these traces, achieving a high level of accuracy.

*Side-channel attacks on AR/VR systems via Rendering Performance Counters* ([Usenix Security'23](#))

- Introduced a taxonomy outlining potential targets and sources of leakage for software-based side-channel attacks on AR/VR systems.
- Demonstrated five end-to-end side-channel attacks across three distinct AR/VR-specific attack scenarios, achieving a high degree of accuracy.

**Research Assistant** | University of California, Irvine, Irvine, CA 08/2018 - 06/2021  
*Remote Side-Channel Attack on FPGA to Steal Neural Network Structure* ([IEEE TIFS'21](#), [FPGA'21](#))

- Developed a novel FPGA power side-channel-based attack on Machine learning models.
- Employed a range of classifiers including Nearest Neighbors, Gradient Boosting, Decision Tree, RandomForest, Neural Network, Naive Bayes, AdaBoost, and XGBoost to effectively recover hyper-parameters of the victim model from side-channel leakages.

#### *Model Stealing Attacks via GPU Context-Switching Side-Channel* ([DSN'20](#))

- 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.

## PRESENTATIONS AND TALKS

---

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

## 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

#### *AR/VR keylogging from user head motions*

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

## TEACHING EXPERIENCE

---

#### *Teaching Assistant at University of California, Irvine*

- |   |             |
|---|-------------|
| • Organization of Digital Computers (EECS112)   | Spring 2021 |
| • Next Generation Search Systems (CS125)        | Winter 2021 |
| • Object Oriented System & Programming (EECS40) | Fall 2020   |
| • System Software (EECS111)                     | Spring 2020 |
| • Continuous-Time Signals and Systems (EECS150) | Winter 2019 |

## ACADEMIC SUPERVISION AND MENTORSHIP

---

- |                    |                                  |
|--------------------|----------------------------------|
| • Gabriel Haresco  | UCR CSE, 2023–Current            |
| • Clarity Shimonik | UCR CSE, 2023–Current            |
| • Cheng Gu         | UCR CSE, 2022–Current            |
| • Xuchang Zhan     | UCI EECS, 2019-2020, Now at VISA |

## HONORS AND AWARDS

---

- |   |           |
|---|-----------|
| • International Peer Educator Training Program Certification (IPTPC) Level 1      | 2023      |
| • 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 |

## VOLUNTEERING, DIVERSITY & INCLUSION

---

- |   |           |
|---|-----------|
| • <b>Challenge Course Judge</b> at Inland Empire Regional Seaperch Competition                                    | 2024      |
| • <b>Volunteer</b> at ACM ASPLOS 2024   | 2024      |
| • <b>Volunteer</b> at IEEE International Symposium on Secure and Private Execution Environment Design (SEED) 2024 |           |
| • <b>Mentor</b> at UCR Graduate Student Mentorship Program (GSMP)   | 2022-2023 |
| • <b>Volunteer</b> at 120th Anniversary of Sichuan University   | 2016.9    |