Ziqi Yuan

College of Computer Science and Technology
Zhejiang University

https://monikerzju.github.io/
yuanzqss@zju.edu.cn
ziqiyuanss@gmail.com

Education

•Zhejiang University *2017-2021*
B.Tech in Computer Science GPA: 3.94/4

•Zhejiang University *2021-2023*
M.S. in Computer Science, advised by Prof. Rui Chang GPA: 89/100

Professional Experience

•ARM EL2 TEE Project *2023-present*
Core Member
- We leverage ARM virtualization extensions to build a flexible and efficient trusted execution environment that protects critical applications against a potentially compromised OS similar to Android Automotive OS.
- Compared with building TEEs for Linux processes, we additionally consider potential attacks from Android system services, IPC integrity, Android package integrity, and the protection of a screen device.
- We are collaborating with a company and aim to **deploy the system** by the end of 2024.
- I have submitted a related paper to a top OS/arch conference as the first author.

•ZJV Project *2021-2022*
Team Leader and Pipeline Designer
- We used **Chisel and Verilog** to build ZJV, a Linux-capable dual-issue RISC-V processor that achieves a Coremark score of 3.03/MHz, and successfully booted Debian Linux on an FPGA.
- We joined the OSCPU Project and completed the fabrication of the processor using the 110nm process from SMIC.
- In 2021, we adapted ZJV to MIPS and won 2nd place in National Student Computer System Capability Challenge.
- In 2022, with the help of ZJV, we emerged as the **champions** of the Chinese Youth IC Technology Contest by defeating a team of several core builders of Xiangshan processor.

Conference Articles

•VDom: Fast and Unlimited Virtual Domains on Multiple Architectures *ASPLOS'23*
***Ziqi Yuan**, Siyu Hong, Rui Chang, Yajin Zhou, Wenbo Shen, Kui Ren*
- VDom is a pure software-based in-process isolation solution that efficiently provides processes with scalable memory domains based on page tables, Intel MPK, and ARM Memory Domains.
- Software used for the prototype implementation: Linux kernel.

•RegVault: Hardware Assisted Selective Data Randomization for Operating System Kernels *DAC'22*
*Jinyan Xu, Haoran Lin, **Ziqi Yuan**, Wenbo Shen, Yajin Zhou, Rui Chang, Lei Wu and Kui Ren*
- RegVault is a hardware-software co-design that enforces the confidentiality and integrity of register-grained data in OS kernels to mitigate data-only attacks.
- Software and hardware used for the prototype implementation: LLVM, Rocketchip.

•Building a Hybrid Randomized Cache Hierarchy for Mitigating Cache Side-Channel Attacks *SEED'21*
*Xingjian Zhang, **Ziqi Yuan**, Rui Chang, Yajin Zhou*
- We apply table-based randomization to L1 caches and computation-based randomization to L2 caches.
- Hardware used for the prototype implementation: ZJV.

Skills and Research Interests

Language Scores: TOEFL 105 (expired), GRE 324/4
Programming Languages: C, **Verilog**, Java, Chisel
Current Direction: expanding my research from security to performance, and from CPU to GPU and FPGA
Areas of Interest: operating system for heterogeneous hardware, hardware-assisted software system design
Research Goals: contributing to emerging areas that may reshape the future, finding new problems by revisiting overlooked old topics

Honors and Awards

•Zhejiang University Scholarship (to those with outstanding all-round performance) *2018, 2020*