

Zheng Yu

zheng.yu@northwestern.edu | github.com | [Homepage](#)

EDUCATION

Northwestern University

Ph.D. Student in Computer Science Department

Sept. 2022 - Present

Shanghai Jiao Tong University

Bachelor of Computer Science in Computer Science, member of ACM Class

Sept. 2018 - June. 2022

RESEARCH EXPERIENCE

Research Intern

Northwestern University, USA

Feb. 2022 – July. 2022

Mentors: Xinyu Xing

- As a research intern at Northwestern University advised by Prof Xinyu Xing.
- Focused on designing next-generation memory corruption protection mechanism.

Student Intern

JD.com, Inc.

June. 2021 – Jan. 2022

JD Security

- As a student intern at the Qiling team on JD.com.
- Focused on microcontroller (MCU) firmware emulation.
- As a core developer of Qiling which is a binary analysis framework.

Research Intern

Southern University of Science and Technology

Feb. 2021 – April. 2021

Mentors: Yinqian Zhang

- As a research intern in SUSTech advised by Prof Yinqian Zhang.
- Focused on the design of remote attestation protocol on distributed TEE systems.
- Develop and improve RISC-V trusted computing platform Keystone-Enclave.

Undergraduate Research Assistant

Sustainable Architectures and Infrastructure Laboratory (SAIL)

July. 2020 – June. 2022

Mentors: Chao Li

- As an undergraduate research assistant in the SAIL lab advised by Prof Chao Li.
- Focused on data center systems and architecture design and cloud computing power management.
- Prof Chao Li's evaluation of me is "He has the potential to become an outstanding graduate student"

TEACHING EXPERIENCE

Student Mentor

Google Summer of Code 2022

Apr. 2022 – Oct. 2022

- As a student mentor of Qiling Improvements projects in GSOC 2022.
- Focused on bridging qiling with other reverse engineering tools (e.g. r2, ghidra).
- Discuss and provide guidance to developers involved in the project.

Teaching Assistant

Shanghai Jiao Tong University

June. 2019 – Sept. 2019

- As a teaching assistant in Programming Design Course (CS151) in SJTU
- Design programming assignments and course projects for students
- Students think I am a helpful and responsible teaching assistant

PUBLICATION

- Lu Zhang; Chao Li; Xinkai Wang; Weiqi Feng; **Zheng Yu**; Quan Chen; Jingwen Leng; Minyi Guo; Pu Yang; Shang Yue. "FIRST: Exploiting the Multi-Dimensional Attributes of Functions for Power-Aware Serverless Computing" IPDPS 2023.
- **Zheng Yu**, KAI JERN LAU, MuChen Su, Anh Quynh NGUYEN. "Reversing MCU with Firmware Emulation" BlackHat Europe 22.

HONORS & AWARDS

5th at Defcon 23 CTF Finals

StrawHat Team

DEFCON

2023

Outstanding graduates

Outstanding Graduate of Shanghai Jiaotong University

SJTU

2022

Zhiyuan Honor Scholarship

Top 2% in SJTU

SJTU

2018, 2019, 2020, 2021

The 35nd China National Olympiad in Informatics

Silver Medal (top 100)

CCF

2017

PROJECTS

Qiling | MCU, Python

[\[Link\]](#)

- Add MCU emulation module to the project, which can emulate MCUs from three top vendors.
- Add support for Cortex-M and RISC-V architectures.
- Support fuzzing test of MCU firmware using afl.

Pymx | Compiler, Python

[\[Link\]](#)

- Pymx is a compiler written in Python3 for compiling a Java-like language.
- Supports compile the source code into rv32im assembly code.
- Implemented many optimization methods, including global value numbering, dead code elimination, and SSA.
- The performance of the assembly code generated by the compiler is better than that generated by gcc with O1.

RV32-CPU | FPGA, Verilog

[\[Link\]](#)

- This project is a RISC-V CPU with Tomasulo algorithm implemented in Verilog HDL,
- The project works fine at 100M on the fpga and it did not show any errors during the experiment.
- Supports many useful features, include out-of-order execution, instruction cache, load buffer, etc.
- All the code of this project is original, not borrowed from any project.

TECHNICAL SKILLS

Languages: Chinese(Native), English(Fluent)

Programming Languages: C, Python, C++, Rust, Javascript, Verilog

Frameworks: Angr, Unicorn, IDA, Qiling, Ghidra

Developer Tools: Git, VSCode, Emacs, Docker, Vivado, Android Studio

Hardware: STM32, Arduino, NXP, FPGA