Weijie Huang

"Way-Jee(-eh) Hwahng"

✉ wh25@iu.edu · ☎ (+1) (346) 504-9503 · @macromogic · in LinkedIn

Education

Indiana University Bloomingon
Bloomington, IN, United States — Jan. 2025 – Present
Ph.D. student in Computer Science
Advisor: Prof. XiaoFeng Wang, Prof. Haixu Tang, Prof. Chenghong Wang

Rice University
Houston, TX, United States — Aug. 2022 – Nov. 2024
Doctoral studies in Computer Science
Advisor: Dr. Nathan Dautenhahn, Prof. Konstantinos Mamouras

Southern University of Science and Technology (SUSTech)
Shenzhen, Guangzhou, China — Sept. 2018 – Jul. 2022
B.Eng. in Computer Science and Engineering
GPA: 3.70/4.00

Research Interests

System security; Trusted execution environment; High-performance Computing; Virtualization; Capability model; Program analysis; Agentic systems; LLM security

Skills

- Languages: C, C++, Rust, Python, Java, Shell, Lua, Go, Assembly (x86, RISC-V)
- Instrumentation & Analysis tools: Intel Pin, LLVM
- AI Infrastructure & Systems: CUDA, PyTorch, NSight, vLLM

Research Projects

High-performance Confidential Oblivious Data Analytics — Jan. 2025 – Present

Designed an efficient oblivious relational analytics framework that utilizes a novel *oblivious late materialization* (OLM) approach to hide access patterns within the confidential GPU HBM. Obtained >1000x speedups over state-of-the-art oblivious databases (Obliviator, USENIX Security '25) on TPC-H SF50. *In submission to USENIX Security '26.*

LLM Censorship and Abliteration — Nov. 2025 – Present

(*In progress*) Investigating direction identification methods for harmfulness detection and refusal in open-source large language models; proposing novel approaches for LLM abliteration to increase refusal rates without harming the overall performance; building benchmarks for relevant works.

Automated LLM-assisted Code Optimization — July 2025 – Present

Produced an open-source LLM agent framework that utilizes *In-context reinforcement learning* with trajectory conditioning and learning-based experience reusing to automatically optimize algorithms. Applied to GPU-oriented algorithms for scientific computing and reached 75–300x speedup against existing implementations. *Preprint available at arXiv; open-sourced at* `https://github.com/annihi1ation/phylo_evolve`.

Intra-process Monitoring and Compartmentalization — Aug. 2022 – Nov. 2024

Designed an inline reference monitor compatible with Intel Pin and LLVM instrumentation to record runtime memory management and accesses. This tool also contains a parser to utilize the DWARF information to transform the *object-encapsulation result (accepted by SPW '23)* to access policies for runtime enforcements.

Trusted Execution Environment on RISC-V — May 2021 – June 2022

Proposed a flexible, software-based TEE architecture on RISC-V with novel memory management for enclaves (*accepted by HASP '21*). This architecture uses the limited standard PMP hardware to support theoretically unlimited number of active enclaves, while related works at date could only support at most 13 with customized hardware primitives.

Publication

*: Co-first authors

- Leyi Zhao*, **Weijie Huang***, Yitong Guo, Jiang Bian, Chenghong Wang, Xuhong Zhang. "*Large Language Model-Powered Evolutionary Code Optimization on a Phylogenetic Tree*". arXiv Preprint, January 2026.
- Fangfei Yang, Bumjin Im, **Weijie Huang**, Kelly Kaoudis, Anjo Vahldiek-Oberwagner, Chia-Che Tsai, and Nathan Dautenhahn. "*Endokernel: A Thread Safe Monitor for Lightweight Subprocess Isolation*". In proceedings of the USENIX Security Symposium (USENIX '24), August, 2024.
- Fangfei Yang, **Weijie Huang**, Kelly Kaoudis, Anjo Vahldiek-Oberwagner, and Nathan Dautenhahn. "*Endoprocess: Programmable and Extensible Subprocess Isolation*". In proceedings of the New Security Paradigms Workshop (NSPW '23), September, 2023.
- Yudi Yang, **Weijie Huang**, Kelly Kaoudis, and Nathan Dautenhahn. "*Whole-Program Privilege and Compartmentalization Analysis with the Object-Encapsulation Model*". In proceedings of the IEEE Security and Privacy Workshops (SPW '23), May, 2023.
- Haonan Li*, **Weijie Huang***, Mingde Ren, Hongyi Lu, Zhenyu Ning, Heming Cui, and Fengwei Zhang. "*A Novel Memory Management for RISC-V Enclaves*". In proceedings of Hardware and Architectural Support for Security and Privacy Workshop (HASP '21), October, 2021.

Work Experience

Teaching Assistant — Aug. 2023 – May 2024; Feb. 2019 – June 2022

Dept. Computer Science Rice University, Houston, TX, US
Dept. Computer Science and Engineering Southern Univeristy of Science and Technology, Shenzhen, China

Responsible for creating/grading assignments and exams, and answering questions in: *Advanced Logic* (Rice), *Graduate Algorithm Design* (Rice), *Intro to Programming* (SUSTech), *Discrete Math* (SUSTech), *C/C++ Programming* (SUSTech).

Summer Intern (Backend) — June 2021 – Aug. 2021

Dept. Data ByteDance Ltd., Shenzhen, China

Responsible for developing and maintaining an automated internal tool that periodically monitors all configuration and runtime statuses across service clusters. This tool is capable of tracking various health and performance indicators of these clusters.

Honors and Awards

Silver Medal, Award on 2019 International Collegiate Programming Contest (ICPC) Asia Regional (Yinchuan Site) Oct. 2019
Bronze Medal, Award on 2019 International Collegiate Programming Contest (ICPC) Asia Regional (Nanjing Site) Oct. 2019
Excellent Undergraduate Student Scholarship, by SUSTech Oct. 2019, Oct. 2020