Yuancheng Jiang

School of Computing, National University of Singapore | yuancheng@comp.nus.edu.sg | +65 8423 4278
https://yuanchengjiang.github.io/

Research Interests

- Intelligent Software Security: Bug Detection via Fuzz Testing; LLM-assisted Vulnerability Discovery
- Software Quality Assessment: Benchmark of Compilers, Database Systems, and Language Models

Education

- **Ph.D. Candidate, Computer Science** *Jan 2022 – Present*
  National University of Singapore (NUS), Singapore
- **Master of Computing** *Aug 2020 – Jan 2022*
  National University of Singapore (NUS), Singapore
- **Bachelor of Science** *Sept 2016 – June 2020*
  Fudan University, Shanghai, China

Publications

- ***Yuancheng Jiang**, Et al.*, **OSS-Bench: Benchmark Generator for Coding LLMs** [preprint], 2025
  Highlights: Paper | Benchmark | Leaderboard
  OSS-Bench takes real open-source software, replaces functions with LLM-generated code, and then checks if that code compiles, tests pass, and is memory-safe. By testing 17 language models, it reveals performance and security using real-world complexities.
- ***Yuancheng Jiang**, Et al.*, **ZendDiff: Differential Testing of PHP Interpreter** [preprint], 2025
  ZendDiff discovers logic bugs in PHP by comparing results between non-JIT and JIT with state probing, program mutation, *etc.*
- ***Yuancheng Jiang**, Et al.*, **FlowFusion: Fuzzing the PHP Interpreter via Dataflow Fusion** [Sec'25][1], 2025
  Highlights: Paper | Fuzzer (becoming official toolchain)) | Bugs (over 300 bug issues)
  FlowFusion is a fully automated fuzzing tool that detects memory errors in the PHP interpreter by generating novel input programs with fused data flows in test cases. It reveals hundreds of bugs in the PHP source code and continues to report them each week.
- ***Yuancheng Jiang**, Et al.*, **ACME: LLM-assisted Clause Mapping for Differential Testing** [preprint], 2024
  ACME leverages LLMs to analyze and generate clause mappings for enhancing differential testing of emerging database engines.
- ***Yuancheng Jiang**, Et al.*, **GraphGenie: Detecting Logic Bugs in Graph Database ..** [ICSE'24][2], 2024
  Highlights: Paper | Code | Slides | Bugs
  GraphGenie is a bug-finding tool for graph database engines that detects logic bugs, performance issues, and internal errors. It uses graph query transformations to generate semantically equivalent or variant queries and compare their results to uncover bugs.
- ***Yuancheng Jiang**, Et al.*, **EVCFI: Extensible Virtual Call Integrity** [ESORICS'22][3], 2022
  EVCFI implements virtual-call checks in just a few instructions, offering greater scalability and flexibility than prior VCFI defenses.
- ***Yuancheng Jiang**, Et al.*, **RecIPE: Revisiting the Evaluation of Memory Error Defenses** [AsiaCCS'22][4], 2022
  RecIPE is an extensible benchmark for revealing each sanitizer's and compiler flag's real-world strengths and weaknesses.
- *Chuqi Zhang, Et al.*, **Erebor: A Drop-In Sandbox Solution for Private Data ..** [EuroSys'25][5], 2025
- *Lambang Akbar, Et al.*, **Evaluating Disassembly Errors With Only Binaries** [AsiaCCS'25][6], 2025
- *Kaihang Ji, Et al.*, **FlowMatrix: GPU-Assisted Information-Flow Analysis ..** [Sec'22][7], 2022

Experience

- Teaching Assistant, CS3213, National University of Singapore, Singapore, 2023 - 2025
- Capture The Flag (CTF), Sixstars, Fudan University, Shanghai, China, 2017 – 2020
- Huawei Summer Internship, Huawei, Shanghai, China, Jun 2019 – Aug 2019
- NUS Summer School, National University of Singapore, Singapore, Jul 2018 – Aug 2018

About Me

- Expertise: Static and Dynamic Program Analysis, Fuzzing Testing, Benchmarking, *etc.*
- Tools: Linux, Git, Docker, Latex, C, C++, Java, JavaScript, PHP, Python, *etc.*
- Speaking languages: Chinese (native), English (proficient)

I enjoy playing various instruments like piano, guitar, and drums. I have completed the ABRSM Music Theory.

[1] The 34th USENIX Security Symposium [2] The 46th International Conference on Software Engineering [3] The 27th European Symposium on Research in Computer Security [4] The 17th ACM ASIA Conference on Computer and Communications Security [5] The 20th ACM European Conference on Computer Systems [6] The 20th ACM ASIA Conference on Computer and Communications Security [7] The 31st USENIX Security Symposium