Jiyuan Wang

wangjiyuan@cs.ucla.edu • http://web.cs.ucla.edu/~wangjiyuan/ • wjy99-c

Education

University of California, Los Angeles — **California, US**
Ph.D. Candidate, Department of Computer Science — *Sep. 2019 – Present*
GPA: 3.74/4.00

Tsinghua University — **Beijing, China**
B.S., Department of Physics — *Aug. 2015 – Jul. 2019*
GPA: 3.63/4.00

University of Zurich — **Zurich, Switzerland**
Exchange student, Department of Physics — *Aug. 2017 – Jan. 2018*
GPA: 5.62/6.00

Research Interest

Testing, Heterogenous Computing, Big Data, Quantum Computing

Research Experience

SOLAR Group — Dept. CS, UCLA
Research Assistant — *Sep. 2019 - Present*
Advisors: **Prof. Miryung Kim and Prof. Harry Xu**

- **Leveraging Hardware Probes and Optimizations for Accelerating Fuzz Testing of Heterogeneous Applications**
  - A novel fuzz testing technique that enables fuzzing on real heterogeneous architectures.
  - We generate test guidance by inserting device-side in-kernel hardware probes and parallelize fuzzing with FPGAs.
  - Our tool is the first to design hardware optimizations to accelerate fuzz testing.
- **HeteroGen: Transpiling C to Heterogeneous HLS Code with Automated Test Generation and Program Repair**
  - A code generation tool takes C/C++ code as input and automatically generates an HLS version with test behavior preservation and better performance.
  - I work on AST transformation for each fix edits, including insert, delete, and move pragma to target location, rewrite pointers, etc.
  - Our tool can produce an HLS-compatible version for nine out of ten real-world heterogeneous applications automatically and produce an HLS version 1.63x faster than the original version.
- **QDiff: Differential Testing for Quantum Software Stacks**
  - A differential testing framework for quantum programming framework.
  - To apply differential testing for quantum, we generate equivalent quantum programs, explore the backends and compiler setting options, and compare the final with K-S test.
  - For Cirq, Pyquil, and Qiskit, we found four new bugs in their simulators and two possible root causes for hardware execution divergence.
  - Selected for the SIGSOFT research highlight!
- **HeteroFuzz: Fuzz Testing to Detect Platform Dependent Divergence for Heterogeneous Applications.**

- A novel fuzz testing tool for heterogeneous applications to detect platform-dependent divergence.
- To reduce the long latency, we design dynamic probabilistic mutations to increase the chance of hitting divergent behavior, and skip the redundant simulator invocation if the input within the seen kernel input value range.
- Our tool is 754X faster in exposing the same set of distinct divergence symptoms than naive fuzzing on seven real-world heterogeneous applications with FPGA kernels.

- **BigFuzz: Efficient Fuzz Testing for Data Analytics Using Framework Abstraction**
  - A novel coverage-guided fuzz testing tool for big data analytics.
  - I perform automated source to source transformation to construct an equivalent big data application suitable for fast test generation.
  - Our tool speeds up the fuzzing time by 78 to 1477X compared to random fuzzing, achieves 33% to 157% improvement in detecting application errors.

Software System Security Asssurance Group Dept. CS, Tsinghua University
Undergraduate Research Assistant *Jan. 2017 - Sept. 2017*
Research Advisor: **Prof. Yu Jiang**

- **QuanFuzz: Fuzz Testing of Quantum Program**
  - A fuzz testing tool for quantum programs focusing on quantum sensitive branches.
  - We regard initial states of the qubits as an input for the quantum program, and achieve mutations by applying specific quantum gates on the initial qubits.

Working Experience

AWS Privacy Engineering Amazon Web Service
Applied Scientist intern *Sep. 2019 - Present*
Advisors: **Dr. Antonio Filleri and Dr. Nico Rosner**

- **Matilda: a debugging tool that facilitates the friction-free generation of test data**
  - Implement a fuzzer to generate test data, with oracles that consider the output statistics of SMT solvers like Z3 and CVC5.
  - Given the statistics, conduct data analysis to pick the most important data that our tool needs to consider.
  - Make matilda works for all input formats instead of only smt2 input format.

Publications

[1] **Jiyuan Wang**, Qian Zhang, Hongbo Rong, Guoqing Harry Xu, Miryung Kim. Leveraging Hardware Probes and Optimizations for Accelerating Fuzz Testing of Heterogeneous Applications. *ESEC/FSE 2023.*
[2] Qian Zhang, **Jiyuan Wang**, Guoqing Harry Xu, Miryung Kim. HeteroGen: Transpiling C to Heterogeneous HLS Code with Automated Test Generation and Program Repair. *ASPLOS 2022.*
[3] **Jiyuan Wang**, Qian Zhang, Miryung Kim, Guoqing Harry Xu. QDiff: Differential Testing of Quantum Software Stacks. *ASE 2021,* **SIGSOFT research highlight.**
[4] Qian Zhang, **Jiyuan Wang**, Miryung Kim. HeteroFuzz: Fuzz Testing to Detect Platform Dependent Divergence for Heterogeneous Applications. *ESEC/FSE 2021.*
[5] **Jiyuan Wang**, Fuchen Ma, Yu Jiang. Poster: Fuzz Testing of Quantum Program. *ICST 2021, Best Poster.*
[6] Qian Zhang, **Jiyuan Wang**, Muhammad Ali Gulzar, Rohan Padhye, Miryung Kim. BigFuzz: Efficient Fuzz Testing for Data Analytics UsingFramework Abstraction. *ASE 2020.*

Skills

- **Programming Languages:** Familiar with Python, Java, C/C++

- **Tools:** America fuzzy loop, Spark