Zu-Ming Jiang

Department of Computer Science, ETH Zurich
https://jzuming.github.io
zuming.jiang@inf.ethz.ch

RESEARCH INTEREST

Reliability and security of systems software including databases and operating systems; my mission is to advance the science and practice of building reliable and secure systems.

EDUCATION

ETH Zurich *Sep. 2021-Jun. 2025 (expected)*
Ph.D. in Computer Science
Advisor: Prof. Zhendong Su

Tsinghua University *Sep. 2018-Jun. 2021*
M.E. in Computer Technology
Advisor: Prof. Shi-Min Hu

Zhejiang University *Sep. 2014-Jun. 2018*
B.E. in Electrical Engineering and Automation
Minor: Advanced Honor Class of Engineering Education (ACEE) in Chu Kochen Honors College

PUBLICATION

First Author

[1] Detecting Logic Bugs in Database Engines via Equivalent Expression Transformation [PDF]
Zu-Ming Jiang, Zhendong Su
In Proceedings of the 18th USENIX Symposium on Operating Systems Design and Implementation (***OSDI***), 2024.

[2] Detecting Transactional Bugs in Database Engines via Graph-Based Oracle Construction [PDF]
Zu-Ming Jiang, Si Liu, Manuel Rigger, Zhendong Su
In Proceedings of the 17th USENIX Symposium on Operating Systems Design and Implementation (***OSDI***), 2023.

[3] DynSQL: Stateful Fuzzing for Database Management Systems with Complex and Valid SQL Query Generation [PDF]
Zu-Ming Jiang, Jia-Ju Bai, Zhendong Su
In Proceedings of the 32nd USENIX Security Symposium (***Security***), 2023.

[4] Context-Sensitive and Directional Concurrency Fuzzing for Data-Race Detection [PDF]
Zu-Ming Jiang, Jia-Ju Bai, Kangjie Lu, Shi-Min Hu
In Proceedings of the 29th Network and Distributed System Security Symposium (***NDSS***), 2022.

[5] Fuzzing Error Handling Code using Context-Sensitive Software Fault Injection [PDF]
Zu-Ming Jiang, Jia-Ju Bai, Kangjie Lu, Shi-Min Hu
In Proceedings of the 29th USENIX Security Symposium (***Security***), 2020.

[6] Fuzzing Error Handling Code in Device Drivers Based on Software Fault Injection [PDF]
Zu-Ming Jiang, Jia-Ju Bai, Julia Lawall, Shi-Min Hu
In Proceedings of the 30th International Symposium on Software Reliability Engineering (***ISSRE***), 2019.

Student Mentoring

[1] Dinkel: Testing Graph Database Engines via State-Aware Query Generation [PDF]
Dominic Wüst*, **Zu-Ming Jiang***, Zhendong Su *(*: Equal Contributions)*
In **arXiv 2024** (This work found **60 bugs** in GDBMSs and is under review for a top-tier venue)

[2] Empowering the Test Oracle for Graph Database Engines: General Cypher Transformations
Dominic Wüst*, **Zu-Ming Jiang***, Zhendong Su *(*: Equal Contributions)*
(This work found **54 bugs** in GDBMSs and is under submission to a top-tier venue)

Collaboration

[1] Blackbox Fuzzing of Distributed Systems with Multi-Dimensional Inputs and Symmetry-Based Feedback Pruning
Yonghao Zou, Jia-Ju Bai, **Zu-Ming Jiang**, Ming Zhao, Diyu Zhou
In Proceedings of the 32nd Network and Distributed System Security Symposium (***NDSS***), 2025.

[2] Testing Error Handling Code with Software Fault Injection and Error-Coverage-Guided Fuzzing [PDF]
Jia-Ju Bai, Zi-Xuan Fu, Kai-Tao Xie, **Zu-Ming Jiang**
In IEEE Transactions on Dependable and Secure Computing (***TDSC***), 2023.

[3] Hybrid Static-Dynamic Analysis of Data Races Caused by Inconsistent Locking Discipline in Device Drivers [PDF]
Jia-Ju Bai, Qiu-Liang Chen, **Zu-Ming Jiang**, Julia Lawall, Shi-Min Hu
In IEEE Transactions on Software Engineering (***TSE***), 2022.

[4] Detecting Data Races Caused by Inconsistent Lock Protection in Device Drivers [PDF]
Qiu-Liang Chen, Jia-Ju Bai, **Zu-Ming Jiang**, Julia Lawall, Shi-Min Hu
In Proceedings of the 26th International Conference on Software Analysis, Evolution and Reengineering (***SANER***), 2019.

RESEARCH IMPACT

Bug Detection for Real-World Database Systems: **276 bugs** (261 confirmed, and 152 fixed)

[OSDI 2024]: 66 bugs (65 confirmed, 37 fixed) in MySQL, PostgreSQL, SQLite, TiDB, and ClickHouse.
[OSDI 2023]: 56 bugs (52 confirmed, 18 fixed) in MySQL, MariaDB, and TiDB.
[USENIX Security 2023]: 40 bugs (38 confirmed, 21 fixed) in MySQL, SQLite, MariaDB, ClickHouse, and MonetDB.
[arXiv 2024]: 60 bugs (58 confirmed, 51 fixed) in Neo4j, RedisGraph, and Apache AGE
[Under Submission]: 54 bugs (48 confirmed, 25 fixed) in Neo4j, FalkorDB, and Memgraph

Bug Detection for Real-World System Software: **147 bugs** (88 confirmed)

[NDSS 2022]: 75 harmful data races (44 confirmed, 19 fixed) in 12 programs (applications and filesystems).
[USENIX Security 2020]: 50 bugs (32 confirmed) in 9 programs.
[ISSRE 2019]: 22 bugs (12 confirmed) in 18 device drivers.

CVE Assignment: **36 CVEs**

MySQL: 22 CVEs, MariaDB:12 CVEs, Vim: 2 CVEs

Open-Source Tools

TxCheck: A fuzzing framework for finding transactional bugs in DBMSs [GitHub]
EET: Automatic DBMS testing tools with a general test oracle [GitHub]

HONORS AND AWARDS

OSDI '23 Student Grant Award, 2023
Outstanding Master's Graduate, Tsinghua University, 2021
Siebel Scholar Class of 2021 ($35k USD), Siebel Scholars Foundation, 2021
Outstanding Bachelor Thesis, Zhejiang University, 2018
Meritorious Winner of Mathematical Contest in Modeling, USA, 2017

ACADEMIC SERVICE

Program Committee Member

(DBTest) International Workshop on Testing Database Systems 2024

Artifact Evaluation Committee (AEC) Member

(OSDI) USENIX Symposium on Operating Systems Design and Implementation 2024, 2023

(ATC) USENIX Annual Technical Conference 2024, 2023

Journal Reviewers

(TOSEM) ACM Transactions on Software Engineering and Methodology 2024, 2023

(TDSC) IEEE Transactions on Dependable and Secure Computing 2022, 2021

INVITED TALKS

NEU 2024, Making Databases Robust and Reliable: from SQL Generation to Test-Oracle Construction
ISCAS 2024, Making Databases Robust and Reliable: from SQL Generation to Test-Oracle Construction
Stanford 2024, Making Databases Robust and Reliable: from SQL Generation to Test-Oracle Construction
UCB 2024, Making Databases Robust and Reliable: from SQL Generation to Test-Oracle Construction
NUS 2024, Detecting Logic Bugs in Database Engines via Equivalent Expression Transformation
Dagstuhl Seminar 2023, Ensuring the Reliability and Robustness of Database Management
HKUST 2023, Bug Detection for Database Systems: Complex-Query Generation and Oracle Construction
CUHK 2023, Bug Detection for Database Systems: Complex-Query Generation and Oracle Construction
PingCAP 2023, Transactional Bugs Detection for Database Systems
Tencent 2022, Fuzzing for Database Systems

TEACHING EXPERIENCE

Compiler Design *2024, 2023, 2022, 2021*
Head Teaching Assistant (2024) and Teaching Assistant (2023, 2022, 2021)

Automated Software Testing *2024, 2023*
Guest Lecturer (2024, 2023) and Teaching Assistant (2024, 2023)

Software Engineering Seminar *2024, 2023, 2022, 2021*
Teaching Assistant

Research Topics in Software Engineering *2024, 2023, 2022*
Teaching Assistant

Data Modelling and Databases *2024*
Teaching Assistant

Computer Science II *2023*
Teaching Assistant