Qingkai Shi

ADDRESS

Department of Computer and Science
Purdue University
305 N. University Street
West Lafayette, IN 47907
Email: shi553@purdue.edu
URL: https://qingkaishi.github.io/
ORCID: 0000-0002-8297-8998

EDUCATION & EMPLOYMENT

Purdue University 2021 - Now
Postdoctoral Research Associate

Hong Kong University of Science and Technology / Sourcebrella Inc. 2015 - 2021
Ph.D. in Computer Science (2020) / Co-founder of Sourcebrella Inc. (2021)
Thesis: Precise and Scalable Static Bug Finding for Industrial-Sized Code

RESEARCH & AWARDS

My research focuses on the use of programming language and compiler techniques, especially static analysis, for rigorously ensuring software security, including static analysis for (1) bug scanning, (2) reverse engineering, and (3) fuzz testing. My research has been extensively published in premium venues and has let me win ACM SIGPLAN Distinguished Paper Award, ACM SIGSOFT Distinguished Paper Award, Google Research Paper Reward, and Hong Kong Ph.D. Fellowship.

My research on bug scanning, known as the *Pinpoint Static Analyzer*, has received 200M CNY ($\approx$ 30M USD) investment. The startup that commercializes my research, Sourcebrella Inc., has been acquired by Ant Group, where *Pinpoint* is deployed in daily operations for improving the quality of Alipay, a popular digital payment app with over a billion monthly active users. To date, we have discovered hundreds of vulnerabilities and CVEs in mature software.

For further information, see https://qingkaishi.github.io/.

REFEREED PUBLICATIONS

My research has been published extensively at premium venues of programming language (PLDI, OOPSLA), software engineering (ICSE, FSE), and cybersecurity (S&P, CCS).

Representative Papers:

1. **Qingkai Shi**, Junyang Shao, Yapeng Ye, Mingwei Zheng, and Xiangyu Zhang. Lifting Network Protocol Implementation to Precise Format Specification with Security Applications. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS'23)*. ACM, 2023.
2. **Qingkai Shi**, Yongchao Wang, Peisen Yao, and Charles Zhang. Indexing the Extended Dyck-CFL Reachability for Context-Sensitive Program Analysis. In *Proceedings of the ACM on Programming Languages (OOPSLA'22)*. ACM, 2022.
3. **Qingkai Shi**, Peisen Yao, Rongxin Wu, and Charles Zhang. Path-Sensitive Sparse Analysis without Path Conditions. In *Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'21)*. ACM, 2021.

4. **Qingkai Shi** and Charles Zhang. Pipelining Bottom-up Data Flow Analysis. In *Proceedings of the ACM/IEEE International Conference on Software Engineering (ICSE'20)*. ACM, 2020.

5. **Qingkai Shi**, Rongxin Wu, Gang Fan, and Charles Zhang. Conquering the Extensional Scalability Problem for Value-Flow Analysis Frameworks. In *Proceedings of the ACM/IEEE International Conference on Software Engineering (ICSE'20)*. ACM, 2020.

6. **Qingkai Shi**, Xiao Xiao, Rongxin Wu, Jinguo Zhou, Gang Fan, and Charles Zhang. Pinpoint: Fast and Precise Sparse Value Flow Analysis for Million Lines of Code. In *Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'18)*. ACM, 2018.

Other Papers:

7. Yapeng Ye, Zhuo Zhang, **Qingkai Shi**, Yousra Aafer, and Xiangyu Zhang. D-ARM: Disassembling ARM Binaries by Lightweight Superset Instruction Interpretation and Graph Modeling. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P'23)*. IEEE, 2023.

8. Xiangzhe Xu, Zhou Xuan, Shiwei Feng, Siyuan Chen, Yapeng Ye, **Qingkai Shi**, Guanhong Tao, Le Yu, Zhuo Zhang, and Xiangyu Zhang. PEM: Representing Binary Program Semantics for Similarity Analysis via A Probabilistic Execution Model In *Proceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE'23)*. ACM, 2023.

9. Xiangzhe Xu, Shiwei Feng, Yapeng Ye, Guangyu Shen, Zian Su, Siyuan Chen, Guanhong Tao, **Qingkai Shi**, Zhuo Zhang, and Xiangyu Zhang. Improving Binary Code Similarity Transformer Models by Semantics-driven Instruction Deemphasis. In *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA'23)*. ACM, 2023.

10. Chengpeng Wang, Wenyang Wang, Peisen Yao, **Qingkai Shi**, Jinguo Zhou, and Charles Zhang. Anchor: Fast and Precise Value-Flow Analysis for Containers via Memory Orientation. In *ACM Transactions on Software Engineering and Methodology (TOSEM'23)*. ACM, 2023.

11. Yuandao Cai, Chengfeng Ye, **Qingkai Shi**, and Charles Zhang. Peahen: Fast and Precise Static Deadlock Detection via Context Reduction. In *Proceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE'22)*. ACM, 2022.

12. Heqing Huang, Yiyuan Guo, **Qingkai Shi**, Peisen Yao, Rongxin Wu, and Charles Zhang. Beacon: Directed Grey-Box Fuzzing with Provable Path Pruning. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P'22)*. IEEE, 2022.
Google Research Paper Reward

13. Chengpeng Wang, Peisen Yao, Wensheng Tang, **Qingkai Shi**, and Charles Zhang. Complexity Guided Container Replacement Synthesis. In *Proceedings of the ACM on Programming Languages (OOPSLA'22)*. ACM, 2022.
ACM SIGPLAN Distinguished Paper Award

14. Yiyuan Guo, Jinguo Zhou, Peisen Yao, **Qingkai Shi**, and Charles Zhang. Precise Divide-By-Zero Detection with Affirmative Evidence. In *Proceedings of the ACM/IEEE International Conference on Software Engineering (ICSE'22)*. ACM, 2022.

15. Peisen Yao, **Qingkai Shi**, Heqing Huang, and Charles Zhang. Program Analysis via Efficient Symbolic Abstraction. In *Proceedings of the ACM on Programming Languages (OOPSLA'21)*. ACM, 2021.

16. Peisen Yao, Heqing Huang, Wensheng Tang, **Qingkai Shi**, Rongxin Wu, and Charles Zhang. Skeletal Approximation Enumeration for SMT Solver Testing. In *Proceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE'21)*. ACM, 2021.

17. Peisen Yao, Heqing Huang, Wensheng Tang, **Qingkai Shi**, Rongxin Wu, and Charles Zhang. Fuzzing SMT Solvers via Two-Dimensional Input Space Exploration. In *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA'21)*. ACM, 2021.

18. Heqing Huang, Peisen Yao, Rongxin Wu, **Qingkai Shi**, and Charles Zhang. Pangolin: Incremental Hybrid Fuzzing with Polyhedral Path Abstraction. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P'20)*. IEEE, 2020.

19. Peisen Yao, **Qingkai Shi**, Heqing Huang, and Charles Zhang. Fast Bit-Vector Satisfiability. In *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA'20)*. ACM, 2020.

20. Yang Feng, **Qingkai Shi**, Xinyu Gao, Jun Wan, Chunrong Fang, and Zhenyu Chen. DeepGini: Prioritizing Massive Tests to Enhance the Robustness of Deep Neural Networks. In *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA'20)*. ACM, 2020.

21. Gang Fan, Chengpeng Wang, Rongxin Wu, Xiao Xiao, **Qingkai Shi**, and Charles Zhang. Escaping Dependency Hell: Finding Build Dependency Errors with the Unified Dependency Graph. In *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA'20)*. ACM, 2020.

22. Chunrong Fang, Zixi Liu, Yangyang Shi, Jeff Huang, and **Qingkai Shi**. Functional Code Clone Detection with Syntax and Semantics Fusion Learning. In *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA'20)*. ACM, 2020.

23. Gang Fan, Rongxin Wu, **Qingkai Shi**, Xiao Xiao, Jinguo Zhou, and Charles Zhang. SMOKE: Scalable Path-Sensitive Memory Leak Detection for Millions of Lines of Code. In *Proceedings of the ACM/IEEE International Conference on Software Engineering (ICSE'19)*. IEEE, 2019.
ACM SIGSOFT Distinguished Paper Award

24. **Qingkai Shi**, Zhenyu Chen, Chunrong Fang, Yang Feng, and Baowen Xu. Measuring the Diversity of a Test Set with Distance Entropy. In *IEEE Transactions on Reliability (TR'16)*. IEEE, 2016.

25. **Qingkai Shi**, Jeff Huang, Zhenyu Chen, and Baowen Xu. Verifying Synchronization for Atomicity Violation Fixing. In *IEEE Transactions on Software Engineering (TSE'16)*. IEEE, 2016.

PATENTS

Defect detection method, device. system, and computer readable medium.

- US Patent No. 20190108003
- China Patent No. 201811013103, 201811013000, 201811015751, 2018110146864

INVITED TALKS

Fast and Precise Static Bug Detection for Industrial-Sized Code. Texas A&M University, College Station, United States, July 2021.

Taming Path-Sensitivity for Static Code Analysis on Industrial Scale. Nanjing University, Nanjing, China, April 2021.

The Next Generation Software Security Analysis. Nanjing University, Nanjing, China, May 2020.

Marrying Taint Analysis with Big Data Analytics. Southern University of Science and Technology, Shenzhen, China, November 2018.

PRESENTATIONS

Path-Sensitive Sparse Analysis without Path Conditions. In *the 42nd ACM SIGPLAN conference on Programming Language Design and Implementation (PLDI'21)*, Virtual, Canada, June 2021.

Pipelining Bottom-up Data Flow Analysis. In *the 42nd ACM/IEEE International Conference on Software Engineering (ICSE'20)*, Seoul, South Korea, May 2020.

Conquering the Extensional Scalability Problem for Value-Flow Analysis Frameworks. In *the 42nd ACM/IEEE International Conference on Software Engineering (ICSE'20)*, Seoul, South Korea, May 2020.

Fast and Precise Sparse Value Flow Analysis for Million Lines of Code. In *the 39th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'18)*, Philadelphia, United States, June 2018.

PROFESSIONAL SERVICES

Reviewer, *ACM Computing Surveys*

Reviewer, *IEEE Transactions on Software Engineering*

Reviewer, *IEEE Transactions on Dependable and Secure Computing*

Reviewer, *IEEE Transactions on Reliability*

Reviewer, *IEEE Transactions on Emerging Topics in Computing*

Member of Artifact Evaluation Committee, *ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'22)*

Member of Artifact Evaluation Committee, *ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'23)*

Member of External Review Committee and Artifact Evaluation Committee, *European Conference on Object-Oriented Programming (ECOOP'23)*

TEACHING EXPERIENCE

Teaching Assistant, COMP3111/3111H: Software Engineering (Fall 2018)

Teaching Assistant, COMP4111: Software Engineering Practices (Spring 2018)

Teaching Assistant, COMP4111: Software Engineering Practices (Fall 2016)