Yuan XIAO

yuan.xiao@smail.nju.edu.cn
Academic Profile · Google Scholar



Education

Nanjing University, PhD candidate 2021.09 – degree expected 2026.09
Major: Software Engineering (Supervisor: Chunrong Fang and Zhenyu Chen) Nanjing, Jiangsu, China
Dissertation submitted: 2026.06; defense expected: 2026.08

National University of Singapore, visiting PhD student 2024.11 – 2025.11
Major: Computer Science (Supervisor: Jinsong Dong) *Singapore*

Sun Yat-sen University, Bachelor degree 2017.09 – 2021.08
Major: Mathematics (Supervisor: Xianping Guo), Minor: Finance *Guangzhou, Guangdong, China*

Publications (†: co-first author)

- **Yuan Xiao**, Shiqing Ma, Juan Zhai, Chunrong Fang, Jinyuan Jia, Zhenyu Chen. Towards General Robustness Verification of MaxPool-Based Convolutional Neural Networks via Tightening Linear Approximation. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2024: 24766–24775. (**CCF A, Core Ranking A⋆, accepted rate: 23.6%**)
- **Yuan Xiao**, Yuchen Chen, Shiqing Ma, Chunrong Fang, Tongtong Bai, Mingzheng Gu, Yuxin Cheng, Yanwei Chen, Zhenyu Chen. Tightening Robustness Verification of MaxPool-based Neural Networks via Minimizing the Over-Approximation Zone. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2025: 20695–20705. (**CCF A, Core Ranking A⋆**)
- **Yuan Xiao**, Yuchen Chen, Shiqing Ma, Haocheng Huang, Chunrong Fang, Yanwei Chen, Weisong Sun, Yunfeng Zhu, Xiaofang Zhang, Zhenyu Chen. DeCoMa: Detecting and Purifying Code Dataset Watermarks through Dual Channel Code Abstraction. Proceedings of the 34th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA), 2025: 1701–1724. (**CCF A, Core Ranking A**)
- **Yuan Xiao**†, Jiaming Wang†, Yuchen Chen†, Wei Song, Jun Sun, Shiqing Ma, Yanzhou Mu, Juan Zhai, Chunrong Fang, Jin Song Dong, Zhenyu Chen. Train in Vain: Functionality-Preserving Poisoning to Prevent Unauthorized Use of Code Datasets. Findings of the Association for Computational Linguistics: ACL 2026, 2026: 31284–31303. (**CCF A, Core Ranking A⋆, accepted; main/findings accepted rates: 18%/19%; Yuan Xiao ranked first among co-first authors**)
- Yuchen Chen†, **Yuan Xiao**†, Chunrong Fang, Zhenyu Chen, Baowen Xu. DuCodeMark: Dual-Purpose Code Dataset Watermarking via Style-Aware Watermark-Poison Design. Proceedings of the ACM on Software Engineering, ACM International Conference on the Foundations of Software Engineering (FSE), 2026: 1–23. (**CCF A, Core Ranking A⋆, accepted**)
- An Guo, Xinyu Gao, Zhenyu Chen, **Yuan Xiao**, Jiakai Liu, Xiuting Ge, Weisong Sun, Chunrong Fang. CooTest: An Automated Testing Approach for V2X Communication Systems. Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA), 2024: 1453–1465. (**CCF A, Core Ranking A**)
- Weisong Sun, Yuchen Chen, Chunrong Fang, Yebo Feng, **Yuan Xiao**, An Guo, Quanjun Zhang, Zhenyu Chen, Baowen Xu, Yang Liu. Eliminating Backdoors in Neural Code Models for Secure Code Understanding. Proceedings of the ACM on Software Engineering, ACM International Conference on the Foundations of Software Engineering (FSE), 2025: 1386–1408. (**CCF A, Core Ranking A⋆**)
- Yuchen Chen, Weisong Sun, Haocheng Huang, **Yuan Xiao**, Chunrong Fang, Yiran Zhang, Tingting Xu, Zhenpeng Chen, An Guo, Peizhuo Lv, Xiaofang Zhang, Zhenyu Chen, Yang Liu, Baowen Xu. Securing Code Understanding: Detecting Natural Backdoor Vulnerability in Code Language Models. IEEE Transactions on Software Engineering, 2026: 1–18. (**CCF A, accepted**)
- Yuchen Chen, Wei Cheng, **Yuan Xiao**, Zhou Yang, Weifeng Sun, Chunrong Fang, Xiang Chen, Baowen Xu, David Lo, Zhenyu Chen. Security Risks for LLM-based Code Generation. ACM International Symposium on Software Testing and Analysis (ISSTA), 2026. (**CCF A, Core Ranking A, accepted**)

- Yuchen Chen, Wei Cheng, **Yuan Xiao**, Weisong Sun, Chunrong Fang, Yang Liu, Zhenyu Chen, Baowen Xu. Breaking Customized LLMs for Coding: Automated Red Teaming for Instruction Backdoor Attacks. Proceedings of the 41st IEEE/ACM International Conference on Automated Software Engineering (ASE), 2026. (**CCF A, Core Ranking A⋆, accepted**)
- Haocheng Huang, Yuchen Chen, Weisong Sun, Peizhuo Lv, **Yuan Xiao**, Chunrong Fang, Yang Liu, Xiaofang Zhang. PuzzleMark: Implicit Jigsaw Learning for Robust Code Dataset Watermarking in Neural Code Completion Models. ACM International Conference on the Foundations of Software Engineering (FSE), 2026. (**CCF A, Core Ranking A⋆, accepted**)

Academic Service

- Reviewer: AAAI 2023, NeurIPS 2024,2025,2026; ICLR 2025,2026; ICML 2025
- Sub-Reviewer: AAAI 2025; USENIX 2026; TASE 2025
- Teaching assistant for the course "Foundation of Data Science" of Zhenyu Chen. 2021 – 2024

Projects

- Zhenyu Chen and **Yuan Xiao**, SMARTLINK Internet of Vehicles Load Analysis System Development Project. 2023
- Siqi Gu, and **Yuan Xiao**, The population measurement of Huadu district Project. 2022
- Project Partcipant: Involved in the industrialization of Construction and Quality Assurance for Safety-Critical Software Systems, 2024(Vertical Research Project: CJGJZD20200617103001003) 2021

Patents

- Chen, Zhenyu; **Xiao, Yuan**; Chen, Ran. A robustness verification method for load prediction models based on linear approximation. Chinese Patent ZL2024102921461.

Prizes

- Outstanding Doctoral Graduate School Level, 2026
- Huawei Scholarship School Level, 2025
- Model Graduate Student School Level, 2025
- Outstanding Graduate Student School Level, 2022
- Graduate Academic Scholarship School Level, 2021 – 2025
- Second and Third Prize of the University Scholarship School Level, 2017-2021
- The National Second Prize of the National Mathematical Modeling Competition. National Level, 2019