Yuan XIAO

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

Education

Nanjing University, PhD candidate 2021.09 – present
Major: Software Engineering (Supervisor: Chunrong Fang and Zhenyu Chen) Nanjing, Jiangsu, China
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, Jingyuan Jia, Zhenyu Chen. Towards General Robustness Verification of MaxPool-based Convolutional Neural Networks via Tightening Linear Approximation, In the proceedings of the IEEE/CVF Computer Vision and Pattern Recognition Conference, CVPR 2024. (**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. In the proceedings of the IEEE/CVF Computer Vision and Pattern Recognition Conference. CVPR 2025. (**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 , International Symposium on Software Testing and Analysis. ISSTA 2025 (**CCF A, Core Ranking A**)
- **Yuan Xiao**, Yuchen Chen, Jiaming Wang, 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, 2026 (**CCF A, Core Ranking A⋆, main and findings accepted rate: 18 and 19 %**)
- 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 Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering. FSE 2026. (**CCF A, Core Ranking A⋆**)
- An Guo, Xinyu Gao, Zhenyu Chen, **Yuan Xiao**, Jiakai Liu, Xiuting Ge, Weisong Sun, and Chunrong Fang, An Automated Testing Approach for V2X Communication, International Symposium on Software Testing and Analysis, ISSTA 2024. (**CCF A, Core Ranking A**)
- Weisong Sun, Yuchen Chen, Chunrong Fang, Yebo Feng, **Yuan Xiao**, An Guo, Quanjun Zhang, Zhenyu Chen, Baowen Xu and Yang Liu. Eliminating Backdoors in Neural Code Models via Trigger Inversion. Proceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering. FSE 2025. (**CCF A, Core Ranking A⋆**)
- 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, Proceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering. FSE 2026. (**CCF A, Core Ranking A⋆**)

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