Congying Xu (PhD Student)

The Hong Kong University of Science and Technology

congying.xu@connect.ust.hk +86 19821250589 https://congyingxu.github.io

Research Interests: **AI for Software Engineering**, **Trustworthy AI Systems**

Education

PhD Candidate@Hong Kong University of Science and Technology 2022.09 – 2026

- Research Topic: LLM-Empowered Software Engineering
- Advisor: Shing-Chi Cheung (Chair Professor, IEEE Fellow)

Visiting Scholar@Carnegie Mellon University 2025.01 – 2025.06

- Research Topic: LLM Agent Engineering
- Advisor: Christian Kästner (Associate Professor)

Master Degree@Fudan University 2019.09 – 2022.06

- Research Topic: Software Supply Chain Security
- Advisors: Bihuan Chen (Associate Professor) and Xin Peng (Professor, Deputy Dean)

Bachelor Degree@Yangzhou University 2015.09 – 2019.06

- Major: Internet of Things Engineering
- Rank: 1/48, Advisor: Xiaobing Sun (Professor)

On-Going Research Projects

Collaborative Generative AI (Co-GenAI) 2025.08 – Now

- PC: **Hongxia Yang** (Full Professor@PolyU)
- Co-PI: **Shing-Chi Cheung** (Chair Professor@HKUST)

The Co-GenAI aims to advance generative AI by **developing LLM, MLLM, and model merging technologies**, addressing the GPU resource monopoly to democratize access, enhance participation, and accelerate innovations in AI, enabling broader researcher involvement and fostering a more inclusive future in AI development.

LLM Agent Safety and Reliability 2025.01 – Now

- PI: **Christian Kästner** (Associate Professor@CMU)
- One research paper submitted to a top-tier venue (CCF-A/CORE A*)

This project aims to advance the safety and reliability of LLM agents empowered with tool-using capabilities. By investigating **verifiably safe tool use**, this project enhances the trustworthiness of AI agents operating on sensitive subjects in complex environments. Instead of relying on end-to-end testing, the project explores **lightweight and localized testing techniques to efficiently detect silent failures**. This project advances more reliable, debuggable, and interpretable LLM agents.

LLM-Empowered Test Code Generation 2023.10 – Now

- PI: **Shing-Chi Cheung** (Chair Professor@HKUST)
- Three research papers published/submitted to top-tier venues (CCF-A/CORE A*)

The project aims to address the challenge of constructing test oracles, a critical step in automated programming and AI-assisted software engineering. By investigating both the capabilities and limitations of LLMs in this context, the project advances our understanding of **AI-assisted test code generation**. Through the integration of **LLMs, program analysis, and metamorphic testing techniques**, this project advances the automated and effective metamorphic test case generation.

Research Experience & Publications

LLM Agent Safety

[1] **[ICSE-NIER 2026] Towards Verifiably Safe Tool Use for LLM Agents**

Aarya Doshi, Yining Hong, **Congying Xu**, Eunsuk Kang, Alexandros Kapravelos, Christian Kästner CCF-A

LLM-Empowered Software Testing

[2] **[ASE 2024] MR-Adopt: Automatic Deduction of Input Transformation Function for Metamorphic Testing.**

Congying Xu, Songqiang Chen, Jiarong Wu, Shing-Chi Cheung, Valerio Terragni, Hengcheng Zhu, Jialun Cao CCF-A

[3] **[TOSEM 2024] MR-Scout: Automated Synthesis of Metamorphic Relations from Existing Test Cases.**

Congying Xu, Valerio Terragni, Hengcheng Zhu, Jiarong Wu, Shing-Chi Cheung CCF-A

LLM-Empowered Code Translation and Generation

[5] **[TOSEM 2025 (Minor-Rev)] On Effective Semantic Translation for Code: A Study Based on Pseudocode**

Songqiang Chen, **Congying Xu**, Jingyi Chen, Jialun Cao, Jiarong Wu, Shing-Chi Cheung CCF-A

[6] **[TSE 2025] Question Selection for Multi-Modal Code Search Synthesis using Probabilistic Version Spaces**

Jiarong Wu, Yanyan Jiang, Lili Wei, **Congying Xu**, Shing-Chi Cheung, Chang Xu CCF-A

Software Supply Chain Security

[7] **[ESEC/FSE 2022] Tracking Patches for Open Source Software Vulnerabilities.**

Congying Xu, Bihuan Chen, Chenhao Lu, Kaifeng Huang, Xin Peng, Yang Liu CCF-A

[8] **[EMSE 2022] Characterizing usages, updates and risks of third-party libraries in Java projects.**

Kaifeng Huang, Bihuan Chen, **Congying Xu**, Ying Wang, Bowen Shi, Xin Peng, Yijian Wu, Yang Liu CCF-B

[9] **[ICSME 2020] An Empirical Study of Usages, Updates and Risks of Third-Party Libraries in Java Projects.** (🏆 **IEEE TCSE Distinguished Paper Award (Rate: 4/58)**)

Ying Wang, Bihuan Chen, Kaifeng Huang, Bowen Shi, **Congying Xu**, Xin Peng, Yijian Wu, Yang Liu CCF-B

[10] **[ESEC/FSE 2020] Interactive, Effort-aware Library Version Harmonization.**

Kaifeng Huang, Bihuan Chen, Bowen Shi, Ying Wang, **Congying Xu**, Xin Peng CCF-A

Recommendation System

[11] **[ICSE 2019] MULAPI: A Tool for API Method and Usage Location Recommendation.**

Congying Xu, Bosen Min, Xiaobing Sun, Jiajun Hu, Bin Li, Yucong Duan CCF-A

[12] **[JSS 2018] MULAPI: Improving API method recommendation with API usage location.**

Congying Xu, Xiaobing Sun, Bin Li, Xintong Lu, Hongjing Guo CCF-B

Academic Service

- Reviewer: TOSEM 2025, ASEJ 2025, AE@ISSRE 2024, AE@ISSRE 2023
- Co-Reviewer: FSE 2025, ASE 2025, ISSTA 2025
- Volunteer: FSE 2025, ASE 2021

Teaching Experience

- COMP4633 Competitive Programming in Cybersecurity — Fall 2025–26
- COMP3021 Java Programming — Fall 2024–25
- COMP1021 Introduction to Computer Science (Python Programming) — Fall 2023-24

Selected Awards

- Overseas Research Award, HKUST — 2025
- Postgraduate Studentship (PGS), HKUST — 2022 – Present
- National Scholarship, Ministry of Education of China — 2019
- Outstanding Graduates of Yangzhou University — 2019
- First Prize · Blue Bridge Cup National Programming Competition, Jiangsu (Java) — 2018
- First Prize · Chemistry Olympiad Contest, Jiangsu Province — 2014