Hanxiao Lu

West Lafayette, IN, United States | 7654763720 |
lu525@purdue.edu | https://lhxxh.github.io |

Research Interest

Large Language Models, Software Engineering

Education

Purdue University, PhD in Computer Science 2025 –

- LLM for Software Engineering
- Being advised by Professor Tianyi Zhang

Columbia University, MS in Computer Science 2020 – 2022

- Natural Language Processing, Computer Vision, Robotics

University of Illinois Urbana Champaign, BEng in Computer Engineering 2016 – 2020

- Computer Architecture and Operating System

Research & Work Experience

Purdue University Aug 2025 –
Graduate Teaching Assistant

- Investigating the use of reinforcement learning Monte Carlo Tree Search for code generation with LLMs.

University of Illinois Urbana Champaign SE Lab June 2024 – June 2025
Research Assistant

- Developed a fully automated benchmarking framework for evaluating LLM agents on authentic security engineering tasks, using a multi-agent scaffold to construct code repositories, reproduce vulnerabilities, and generate gold patches for evaluation.
- Conducted experiments to evaluate how hyperparameters in different knowledge distillation techniques influence membership inference attacks and memorization rates with popular LLMs.

Purdue University PurSec Lab May 2023 – May 2024
Research Assistant

- Proposed ProTST, a transformer-based foundation model for binary code embedding using a hierarchical training approach and eliminating the need for complex feature engineering.

Illinois Institute of Technology TIML Lab June 2022 – Apr 2023
Research Assistant

- Proposed a robust recovery method to purify CNN-based deep learning model contaminated by various noise types, providing theoretical guarantees and demonstrating practical effectiveness on real-world datasets.

Peer-Reviewed Conference Papers

[C.3] **SEC-bench: Automated Benchmarking of LLM Agents on Real-World Software Security Tasks**
Hwiwon Lee, Ziqi Zhang, ***Hanxiao Lu***, Lingming Zhang
to appear *In Advances in Neural Information Processing Systems 2025 (NeurIPS 2025)*

[C.2] **Membership and Memorization in LLM Knowledge Distillation**
Ziqi Zhang, Ali Shahin Shamsabadi, ***Hanxiao Lu***, Yifeng Cai, Hamed Haddadi
In Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing (EMNLP 2025)

[C.1] **A Progressive Transformer for Unifying Binary Code Embedding and Knowledge Transfer**
Hanxiao Lu, Hongyu Cai, Yiming Liang, Antonio Bianchi, Z. Berkay Celik
In IEEE International Conference on Software Analysis, Evolution and Reengineering 2025 (SANER 2025)

Journal Papers

[J.1] **Purification of contaminated convolutional neural networks via robust recovery: An approach with theoretical guarantee in one-hidden-layer case**

Hanxiao Lu, Zeyu Huang, Ren Wang

In IEEE Journal of Selected Topics in Signal Processing 2025 (JSTSP 2025)

Workshop Papers

[W.1] **Enhancing Healthcare Model Trustworthiness Through Theoretically Guaranteed One-Hidden-Layer CNN Purification**

Hanxiao Lu, Zeyu Huang, Ren Wang

In International Workshop on Trustworthy Machine Learning for Healthcare 2023 (ICLR Workshop TML4H 2023)

Teaching Experience

Course Assistant Aug 2025 – Present

Computer Science Department, Purdue University

- CS 25000 Computer Architecture Fall 2025

Skills

Languages: Python, C/C++, FPGA Verilog, Assembly, Ocaml, CUDA

Machine Learning Tools: Pytorch, Tensorflow, Keras, Flax

References

Tianyi Zhang
Assistant Professor
Purdue University
tianyi@purdue.edu

Z. Berkay Celik
Assistant Professor
Purdue University
zcelik@purdue.edu

Antonio Bianchi
Assistant Professor
Purdue University
antoniob@purdue.edu

Lingming Zhang
Associate Professor
University of Illinois Urbana Champaign
lingming@illinois.edu

Ren Wang
Assistant Professor
Illinois Institute of Technology
rwang74@iit.edu