Taoran Li

taoranl2@illinois.edu | +1-217-819-9251 | taoranl2.github.io
College Station, TX, US

EDUCATION

Texas A&M University — College Station, TX, US
Doctor of Philosophy in Computer Science — Jan. 2026 – Present
Advisor: Prof. Zhiyuan Yu

University of Illinois at Urbana-Champaigns — Urbana, IL, US
Master of Engineering in Computer Engineering — Aug. 2023 – Dec. 2024
Advisor: Prof. Varun Chandrasekaran
Bachelor of Science in Computer Engineering — Aug. 2018 – Jun. 2023

Zhejiang University — Hangzhou, China
Bachelor of Engineering in Computer Engineering — Aug. 2018 – Jun. 2023

RESEARCH INTERESTS

Computer Security & Privacy, Trustworthy Machine Learning, AI Safety, Applied Cryptography

APPOINTMENTS

University of Illinois at Urbana-Champaign — Urbana, IL, US
Academic Hourly Employee — Jan. 2025 – Dec. 2025
Advisor: Prof. Varun Chandrasekaran

PUBLICATIONS

1. Xiaomin Li*, Mingye Gao*, Yuexing Hao, **Taoran Li**, Guangya Wan, Zihan Wang, Yijun Wang.
MedGUIDE: Benchmarking Clinical Decision-Making in Large Language Models.
NeurIPS GenAI4Health Workshop 2025. arXiv: 2505.11613.

2. Qilong Wu*, **Taoran Li***, Tianyang Zhou*, Varun Chandrasekaran.
SoK: Understanding (New) Security Issues Across AI4Code Use Cases.
Under review at Network and Distributed System Security Symposium 2026. arXiv: 2512.18456.

3. Hengrui Jia, **Taoran Li**, Jonas Guan, Varun Chandrasekaran.
The Metric Mirage: A False Sense of Unlearning.
Under review at ACM Conference on Computer and Communications Security 2026. arXiv: 2512.19025.

(* indicates equal contribution)

RESEARCH EXPERIENCE

Concept Unlearning in Large Language Models — Jun. 2024 – Aug. 2025
Collaborator: Prof. Varun Chandrasekaran and Hengrui Jia

- Developing a framework for removing user-specified information from LLMs while preserving model utility.
- Identified unique concepts within sensitive datasets using semi-supervised clustering to ensure minimal overlap with other training data.
- Designed targeted unlearning algorithms to eliminate sensitive conceptual information rather than entire documents, reducing utility degradation.
- Validated framework effectiveness on diverse datasets (positive, negative, fan fiction) to minimize residual knowledge.

SoK: AI for Code — Mar. 2025 – Aug. 2025
Collaborator: Tianyang Zhou, Qilong Wu, Prof. Varun Chandrasekaran

- Investigated security & privacy issues in AI-driven code generation, vulnerability detection, and translation.
- Synthesized insights for future studies on the security of AI4Code; targeted for USENIX Security 2026.

Zk-SNARK (Gnark) for Secure String Matching — Aug. 2024 – Dec. 2024
Advisor: Prof. Yupeng Zhang

- Developed a platform for secure string matching using zk-SNARKs to monitor sensitive info leaks.
- Leveraged the Gnark library to generate efficient verifiable proofs for private data verification.
- Optimized performance using sliding window technique and Rabin-Karp algorithm. arXiv: 2505.13964.

SELECTED PROJECTS

Checking Consistency Is Not Good Enough (MPC Security) Jan. 2024 – May 2024
Course Project: Prof. Varun Chandrasekaran

- Addressed vulnerabilities in MPC frameworks (e.g., Cerebro) regarding data poisoning attacks.
- Proposed solutions including Auditor role, Normalizing Flows for anomaly detection, and SISA training.
- Demonstrated that Normalizing Flows could successfully distinguish poisoned datasets.

Comprehensive Survey on Secure Machine Learning Jan. 2024 – May 2024
Course Project: Prof. David Heath

- Reviewed key contributions leveraging MPC for privacy-preserving ML tasks.
- Explored applications of SecureML in gaming environments. arXiv: 2505.15124.

TEACHING & ACADEMIC SERVICES

Teaching Assistant

- **Math 241 (Calculus III)**, Prof. Thomas Honold Fall 2022
- **Math 285 (Differential Equations)**, Prof. Thomas Honold Spring 2023
- Responsibilities: Leading discussion sections, holding office hours, grading exams.

Academic Service

- **Reviewer**: NeurIPS 2025, ACL 2026

LEADERSHIP & ACTIVITIES

- **Student Leadership Award**, Zhejiang University 2018 – 2019
- **Class President**, Computer Engineering, Zhejiang University Oct. 2018 – Oct. 2019
- **Member**, Student Union, Zhejiang University Oct. 2018 – Oct. 2019
- **Volunteer Teaching**, Guilin, Guangxi Province, China Summer 2019

SKILLS

- **Languages:** Python, C, C++, System Verilog, HTML, CSS, JavaScript, LC-3, x86 Assembly
- **Tools & Frameworks:** PyTorch, MATLAB, SQL, LaTeX, Git, CUDA