TAOBO LIAO

Curriculum Vitae

✉ Yunkai1ping@gmail.com ☎ +1 (858) 336-0599 *1102 Stoughton St Apt 8, Urbana, IL 61801*

Education

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN **January 2024 – May 2025**
Master of Science in Computer Science *GPA: **3.80**/4.00*
Relevant Coursework: Trustworthy Machine Learning, Deep Learning, Secure Multiparty Computation, Cryptography, Information Retrieval, Game Development

UNIVERSITY OF CALIFORNIA SAN DIEGO **September 2019 – September 2023**
Bachelor of Science in Mathematics-Computer Science *GPA: **3.66**/4.00*
Relevant Coursework: Deep Learning, Computer Vision, Machine Learning, Supervised ML Algorithms, Software Engineering, Discrete Math & Graph Theory, Design & Analysis of Algorithms, Abstract Algebra

Research Interests

Primary Areas: Zero-Knowledge Proofs and Cryptographic Protocols • Machine Learning Security and Privacy
Secondary Areas: Secure Multiparty Computation • Neural Network Verification • Privacy-Preserving Data Analysis

Research Experience

AutoSpec: Automated Neural Network Specification Generation **August 2024 – Present**
*Team Member • Advisors: Prof. Huan Zhang, UIUC; Prof. Francis Y. Yan, UIUC • Paper submitted to **NeurIPS 2025***

- Developed **statistical certification framework** using Hoeffding's inequality for PAC accuracy bounds
- Created novel certified pass rate metric for robustness validation
- Designed evaluation metrics achieving $\sim$ **100% pass rate** across all test datasets

Privacy-Preserving String Matching with zk-SNARKs **September 2024 – December 2024**
Team Member • Advisor: Prof. Yupeng Zhang, UIUC

- Implemented **zk-SNARK-based** platform using gnark library for cryptographic proof generation
- Achieved efficient verification: **3m46s preprocessing**, **1m48s proof generation** for 1000 requests against 100 dangerous URLs
- Conducted comprehensive complexity analysis of four string-matching approaches
- Developed secure protocol for detecting sensitive information

MPC Frameworks Against Data Poisoning Attacks **January 2024 – May 2024**
Student Researcher • Advisor: Prof. Varun Chandrasekaran, UIUC

- Enhanced Cerebro platform with **zero-knowledge proofs** and trusted third-party auditor
- Achieved **92% detection rate** for adversarial inputs on MNIST dataset
- Developed anomaly detection using normalization flows and SISA training
- Strengthened privacy guarantees in collaborative machine learning

CBAM-Enhanced DCGAN for Image Generation **March 2023 – May 2023**
Project Lead • Advisor: Prof. Zhuowen Tu, UCSD

- Applied Convolutional Block Attention Module achieving **15% image quality improvement**
- Tested on CIFAR-10 and CelebA datasets with comprehensive metrics
- Conducted literature review and experimental design

Side-Channel Analysis Attacks Using Logistic Regression **August 2022 – October 2022**
Project Lead • Advisor: Prof. Mark Vogelsberger, MIT

- Achieved **78% key recovery rate** through optimized feature selection
- Analyzed ASCAD dataset for encryption vulnerability assessment
- Built and tuned logistic regression models for cryptographic attacks

Professional Experience

YALI HIGH SCHOOL **September 2023 – December 2023**
Machine Learning Instructor *China*

- Developed and taught an introductory machine learning course for high school students, focusing on fundamental concepts and practical applications
- Created lesson plans, prepared instructional materials, and guided students through hands-on projects to deep learning
- Fostered an engaging learning environment that encouraged curiosity and critical thinking, providing foundational knowledge in machine learning

TALKWEB INFORMATION SYSTEM CO., LTD. **August 2022**
Data Analysis Intern *Remote*

- Assisted the project manager to identify business requirements and develop feasible solutions
- Assisted the senior staff to conduct data analysis in the field of artificial intelligence, including customer insight, competitiveness analysis, industry chain, future development trend analysis, proposed instructive suggestions, and made regular reports, etc.

Technical Skills

Programming:	Python, Java, C++, JavaScript
Machine Learning:	PyTorch, TensorFlow, Scikit-learn, Deep Learning
Security & Crypto:	zk-SNARKs (gnark), Zero-Knowledge Proofs, MPC Frameworks
Tools:	Git, Docker, Linux, LaTeX, Jupyter Notebook

Selected Coursework Projects

***RecipeHunter*: Recipe Management Web Application** **September 2021 – December 2021**
Team Member for Frontend Development • CSE110 Software Engineering

- Led frontend design and JavaScript implementation for recipe recommendation system
- Developed responsive UI for budget-conscious meal planning

Publications & Preprints

[1] **T. Liao**, et al. "Privacy-Preserving String Matching with zk-SNARKs," *arXiv preprint arXiv:2505.13964*, 2025. Available: `https://arxiv.org/abs/2505.13964`

[2] **T. Liao**, et al. "Checking Consistency Is Not Good Enough: Enhancing MPC Frameworks Against Data Poisoning," 2024. Available: https://taobol2.github.io/assets/Checking%20Consistency%20Is%20Not%20Good%20Enough.pdf

[3] **T. Liao**. "Logistic Regression-based Side-Channel Analysis Attacks," *Theoretical Natural Science*, vol. 18, pp. 216-223, 2023. DOI: 10.54254/2753-8818/18/20230394. Available: https://www.ewadirect.com/proceedings/tns/article/view/8407

Survey Papers

[1] Contributing author, "On Secure Machine Learning," *arXiv preprint arXiv:2505.15124*, 2025. Available: https://arxiv.org/abs/2505.15124

Honors & Awards

ASDAN China Championship **August 2017**

Languages

Chinese (Native) • **English** (Fluent) • **Japanese** (Basic)