Resume

Personal Information

Name: Taobo Liao **Gender: Male** **DOB: 06/21/2001**
Email: Yunkai1ping@gmail.com **Tel: +1 858-336-0599**
Current Address: 1007 W. Clark St. Urbana, Illinois IL 61801

Education Background

- **University of California San Diego** **September 2019-September 2023**

Major: Mathematics- Computer Science
GPA: 3.661/4.00
Graduation Date and Degree: September 2023, Bachelor of Science
Major Courses: Deep Learning, Intro to Comp Vision, Intro to Machine Learning, Supvr Mach Learning Algorithms, Software Engineering, Discrete Math & Graph Theory, Design & Analysis of Algorithm, Math/Algorithm & Systems Analys, and Abstract Algebra

- **University of Illinois Urbana-Champaign** **January 2024-**

Major: Computer Science
GPA: 4.00/4.00
Expected Graduation Date and Degree: June 2025, Master of Science
Major Courses: Trustworthy Machine Learning, Deep Learning, Secure Multiparty Computation, Cryptography, Information Retrieval, and Game Development.

Internship Experience

- **Talkweb Information System Co., Ltd.** **August 2022**

Position: Intern Student
Responsibilities:

- 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.

- **YALI High School Machine Learning Instructor** **September 2023-December 2023**

Position: Instructor
Responsibilities:

- 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.

Projects and Course Assignments

- **Logistics Regression-based Side-Channel Analysis Attacks** **August 2022-October 2022**

Position: Team Member, supervised by Professor Mark Vogelsberger from Massachusetts Institute of

Technology

Project Goal:

- ✓ Testing and analyzing the performance of the logistic regression model in the side-channel analysis attack on the encryption machine by using the ASCAD data set.

Responsibilities:

- ✓ Took charge of selecting the topics, finding references, reviewing research papers, making a general plan, and revising the plan.
- ✓ Built the logistic regression model, conducted tests related tasks, recorded the results, and made adjustments.
- ✓ Completed the research report and gave a presentation.
- ✓ Deepened my understanding of the research methods in the field of artificial intelligence.

➢ **Convolutional Block Attention Module on Deep Convolutional Generative Adversarial Network**

March 2023-May 2023

Position: Team Member, supervised by Professor Zhuowen Tu from University of California San Diego

Project Goal:

- ✓ Using Convolutional Block Attention Module to enhance the performance of the DCGAN model on multiple data set.

Responsibilities:

- ✓ Took charge of selecting the topics, finding references, reviewing research papers.
- ✓ Applied the Convolutional Block Attention Module to an existing DCGAN, recorded the improvements for each of the data sets, analyzed the results
- ✓ Completed the research report.

➢ **Enhancing Multi-Party Computation Frameworks for Robustness Against Data Poisoning Attacks**

January 2024-May 2024

Position: Team Member, supervised by Professor Varun Chandrasekaran from University of Illinois Urbana Champaign

Project Goal:

- ✓ Strengthen the privacy and integrity of multi-party computations (MPC) in collaborative machine learning by addressing vulnerabilities in existing frameworks, with a focus on preventing data poisoning attacks.

Responsibilities:

- ✓ Identified limitations in current MPC platforms, specifically Cerebro, in detecting malicious data prior to computation.
- ✓ Proposed and implemented enhancements to Cerebro, including:
  - ✓ Integration of a trusted third-party auditor using zero-knowledge proofs.
  - ✓ Development of anomaly detection mechanisms using normalization flows for outlier analysis.
  - ✓ Implementation of SISA (Shard, Isolated, Sliced, and Aggregated) training to secure model training against adversarial inputs.
- ✓ Conducted experiments using datasets such as MNIST, testing the resilience of these methods against data perturbation attacks.
- ✓ Analyzed and documented findings, demonstrating the potential of these methods to increase MPC robustness in privacy-preserving machine learning applications.

- ✓ Completed the research report and gave a presentation.

- ➢ **Privacy-Preserving String Matching with zk-SNARKs** **September 2024-December 2024**

Position: Team Member, supervised by Professor Yupeng Zhang from the University of Illinois Urbana-Champaign.

Project Goal:

- ✓ To develop a secure and efficient string-matching protocol leveraging zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) for detecting sensitive information leakage while maintaining data privacy.

Responsibilities:

- ✓ Designed a zk-SNARK-based platform integrating Rabin–Karp algorithm and Merkle Trees for efficient and scalable verification.
- ✓ Implemented the system using the gnark zk-SNARK library, optimizing rolling hash computations and proof generation.
- ✓ Conducted complexity analysis comparing string-matching techniques (naive, Rabin–Karp, Merkle Tree, and polynomial-based methods).
- ✓ Completed the research report.

Honors and Awards

- ➢ **Championship during the ASDAN China** **August 2017**

Other Skills and Interests

- ➢ Computer Skills: proficient in Java, Python, C++, JavaScript, and Linux
- ➢ Chinese: native speaker
- ➢ English: proficient in listening, speaking, reading, and writing
- ➢ Japanese: basic in listening, speaking, reading, and writing
- ➢ Personal Interest: reading, video editing, watching movies, traveling, and mountain climbing

Self-assessments

- ➢ Strong independent learning, researching, and thinking capacities
- ➢ Strong sense of responsibility, high efficiency, good communication skill, and logical thinking