Yifei Pang

Pittsburgh, PA 15213
yifeip@andrew.cmu.edu
https://2020pyfcrawl.github.io/

EDUCATION

M.S.: Carnegie Mellon University (CMU), Pittsburgh, USA Aug. 2023 - May. 2025
Major: Information Security
CQPA: 4.0/4.0
Award: Outstanding Student Services Award - Research Assistant (Information Networking Institute)

B.Eng.: Zhejiang University (ZJU), Hangzhou, China Sept. 2019 - Jun. 2023
Major: Computer Science and Technology
Overall GPA: 3.80/4.00 **The last two years GPA**: 3.94/4.00

RESEARCH INTERESTS

My research focuses on **AI safety.** Specifically, I am deeply interested in **identifying the vulnerabilities in machine learning (ML) models** and **developing practical safety solutions for ML applications**. *I am also interested in advancing research on large language models (LLMs) and vision-language models (VLMs), exploring their capabilities, limitations, and safe deployment.*

PUBLICATONS

Xiaoyu Wu, **Yifei Pang**, Terrance Liu, Steven Wu. "Winning the MIDST Challenge: New Membership Inference Attacks on Diffusion Models for Tabular Data Synthesis" *Theory and Practice of Differential Privacy 2025*.

Yifei Pang, Sreenidhi Ganachari, Yuan Yuan, Steven Wu, Xiaojing Dong, Jin Xu, Zhenyu Yan. "A New Approach to Generate Individual Level Data of Walled Garden Platforms: Linear Programming Reconstruction" *NeurIPS 2024 Workshop on Behavioral ML*.

He, Anxiao, Kai Bu, Jiongrui Huang, **Yifei Pang**, Qianping Gu, and Kui Ren. "SwiftParade: Anti-burst Multipath Validation." *IEEE Transactions on Dependable and Secure Computing (2023)*.

Yifei Pang, Anxiao He, Wenjie Hou, Yunyi Teng, Kai Bu, Qianping Gu, and Kui Ren. "SwiftOracle: Orthogonality-driven Private Multipath Validation", submitted to *IEEE Transactions on Dependable and Secure Computing* in Mar. 2025.

RESEARCH PROJECTS

Machine Unlearning | Research intern | CMU Mar. 2025 - May. 2025
[submitted, details unrevealed]

The Vector Institute MIDST challenge (Membership Inference over Diffusion-models-based Synthetic Tabular data)
| Research intern | CMU Dec. 2024 - Mar. 2025
Advisor: Steven Wu, Assistant Prof., School of Computer Science, CMU

- This project aims to evaluate the privacy leakage of diffusion-model-based tabular data synthesis by developing membership inference attacks (MIA) against both black-box and white-box scenarios, targeting TabDDPM (single table) and ClavaDDPM (multi-table) models.
- Key contributions:
  - Demonstrate that existing image-based MIA methods (e.g., SecMI) are ineffective for tabular data.
  - Identified that naive loss functions improve results but are sensitive to noise selection and temporal parameters.
  - Developed a novel machine-learning-driven approach using a three-layer MLP to automatically learn loss-to-membership relationships, eliminating manual optimization or heuristic selection.
- Our method achieved **the first-place across all four competition tracks** among 71 distinct participants [announcement]. Our research is culminated into the paper "Winning the MIDST Challenge: New Membership Inference Attacks on Diffusion Models for Tabular Data Synthesis", and accepted at **Theory and Practice of Differential Privacy 2025** [paper, code, poster].

A New Approach to Generate Individual Level Data of Walled Garden Platforms: Linear Programming Reconstruction | Research intern | CMU Apr. 2024 - Oct. 2024

Advisor: Steven Wu, Assistant Prof., School of Computer Science, CMU; Xiaojing Dong, Associate Prof., Leavey School of Business, SCU; Yuan Yuan, Austin Xu, Adobe.

- This project aims to bridge the gap between aggregate statistics released under privacy regulations and individual-level data needed for machine learning applications.
- I proposed and implemented a novel Linear Programming-based three-step algorithm to reconstruct individual-level data from aggregated statistics of Walled Garden Platforms, and evaluated its effectiveness using the Markov attribution model.
- The reconstruction achieved less than 10% error in most cases; the paper was accepted by **NeurIPS 2024 Workshop on Behavioral ML** [paper, code, poster].

SwiftOracle: Orthogonality-driven Private Multipath Validation | Research Assistant | ZJU Feb. 2023 - Jan. 2025

Advisor: Kai Bu, Associate Prof., College of Computer Science and Technology, ZJU

- This project focuses on designing a private multipath validation protocol that efficiently enforce and verify packet transmission paths while preserving path privacy.
- I proposed a novel orthogonality-driven approach, leveraging linearly independent orthogonal vectors to construct a privacy-preserving multipath validation algorithm, and implemented it in DPDK using C++ for real-world performance evaluation.
- The approach demonstrated over a 20-fold throughput improvement and applicability for larger-scale networks compared to state-of-the-art methods. The paper is submitted to **IEEE Transactions on Dependable and Secure Computing** (TDSC) in Mar. 2025.

SwiftParade: Anti-burst Multipath Validation | Research Assistant | ZJU Jul. 2022 - Jun. 2023

Advisor: Kai Bu, Associate Prof., College of Computer Science and Technology, ZJU

- This project focuses on designing an efficient multipath validation protocol to process burst traffic, using a noncommutative homomorphic asymmetric encryption scheme with constant proof size and group-wise proof generation and verification.
- I refined the algorithm by identifying and fixing vulnerabilities, pruning dispensable parts, enabling group-wise computation to improve efficiency, and implemented the algorithm in DPDK using C++ for multi-core performance evaluation.
- The algorithm speeds up packet processing by 2.5×∼8.3× and increases communication throughput by 2.8×∼10.2× compared to state-of-art approach. The paper was accepted by **IEEE Transactions on Dependable and Secure Computing** (TDSC) in Sep. 2023 [paper].

TEACHING

14740 Fundamentals of Telecommunications Networks, CMU, Teaching Assistant 2024 Fall

EXTRACURRICULAR ACTIVITIES

Mental Health Association Union | Member | ZJU Oct. 2020 - Jun. 2021

- Participated in organizing college psychological association communication activities in Hangzhou
- Organized activities about mental health in school, and did volunteer work

SKILLS

Programming Languages: C/C++, Python