Guopeng Lin

Phone: (+86)18616360015 Email: 17302010022@fudan.edu.cn

Research Interests:

- Secure Multi-party Computation
- Privacy-preserving Machine Learning

Education

Fudan University Sep. 2021 – Present

Ph.D. Candidate in Computer Science and Technology

Fudan University Sep. 2017 – Jun. 2021

B.Eng. in Software Engineering

Selected Publications

1. Is MPC Secure? Leveraging Neural Network Classifiers to Detect Data Leakage Vulnerabilities in MPC Implementations (**IEEE S&P 2025, First Author**)
   - Designed a neural network-based tool to detect data leakage vulnerabilities in MPC implementations
   - Discovered 12 data leakage vulnerabilities across TF-Encrypted, CrypTen, and MP-SPDZ; awarded 2 CVE-IDs (first CVE-IDs ever granted for data leakage vulnerabilities in MPC implementations)
2. Kona: An Efficient Privacy-Preservation Framework for KNN Classification by Communication Optimization. (**ICML 2025, First Author)**
   - Designed and implemented an efficient privacy-preserving KNN classification framework using MPC protocols
   - Eliminated online communication for Euclidean distance calculation and significantly reduced communication rounds for nearest neighbor selection
   - Achieved 1.1~232.6× speedup, 1.1~3121.2× communication reduction, and 19.1~5783.2× fewer rounds compared to prior SOTA (TIFS 2024)
3. Ents: An Efficient Three-party Training Framework for Decision Trees by Communication Optimization. (**CCS 2024, 🏆 Distinguished Artifact Award, First Author)**
   - Designed and implemented a privacy-preserving decision tree training framework based on MPC
   - Achieved 3.5–6.7× efficiency improvement, 5.5–9.3× communication reduction, and 3.9–5.3× fewer rounds compared to prior SOTA (PETS 2023)

Projects

Garnet: Secure Multi-Party Learning Platform - Project Leader Mar. 2023 – Present

- Led the design, development, and deployment of Garnet
- Project repository: https://github.com/FudanMPL/Garnet

National and Industry Research Projects

- Led or participated in national key R&D programs, the National Cryptography Fund, National Natural Science Foundation projects, and joint research projects with Huawei and Ant Group

Work Experience

Microsoft Shanghai – Software Development Engineer Intern Jun. 2020 – Feb. 2021

- Independently developed autorest-ansible, a tool to automatically generate Ansible API code for Microsoft Azure

XMAN Camps, Shanghai Pudong Development Bank, etc. – CTF Binary Exploitation Instructor)

- Delivered lectures on binary vulnerability exploitation techniques

Awards

🏆 ACM CCS 2024 Distinguished Artifact Award (First Author)

🥇 Gold Medal, College Student Invention Competition 2024 (Team Leader)

🌟 Outstanding Graduate of Shanghai (2021)

🏅 First Prize, National Cybersecurity Competition 2019 (Team Leader)

🎓 Fudan University First-class Scholarships, Excellent Student, Outstanding Youth League Member, etc.