Fengrun Liu

Email: fengrun.liu@gmail.com | Github: @f7ed | Website: https://f7ed.com/liu/

Research Interests

Theoretical and applied cryptography, especially secure multi-party computation (MPC) and succinct non-interactive arguments of knowledge (SNARK).

Education

University of Science and Technology of China (USTC) Anhui, China
M.Eng. in Cyberspace Security 2022 – Expected 2025

- GPA: 4.08/4.30 (Rank: 2/107); TOEFL: 102;

University of Electronic Science and Technology of China (UESTC) Sichuan, China
B.Eng. in Software Engineering 2018 – 2022

- GPA: 3.91/4.00 (Rank: 8/209); Outstanding Graduate;
- Thesis: Secure Multi-Party Computation Based on the BGW Protocol (Outstanding Undergraduate Thesis), advised by Prof. Yu Yu.

Publications & Presentations

Scalable Multi-Party Computation Protocols for Machine Learning in the Honest-Majority Setting. Fengrun Liu*, Xiang Xie, Yu Yu. *(Accepted by USENIX Security 2024.)* [pdf] [code] [video]

- J.P. Morgan's AlgoCRYPT Seminar Presented in Jun. 2024
- 33rd USENIX Security Symposium Presented in Aug. 2024
- Ant Group's SecretFlow Live Presented in Oct. 2024

HasteBoots: Proving FHE Bootstrapping in Seconds. Fengrun Liu*, Haofei Liang, Tianyu Zhang, Yuncong Hu, Xiang Xie, Haisheng Tan, Yu Yu. *(Under Review at Security and Privacy 2025)*

Research Experience

MPC Protocols Tailored for Privacy-preserving Machine Learning (PPML) Remote
Supervised by Prof. Yu Yu and Dr. Xiang Xie Jun. 2022 - May. 2023

This work was based on my undergraduate thesis completed at Shanghai Qi Zhi Institute.

- Focus: Explored scalable MPC protocols that address inefficiencies in non-linear functions.
- Developed a practical truncation method with only a 1-bit gap by leveraging distinct properties of Mersenne primes, which can be extended to support fixed-point multiplication without any overhead.
- Proposed an efficient bitwise comparison protocol that reduced online rounds from 5 to 1 by introducing an MPC-friendly approach to computing prefix-OR within finite fields, enabling efficient protocols for ReLU and MaxPool.
- Built a full-fledged PPML framework for oblivious inference with 15.4k lines of **C++** and conducted experiments across different settings with 3 to 63 parties.
- Outcome: This work led to my first lead-authored paper, presented at **USENIX Security 2024**.

Generating Publicly Verifiable SNARGs for FHE Operations Shanghai Qi Zhi Institute, China
Supervised by Prof. Yuncong Hu, Prof. Yu Yu and Dr. Xiang Xie Sep. 2023 – Nov. 2024

- Focus: Addressing integrity issues in outsourcing FHE by generating SNARGs for the bootstrapping procedure.
- Developed custom polynomial IOP (PIOP) protocols tailored for FHE NADN circuit operations, including LWE addition, batched lift, modulus switching, and critical accumulator updating.
- Designed specialized PIOPs for key atomic operations, such as the fast NTT/INTT where the evaluation vector is arranged in bit-reversed order; additionally, introduced an optimization for proving batched NTT of monomials.
- Implemented SNARGs for the FHE NAND in 33k lines of **Rust**, achieving the prover time of **3 seconds** on Apple M4, significantly outperforming the state-of-the-art (Zama), which requires about half an hour.
- Outcome: This work led to my second lead-authored paper, currently under review at **S&P 2025**.

Generating SNARKs for R1CS on Hidden Values in FHE Remote
Supervised by Prof. Yupeng Zhang at UIUC Mar. 2024 – Ongoing

- Focus: Aiming to obliviously prove the statement on hidden values in FHE ciphertexts.
- Explored the potential of FRI-based PCS and code-based PCS to commit hidden values.

- Evaluated the overhead of various IOPs (e.g. Plonk IOP, the GKR protocol, and Spartan) when compiled with PCS on hidden values.
- Designed SNARKs for R1CS compiled with an FHE-friendly PCS on hidden values and proposed an optimization for prover time by leveraging SIMD operations in the BGV/BFV scheme supporting batching.
- Current status: Addressing the limitation of the existing FHE library (SEAL) in supporting general SIMD encoding over plaintext, which leads to insecure soundness errors.

Exploring Learning Parity with Noise (LPN) USTC, China
Supervised by Prof. Xue Chen Feb. 2023 – May 2023

- Focus: Explored BKW-based algorithms for solving LPN.
- Investigated the BKW algorithm and its optimizations using techniques such as the Leftover Hash Lemma, fast Walsh-Hadamard transform, and covering codes.
- Explored optimizations for solving sparse LPN, including recent work leveraging Fourier analysis to attack sparse LPN with constant noise.

Improving Fuzzing Using AI technology Tsinghua University, China
Supervised by Prof. Chao Zhang Feb. 2021 – Jun. 2021

- Focus: Applied reinforcement learning algorithms to enhance fuzzing.

Open Source Software

Scalable Multi-Party Computation Protocols for Machine Learning in the Honest-Majority Setting. Awarded with *Available, Functional, Reproduced* badges in **USENIX Security '24 AE**. [code]

- A **C++** implementation of scalable MPC protocols for oblivious inference with semi-honest security in the honest-majority setting. It can complete the online oblivious inference of a 4-layer CNN with **63 parties in 0.1s and 4.6s** in the LAN and WAN settings, respectively.

Secure Processing Unit (SPU). Forked from secretflow/spu. [code]

- Contribute to integrating scalable MPC protocols, derived from my USENIX Security paper, into SecretFlow, a unified privacy-preserving computing framework developed by Alibaba Gemini Lab.

Selected Scholarships & Honors

USENIX Security '24 Student Grant — $625	2024
Cybersecurity School Student Sponsorship by Ant Group — ¥60,000	2022, 2024
National Scholarship for Graduate Students (Award rate: 0.2%) — ¥20,000	2023
Financial Cryptography Cup— Third Prize, Excellent Individual Award	2022
USTC Graduate Study Scholarship — ¥10,000	2022, 2023, 2024
Outstanding Graduate of Sichuan Province	2022
Outstanding Graduate of UESTC	2022
UESTC Outstanding Undergraduate Thesis Award	2022
UESTC Shiqiang Scholarship (Awarded to only 6 students university-wide) — ¥10,000	2020
UESTC Wuliangye Scholarship (Ranked 2/666) — ¥10,000	2019
National College Student Information Security Competition — Second Prize	2019
UESTC Undergraduate Study Scholarship — ¥2,000	2019, 2020, 2021
National Olympiad in Informatics in Provinces — Second Prize	2016

Work Experience

Shanghai Qi Zhi Institute | Research Intern hosted by Prof. Yu Yu	Sep. 2023 - Nov. 2024
Shanghai Qi Zhi Institute | Research Intern hosted by Prof. Yu Yu	Oct. 2021 - Jun. 2022
Tsinghua University | Research Intern hosted by Prof. Chao Zhang	Feb. 2021 - Jun. 2021
Tencent | Backend Engineering Intern	Jul. 2020 - Aug. 2020

Extracurricular Activities

Sub-Reviewer: PKC 2024; Asiacrypt 2024;
Blogger: Have been writing posts on my website since 2020, attracting over 30k visitors.

- 17 English posts about Foundations of Cryptography (MIT 6.875) lectured by Vinod Vaikuntanathan
- 4 English posts about Zero Knowledge Proofs MOOC
- 8 Chinese posts about Cryptography lectured by Dan Boneh
- 3 Chinese posts about MPC lectured by Mike Rosulek
- 15 Chinese posts about Machine Learning lectured by Hung-yi Lee

Class Academic Representative at UESTC 2018-2022