Fengrun Liu

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

Research Interests

I am broadly interested in cryptography and recently I have been focusing on **secure multi-party computation (MPC)** and **zero-knowledge proofs (ZKP)**.

Education

University of Science and Technology of China (USTC) Hefei, China
M.S. in Cyberspace Security; ***GPA: 4.08/4.30*** *(Rank: 2/107)* *Sep. 2022 – Expected Dec. 2024*

University of Electronic Science and Technology of China (UESTC) Chengdu, China
B.Eng. in Software Engineering; ***GPA: 3.91/4.00*** *(Rank: 8/209)* *Sep. 2018 – Jun. 2022*

Publications

Scalable Multi-Party Computation Protocols for Machine Learning in the Honest-Majority Setting [pdf]
Acclaimed for challenging the state of the art of truncations and comparisons [CH10] basically set up 13 years ago in the review.
Fengrun Liu, Xiang Xie, Yu Yu
USENIX Security 2024 (Acceptance rate in summer: 98/515=19.0%)

Research Experience

Generate SNARKs for FHE Operations Shanghai Qi Zhi Institute, China
Research Intern, supervised by Yuncong Hu, Xiang Xie, and Yu Yu *Oct. 2023 – Present*

- FHE is designed to protect data privacy by enabling computations to be performed on encrypted data. However, integrity concerns have been overlooked, allowing malicious servers to perform incorrect computations instead of the intended operations. ZKPs can be utilized to tackle these issues but snarking FHE operations faces formidable challenges.
- The starting point is the SNARKs for lookup tables, considering some unusual custom gates in the bootstrapping procedure, which is the heaviest operation in FHE. I have carefully investigated the cutting-edge lookup techniques and made some slides to facilitate discussions, e.g. [slides] for plookup and logUp, and [slides] for Lasso.
- As the primary contributor, I have completed the intricate task of designing the poly-IOP protocols for each essential step within the bootstrapping procedure. Some non-trivial optimizations and key observations are involved in the design, specifically addressing the round operation required in module switching and the transformation from LWE to Ring-LWE. In addition to the design aspect, I have assumed responsibility for implementing these protocols using **Rust**.

MPC Protocols Tailored for Privacy-preserving Machine Learning (PPML)
Supervised by Xiang Xie and Yu Yu *2022 – Jun. 2023*
This work was partially done when interning at Shanghai Qi Zhi Institute

- The widespread use of ML models has raised significant privacy concerns. To enable effective machine learning while preserving privacy, there have been many researches leveraging MPC techniques to ensure security in different settings. However, existing PPML protocols focus on 2-4 parties only, falling short of scalability for a large number of parties.
- After my undergraduate thesis mainly focused on [DN07] and [GS20] protocols, I aimed to design PPML protocols based on the general-purpose DN protocol. Through extensive investigation, I keenly observed and discerned that the existing truncation primitives (for decimal multiplication) and the bitwise comparison primitives (for various non-linear functions) pose as bottlenecks. They either exhibit inefficiencies or have a large gap between the secrets and modulus.
- By leveraging the distinctive properties of the prime fields with Mersenne primes, I devised highly optimized MPC primitives. These include a novel probabilistic truncation protocol with only a 1-bit gap, which can be seamlessly combined with DN protocol. Additionally, I presented an efficient bitwise comparison protocol that requires just 1 round with no gap. To build a full-fledged PPML framework, I also proposed round-efficient protocols to securely compute non-linear functions such as ReLU and Maxpool.
- This work has been accepted by **USENIX Security 2024** and received unanimous acceptance from all 5 reviewers in the review procedure. Through this hands-on research experience, I have acquired extensive training and expertise in both the professional field and scientific literacy.

Open Source Software

Scalable Multi-Party Computation Protocols for Machine Learning in the Honest-Majority Setting [Github]

Awarded with *Available, Functional, Reproduced* badges in **USENIX Security '24 Artifact Evaluation (AE)**.

- A **C++** implementation of scalable multi-party computation protocols tailored for privacy-preserving inference with semi-honest security in the honest-majority setting.
- The protocol is very scalable in terms of the number of parties involved. For instance, it completes the online oblivious inference of a 4-layer convolutional neural network with 63 parties in 0.1 seconds and 4.6 seconds in the LAN and WAN settings, respectively. To the best of our knowledge, this is the first fully implemented protocol in the field of PPML that can successfully run with such a large number of parties.

Selected Scholarships & Honors

National Scholarship for Graduate Students (Award rate: 0.2%)	2023
Excellent Graduate of Sichuan Province (Award rate: 4%)	2022
Excellent Graduate of UESTC (Award rate: 10%)	2022

Service

Sub-Reviewer: PKC 2024

Selected Coursework

Aside from the school curriculum, I enjoy watching open online courses and writing blogs on my website *to deepen my understanding and embody the spirit of sharing on the Internet.*

USTC: Design and Analysis of Algorithms(99), Advanced Algorithms Design and Analysis(95), Formal Languages and Computational Complexity(94), Modern Cryptography(96), Matrix Analysis and Applications(93), Privacy Issues in Big Data(93), Advanced Computer Networks(95)

UESTC: Probability and Mathematical Statistics(100), Mathematic Basis of Information Security(95), Modern Cryptography(95), Network Security: Attack and Defense(96), Computer Networks System(98), Principles of Computer Operating System, Principles of Computer Organization and Architecture, Database Principles and Applications, Digital Logic Design, Calculus, Linear Algebra and Space Analytic Geometry

MOOC: Foundations of Cryptography (MIT 6.875) [course][blogs-en], Zero Knowledge Proofs MOOC [course][blogs-en], Cryptography Course (on Coursera) [course][blogs-zh-CN], MPC Lectures [blogs-zh-CN]