

Zhenghao Lu

+86 15715880829 ◇ zhenghao.lu.sh@gmail.com ◇ [zhenghaolu22.github.io](https://github.com/zhenghaolu22)

RESEARCH INTERESTS

Cryptography, Multi-Party Computation, Blockchain Technology

EDUCATION

Shanghai Jiao Tong University

Sept. 2022 - Mar. 2025 (Expected)

M.S. in Cyber Science and Engineering

GPA: 3.92/4.00

Advisor: Prof. Lei Fan

Shanghai Jiao Tong University

Sept. 2018 - Jun. 2022

B.S. in Cyber Science and Engineering

GPA: 90.85/100, Rank: 3/127

RESEARCH

Papers and Manuscripts

(Aligned with the convention in cryptography research, the authors are listed in alphabetical order.)

- *Efficient Garbled Pseudorandom Functions and Lookup Tables from Minimal Assumption*
Wei-Kai Lin, Zhenghao Lu, Hong-Sheng Zhou
In Submission
- *Column-wise Garbling, and How to Go Beyond the Linear Model*
Lei Fan, Zhenghao Lu, Hong-Sheng Zhou
In Submission
<https://eprint.iacr.org/2024/415>
- *Brief Announcement: Best-Possible Unpredictable Proof-of-Stake*
Lei Fan, Jonathan Katz, Zhenghao Lu, Phuc Thai, Hong-Sheng Zhou
In 38th International Symposium on Distributed Computing (DISC 2024)
<https://eprint.iacr.org/2021/660>

Review Experience

- Conference Paper Reviewer: Asiacrypt 2023/2024, Eurocrypt 2024, ACM CCS 2024
- Journal Paper Reviewer: ACM Transactions on Privacy and Security 2024

Research Talks

- *Garbled Circuits, Overview* *Nov. 2023*
Institute of Information Security and Cryptology, Shanghai Jiao Tong University
Hosted by Prof. Lei Fan

INTERN EXPERIENCE

TikTok, Shanghai
Intern in *Privacy and Security*

Jun. 2023 - Sept. 2023

Alibaba Cloud, Shanghai
Intern in *System Security*

Jun. 2021 - Sept. 2021

TEACHING EXPERIENCE

NIS8020: Blockchain and Its Applications
Teaching Assistant at Shanghai Jiao Tong University

Fall 2023, Spring 2024

IS304: Innovative Information Security Technology
Teaching Assistant at Shanghai Jiao Tong University

Spring 2023

TECHNICAL SKILLS

Programming Languages: Rust, Golang, C++, Python

Cryptography/Cybersecurity Related Skills: EMP-Toolkit, Teaclave SGX SDK