

Hancheng Lou

📍 Shanghai Jiao Tong University ✉️ louhancheng@sjtu.edu.cn 🌐 louhc.github.io

Research Interests

I am interested in code-based cryptography and zero-knowledge proof systems, including code-based polynomial commitments, prover-efficient and distributed proving protocols, and communication-efficient constructions for practical deployment.

Education

Shanghai Jiao Tong University

Sept 2022 – June 2026

Computer Science and Technology (Zhiyuan Honors Project, JOHN Class)

- GPA: 3.7/4.3

Publications

- **zkAgent: Verifiable Agent Execution via One-Shot Complete LLM Inference Proof** [🔗](#)

*Lizheng Wang, **Hancheng Lou**, Chongrong Li, Yu Yu, and Yuncong Hu.*

Submitted to USENIX Security (under review).

This work proves end-to-end LLM agent execution, including complete inference and tool interactions, with one-shot transcript proving for better scalability.

- **LigeSIS: Distribution-friendly Polynomial Commitment Based on Error-correcting Code**

*Yanpei Guo, **Hancheng Lou**, Wenjie Qu, Zhuoyuan Xu, and Jiaheng Zhang.*

Submitted to USENIX Security (under review).

This work proposes a distribution-friendly code-based multilinear PCS with sublinear cross-node communication and proof size independent of the number of machines.

Research Experience

National University of Singapore

Aug 2025 – Feb 2026

Research Intern, Advisor: Prof. Jiaheng Zhang

- Conducted research on distribution-friendly code-based polynomial commitment schemes for large-scale zkSNARK proving.
- Co-authored *LigeSIS: Distribution-friendly Polynomial Commitment Based on Error-correcting Code*, submitted to USENIX Security (under review).

Research Explorations

Preliminary Exploration on BIKE Decoding

[Louhc/LDPC-BIKE](#) [🔗](#)

Advisor: Prof. Yu Yu, John Hopcroft Center, Shanghai Jiao Tong University

- Implemented and benchmarked several soft-decision decoder variants for BIKE in a preliminary study (no publication).

Preliminary Exploration on CFS Signature

Advisor: Prof. Yu Yu, John Hopcroft Center, Shanghai Jiao Tong University

- Investigated higher-weight error strategies and practical bottlenecks for more efficient CFS signing in a preliminary study (no publication).

Projects

MiniVim

Dec 2022

Course Project in Programming Languages Design and Implementation

- I implemented a vim-like text editor in C++.

Gobang AI

Jun 2023

Course Project in Programming Languages Design and Implementation

- Built a Gobang AI in C++ using Monte Carlo search.

Technologies

Languages: Rust, C++, C, Python, Sage, Coq