Zhifan Luo

Zhejiang University – Hangzhou, China

+86 182-5796-1627 • luozf0105@gmail.com • sio-2.github.io

Education

Zhejiang University — **Hangzhou, China**
M.S. in Cyberspace Security, Advisor: Prof. Zhan Qin — *Sept. 2023 – June 2026 (Expected)*
State Key Laboratory of Blockchain and Data Security

Zhejiang University — **Hangzhou, China**
B.S. in Information Security, GPA: 3.76/4.00 — *Sept. 2019 – June 2023*

Publications

1. **Shadow in the Cache: Unveiling and Mitigating Privacy Risks of KV-cache in LLM Inference**
   Zhifan Luo, Shuo Shao, Su Zhang, Lijing Zhou, Yuke Hu, Chenxu Zhao, Zhihao Liu, Zhan Qin.
   Network and Distributed System Security Symposium (NDSS) 2026.

2. **Calibrate After Privatize: Privacy-Performance Balanced Split Learning for LLM Fine-Tuning**
   Chenxu Zhao, Xiaoyi Pang, Zhibo Wang, **Zhifan Luo**, Su Zhang, Lijing Zhou.
   Under Submission.

Research Experience

State Key Laboratory of Blockchain and Data Security, Zhejiang University
Graduate Research Assistant, Advisor: Prof. Zhan Qin
Research Topic: Theoretical Privacy Analysis of Large Language Models

- **Research Focus:** Investigated privacy leakage mechanisms in Transformer-based Large Language Models (LLMs) as part of the master's thesis research.
- **Theoretical Contribution:** Developed a mathematical optimization method to mitigate privacy risks in Key-Value caches, ensuring data security during the inference phase.
- **Validation:** Verified the proposed theory using public open-source models (e.g., Llama, Qwen) within the university laboratory environment.
- **Outcome:** The research results were summarized into a paper and accepted by **NDSS 2026**.

Research Interests

Fields: Computer Security, Privacy Preservation, Machine Learning Theory.

Technical Skills

Languages
Python, C/C++

Frameworks
PyTorch, Transformers, vLLM

Tools
Git, Docker, LaTeX