

Zhifan Luo

Zhejiang University – Hangzhou, China

■ +86 182-5796-1627 • ✉ luozhifan@zju.edu.cn • ⚡ sio-2.github.io

Education

Zhejiang University

M.S. in Cyberspace Security, Advisor: Prof. Zhan Qin
State Key Laboratory of Blockchain and Data Security

Hangzhou, China

Sept. 2023 – June 2026 (Expected)

Zhejiang University

B.S. in Information Security, GPA: 3.75/4.00 (Last 2 Years: 3.87/4.00)
Awards: Outstanding Graduate of Zhejiang University, Third-Class Scholarship.

Hangzhou, China

Sept. 2019 – June 2023

Research Interests

Fields: Large Language Model (LLM) Security & Privacy, Machine Learning Systems (MLsys).

Focus: Inference System Security, KV-Cache Privacy, Side-channel Analysis, Endogenous Security.

Publications & Manuscripts

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

Huawei 2012 Laboratories

Research Intern

Shanghai, China

Sept. 2024 – Aug. 2025

Topic: Privacy-Preserving LLM Inference in Untrusted Clouds

- **Gap Analysis:** Identified critical privacy leaks in cloud inference due to vulnerable externalized KV-caches.
- **Vulnerability Analysis:** Analyzed reconstruction risks, providing the **first empirical evidence** of prompt leakage in Llama/Qwen architectures without raw input access.
- **System Design (KV-Cloak):** Architected a lightweight obfuscation defense natively integrated with **PagedAttention**, mitigating privacy risks while ensuring lossless accuracy with **<1% latency overhead**.
- **Impact:** Core algorithms were integrated into **large-scale production inference frameworks**; yielded 1 top-tier paper and 1 patent.

Patents

- Zhifan Luo, Su Zhang, Lijing Zhou, Wen Tang. "An Inference Method for Artificial Intelligence Models and Related Systems." (CN Patent, Under Review).

Technical Skills

Languages

Python, C/C++

Frameworks

PyTorch, Transformers, vLLM

Tools

Git, Docker, LaTeX