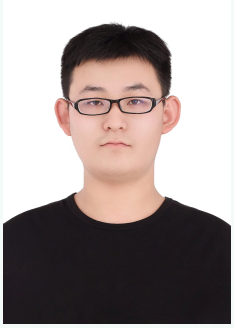

Qianli Ma

Ph.D. Student · AI Systems & Security

Email: mql16899@163.com
Phone/WeChat: +86 188-2170-7389
Website: maqianli.xyz

EDUCATION

Beijing Normal University
Ph.D. student, Intelligent Science and Technology · Zhuhai
Faculty of Arts and Science; Institute of Artificial Intelligence and Future Networks.

Inner Mongolia University of Technology
M.S., Cyberspace Security · Hohhot

Xidian University
B.S., Information Security · Xi'an

RESEARCH INTERESTS

- Efficient LLM inference, KV-cache transfer, disaggregated serving
- Model compression, state reuse, selective recomputation
- AI security, backdoor attacks, frequency-domain robustness
- Computer vision for smart agriculture and livestock systems

SKILLS

- Python, PyTorch, deep learning experimentation
- LLM serving and evaluation pipelines
- Computer vision, image manipulation, applied ML systems
- Academic writing, reproducible experiment design

AWARDS

- 3rd Prize, China Graduate Mathematical Contest in Modeling
- 3rd Prize, National Cryptography Technology Competition
- 2nd Prize, IMUT 2023 Internet+ Innovation and Entrepreneurship Competition
- 2nd Prize, IMUT Master's Academic Scholarship

PROFILE

Researcher working at the intersection of efficient LLM systems, semantic state transfer, and trustworthy machine learning. Recent work focuses on bandwidth-efficient KV-cache reuse across heterogeneous models and the interface bottlenecks that prevent generated reasoning candidates from being selected by fixed verifiers.

SELECTED PUBLICATIONS

1. Semantic Cache Distillation: Efficient State Transfer via Reuse and Selective Patching
Qianli Ma, Zhiqing Tang, Hanshuai Cui, Zhi Yao, Weijia Jia
Proceedings of the 43rd International Conference on Machine Learning (ICML), 2026.

2. Correct but Unselectable: The Hidden Interface Tax in Multi-Candidate Reasoning
Qianli Ma
Manuscript under review, NeurIPS 2026.

3. Stealthy Frequency-Domain Backdoor Attacks: Fourier Decomposition and Fundamental Frequency Injection
Qianli Ma, Junping Qin, Kai Yan, Lei Wang, Hao Sun
IEEE Signal Processing Letters (SPL), 2023. CCF-C, JCR-Q2.

4. Perceptually Imperceptible Backdoor Attacks Using High-Frequency Information in Deep Learning Models
Qianli Ma, Junping Qin, Yin Cao, Jiaqi Ren
4th International Conference on Neural Networks, Information and Communication Engineering (NNICE), 2024. EI.

5. FastFaceCLIP: A Lightweight Text-driven High-Quality Face Image Manipulation
Jiaqi Ren, Junping Qin, Qianli Ma, Yin Cao
IET Computer Vision, 2024. JCR-Q4.

6. A Survey of Text-to-Image Generation
Huang Cao, Junping Qin, Qianli Ma, Hao Sun, Kai Yan, Lei Wang, Jiaqi Ren
Journal of Zhejiang University (Engineering Science), 2024. EI.

7. A Two-Stage GAN-Based Method for High-Quality Text-to-Image Generation
Huang Cao, Junping Qin, Peng Gao, Qianli Ma, Jiaqi Ren
Journal of Zhejiang University (Engineering Science), 2024. EI.

SELECTED RESEARCH EXPERIENCE

Semantic Cache Distillation for LLM Serving
Designed a bandwidth-efficient state-transfer framework for shared-architecture, weight-mismatched producer-consumer models. Proposed REUSE and PATCH mechanisms to reduce KV transmission while controlling semantic drift; demonstrated up to 2.65x TTFT speedup in bandwidth-constrained regimes.

Backdoor Attacks and Defenses in Machine Unlearning
Explored frequency-domain and trigger-based mechanisms for stealthy backdoor behavior, model memorization, and mitigation-oriented analysis.

Computer Vision for Smart Livestock Systems
Built applied CV pipelines for cattle image acquisition, identity-related visual signals, weight estimation, feed-cost calculation, lambing detection, and methane-recovery research support.

TEACHING

Teaching Assistant, Data Structures and Algorithm Analysis
Autumn 2022
Assisted undergraduate coursework, including assignment grading, feedback, and teaching preparation for four classes.