

# Kainan Cao

+852 66428307 ◇ kainan\_cao@connect.hku.hk

## EDUCATION

### The University of Hong Kong

Master of Computer Science

Hong Kong

Sep 2025 - Nov 2026 (expected)

### Beijing University of Posts and Telecommunications

Bachelor of Engineering & Bachelor of Management (GPA: 3.6/4.0)

Beijing, China

Sep 2021 - Jun 2025

Relevant Coursework: Software Engineering, Natural Language Processing, Python Data Analysis

## RESEARCH EXPERIENCE

### Data Poisoning Attacks and Defense for Federated Learning

Beijing University of Posts and Telecommunications | Advisor: Prof. Shengli Pan

Jan 2025 - May 2025

Beijing, China

- Designed and implemented label-flipping attack strategies in Federated Learning framework, training a ResNet-18 model on the CIFAR-10 dataset to systematically evaluate model vulnerability under different data distribution types (IID vs. Non-IID).
- Proposed and validated a median-based defense mechanism, demonstrating its effectiveness in mitigating attack impact and enhancing system robustness.
- Conducted systematic experiments varying the proportion of malicious clients and revealed the non-linear degradation pattern of global model accuracy under increasing adversarial participation.

## PROJECTS

### RAG-Based Intelligent Travel Agent Itinerary Planner

- Architected a hybrid LLM system enabling flexible switching between cloud-based models DeepSeek for low-latency generation and local deployment llama3.2 using Ollama for privacy-preserving execution.
- Engineered a robust Retrieval-Augmented Generation (RAG) pipeline using LangChain and FAISS. Implemented semantic search with sentence-transformers to retrieve top-k relevant contexts from multi-source data (Google Search results, user-defined unstructured text, and historical knowledge bases).
- Optimized the context window management by implementing dynamic token allocation based on itinerary duration, effectively balancing generation quality with computational costs.

### Large Language Model Post-training Optimization using veRL Framework

- Implemented the GRPO using veRL to fine-tune the Qwen2.5 series (0.5B/1.5B/7B) on the GSM8K benchmark, leveraged ray and vLLM to optimize distributed training efficiency.
- Conducted systematic evaluations using LightEval to benchmark RL-based alignment performance, analyzing stability and convergence metrics across diverse datasets to validate the effectiveness of the fine-tuning process.

### Optimization of Mathematical Reasoning via Hybrid Prompt Engineering Strategies

- Integrated the Skills-in-Context planning approach with the Progressive-Hint self-correction mechanism to create a hybrid framework on the GSM8K benchmark. The method uses skill-based examples to guide the initial reasoning step and applies an iterative process to refine the output based on answer consistency.
- Conducted ablation studies on DeepSeek-chat and Qwen2.5-7b-instruct models to evaluate the performance of the proposed strategy. Experiments demonstrated that the hybrid approach achieved higher accuracy than individual baselines by effectively reducing reasoning and calculation errors.

## SKILLS

**Programming Languages** Python, PyTorch, veRL, SQL, Java  
English, Chinese (Mandarin)