

Su Zhang

suzhang1@umd.edu
UMD CS Profile | GitHub

Ph.D. Student in Computer Science · University of Maryland, College Park

EDUCATION

University of Maryland, College Park

Ph.D. in Computer Science; Advisor: Prof. Heng Huang

2024–Present

College Park, MD

Tsinghua University

Weiyang College; B.S. in Energy and Power Engineering; B.S. in Mathematics and Physics

2020–2024

Beijing, China

SELECTED PUBLICATIONS AND MANUSCRIPTS

- [1]. **Su Zhang**, Junfeng Guo, and Heng Huang. “FedAttr: Towards Privacy-preserving Client-Level Attribution in Federated LLM Fine-tuning.” *arXiv:2605.06596*, 2026. *Submitted to NeurIPS 2026*.
- [2]. **Su Zhang**, Peiran Yu, and Heng Huang. “Mitigating Data Heterogeneity Effect in Client-Reshuffling-Based Federated Learning.” *Submitted to NeurIPS 2026*.

RESEARCH EXPERIENCE

FedAttr: Privacy-preserving Client-Level Attribution in Federated LLM Fine-tuning

2026

University of Maryland, College Park · Advisor: Prof. Heng Huang

- Proposed **FedAttr**, a client-level data-use attribution protocol that identifies which federated clients trained on protected data while operating entirely through secure aggregation, without plaintext access to individual client updates.
- Developed a paired-subset client-update estimator with differential watermark scoring and cross-round Stouffer aggregation; proved estimator unbiasedness and variance guarantees and bounded per-round mutual-information leakage by $O(d^*/N)$.
- Evaluated federated LoRA fine-tuning across Llama/Qwen models, multiple datasets, two watermark families, and two aggregation strategies; achieved **100% TPR and 0% FPR** in the main settings with **6.3%** additional runtime.

FedCDR: Federated Optimization under Client Reshuffling and Data Heterogeneity

2025–2026

University of Maryland, College Park · Advisor: Prof. Heng Huang

- Proposed **FedCDR**, a nonconvex federated optimization method combining client reshuffling with Douglas–Rachford splitting and supporting inexact local proximal solvers.
- Established an $O(\epsilon^{-1})$ communication complexity for reaching $\mathbb{E}\|\nabla f(\bar{x})\|^2 \leq \epsilon$, with a leading constant independent of standard measures of client data heterogeneity.
- Developed a meta-epoch-level convergence analysis for the conditional bias and inter-round dependence of without-replacement reshuffling; experiments show up to **5.1×** communication-round speedup over FedDR at 5% participation and scale to **10,000 clients**.

Large Graph Neural Networks with Mixture-of-Experts

2023

Tsinghua University · Collaborators: Prof. Jie Tang and Weikai Li

- Co-developed a Mixture-of-Experts architecture to enlarge GNN capacity and improve model expressiveness; co-authored the manuscript *GMoE: Enlarging Graph Neural Networks with Mixture-of-Experts*.

Stackelberg Information Design in Human-in-the-Loop Reinforcement Learning

2023

University of Maryland, College Park · Advisor: Prof. Kaiqing Zhang

- Formulated active human-in-the-loop reinforcement learning as a Stackelberg information-design problem and developed an algorithm that optimizes information disclosure to guide human decision-making toward the agent’s objective.

TECHNICAL SKILLS

Languages: Python, C++ **ML/LLM:** PyTorch, Hugging Face Transformers, PEFT (LoRA), TRL, Accelerate, Datasets
Distributed/HPC: CUDA, PyTorch DDP, SLURM, Linux