

Hanling Tian

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

Advisor: Prof. Heng Huang

hanling@umd.edu — blueblood6.github.io — [GitHub](#)

Research Interests: Machine Learning, LLM Agents, AI Safety, Efficient LLM Systems

EDUCATION

University of Maryland, College Park, College Park, MD, USA

Ph.D. in Computer Science

08 2026 – Present

Advisor: Prof. Heng Huang

Shanghai Jiao Tong University, Shanghai, China

M.S. in Automation Science and Engineering

Advisor: Prof. Xiaolin Huang

09 2023 — 03 2026

GPA: 3.83/4.00

Xi'an Jiaotong University, Xi'an, China

B.E. in Automation

09 2019 — 06 2023

GPA: 4.11/4.30, Average Grade: 94.15/100

Young Gifted Program, Qian Xuesen Honors College, Outstanding Graduate; National Scholarship (0.2%)

PUBLICATIONS

Peer-Reviewed Publications

H. Tian, G. Zhang, Z. Sha, J. Wang, Y. Liu, Z. Huang, K. Yang & X. Huang (2026). **InjecMEM: Memory Injection Attack on LLM Agent Memory Systems**. COLM 2026. [Paper] [Code]

J. Zhang, Y. Qiu, **H. Tian**, J. Zhang, X. Yin & X. Huang (2026). **Stochastic Optimal Control Sampling for Diffusion Inverse Problems**. ECCV 2026. [Paper]

Z. Huang, Y. Liu, B. Lin, Y. Lou, Z. He, **H. Tian**, T. Li & X. Huang (2026). **RAIN-Merging: A Gradient-Free Method to Enhance Instruction Following in Large Reasoning Models with Preserved Thinking Format**. ICLR 2026, Oral. [Paper]

M. He, R. Yang, **H. Tian**, Y. Qiu & X. Huang (2025). **Primphormer: Efficient Graph Transformers with Primal Representations**. ICML 2025. [Paper]

H. Tian, Y. Liu, M. He, Z. He, Z. Huang, R. Yang & X. Huang (2025). **Simulating Training Dynamics to Reconstruct Training Data from Deep Neural Networks**. ICLR 2025. [Paper] [Code] [Slides] [Poster]

Preprints

J. Zhang, Y. Bai, P. Wen, Z. Huang, Z. He, **H. Tian**, X. Cheng, H. Ran & X. Huang (2026). **SAGE: Retain-Aware Post-Hoc Sanitization of Final Unlearning Vector**. arXiv preprint. [arXiv]

Q. Xiao, **H. Tian**, Z. Huang & X. Huang (2026). **GradCFG: Gradient Inversion of Classifier-Free Guidance Diffusion Models**. Under review at IEEE TPAMI. [OpenReview]

D. Huang, J. Guo, S. Sun, **H. Tian**, J. Lin, Z. Hu, C.-Y. Lin, J.-G. Lou & D. Zhang (2023). **A Survey for Graphic Design Intelligence**. arXiv preprint. [arXiv]

PROFESSIONAL EXPERIENCE

Microsoft Research Asia (MSRA), Beijing, China

Research Intern of Data, Knowledge, and Intelligence Group. Mentor: Shizhao Sun

07 2022 — 06 2023

Pre-training of Graphic Layout Generation & Design Image Generation with Text Constraints

Ant Group, Shanghai, China

Research Intern of Security and Risk Management Group - LLM Safety.

05 2025 — 08 2025

Agent Safety Alignment via Reinforcement Learning & Attacks on Agent Memory System