Xiangyu Liu

CONTACT INFORMATION

2104, Brendan Iribe Center
College Park, MD 20740

xyliu999@umd.edu
https://xiangyu-liu.github.io/

EDUCATION

University of Maryland, College Park, MD, USA
Ph.D. in Computer Sciences Aug. 2021 – May 2026 (expected)
- Advisor: Kaiqing Zhang

Shanghai Jiao Tong University (SJTU), Shanghai, CN
Bachelor in Computer Science Sep. 2017 – Jun. 2021
- Zhiyuan Honors Program of Engineering (an elite program for top 5% talented students)

University of California, Berkeley, CA, USA
Exchange student Jan. 2020 – May 2020
- GPA: 4.0/4.0

RESEARCH INTERESTS

- Multi-agent reinforcement learning and game theory: paper [J1, C1, C2, C6]
- LLM agents, fine-tuning, and alignment: paper [C7, C8]
- Responsible AI and robustness: paper [C3, C4, C5, C7]

JOURNAL PUBLICATIONS

[J1] **Xiangyu Liu**, Kaiqing Zhang
Partially Observable Multi-Agent Reinforcement Learning with Information Sharing.
Accepted to **SIAM Journal on Control and Optimization (SICON)** under major revision.
Shorter version appeared at ICML 2023.

CONFERENCE PUBLICATIONS

[C8] (*denotes equal contribution) Chanwoo Park*, **Xiangyu Liu***, Asuman E. Ozdaglar, Kaiqing Zhang
Do LLM Agents Have Regret? A Case Study in Online Learning and Games
International Conference on Learning Representations **(ICLR 2025)**
Oral talk at ICLR 2024 workshop: How Far Are We From AGI?

[C7] Pankayaraj Pathmanathan, Souradip Chakraborty, **Xiangyu Liu**, Yongyuan Liang, Furong Huang
Is Poisoning a Real Threat to LLM Alignment? Maybe More So Than You Think
AAAI Conference on Artificial Intelligence **(AAAI 2025)**

[C6] (Alphabetical order) Yang Cai†, **Xiangyu Liu**†, Argyris Oikonomou†, Kaiqing Zhang†
Provable Partially Observable Reinforcement Learning with Privileged Information

Conference on Neural Information Processing Systems **(NeurIPS 2024)**

[C5] Yongyuan Liang, Yanchao Sun, Ruijie Zheng, **Xiangyu Liu**, Tuomas Sandholm, Furong Huang, Stephen McAleer

Game-theoretic Robust Reinforcement Learning Handles Temporally-coupled Perturbations

International Conference on Learning Representations **(ICLR 2024)**

[C4] **Xiangyu Liu**, Chenghao Deng, Yanchao Sun, Yongyuan Liang, Furong Huang

Beyond Worst-case Attacks: Robust RL with Adaptive Defense via Non-dominated Policies

International Conference on Learning Representations **(ICLR 2024)**, ***Spotlight***

[C3] **Xiangyu Liu**, Souradip Chakraborty, Yanchao Sun, Furong Huang

Rethinking Adversarial Policies: A Generalized Attack Formulation and Provable Defense in RL

International Conference on Learning Representations **(ICLR 2024)**

Outstanding Paper Award at NeurIPS 2022 Workshop on Trustworthy and Socially Responsible Machine Learning.

[C2] **Xiangyu Liu**, Kaiqing Zhang

Partially Observable Multi-agent RL with (Quasi-)Efficiency: The Blessing of Information Sharing

International Conference on Machine Learning **(ICML 2023)**

[C1] **Xiangyu Liu**, Hangtian Jia, Ying Wen, Yujing Hu, Yingfeng Chen, Changjie Fan, Zhipeng Hu, Yaodong Yang

Towards Unifying Behavioral and Response Diversity for Open-ended Learning in Zero-sum Games

Conference on Neural Information Processing Systems **(NeurIPS 2021)**

EXPERIENCES

Bloomberg AI Group, NY, USA

Research intern June. 2022 – Sep. 2022

- Research on bond pricing with recurrent neural networks.
- Developed a novel attention mechanism for dynamically capturing correlations among multiple time series

HONORS AND AWARDS

Outstanding Paper Award, NeurIPS 2022 Workshop on Trustworthy and Socially Responsible Machine Learning. 2022

Dean's Fellowship, University of Maryland, College Park. 2021

National Scholarship (Top 0.2% in China), Ministry of Education of P.R.China. 2018&2019

1st Prize in Chinese College Mathematics Competitions (Top 1 at SJTU, selected for final). 2018

A-class Scholarship for Excellent Academic Performance (Top 1% at SJTU), SJTU. 2018

TALKS

2024 INFORMS Optimization Society Conference (IOS 2024), Houston, Texas, 2024
Invited talk on partially observable multi-agent RL (paper [J1] and [C2])

TSRML workshop of NeurIPS 2022
Contributed talk on adversarial policies in competitive games (paper [C3])

RL China seminar series, online, China
Invited talk on unifying diversity in open-ended learning for zero-sum games (paper [C1])

ACADEMIC SERVICES

Conference reviewer for UAI 2024-2025, NeurIPS 2024, ICLR 2025, AISTATS 2025, AAMAS 2025, ICML 2025

TEACHING EXPERIENCE

Student organizer of summer AI camps at UMD for K-12 students Summer 2023/2024

TA for crypotography at UMD Spring 2022

TA for common sense reasoning in NLP at UMD Fall 2021

COMPUTER SKILLS

- Programming Languages: Python, C/C++, Java, MATLAB, LaTeX
- Deep Learning Packages: PyTorch, TensorFlow