

Xiang Li

Address: 113 West 60th street, LL Room 601, New York, NY 10023
☎ (+1) 551-338-2219 | ✉ xiang.li@fordham.edu | 🌐 Github | 🏠 Personal website

EDUCATION

Fordham University

Ph.D. in Computer Science

Aug. 2023 - Present

Huazhong University of Science and Technology

Bachelor of Engineering in Automation (GPA: 3.91/4.0)

Sep. 2019 - Jun. 2023

PUBLICATIONS

- **Xiang Li**, Pin-Yu Chen, Wenqi Wei. “Scaling Behavior in Model Fine-tuning for Audio Deepfake Detection”, International Conference on Machine Learning (ICML), PMLR, 2026.
- **Xiang Li**, Wenqi Wei. “Protecting Membership Privacy through Adaptive Logit Scaling”, in submission, 2026.
- **Xiang Li**, Pin-Yu Chen, Wenqi Wei. “Measuring the Robustness of Audio Deepfake Detectors under Real-World Corruptions”, ACM Conference on Data and Application Security and Privacy (CODASPY), 2026.
- **Xiang Li**, Bhavani Thuraisingham, Wenqi Wei. “MUBox: A Critical Evaluation Framework of Deep Machine Unlearning”, The 30th ACM Symposium on Access Control Models and Technologies (SACMAT), 2025.
- **Xiang Li**, Pin-Yu Chen, Wenqi Wei, “Where Are We in Audio Deepfake Detection? A Systematic Analysis Over Generative and Detection Models”, ACM Transactions on Internet Technology (TOIT), 2025.
- Wenqi Wei, **Xiang Li**, Hüseyin Tanriverdi. *Software Generation With LLMs: Privacy, Utility, and Cybersecurity Tensions*, International Conference on Information Systems (ICIS), 2025.
- Nashrah Haque, **Xiang Li**, Zhehui Chen, Yanzhao Wu, Lei Yu, Arun Iyengar, Wenqi Wei. “Boosting Imperceptibility of Stable Diffusion-based Adversarial Examples Generation with Momentum”, IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS), 2024.
- Xueqing Zhang, Junkai Zhang, Ka-Ho Chow, Juntao Chen, Ying Mao, Mohamed Rahouti, **Xiang Li**, Yuchen Liu, Wenqi Wei. “Visualizing the Shadows: Unveiling Data Poisoning Behaviors in Federated Learning”, IEEE International Conference on Distributed Computing Systems (ICDCS), 2024.
- Xirong Cao, **Xiang Li**, Divyesh Jadav, Yanzhao Wu, Zhehui Chen, Chen Zeng, Wenqi Wei. “Invisible Watermarking for Audio Generation Diffusion Models”, IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS), 2023.
- Shaolin Ran, **Xiang Li**, Beizhen Zhao, Yinuo Jiang, Xiaoyun Yang and Cheng Cheng. “Label Correlation Embedding Guided Network for Multi-label ECG Arrhythmia Diagnosis”, Knowledge-Based Systems, 2023.

RESEARCH EXPERIENCE

Research Engineer Intern

Syntra Inc.

Jul. 2025 - Aug. 2025

New York, USA

- Developed an audio deepfake detection model achieving state-of-the-art performance.
- Ranked #1 in the HuggingFace benchmark arena for audio deepfake detection, surpassing both open-source and proprietary models.
- Applied few-shot fine-tuning techniques to adapt the model to new domains, including call center applications.

Fordham-IBM Research Intern

Fordham University & IBM, Advisor: Dr. Pin-Yu Chen, Prof. Wenqi Wei

May 2024 - Aug. 2024

New York, USA

- Trained/Finetuned state-of-the-art detection models/audio foundation models for audio deepfake detection tasks.
- Collected an AI-synthesized audio dataset using state-of-the-art TTS models and conducted a systematic evaluation of audio deepfake detection models.
- Proposed to utilize few-shot fine-tuning to effectively improve model generalization.

Graduate Assistant

Fordham University, Advisor: Prof. Wenqi Wei

Aug. 2023 - Present

New York, USA

- Proposed Adaptive Logit Scaling Loss to mitigate overconfidence issue in models training to defense against Membership Inference Attacks.
- Implemented Machine Unlearning benchmark toolkit and conducted systematic evaluations of existing unlearning algorithms.
- Conducted research on stable diffusion-based adversarial examples generation, improving the attack success rate by 35% over the state-of-the-art baseline.
- Investigated watermarking techniques for the audio diffusion models.

AWARDS AND HONORS

- | | |
|--|------|
| • ACM CODASPY Travel Grant | 2026 |
| • Fordham-IBM Research Grant | 2025 |
| • ICDCS Travel Grant | 2024 |
| • Fordham-IBM Research Grant | 2024 |
| • Outstanding Graduate, School of Artificial Intelligence and Automation, HUST | 2023 |
| • People Scholarship, Huazhong University of Science and Technology | 2022 |
| • Honorable Mention Award in Mathematical Contest In Modeling (MCM) | 2022 |
| • People Scholarship, Huazhong University of Science and Technology | 2020 |
| • Freshman Scholarship, Huazhong University of Science and Technology | 2020 |

ACADEMIC SERVICES

Journal Reviewer

- IEEE Journal of Biomedical and Health Informatics (JBHI)
- ACM Transactions on Internet Technology (TOIT)
- IEEE Open Journal of Signal Processing (IEEE-OJSP)
- ACM Computing Surveys

Conference Reviewer

- ICLR('24, '25, '26, '27), ICML('25), NeurIPS('24, '25, '26), ECCV('24), COLM('26), COLING('25), AAAI('25, '26, '27), KDD('24, '25), CODASPY('25, '26).

TEACHING EXPERIENCE

- Instructor for CISC 4080: Computer Algorithms, Fall 2026.
- Teaching Assistant and Guest Lecturer for CISC 4080: Computer Algorithms, Spring 2026 and Fall 2025.
- Undergraduate Tutor in CIS Department, Fordham University, Spring 2025.
- Teaching Assistant for CISC 5325: Database, Fall 2024.

SKILLS

- **Programming:** Python(Pytorch,Tensorflow); C; Matlab.
- **Deep Learning/ Machine Learning:** LLMs, Diffusion Models, CNNs, GANs, Transformers, SVM, Decision Trees, etc.
- **Tools:** Git; Slurm; Latex.
- **Languages:** Mandarin(native); English(TOEFL: 107, GRE: 332); Italian.