Qiuling Xu

765-701-5968 | xu1230@purdue.edu | qiulingxu.github.io

Education

Purdue University
PhD in Computer Science, West Lafayette, Indiana, USA — *Aug. 2018 – Aug 2023 (expected)*

Nanjing University
BS in Computer Science, Nanjing, Jiangsu, China — *Aug. 2014 – May 2018*

Experience

Netflix, *Research Intern, California* — *May. 2022 – Aug 2022*
- Fairness on Recommendation System

Adobe, *Research Intern, California* — *May. 2021 – Aug 2021*
- Improve the **Consistency Learning** in model development.

Microsoft Research, *Research Intern, Beijing* — *Mar. 2018 – June 2018*
- Designed hyper-parameter searching space representation for ***user-friendly automatic machine learning***.

Purdue University, *Research Assistant, Indiana* — *Aug. 2018 – Present*
- Studied methods for defense, explanation, and analysis of adversarial attack in ***adversarial learning***.

Nanjing University, *Research Assistant, China* — *Aug. 2016 – June 2018*
- Devised an end-to-end module to learn **logical reasoning** and **neural perception** simultaneously.

Awards

Top 1% in ACM-ICPC International Programming Contest China ***Final*** (16/1500) — *2016, Shanghai, China*

Publications (* represents equal contribution)

Deep Distribution Bound for Nature-looking Adversarial Attack
***Qiuling**, Guanhong and Xiangyu* — **CVPR 2022**

Better Trigger Inversion Optimization in Backdoor Scanning
*Guanhong, Guangyu, Yinqi, Shengwei, **Qiuling** and Xiang* — **CVPR 2022 (Oral)**

Model Orthogonalization: Class Distance Hardening in Neural Networks for Better Security
*Guanhong, Guangyu, Yinqi, **Qiuling**, Shengwei, Zhuo and Xiangyu* — **S&P 2022**

Constrained Optimization with Dynamic Bound-scaling for Effective NLP Backdoor Defense
*Guangyu, Yinqi, Guanhong, **Qiuling**, Zhuo and Xiangyu* — **ICML 2022**

Backdoor Scanning for Deep Neural Networks through K-Arm Optimization
*Guangyu, Yinqi, Guanhong, Shengwei, **Qiuling** and Xiangyu* — **ICML 2021**

A Le Cam Type Bound for Adversarial Learning and Applications
Qiuling, Kevin* and Jean* — **ISIT 2021**

Towards Feature Space Adversarial Attack by Style Perturbation
***Qiuling**, Guanhong, Siyuan and Xiangyu* — **AAAI 2021**

Trace Divergence Analysis and Embedding Regulation for Debugging Recurrent Neural Networks
*Guanhong, Shiqing, Yingqi, **Qiuling** and Xiangyu* — **ICSE 2020**

Bridging Machine Learning and Logical Reasoning by Abductive Learning
WangZhou, **Qiuling***, Yang* and Zhihua* — **NIPS 2019**

Reducing Accuracy Gap in Adversarial Training by Discriminating Adversarial Samples
***Qiuling**, Guanhong, Shengwei, Jean and Xiangyu Zhang* — Preprint

Technical Skills

Courses: NLP, Machine Learning(ML) Theory, Reinforcement Learning, Graph ML,

Operating System, Programming Language, Network, Database, Algorithm, Data Structure, Algorithm Analysis
Languages: Python, C, C++, SQL **Frameworks**: Tensorflow, Pytorch, Mxnet **Libraries**: NumPy, Matplotlib

Projects

Operating System | ***C, Assembly Language, Operating System*** *June 2016*

- Implemented OS from scratch, including boot, system call, driver, memory, file, process, and shell.

Sub C Compiler | ***C, Bison, Lex*** *June 2017*

- Implemented term extraction, syntax & semantic analysis, and grammar tree & intermediate code translation.

Gender-fair Word Embedding | ***Python, NLP, Adversarial Learning*** *June 2020*

- Enforced word embedding's fairness by Adversarial Training; decreased 20%+ more correlation than the SOTA.