Xilie Xu

☎ *+86-188-6127-2649*
✉ *xuxilie@comp.nus.edu.sg*
GodXuxilie
Google Scholar

Education Background

Aug. 2021 - Present **Ph.D. Candidate**, Department of Computer Science, School of Computing, National University of Singapore, Singapore.

Supervised by Prof. Mohan Kankanhalli and co-advised by Dr. Jingfeng Zhang

- Research topic: adversarial machine learning [1, 2, 3].

Sep. 2017 - Jun. 2021 **Undergraduate**, Taishan College, Shandong University, Jinan, China.

Taishan College is an elite program, which is committed to cultivating compound and creative elite students in science and engineering disciplines. The selection of this college is really competitive, admitting only about 15 students of CS major.

Academic Experience

Jun. 2019 - Jun. 2021 **Research Assistant in Research Center of Software and Data Engineering**, Shandong University, Jinan, China.

Supervised by Prof. Lizhen Cui and Dr. Jingfeng Zhang

- Research topic: adversarial machine learning [4, 5, 6].

Jul. 2019 **NUS School of Computing Summer Workshop 2019** , National University of Singapore, Singapore.

- Project “Save Shanghai: Garbage Classification” was awarded the 1st prize among about 100 competitive teams in the “Big Data and Cloud Computing” cluster.

Internship Experience

Jun. 2021 - Jul. 2021 **Research Intern**, Department of Ant Group-CRO Line-Security and Risk Management, Ant Z Space, Hangzhou, China.

Mentored by Dr. Lingjuan Lyu

- Research topic: adversarial machine learning and privacy.
- Proposed an innovative patent to protect model intellectual property and data privacy

Award and Grant

Aug. 2022 **Graduate Student Travel Grant**, *3100 SGD*, School of Computing, National University of Singapore.

Aug. 2022 **Research Achievement Award**, School of Computing, National University of Singapore.

Jun. 2022 **ICML 2022 Participation Grant**, ICML 2022.

Oct. 2021 **Outstanding Reviewer Award**, NeurIPS 2021.

Jun. 2021 **Outstanding Undergraduate Thesis Award**, Shandong University.

Sep. 2020 **Specialty Scholarship (Research Innovation Award)**, *First Prize*, Shandong University.

Sep. 2018 - Sep. 2020 **Outstanding Student Scholarship**, Shandong University.

Oct. 2018 **First Prize at the 10th Mathematics Competition of Chinese College Student**, Chinese Mathematical Society.

Professional Service

2021-Present **Serve as a conference reviewer at NeurIPS'21-23, ICML'22-23, ICLR'22-24**.

2022-Present **Serve as a journal reviewer at TAI, TMLR, IPL**.

Aug. 2023 - Dec. 2023 **Serve as a teaching assistant for CS3244 Machine Learning**, School of Computing, National University of Singapore.

Apr. 2023 **Create the website of N-CRiPT Technical Workshop 2023 [link] and present a poster at the workshop**, National University of Singapore.

Oct. 2022 **Serve as a member of the executive group of TrustML Young Scientist Seminars**, RIEKN-AIP, Tokyo.

Apr. 2022 **Serve as a student reviewing member of the Master of Computing admission**, School of Computing, National University of Singapore.

Jan. 2022 - May. 2022 **Serve as a teaching assistant for CS5242 Deep Learning and Neural Networks**, School of Computing, National University of Singapore.

Research Work

[1] Xilie Xu*, Jingfeng Zhang*, Feng Liu, Masashi Sugiyama, and Mohan Kankanhalli. Efficient adversarial contrastive learning via robustness-aware coreset selection. *NeurIPS'23 (Spotlight)*, 2023.

[2] Xilie Xu*, Jingfeng Zhang*, Feng Liu, Masashi Sugiyama, and Mohan Kankanhalli. Enhancing adversarial contrastive learning via adversarial invariant regularization. *NeruIPS'23*, 2023.

[3] Xilie Xu*, Jingfeng Zhang*, Feng Liu, Masashi Sugiyama, and Mohan Kankanhalli. Adversarial attack and defense for non-parametric two-sample tests. In *International Conference on Machine Learning*, pages 24743–24769. PMLR, 2022.

[4] Jingfeng Zhang*, Xilie Xu*, Bo Han, Tongliang Liu, Gang Niu, Lizhen Cui, and Masashi Sugiyama. Noilin: Improving adversarial training and correcting stereotype of noisy labels. *Transactions on Machine Learning Research*, 2022.

[5] Chen Chen*, Jingfeng Zhang*, Xilie Xu, Lingjuan Lyu, Chaochao Chen, Tianlei Hu, and Gang Chen. Decision boundary-aware data augmentation for adversarial training. *IEEE Transactions on Dependable and Secure Computing*, 2022.

[6] Jingfeng Zhang*, Xilie Xu*, Bo Han, Gang Niu, Lizhen Cui, Masashi Sugiyama, and Mohan Kankanhalli. Attacks which do not kill training make adversarial

[0] An asterisk (*) beside authors' names indicates equal contributions.

learning stronger. In *International Conference on Machine Learning*, pages 11278–11287. PMLR, 2020.