Wenxiao Wang

wwx@umd.edu | PhD student at UMD

Education

University of Maryland, College Park — *College Park, US*

Ph.D. in Computer Science — *Sept. 2021 - present*

Institute for Interdisciplinary Information Sciences, Tsinghua University — *Peking, China*

B.Eng. in Computer Science and Technology. — *Sept. 2016 - June. 2020*

Research

Institute for Interdisciplinary Information Sciences, Tsinghua University — *Peking, China*

research assistant mentored by Prof. **Hang Zhao** — *Sep. 2020 - Aug. 2021*

self-supervised learning

University of California, Berkeley — *Berkeley, US*

visiting student researcher advised by Prof. **Dawn Song** — *Apr. 2019 - Aug. 2019*

watermarking of neural networks & differentially private deep learning

Bytedance AI Lab — *Peking, China*

intern in visual search group mentored by **Yi He** and **Lei Li** — *May. 2018 - Nov. 2018*

deep representation learning for large scale near duplicate video retrieval

Publication

Lethal Dose Conjecture on Data Poisoning [url]

Wenxiao Wang, Alexander Levine, Soheil Feizi — *2022*

Conference on Neural Information Processing Systems (NeurIPS)

Improved Certified Defenses against Data Poisoning with (Deterministic) Finite Aggregation [url]

Wenxiao Wang, Alexander Levine, Soheil Feizi — *2022*

International Conference on Machine Learning (ICML)

On Feature Decorrelation in Self-Supervised Learning [url]

Tianyu Hua*, **Wenxiao Wang***, Zihui Xue, Sucheng Ren, Yue Wang, Hang Zhao — *2021*

(*equal contribution)

International Conference on Computer Vision (ICCV)[**oral**]

DPlis: Boosting Utility of Differentially Private Deep Learning via Randomized Smoothing [url]

Wenxiao Wang, Tianhao Wang, Lun Wang, Nanqing Luo, Pan Zhou, Dawn Song, Ruoxi Jia — *2021*

Privacy Enhancing Technologies Symposium (PETS)

REFIT: A Unified Watermark Removal Framework For Deep Learning Systems With Limited Data [url]

Xinyun Chen*, **Wenxiao Wang***, Yiming Ding, Chris Bender, Ruoxi Jia, Bo Li, Dawn Song

(*equal contribution) *2021*

ACM Asia Conference on Computer and Communications Security (AsiaCCS)

The Secret Revealer: Generative Model Inversion Attacks Against Deep Neural Networks [url]

Yuheng Zhang*, Ruoxi Jia*, Hengzhi Pei, **Wenxiao Wang**, Bo Li, Dawn Song

(*equal contribution) *2020*

Conference on Computer Vision and Pattern Recognition (CVPR)[**oral**]

Leveraging Unlabeled Data for Watermark Removal of Deep Neural Networks [url]

Xinyun Chen*, **Wenxiao Wang***, Yiming Ding, Chris Bender, Ruoxi Jia, Bo Li, Dawn Song

(*equal contribution) *2019*

ICML2019 Workshop on Security and Privacy of Machine Learning

Services

Program Committee / Reviewer of:

- NeurIPS 2022
- ICML 2022 (Outstanding Reviewer)
- Workshop on Adversarial Robustness In the Real World (ECCV 2022 , ICCV 2021)
- Workshop on Socially Responsible Machine Learning (ICML 2021)
- Workshop on Adversarial Machine Learning in Real-World Computer Vision Systems and Online Challenges (CVPR 2021)
- Workshop on Security and Safety in Machine Learning Systems (ICLR 2021)

Awards

Gold Medal(**4th place**)	National Olympiad in Informatics	2015
Gold Medal(**1st place**)	Asia and Pacific Informatics Olympiad in China District	2015
Gold Medal(**10th place**)	China Team Selection Competition	2015
Gold Medal	National Olympiad in Informatics	2014
Bronze Medal	Asia and Pacific Informatics Olympiad in China District	2014
Silver Medal	China Team Selection Competition	2014