

Wenxiao Wang

✉ wwx@umd.edu | PhD student at UMD

Education

University of Maryland, College Park

PH.D. IN COMPUTER SCIENCE

College Park, US

Sept. 2021 - present

Institute for Interdisciplinary Information Sciences, Tsinghua University

B.ENG. IN COMPUTER SCIENCE AND TECHNOLOGY.

Peking, China

Sept. 2016 - June. 2020

Research

Bytedance

RESEARCH INTERN MENTORED BY **LINJIE YANG**, **HENG WANG** AND **YU TIAN**

self-supervised pre-training of visual models

Remote, US

June. 2022 - Nov. 2022

Institute for Interdisciplinary Information Sciences, Tsinghua University

RESEARCH ASSISTANT MENTORED BY PROF. **HANG ZHAO**

self-supervised learning

Peking, China

Sep. 2020 - Aug. 2021

University of California, Berkeley

VISITING STUDENT RESEARCHER ADVISED BY PROF. **DAWN SONG**

watermarking of neural networks & differentially private deep learning

Berkeley, US

Apr. 2019 - Aug. 2019

Bytedance AI Lab

INTERN IN VISUAL SEARCH GROUP MENTORED BY **YI HE** AND **LEI LI**

deep representation learning for large scale near duplicate video retrieval

Peking, China

May. 2018 - Nov. 2018

Publications

Lethal Dose Conjecture on Data Poisoning [\[url\]](#)

WENXIAO WANG, ALEXANDER LEVINE, SOHEIL FEIZI

Conference on Neural Information Processing Systems (NeurIPS)

2022

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

WENXIAO WANG, ALEXANDER LEVINE, SOHEIL FEIZI

International Conference on Machine Learning (ICML)

2022

On Feature Decorrelation in Self-Supervised Learning [\[url\]](#)

TIANYU HUA*, **WENXIAO WANG***, ZIHUI XUE, SUCHENG REN, YUE WANG, HANG ZHAO

(*EQUAL CONTRIBUTION)

International Conference on Computer Vision (ICCV)[\[oral\]](#)

2021

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
Privacy Enhancing Technologies Symposium (PETS)

2021

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)
ACM Asia Conference on Computer and Communications Security (AsiaCCS)

2021

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

2020

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)
ICML2019 Workshop on Security and Privacy of Machine Learning

2019

Talks

- **Lethal Dose Conjecture: From Few-shot Learning to Potentially Nearly Optimal Defenses against Data Poisoning**, TMLR Group, Hong Kong Baptist University, December 2022.

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