MINXING ZHANG

Im Oberen Werk 1, 66386 St. Ingbert, Germany

minxing.zhang@cispa.de | https : //minxingzhang.github.io/

EDUCATION

CISPA – Helmholtz Center for Information Security, Germany   10/2022 - now
Phd Student   *Supervisor: Michael Backes and Xiao Zhang*

Universität des Saarlandes, Saarbrücken, Saarland, Germany   05/2021 - 09/2022
Preparatory Phase

Information Retrieval Lab, Shandong University, China   06/2020 - 02/2021
Research Assistant   *Supervisor: Zhaochun Ren*

Shandong University(SDU), China   09/2016 - 06/2020
Computer Science and Technology (Elite Program)

RESEARCH AREAS

Trustworthy Machine Learning, Security & Privacy, Model Behavior Explanation

PUBLICATIONS

Generating Less Certain Adversarial Examples Improves Robust Generalization
Minxing Zhang, Michael Backes, Xiao Zhang   *arXiv*

In Transactions on Machine Learning Research (TMLR), October 2024

**Generated Distributions Are All You Need for Membership Inference Attacks
Against Generative Models**
Minxing Zhang, Ning Yu, Rui Wen, Michael Backes, Yang Zhang   *arXiv*

In 2024 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), January 2024

Membership Inference Attacks Against Recommender Systems
Minxing Zhang,[*] Zhaochun Ren,[*] Zihan Wang,[*] Pengjie Ren,
Zhumin Chen, Pengfei Hu, Yang Zhang[†]   *arXiv*

In 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS), November 2021
(∗ equal contribution, † corresponding author)

Invisibility Cloak: Disappearance under Human Pose Estimation via Backdoor Attacks
Minxing Zhang, Michael Backes, Xiao Zhang   *arXiv*

Vera Verto: Multimodal Hijacking Attack
Minxing Zhang, Ahmed Salem, Michael Backes, Yang Zhang   *arXiv*

PROFESSIONAL SERVICES

External Reviewer.

- ACM SIGSAC Conference on Computer and Communications Security (CCS)

- International Conference on World Wide Web (WWW)

- ACM Asia Conference on Computer and Communications Security (ASIACCS)

- Privacy Enhancing Technologies Symposium (PETS)
- Privacy Preserving Machine Learning (PPML)