

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 <i>Phd Student</i>	10/2022 - now <i>Supervisor: Michael Backes and Xiao Zhang</i>
Universität des Saarlandes, Saarbrücken, Saarland, Germany <i>Preparatory Phase</i>	05/2021 - 09/2022
Information Retrieval Lab, Shandong University, China <i>Research Assistant</i>	06/2020 - 02/2021 <i>Supervisor: Zhaochun Ren</i>
Shandong University(SDU), China <i>Computer Science and Technology (Elite Program)</i>	09/2016 - 06/2020

RESEARCH AREAS

Trustworthy Machine Learning, Security & Privacy, Model Behavior Explanation

PUBLICATIONS

**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)

Generating Less Certain Adversarial Examples Improves Robust Generalization

Minxing Zhang, Michael Backes, Xiao Zhang *arXiv*
Under review

Vera Verito: Multimodal Hijacking Attack

Minxing Zhang, Ahmed Salem, Michael Backes, Yang Zhang *arXiv*
Under review

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)