MINXING ZHANG

Stuhlsatzenhausweg 5, 66123, Saarbrucken, 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

PUBLICATIONS

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

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

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

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

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

arXiv

SERVICE

External Reviewer

AsiaCCS22, WWW 2022, PoPETs 2022, CCS 2021, PPML 2021