

ZHANG, MINXING

PhD Candidate

🏛️ Saarland University, Germany

@ minxing.zhang@cispa.de

📍 minxingzhang.github.io



Education

2021.04 - Now	Saarland University, Germany	Ph.D. Student
	Supervisor: Prof. Michael Backes	
	Advisor: Prof. Yang Zhang and Dr. Xiao Zhang	
2016.09 - 2020.06	Shandong University, China	Computer Science and Technology
	Advisor: Prof. Zhaochun Ren	Bachelor

Working

2023.10 - 2024.03	Saarland University, Germany	
	Lecture: Robustness in Machine Learning	Teaching Assistant
2020.07 - 2021.01	Shandong University	Computer Science and Technology
	Advisor: Prof. Zhaochun Ren	Research Assistant

Research Interests

- › Trustworthy AI
 - › AI Security and Privacy
 - › Robust and Reliable Machine Learning
 - › Trustworthiness Evaluation

Services

- › IEEE European Symposium on Security and Privacy (Euro S&P), 2026.
- › ACM International Conference on Multimedia (MM), 2025.

Publications

(**Bold** for me, * for equal contribution)

- DivTrackee versus DynTracker: Promoting Diversity in Anti-Facial Recognition against Dynamic FR Strategy.
Wenshu Fan, **Minxing Zhang***, Hongwei Li, Wenbo Jiang, Hanxiao Chen, Xiangyu Yue, Michael Backes, Xiao Zhang.*
In ACM SIGSAC Conference on Computer and Communications Security (CCS), ACM, 2025.
(This paper was awarded as the *Distinguished Paper*.)
- Generated Distributions Are All You Need for Membership Inference Attacks Against Generative Models.
***Minxing Zhang**, Ning Yu, Rui Wen, Michael Backes, Yang Zhang.*
In IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), IEEE, 2024.

- 3 Generating Less Certain Adversarial Examples Improves Robust Generalization.
Minxing Zhang, *Michael Backes, Xiao Zhang*.
In Transactions on Machine Learning Research (TMLR) – J2C Certification, 2024;
In International Conference on Learning Representations (ICLR), 2025.
- 4 Membership Inference Attacks Against Recommender Systems.
Minxing Zhang*, *Zhaochun Ren*, Zihan Wang*, Pengjie Ren, Zhunmin Chen, Pengfei Hu, Yang Zhang*.
In ACM SIGSAC Conference on Computer and Communications Security (CCS), ACM, 2021.
- 5 Invisibility Cloak: Disappearance under Human Pose Estimation via Backdoor Attacks.
Minxing Zhang, *Wenshu Fan, Wenbo Jiang, Shui Yu, Michael Backes, Xiao Zhang*.
Preprint, arXiv.
- 6 Vera Verito: Multimodal Hijacking Attack.
Minxing Zhang, *Abmed Salem, Michael Backes, Yang Zhang*.
Preprint, arXiv.