Zheng Li | CV

✉ zheng.li@cispa.de • https://zhenglisec.github.io/

last update: March 3, 2023

Education

CISPA Helmholtz Center for Information Security — **Saarbrücken, Germany**
Ph.D. in Computer Science — *February 2021 – July 2023 (Expected)*
Advisor: Dr. Yang Zhang

Shandong University — **Jinan, China**
Master in Computer Science — *September 2017 – June 2020*
Advisor: Prof. Shanqing Guo

Shandong University — **Jinan, China**
Bachelor in Computer Science — *September 2013 – June 2017*
Advisor: Prof. Shanqing Guo

Research Interests

Security and Privacy of Machine Learning

Publication

Conference

[1] **Zheng Li**, Ning Yu, Ahmed Salem, Michael Backes, Mario Fritz, and Yang Zhang. UnGANable: Defending Against GAN-based Face Manipulation. In *USENIX Security Symposium (USENIX Security)*. USENIX, 2023.

[2] Yugeng Liu, **Zheng Li**, Michael Backes, Yun Shen, and Yang Zhang. Backdoor Attacks Against Dataset Distillation. In *Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2023.

[3] **Zheng Li**, Yiyong Liu, Xinlei He, Ning Yu, Michael Backes, and Yang Zhang. Auditing Membership Leakages of Multi-Exit Networks. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2022.

[4] **Zheng Li** and Yang Zhang. Membership Leakage in Label-Only Exposures. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2021.

[5] **Zheng Li**, Chengyu Hu, Yang Zhang, and Shanqing Guo. How to Prove Your Model Belongs to You: A Blind-Watermark based Framework to Protect Intellectual Property of DNN. In *Annual Computer Security Applications Conference (ACSAC)*. ACM, 2019.

[6] **Zheng Li**, Ge Han, Shanqing Guo, and Chengyu Hu. How to Prove Your Model Belongs to You: A Blind-Watermark based Framework to Protect Intellectual Property of DNN. In *International Conference on High Performance Computing and Communications (HPCC)*. IEEE, 2019.

Technical Report

[7] Xinlei He*, **Zheng Li***, Weilin Xu, Cory Cornelius, and Yang Zhang. Membership-Doctor: Comprehensive Assessment of Membership Inference Attacks Against Machine Learning Models.

[8] Zeyang Sha, **Zheng Li**, Ning Yu, and Yang Zhang. DE-FAKE: Detection and Attribution of Fake Images Generated by Text-to-Image Generation Models.

[9] Ziqing Yang, Xinlei He, **Zheng Li**, Michael Backes, Mathias Humbert, Pascal Berrang, and Yang Zhang. Data Poisoning Attacks Against Multimodal Encoders.

[10] Yixin Wu, Ning Yu, **Zheng Li**, Michael Backes, and Yang Zhang. Membership Inference Attacks Against Text-to-image Generation Models.

[11] Xinyue Shen, Xinlei He, **Zheng Li**, Yun Shen, Michael Backes, and Yang Zhang. Backdoor Attacks in the Supply Chain of Masked Image Modeling.

Internship

Research Intern — **Nokia Bell Lab**
Mentor: Ruichuan Chen — *July 2022 - October 2022, Stuttgart*

Teaching

Teaching Assistant — **Advanced Lecture: Machine Learning Privacy**
April 2022 - October 2022, Saarland University

Teaching Assistant — **Seminar: Data-driven Understanding of the Disinformation Epidemic**
April 2022 - June 2022, Saarland University

Teaching Assistant — **Seminar: Privacy of Machine Learning**
December 2021 - February 2022, Saarland University

Teaching Assistant — **Advanced Lecture: Privacy Enhancing Technologies**
April 2021 - October 2021, Saarland University

Teaching Assistant — **Seminar: Data-driven Understanding of the Disinformation Epidemic**
April 2021 - October 2021, Saarland University

Awards

ACSAC Student Travel Grant (2019)
First Level Scholarship (Shandong University, 2019)
Second Level Scholarship (Shandong University, 2018)
Second Level Scholarship (Shandong University, 2017)
Third Level Scholarship (Shandong University, 2016)
Second Level Scholarship (Shandong University, 2014)

Service

- External Reviewer
  - 2023: S&P, CCS, CVPR

- 2022: USENIX Security, CCS, NDSS, S&P, AAAI, PoPETs
- 2021: USENIX Security, CCS, ICLR, AAAI, AISACCS, PETS, PPML, AISec
- 2020: RAID

References

Dr. Yang Zhang
CISPA Helmholtz Center for Information Security
Email: zhang@cispa.de

Prof. Dr. Shanqing Guo
Shandong University
Email: guoshanqing@sdu.edu.cn