Peng Kuang

NO.866 Yuhangtang Road, Hangzhou, China, 310058 | pengkuang@zju.edu.cn | +86 15527025129

Education

Zhejiang University, M.Eng. in Network and Information Security — Expected, Mar 2026

- Provisional thesis title: Towards debiasing deep neural networks under real-world scenarios.

Wuhan University, B.Sc. in Computer Science and Technology — May 2023

- GPA: 3.85/4.0
- 2020,2021,2022. Scholarship of Excellent Undergraduate Student, Wuhan University
- 2021 Ministry of Education-Huawei Intelligent Base Scholarship, Huawei Technologies Co.

Research Experience

Research Assistant, Zhejiang University — Sept 2023 – Present

- Empirically and theoretically identified characteristics of real-world biases previously overlooked by the community with a novel analysis framework, based on which a new benchmark is proposed.
- Uncovered a critical failure mode of existing unsupervised debiasing methods with comprehensive evaluation on proposed benchmarks.
- Proposed a novel debiasing method that better adapts to the characteristics of real-world biases.
- Wrote a paper on the above research results, currently under review.

Undergraduate Research Intern, Wuhan University — June 2021 – May 2022

- Designed and implemented an evolution-based black-box adversarial attack on speech recognition and voice identification systems. Comprehensive digital and physical experiments demonstrate its effectiveness.
- Built a web-based automatic data collection system that greatly accelerates the experiments of adversarial attacks in the physical world scenario. The system was used in the group's subsequent works and received unanimous praise.
- Designed and implemented a transformer-based model for in-car detection on WIFI signals.

Publications

Rethinking Debiasing: Real-World Bias Analysis and Mitigation

Peng Kuang, Zhibo Wang, Zhixuan Chu, Jingyi Wang, and Kui Ren.

Preprint, arXiv: 2405.15240 (Under review)

Echo: Reverberation-based Fast Black-Box Adversarial Attacks on Intelligent Audio Systems

Meng Xue, ***Peng Kuang***, Xuluan Gong, Qian Zhang, and Routing Li.

Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies

DetectDUI: An In-Car Detection System for Drink Driving and BACs

Yanjiao Chen, Meng Xue, Jian Zhang, Runmin Ou, Qian Zhang, and ***Peng Kuang***.

IEEE/ACM Transactions on Networking

Projects

Artificial Intelligence Security Theory and Verification Platform — github.com/ZJUICSR/AIcert

Module Lead, ZJU-State Key Laboratory of Blockchain and Data Security

- Research existing fairness platforms and codebases.
- Assembled 30+ fairness metrics covering various fairness principles.
- Assembled 15+ debiasing algorithms for structured and unstructured data.
- Assembled 5+ model structure and 5+ fairness benchmarks.
- Designed interface and dashboard for bias evaluation and mitigation.