

YICHI ZHANG

Graduate Research Assistant
College of Information Sciences and Technology
The Pennsylvania State University
University Park, PA 16802

✉ yichi.zhang@psu.edu
☎ (814) 680-9009
🌐 <https://yichics.github.io>
📍 413 Eric J. Barron Innovation Hub

EXPERIENCES

Graduate Research Assistant for [Dr. Yuchen Yang](#) 2025.08 - Current
The Pennsylvania State University, PA, United States

EDUCATION

Ph.D. The Pennsylvania State University 2025 – Current
Informatics PA, United States
Advisor: [Dr. Yuchen Yang](#)

B.E. Zhejiang University 2021 – 2025
Information Engineering Hangzhou, China

PUBLICATIONS

PEER-REVIEWED CONFERENCE PAPERS (* INDICATES CO-FIRST AUTHORS)

- 2026 **PREFed: An Effective and Stealthy Static-Anchor Backdoor Attack via Trigger Pre-Optimization in Federated Learning**
Xi Chen, Rui Zeng, Chunyi Zhou, **Yichi Zhang**, Yuwen Pu, Qingming Li, Lu Zhou, Zhe Liu, Shouling Ji
IEEE Transactions on Information Forensics and Security (TIFS), 2026.
- HijackKV: New Threat in Position-Independent KV Cache Reuse**
Yichi Zhang, Zhiqi Wang, Huan Zhang, Yuchen Yang
In Proceedings of the 35th USENIX Security Symposium, 2026.
- Rethinking Forgery Attacks on Semantic Watermarks in Black-Box Settings: A Geometric Distortion Perspective**
Cheng-Yi Lee, **Yichi Zhang**, Yuchen Yang, Chun-Shien Lu, Jun-Cheng Chen
In Proceedings of the 43rd International Conference on Machine Learning (ICML), 2026.
- 2025 **Diffusion Noise Feature: Accurate and Fast Generated Image Detection**
Yichi Zhang, Xiaogang Xu
In proceedings of the European Conference on Artificial Intelligence (ECAI), 2025

PREPRINTS

- 2026 **Lost in Compaction: Evaluating Side-Constraint Loss under Context Compaction**
Zhiqi Wang, **Yichi Zhang**, Dongwon Lee, Yuchen Yang.
Under review
- Rethinking Quality in Large Language Model Routing: Security-Conditioned Model-and-Budget Selection**
Zhenxiang Huang*, **Yichi Zhang***, Yuchen Yang
Under review
- The Refusal Signal Survives Quantization but Goes Unconsumed**
Deekshith Reddy Bhoomireddy, Rishit Rai, Zhiqi Wang, **Yichi Zhang**, Yuchen Yang
Under review

One Framework, Two Learners: Exploring Psychological Techniques for Generalizable Scam Detection in Humans and AI

Zhiqi Wang, **Yichi Zhang**, Xiaozhi Yang, Dongwon Lee, Yuchen Yang

Under review

2025 **Efficient Implicit Neural Compression of Point Clouds via Learnable Activation in Latent Space**

Yichi Zhang, Qianqian Yang

Under review

SERVICES

CONFERENCE/JOURNAL REVIEWING

International Conference on Machine Learning (ICML)

2026

AAAI Conference on Artificial Intelligence (AAAI)

2026-2027