

YE ZHENG

Ph.D. candidate in Computer Science, Rochester Institute of Technology (RIT)

🌐 zhengyeah.com | ✉ zhengye.cn@gmail.com

RESEARCH EXPERIENCE

I focus on the design and analysis of foundational algorithms. Over the past five years, my research has spanned formal privacy and formal safety.




EDUCATION

- | | |
|---|---------------------|
| Rochester Institute of Technology (Rochester, USA) | Sep 2023 – Present |
| <ul style="list-style-type: none">◦ Ph.D. candidate in Computer Science, advised by Dr. Yidan Hu◦ Research Topics: AI Privacy, Differential Privacy (Formal Privacy) | |
| Shenzhen University (Shenzhen, China) | Sep 2020 – Jun 2023 |
| <ul style="list-style-type: none">◦ M.S. in Software Engineering, advised by Dr. Jiaxiang Liu◦ Research Topics: Neural Network Verification (Formal Verification) | |
| Henan University (Kaifeng, China) | Sep 2016 – Jun 2020 |
| <ul style="list-style-type: none">◦ B.S. in Mathematics, advised by Dr. Zhonghua Wang◦ Major: Pure Mathematics | |





PUBLICATIONS

(1st-author then co-author; full list at Google Scholar)


Preprints:

1. AUDAGENT: Automated Auditing of Privacy Policy Compliance in AI Agents 
Ye Zheng, Yidan Hu
2. Quantifying Classifier Utility under Local Differential Privacy 
Ye Zheng, Yidan Hu
3. TraCS: Trajectory Collection in Continuous Space under Local Differential Privacy 
Ye Zheng, Yidan Hu

Conference Publications:

4. [PETS'25] Optimal Piecewise-based Mechanism for Collecting Bounded Numerical Data under Local Differential Privacy  | *Artifact Award Runner-up*
Ye Zheng, Sumita Mishra, and Yidan Hu
5. [PETS'25] Locally Differentially Private Frequency Estimation via Joint Randomized Response 
Ye Zheng, Shafizur Rahman Seeam, Yidan Hu, Rui Zhang, and Yanchao Zhang
6. [FSE'22 Demonstrations] MpBP: Verifying Robustness of Neural Networks with Multi-path Bound Propagation 
Ye Zheng, Jiaxiang Liu, and Xiaomu Shi
7. [JOS'22] (in Chinese) Multi-path Back-propagation Method for Neural Network Verification 
Ye Zheng, Xiaomu Shi, and Jiaxiang Liu

8. [CNS'24] Multi-sensor Data Privacy Protection with Adaptive Privacy Budget for IoT Systems 
Xinyi Liu, Ye Zheng, Zhengxiong Li, and Yidan Hu

9. [SAS'23] Boosting Multi-neuron Convex Relaxation for Neural Network Verification 
Xuezhou Tang, Ye Zheng, and Jiaxiang Liu

SELECTED AWARDS

Outstanding Graduate , Shenzhen University	Jun 2023
National Scholarship , Ministry of Education, China	Sep 2022

ACADEMIC SERVICES

Reviewer: TASE'24, and SAS'24