Wenjie Qu
Email: wen_jie_qu@outlook.com

EDUCATION

National University of Singapore 2023.8-
Ph.D. student in Computer Science Advisor: Prof. Jiaheng Zhang
Huazhong University of Science and Technology 2019.9-2023.6
B.E. in Automation

PUBLICATIONS

Total Citations: **576**, Google Scholar Link

[1] **W. Qu***, Y. Guo*, Y. Ying, J. Zhang. "VerfCNN, A Zero-Knowledge Proof System for Convolutional Neural Network inference with Optimal Complexity" in *IEEE Symposium on Security and Privacy (**SP**), 2026*

[2] S. Zhai, J. Li, Y. Liu, H. Chen, Z. Tian, **W. Qu**, Q. Shen, R. Jia, Y. Dong, J. Zhang. "Prompt Inversion Attack against Collaborative Inference of Large Language Models" in *International Conference on Computer Vision (**ICCV**), 2025*

[3] **W. Qu**, Y. Zhou, Y. Wu, T. Xiao, B. Yuan, Y. Li, J. Zhang. "Prompt Inversion Attack against Collaborative Inference of Large Language Models" in *IEEE Symposium on Security and Privacy(**SP**), 2025*

[4] C. Li, P. Zhu, Y. Li, C. Hong, **W. Qu**, J. Zhang. "HyperPianist: Pianist with Linear-Time Prover and Logarithmic Communication Cost" in *IEEE Symposium on Security and Privacy(**SP**), 2025*

[5] **W. Qu**, Y. Sun, X. Liu, T. Lu, Y. Guo, K. Chen, J. Zhang. "zkGPT: An Efficient Non-interactive Zero-knowledge Proof Framework for LLM Inference" in *USENIX Security (**SEC**), 2025*

[6] **W. Qu**, W. Zheng, T. Tao, D. Yin, Y. Jiang, Z. Tian, W. Zou, J. Jia, J. Zhang. "Provably Robust Multi-bit Watermarking for AI-generated Text " in *USENIX Security (**SEC**), 2025*

[7] Y. Guo, X. Liu, K. Huang, **W. Qu**, W. Zheng, T. Tao, D. Yin, Y. Jiang, T. Tao, J. Zhang. "DeepFold: Efficient Multilinear Polynomial Commitment from Reed-Solomon Code and Its Application to Zero-knowledge Proofs" in *USENIX Security (**SEC**), 2025*

[8] **W. Qu**, J. Jia, N. Gong. "REaaS: Enabling Adversarially Robust Downstream Classifiers via Robust Encoder as a Service" in *Network and Distributed System Security (**NDSS**), 2023*

[9] **W. Qu***, Y. Li*, B. Wang. "A Certified Radius-Guided Attack Framework to Image Segmentation Models" in *IEEE European Symposium on Security and Privacy (**EuroSP**), 2023*

[10] J. Wang, **W. Qu**, Y. Rong, H. Qiu, Q. Li, Z. Li, C. Zhang. "MPass: Bypassing Learning-based Static Malware Detectors" in *Design Automation Conference (**DAC**), 2023*

[11] J. Jia*, **W. Qu***, and N. Gong. "MultiGuard: Provably Robust Multi-label Classification against Adversarial Examples" in *Advances in Neural Information Processing Systems (**NeurIPS**), 2022, **Spotlight***

[12] H. Wang*, **W. Qu***, G. Katz, W. Zhu, Z. Gao, H. Qiu, J. Zhuge, and C. Zhang. "jTrans: Jump-Aware Transformer for Binary Code Similarity Detection" in *International Symposium on Software Testing and Analysis (**ISSTA**), 2022*

[13] H. Liu*, J. Jia*, **W. Qu**, and N. Gong. "EncoderMI: Membership Inference against Pre-trained

Encoders in Contrastive Learning" in *ACM Conference on Computer and Communications Security (**CCS**), 2021*

ACADEMIC SERVICE

Program Committee
- CCS 2025, 2026

Workshop Organizer
- ICLR 2025 Workshop on Foundation Models in the Wild

Journal Reviewer
- IoT-J, TIFS, TDSC, JSS.

Reviewer
- ICML 2022, MM 2024, NeurIPS 2025, COLM 2025

Sub-Reviewer
- PKC 2024

INVITED TALKS

Towards LLM auditing, Peking University	2025.7
Zero-knowledge proofs and its applications, Shanghai Jiaotong University	2025.6
Towards reliable large language models, risks and solutions, Tsinghua University	2023.12
Towards reliable large language models, risks and solutions, Zhejiang University	2023.12

SELECTED AWARDS & HONORS

- **NUS President's Graduate Fellowship** 2023
- Stars of Tomorrow, Microsoft Research Asia 2023
- Outstanding Graduate, HUST 2023
- Huawei Scholarship 2022
- **National Scholarship** 2020
- Outstanding Undergraduate of Academic Performance 2020
- Merit Student 2020
- Bronze Medal, National Olympiad in Informatics Winter Camp 2018
- First Prize, National Olympiad in Informatics in Provinces 2017