

## Wenjie Qu

Email: wen\_jie\_qu@outlook.com

### EDUCATION

National University of Singapore

*Ph.D. student in Computer Science*

Huazhong University of Science and Technology

*B.E. in Automation*

2023.8-2027.6(Expected)

Advisor: Prof. Jiaheng Zhang

2019.9-2023.6

### PUBLICATIONS

- [1] **W. Qu**, Y. Sun, X. Liu, T. Lu, Y. Guo, K. Chen, J. Zhang. “ZK-GPT: An Efficient Non-interactive Zero-knowledge Proof Framework for LLM Inference” in *USENIX Security (SEC)*, 2025
- [2] **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
- [3] 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
- [4] **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
- [5] **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
- [6] 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
- [7] 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*
- [8] 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
- [9] 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

- ACM Conference on Computer and Communications Security (CCS), 2025

Journal Reviewer

- IEEE Internet of Things Journal (IoT-J), IEEE Transactions on Information Forensics and Security (TIFS)

Reviewer

- ACM International Conference on Multimedia(MM), 2024
- International Conference on Machine Learning (ICML), 2022

Sub-Reviewer

- International Conference on Practice and Theory in Public Key Cryptography (PKC), 2024

## INVITED TALKS

Towards reliable large language models, risks and solutions, Tsinghua University	2023.12
Towards reliable large language models, risks and solutions, Zhejiang University	2023.12

## HONORS & AWARDS

• <b>NUS President's Graduate Fellowship</b>	2023
• Stars of Tomorrow, Microsoft	2023
• Outstanding Graduate, HUST	2023
• Optics Valley Rising Star Scholarship	2022
• Science and Technical Innovation Scholarship	2022
• Autodriving CTF, DEFCON 29, Runner-up Winner	2021
• 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