

Juantao Zhong

Email: jzhong012@e.ntu.edu.sg

Homepage: <https://p4stry.github.io>

Google Scholar: <https://scholar.google.com/citations?user=64oGR1MAAAAJ>

Research Interests: Large Language Models for Security, Blockchain Security, Large Language Model Compliance

EDUCATION

Nanyang Technological University

Aug. 2023-Jun. 2024

Msc. in Blockchain Technology

GPA: 4.95/5.0 Awarded First Place in the Merit Award 2024

South China University of Technology (Project 985&211)

Sept. 2018-Jun. 2022

B.Eng. in Information Security

GPA: 3.63/4.0 Rank: 9/67

WORKING EXPERIENCE

City University of Hong Kong (Shenzhen Research Institute)

Sept. 2024 - Jan. 2025

Research Assistant

Supervised by Prof. Ning Liu, Prof. Daoyuan Wu

- Extending the compl-ai framework to test the compliance of Large Language Models (LLMs).

Hong Kong University of Science and Technology

Apr. 2025 – Oct. 2025

Research Assistant

Supervised by Prof. Daoyuan Wu

- Developing and maintaining an interactive web-based platform for instant trails and analytics of smart contracts.

Lingnan University

Nov. 2025 – Present

Research Assistant

Supervised by Prof. Daoyuan Wu

- Exploring methods to enhance large language models' reasoning ability for smart contract vulnerability detection.

PUBLICATIONS

Equal contribution

[1] **Juantao Zhong**[#], Daoyuan Wu[#], Ye Liu, Maoyi Xie, Yang Liu, Yi Li, and Ning Liu. **Detecting Various DeFi Price Manipulations with LLM Reasoning**. *Proceedings of the 40th IEEE/ACM International Conference on Automated Software Engineering (ASE 2025)*. (CCF-A) [Paper](#) [Artifact](#)

[2] Yufan Chen[#], Daoyuan Wu[#], **Juantao Zhong**, Zicheng Zhang, Debin Gao, Shuai Wang, Yingjiu Li, Ning Liu, Jiachi Chen, and Rocky K. C. Chang. **Rethinking and Exploring String-Based Malware Family Classification in the Era of LLMs and RAG**. *arXiv preprint arXiv:2507.04055*. (Under review as a conference paper at ICDE 2026) [Paper](#) [Artifact](#)

[3] Xu Yang[#], **Juantao Zhong**[#], Daoyuan Wu, Xiao Yi, Jimmy Lee, and Tan Lee. **Effective Online Exam Proctoring by Combining Lightweight Face Detection and Deep Recognition**. *arXiv preprint arXiv:2206.13356*. (Under review as a conference paper at PerCom 2026) [Paper](#) [Artifact](#)

TECHNICAL SKILLS

Languages: English (IELTS 7.0); Mandarin (Native)

Developer tools:

- *Programming Languages:* Python, C++, Solidity, Rust
- *Machine Learning & AI:* PyTorch, Transformers, Neural Network (ResNet), Large Language Models (LLMs), Facebook AI Similarity Search (FAISS)
- *Cybersecurity:* Kali, Burp Suite, Wireshark, CodeQL, Slither

SERVICES

Conference Sub-reviewer: ICLR 2026, AAAI 2026, NDSS 2026, USENIX Security 2026, NDSS 2025, USENIX Security 2025, CCS 2025, ISSTA 2025, and ICSE 2025

Journal Sub-reviewer: PNAS, PNAS Nexus, IEEE Transactions on Information Forensics and Security (TIFS), IEEE Transactions on Dependable and Secure Computing (TDSC), and Transactions on Pattern Analysis and Machine Intelligence (TPAMI)