WeChat: liu_zhi_bo
Phone: (852)-57499912
Email: zhiboliu@ust.hk

Zhibo Liu

PhD

Department of Computer Science and Engineering
Hong Kong University of Science and Technology
Homepage: https://monkbai.github.io

I am a postdoc researcher at the Hong Kong University of Science and Technology, supported by the **HK RGC postdoc fellowship scheme**.
I obtained my Ph.D. supervised by Prof. Shuai Wang at the Department of Computer Science and Engineering, HKUST, in 2023. Before joining HKUST, I received my B.Eng. degree from Nankai University, Tianjin, China, in 2019.
My research currently focuses on **Software Reverse Engineering**, and my research interests include **Computer Security** and **Software Engineering**.

Experience

Postdoctoral fellow, Hong Kong University of Science and Technology **10 2023 — Now**

Education

Ph.D., Hong Kong University of Science and Technology **09 2019 — 09 2023**
Bachelor of Engineering in information security, Nankai University **09 2015 — 06 2019**

Publications

1. Wang, H. *et al. Preserving Privacy in Software Composition Analysis: A Study of Technical Solutions and Enhancements* in *ICSE* (2025).
2. Peng, Y. *et al. Testing and Understanding Deviation Behaviors in FHE-hardened Machine Learning Models* in *ICSE* (2025).
3. Yuan, Y. *et al. CipherSteal: Stealing Input Data from TEE-Shielded Neural Networks with Ciphertext Side Channels* in *IEEE SP* (2025).
4. Xiao, D., Liu, Z., Peng, Y. & Wang, S. *MTZK: Testing and Exploring Bugs in Zero-Knowledge (ZK) Compilers* in *NDSS* (2025).
5. Chen, Y. *et al. Compiled Models, Built-In Exploits: Uncovering Pervasive Bit-Flip Attack Surfaces in DNN Executables* in *NDSS* (2025).
6. Chen, Y. *et al. The Devil is in the (Micro-) Architectures: Uncovering New Side-Channel and Bit-Flip Attack Surfaces in DNN Executables* in *Blackhat Europe* (2024).
7. Liu, Z. *et al. DeepCache: Revisiting Cache Side-Channel Attacks in Deep Neural Networks Executables* in *CCS* (2024).
8. Yuan, Y. *et al. HyperTheft: Thieving Model Weights from TEE-Shielded Neural Networks via Ciphertext Side Channels* in *CCS* (2024).
9. Wang, H. *et al. Are We There Yet? Filling the Gap Between ML-Based Binary* in *Euro SP* (2024).
10. Lu, H., Liu, Z., Wang, S. & Zhang, F. *DTD: Comprehensive and Scalable Testing for Debuggers* in *FSE* (2024).
11. Li, Y., Xiao, D., Liu, Z., Pang, Q. & Wang, S. *Metamorphic Testing of Secure Multi-Party Computation (MPC) Compilers* in *FSE* (2024).
12. Li, Z., Liu, Z., Wong, W. K., Ma, P. & Wang, S. *Evaluating C/C++ Vulnerability Detectability of Query-Based Static Application Security Testing Tools* in *TDSC* (2023).
13. Liu, Z. *et al. BTD: Unleashing the Power of Decompilation for x86 Deep Neural Network Executables* in *Blackhat USA* (2023).
14. Xiao, D., Liu, Z. & Wang, S. *PHYFU: Fuzzing Modern Physics Simulation Engines* in *ASE* **Distinguished Paper** (2023).
15. Liu, Z., Xiao, D., Li, Z., Wang, S. & Meng, W. *Exploring Missed Optimizations in WebAssembly Optimizers* in *ISSTA* (2023).
16. Xiao, D., Liu, Z. & Wang, S. *Metamorphic Shader Fusion for Testing Graphics Shader Compilers* in *ICSE* (2023).
17. Li, Z. *et al. CCTEST: Testing and Repairing Code Completion Systems* in *ICSE* (2023).
18. Yuan, Y., Liu, Z. & Wang, S. *CacheQL: Quantifying and Localizing Cache Side-Channel Vulnerabilities in Production Software* in *USENIX Security* (2023).
19. Liu, Z., Yuan, Y., Wang, S., Xie, X. & Ma, L. *Decompiling x86 Deep Neural Network Executables* in *USENIX Security* (2023).
20. Jiang, K., Bao, Y., Wang, S., Liu, Z. & Zhang, T. *Cache Refinement Type for Side-Channel Detection of Cryptographic Software* in *CCS* (2022).
21. Liu, Z., Yuan, Y., Wang, S. & Bao, Y. *SoK: Demystifying Binary Lifters Through the Lens of Downstream Applications* in *Symposium on Security and Privacy (SP)* (2022), 453–472.
22. Xiao, D., Liu, Z., Yuan, Y., Pang, Q. & Wang, S. Metamorphic Testing of Deep Learning Compilers. *SIGMETRICS* (2022).
23. Ma, P., Liu, Z., Yuan, Y. & Wang, S. NeuralD: Detecting Indistinguishability Violations of Oblivious RAM with Neural Distinguishers. *T-IFS* (2022).
24. Wang, H. *et al.* Enhancing DNN-Based Binary Code Function Search With Low-Cost Equivalence Checking. *TDSC* (2022).
25. Liu, Z. & Wang, S. *How Far We Have Come: Testing Decompilation Correctness of C Decompilers* in *ISSTA* (2020).

Awards & Honors

2023 HK RGC Postdoctoral Fellowship Scheme (HK$1.2 million over 36 months)
2023 HKUST CSE Best PhD Dissertation Award - Honorable Mention
2023 ACM SIGSOFT **Distinguished Paper Award** at ASE 2023
2023 Black Hat USA Speaker Honorarium
2022 HKUST Research Travel Grant
2022 HKUST RedBird Academic Excellence Award
2019 China National Cyber Security Scholarship

Professional Service

Reviewer	2023	T-IFS, TDSC
AE Committee	2023	USENIX Security
	2022	OSDI, USENIX ATC, ISSTA, WiSec
External Reviewer	2024	USENIX Security, IEEE S&P
	2023	USENIX Security, IEEE S&P, ISSTA, NeurIPS, SANER ERA Track
	2022	ASE, NDSS BAR, CCS, AsiaCCS
	2020	TIFS, ICICS, ICSE SEIP