Computer Science and
Technology Building 706
Email: zhiboliu@nju.edu.cn

Zhibo Liu

Associate Professor

School of Computer Science
Nanjing University
Homepage: https://monkbai.github.io

Zhibo Liu is an Associate Professor in the School of Computer Science at Nanjing University. Previously, he was a Postdoctoral Researcher at the Hong Kong University of Science and Technology (HKUST) from 2023 to 2025, supported by the HK RGC Postdoctoral Fellowship Scheme. He obtained his Ph.D. in 2023 from the Department of Computer Science and Engineering at HKUST, under the supervision of Prof. Shuai Wang. Before joining HKUST, he received his B.Eng. degree from Nankai University in 2019. His current research focuses on **software reverse engineering**, with broader interests in **computer security** and **software engineering**.

Experience

Associate Professor, Nanjing University — **01 2026 — now**
Postdoctoral Fellow, Hong Kong University of Science and Technology — **10 2023 — 12 2025**

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. Liu, Z., Wang, H., Wong, W. K., Wu, D. & Wang, S. *No More Translation at Runtime: LLM-Empowered Static Binary Translation* in *EuroSys* (2026).
2. Deng, S., Liu, Z., Wang, S. & Zhang, Y. *An Empirical Study Measuring In-The-Wild Cryptographic Microarchitectural Side-Channel Patches* in *CCS* (2025).
3. Xiao, D. *et al. Divergence-aware Testing of Graphics Shader Compiler Back-ends* in *PLDI* (2025).
4. Wong, W. K. *et al. DecLLM: LLM-Augmented Recompilable Decompilation for Enabling Programmatic Use of Decompiled Code* in *ISSTA* (2025).
5. Wang, H. *et al. Preserving Privacy in Software Composition Analysis: A Study of Technical Solutions and Enhancements* in *ICSE* (2025).
6. Peng, Y. *et al. Testing and Understanding Deviation Behaviors in FHE-hardened Machine Learning Models* in *ICSE* (2025).
7. Yuan, Y. *et al. CipherSteal: Stealing Input Data from TEE-Shielded Neural Networks with Ciphertext Side Channels* in *IEEE SP* (2025).
8. Xiao, D., Liu, Z., Peng, Y. & Wang, S. *MTZK: Testing and Exploring Bugs in Zero-Knowledge (ZK) Compilers* in *NDSS* (2025).
9. Chen, Y. *et al. BitShield: Defending Against Bit-Flip Attacks on DNN Executables* in *NDSS* (2025).
10. Chen, Y. *et al. Compiled Models, Built-In Exploits: Uncovering Pervasive Bit-Flip Attack Surfaces in DNN Executables* in *NDSS* (2025).
11. 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).
12. Liu, Z. *et al. DeepCache: Revisiting Cache Side-Channel Attacks in Deep Neural Networks Executables* in *CCS* (2024).
13. Yuan, Y. *et al. HyperTheft: Thieving Model Weights from TEE-Shielded Neural Networks via Ciphertext Side Channels* in *CCS* (2024).
14. Wang, H. *et al. Are We There Yet? Filling the Gap Between ML-Based Binary* in *Euro SP* (2024).
15. Lu, H., Liu, Z., Wang, S. & Zhang, F. *DTD: Comprehensive and Scalable Testing for Debuggers* in *FSE* (2024).
16. Li, Y., Xiao, D., Liu, Z., Pang, Q. & Wang, S. *Metamorphic Testing of Secure Multi-Party Computation (MPC) Compilers* in *FSE* (2024).
17. 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).
18. Liu, Z. *et al. BTD: Unleashing the Power of Decompilation for x86 Deep Neural Network Executables* in *Blackhat USA* (2023).
19. Xiao, D., Liu, Z. & Wang, S. *PHYFU: Fuzzing Modern Physics Simulation Engines* in *ASE (***Distinguished Paper***)* (2023).
20. Liu, Z., Xiao, D., Li, Z., Wang, S. & Meng, W. *Exploring Missed Optimizations in WebAssembly Optimizers* in *ISSTA* (2023).
21. Xiao, D., Liu, Z. & Wang, S. *Metamorphic Shader Fusion for Testing Graphics Shader Compilers* in *ICSE* (2023).
22. Li, Z. *et al. CCTEST: Testing and Repairing Code Completion Systems* in *ICSE* (2023).
23. Yuan, Y., Liu, Z. & Wang, S. *CacheQL: Quantifying and Localizing Cache Side-Channel Vulnerabilities in Production Software* in *USENIX Security* (2023).
24. Liu, Z., Yuan, Y., Wang, S., Xie, X. & Ma, L. *Decompiling x86 Deep Neural Network Executables* in *USENIX Security* (2023).
25. Jiang, K., Bao, Y., Wang, S., Liu, Z. & Zhang, T. *Cache Refinement Type for Side-Channel Detection of Cryptographic Software* in *CCS* (2022).
26. 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.

27. Xiao, D., Liu, Z., Yuan, Y., Pang, Q. & Wang, S. Metamorphic Testing of Deep Learning Compilers. *SIGMETRICS* (2022).
28. Ma, P., Liu, Z., Yuan, Y. & Wang, S. NeuralD: Detecting Indistinguishability Violations of Oblivious RAM with Neural Distinguishers. *T-IFS* (2022).
29. Wang, H. *et al.* Enhancing DNN-Based Binary Code Function Search With Low-Cost Equivalence Checking. *TDSC* (2022).
30. Liu, Z. & Wang, S. *How Far We Have Come: Testing Decompilation Correctness of C Decompilers* in *ISSTA* (2020).

Awards & Honors

2025 IEEE S&P **Distinguished Paper Award**
2024 Black Hat Europe Speaker Honorarium
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

Program Committee	CCS	2026
Reviewer	TDSC	2023, 2024, 2025
	TIFS	2023, 2025
AE Committee	Security	2023
	OSDI	2022
	ATC	2022
	ISSTA	2022