

# Xin Zhang, Ph.D.

✉ zhangxin00@stu.pku.edu.cn

🌐 LinkedIn

🌐 <https://zhangxin00.github.io/>



## Education

- 2022 – present **Ph.D., Peking University**, Software Engineering (Cybersecurity).  
Advisor: Prof. Qingni Shen
- 2024 – present **Research Assistant, National University of Singapore**.  
Advisor: Prof. Trevor Carlson
- 2018 – 2022 **B.Sc., Hunan University**, Information Security.  
Thesis title: *Research on analysis and optimization technology of vehicle operating system permission management model*.  
Advisor: Prof. Jiliang Zhang

## Research Publications

### Conference Proceedings (7 CCF-A)

- 1 **X. Zhang**, J. Zou, Y. Yang, *et al.*, “LeakyDSP: Exploiting digital signal processing blocks to sense voltage fluctuations in fpgas,” in *ACM/IEEE Design Automation Conference*, 2025.
- 2 **X. Zhang**, J. Zou, Y. Yang, *et al.*, “AmpereBleed: Exploiting on-chip current sensors for circuit-free attacks on arm-fpga socs,” in *ACM/IEEE Design Automation Conference*, 2025.
- 3 **X. Zhang**, Z. Zhang, Q. Shen, *et al.*, “SegScope: Probing fine-grained interrupts via architectural footprints,” in *IEEE International Symposium on High-Performance Computer Architecture (HPCA)*, 2024, pp. 424–438.
- 4 **X. Zhang**, Z. Zhang, Q. Shen, *et al.*, “ThermalScope: A practical interrupt side channel attack based on thermal event interrupts,” in *ACM/IEEE Design Automation Conference*, 2024.
- 5 J. Liang, **X. Zhang**, D. Hu, *et al.*, “ZK-Hammer: Leaking secrets from zero-knowledge proofs via rowhammer,” in *ACM/IEEE Design Automation Conference*, 2025.
- 6 J. Liang, Z. Zhang, **X. Zhang**, *et al.*, “Achilles: A formal framework of leaking secrets from signature schemes via rowhammer,” in *Usenix Security*, 2025.
- 7 W. Chen, Z. Zhang, **X. Zhang**, *et al.*, “HyperHammer: Breaking free from kvm-enforced isolation,” in *International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2025.


## Skills

- Languages **Strong** reading, writing and speaking competencies for English and Mandarin Chinese.
- Coding **Strong** C/C++, Python, Verilog/VHDL,  $\LaTeX$ , ...
- Misc. **Strong** Academic research, teaching, training,  $\LaTeX$  typesetting and publishing.

## Miscellaneous Experience

---

### Awards and Achievements

- 2024  **First Prize of Science and Technology Progress Award**, Chinese Institute of Electronics.
- 2022  **Runner-up (2/3304) in ECS CloudBuild Developer Competition**, Alibaba Cloud.
-  **College Graduate Excellence Award**, Hunan Province, China
- 2019  **National Scholarship**, China.