Xuanyao Peng

☎ +86 199 5080 8841 | ✉ pengxuanyao23s@ict.ac.cn

Education

University of Chinese Academy of Sciences **Sep 2023 – Present**

- State Key Laboratory of Processors, Institute of Computing Technology, Chinese Academy of Sciences, supervised by Professor Hang Lu.
- M.Eng. in Computer Technology, GPA: 3.86/4.0
- **National Scholarship** (2025), Outstanding Graduate Student Award

Xi'an Jiaotong University **Sep 2019 – Jun 2023**

- B.Eng. in Automation, GPA: 3.97/4.3
- **National Scholarship**(2022)

Experience and projects

SecNPU Project Sep 2024 – Aug 2025

- The project focuses on protecting LLM inference on CPU-NPU collaborative systems. SecNPU introduces a unified security metadata and leverages the memory-access characteristics of different inference stages to eliminate security overhead.
- Published a paper at International Conference on Computer Design (ICCD) 2025: "SecNPU: Securing LLM Inference on NPU."

Secretflow Cup Confidential Computing Challenge Jul 2025 – Aug 2025

- Developed MotarTEE, a secure and efficient solution for LLM inference within Confidential VMs (Intel TDX), by implementing end-to-end remote attestation, encrypted operators, and full-process data protection to ensure user's privacy and parameter's confidentiality.
- Awarded second prize in the competition. (3/320)

RISC-V CPU Security Enhancement Mar 2023 – Jun 2024

- Extended the Xiangshan (simulator and hardware) with SPMP and PMP-Table security extensions[github repo], successfully booting the Penglai trusted execution environment(TEE) on Xiangshan core to prove S-mode memory isolation.
- The Xiangshan Nanhu-V3a chip taped out successfully on first pass and booted a highly scalable TEE.

Intel Cup National Undergraduate Electronics Design Contest Apr 2022 – Aug 2022

- Designed and optimized an emotion-recognition and learning-state analysis system for edge devices. Fine-tuned lightweight emotion-recognition models and deployed the system using quantization and pruning techniques.
- Achieved second prize at the national level. (Top 5%)

Publications

Pan, Shangjie, **Xuanyao Peng**, Zeyuan Man, Xiquan Zhao, Dongrong Zhang, Bicheng Yang, Dong Du, Hang Lu, Yubin Xia, and Xiaowei Li (2025). "Dep-TEE: Decoupled Memory Protection for Secure and Scalable Inter-enclave Communication on RISC-V". In: *Proceedings of the 30th Asia and South Pacific Design Automation Conference*, pp. 454–460.

Pan, Shangjie, Yinghao Yang, **Xuanyao Peng**, Xiquan Zhao, Dong Du, Hang Lu, Yubin Xia, and Xiaowei Li (2025). “LayerTEE: Decoupled Memory Protection for Scalable Multi-Layer Communication on RISC-V”. In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.*

Peng, **Xuanyao**, Shangjie Pan, Yinghao Yang, Huang Junjie, Liang Yujun, Hang Lu, Zhang Fengwei, and Xiaowei Li (2025). “SecNPU: Securing LLM Inference on NPU”. In: *To appear in the Proceedings of the 43rd IEEE International Conference on Computer Design (ICCD 2025).*

Others

Programing Languagues	C/C++, Verilog, Python, Rust
English	CET-6 (554), TOEFL iBT (in preparation)