彭宣尧

(+86) 199-5080-8841 · pengxuanyao23s@ict.ac.cn

教育背景

中国科学院大学, 电子信息, *在读硕士研究生* 导师：路航[主页] 2023.9 - 至今

GPA 3.86/4.0 处理器芯片全国重点实验室, 计算技术研究所
获奖情况：国家奖学金 (2025), 中国科学院大学学业奖学金 (2 次), 三好学生 (2 次), 优秀学生干部
突出课程：计算机体系结构 95, VSLI 设计基础 95, 高级操作系统 94

西安交通大学, 自动化, *工学学士* 2019.9 - 2023.6

GPA 3.97/4.3 排名 5/182(前 3%)
获奖情况：国家奖学金 (2022), 感恩中国近现代科学家奖学金, 校优秀毕业生, 优秀学生干部
突出课程：数字逻辑电路 98, 模拟电路 100, 电路 100, 微机原理与嵌入式 94

实习经历

北京开源芯片研究院 | 实习生 | 开发 RTL 和移植系统软件 2023.3-2024.9

- **描述**：开发香山可信执行环境系统（“香山 TEE 1.0”），增强香山处理器核的安全能力。[github repo]
- **职责**：在硬件和模拟器上开发新安全功能 SPMP 和 PMPTable，以及相关的测试和验证工作。
- **成果**：在**南湖 v3a 一次流片成功**，其中集成了 SPMP 硬件功能，并成功启动 30 个 Enclave（大于 PMP 个数），证明了高可拓展性；在香山**主线中合入了 PMPTable 功能**，支持基于该功能进一步开发。

西安交大人工智能与机器人研究所 | 实习生 | 开发 RTL 2021.10-2022.5

- **描述**：针对机器人建图过程中的 **SLAM 算法进行加速**，基于 FPGA 硬件进行设计，加入**并行 Padding 和非极大值抑制硬件加速**实现高效的图像预处理。
- **职责**：开发 FPGA 的 Verilog 代码，FPGA 模块的仿真和验证。
- **成果**：完成相关模块 Verilog 代码。

项目经历

蚂蚁集团“隐语杯”隐私计算大赛 | 队长 2025.6-2025.9

- **描述**：赛题“密态大模型推理的隐私保护”——在 Intel TDX 机密虚拟机中部署大语言模型的推理服务，保证安全和性能的平衡。
- **职责**：1. 提升推理框架性能，提高约 **50%(11 tokens/s) 的性能**；2. 部署**远程证明机制**，对推理框架和平台进行验证；3. 设计**全链加密机制**，对用户数据和模型参数进行保护。
- **成果**：获**全国二等奖**（第三名）（获奖新闻）

SecNPU 项目 | 论文一作 2024.9-2025.6

- **描述**：论文题目为”SecNPU: Securing LLM inference on NPU”，该项目对 NPU 可信执行环境（TEE）中的性能问题进行优化，针对大模型推理应用设计安全高效的系统级 NPU TEE。
- **职责**：研究 NPU TEE 中的通信开销和计算瓶颈，进行优化：设计统一安全元数据，减少冗余的元数据生成开销；通过利用大模型 prefill 阶段计算密集型特点，利用闲置的传输带宽掩盖通信开销。
- **成果**：以**第一作者完成一篇 International Conference on Computer Design (ICCD)（CCF-B）**论文

英特尔杯 2022 年全国大学生电子设计大赛 | 参赛队员 2022.3-2022.6

- **描述**：大赛主题为人工智能与边缘计算，自选题为基于**多模态情感分析的学习状态评估系统**。包括建立情感分析模型，基于英特尔的边缘计算设备，设计疫情期间分析网课学生学习状态的实时系统。
- **职责**：1. 采用多模态信息，包括语音、视频和环境信息等；2. 微调情感分析模型，使其实用于学生网课学习场景；3. 对状态进行全过程的分析，进行信号处理，消除噪声干扰。
- **成果**：获**全国二等奖**（获奖名单）

论文发表情况

[1] Shangjie Pan, **Xuanyao Peng**, Zeyuan Man, Xiquan Zhao, Dongrong Zhang, Bicheng Yang, Dong Du, Hang Lu, Yubin Xia, and Xiaowei Li. “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 (ASP-DAC)*. 2025, pp. 454–460.

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

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

其他竞赛获奖/实践经历

- 2021 年全国大学生电子设计大赛**省三等奖**，2022 年陕西省工科校际电子设计联赛**一等奖**，2022 年蓝桥杯嵌入式赛道全**国三等奖**
- 助教工作：2025 开源 RVGPU 课程, RIOS Lab, 清华伯克利深圳学院 (课程资料)
- 英语：CET6（554）编程语言: C/C++, Verilog, Python, Rust