刘昶旭

(+86) 13585972865 · liucx22@m.fudan.edu.cn · https://austinliu01.github.io/

教育背景

复旦大学, 微电子学院，电子科学与技术, 博士 2022.9 - 2027.6

导师：杨帆教授 研究方向：隐私保护计算；AI 算法硬件加速；SoC 设计

武汉大学, 弘毅学堂（荣誉学院）, 微电子科学与工程, 本科 2018.9 - 2022.6

GPA: 3.88/4.00, 集创赛全国一等奖，甲等/一等奖学金，优秀团员/三好学生，学院优秀毕业生

学术及项目经历

针对多标量乘法 MSM 的算法及调度机制优化 2023.03-2023.08

- 针对零知识证明中计算复杂度极高的多标量乘法，通过提出优先级调度机制和并行桶聚合算法加速 MSM 的实现，设计空间探索和 ATP 优化使架构相比定制硬件提升 10.9 倍，较 GPU 提升 3.9 倍。
- 研究成果发表在 ACM TODAES (第一作者,CCF-B 期刊)

针对多 MSM 场景下的硬件加速架构设计 2023.06-2024.05

- 我们提出了两种灵活架构，Gypsophila 和 Myosotis，用于更大规模的多 MSM 任务并行计算，提升计算效率。Gypsophila 通过平衡桶算法步骤的吞吐量和数据流优化，利用共享输入通道和后处理单元提高资源利用率，减少 7.8% 的面积。Myosotis 在 Gypsophila 基础上优化缓存模块设计和调度机制，降低带宽需求，较 FPGA 和 ASIC 加速 3.32 倍和 6.72 倍，并支持灵活配置计算核心和缓存的数量，带来更高的 ATP 表现。
- 研究成果分别发表在 **DAC 2024 (第一作者，CCF-A 会议)** 和 **IEEE TCAD (第一作者,CCF-A 期刊)**。

针对 MDC 型结构的快速数论变换 NTT 硬件加速器设计 2023.11-2024.02

- 针对后量子密码学和全同态加密中的多项式乘法，优化了 NTT 运算。通过四步 NTT 算法和流水线转置模块，提高了效率和可扩展性。MDC 结构优化的 PE 减少数据冲突，模乘模块降低资源使用并提升频率。与最新流水线架构相比，面积时间积减少了 2.34 倍和 1.26 倍。
- 研究成果分别发表在 GLSVLSI (第一作者，CCF-C 会议)。

针对哈希及 Merkle Tree 计算的硬件加速器设计及资源利用率优化 2024.08-2024.12

- 针对 zk-STARK 方案中计算密集型 Hash 和 Merkle Tree 的优化，我们设计了一个面积高效的硬件加速架构。通过对哈希数据流的调度优化和融合，输入数据流的流水线处理，以及层次化存储结构设计，提高了硬件资源利用率并显著降低了缓存需求。与未优化设计相比，整体面积减少了约 13.9%。此外，与软件实现相比，最大加速可达 1665 倍。
- 研究成果分别发表在 **DAC 2025 (第一作者，CCF-A 会议)**。

基于 Coretx-M 系列处理器的 SoC 设计 2024.11-至今

- 基于 Cortex-M4 处理器, 面向 ASIC 开发低功耗 SoC。硬件部分包括 AMBA 总线协议下的外设、DMA、定制矩阵乘法等子系统模块开发，并在 Xilinx FPGA 平台上进行硬件验证，基于 TSMC 28nm 工艺进行综合评估；软件部分涉及驱动代码开发、FreeRTOS 系统移植，并使用 Keil 进行整体调试。
- 该项目主体已完成，目前正在进行低功耗设计优化。

实习经历

蚂蚁集团 | 蚂蚁技术研究院, 研究实习生 2023.08-2024.01

- 调研全同态加密算法及领域现有的加速器工作，向公司提交了 42 页的针对加速器的调研报告。
- 针对快速数论变换 NTT 进行基于 FPGA 的加速器研究，研究成果发表在 GLSVLSI 2024 (CCF-C)。

中昊芯英科技有限公司, 数字芯片设计工程师实习生 2021.10-2022.04

- 参与低功耗 SoC 的设计，该 SoC 用于启动，监控和配置公司的大型 AI 训练芯片。
- 设计及维护 CSR Ring 模块，存储模块；调试负责的 SoC 系统；提交两项发明专利（已授权）。