

周报 - 第三篇论文性能分析完成

2025-08-12

概述

本周研究摘要

本周成功完成第三篇论文《Thread-Adaptive: High-Throughput Parallel Architectures of SLH-DSA on GPUs》的核心修订任务4:

- 完成性能分解分析实验: 量化 ATA 技术 11.7% 吞吐量提升和 FLP 技术额外 3.5% 性能增益
- 完成分析方法学准确性讨论: 回应审稿意见 p1.1、p2.2 和 p3.1 的技术关切

论文回复

定量性能分解结果 p1.1

通过系统性实验设计，成功量化了自适应线程分配（ATA）和函数级并行（FLP）两种核心技术的独立贡献：

基准性能： Wang et al. 2025 实现 → 53,804 tasks/sec

ATA 技术贡献：

- 吞吐量提升至 60,127 tasks/sec
- 性能改进：+11.7% (增益 6,323 tasks/sec)

定量性能分解结果 p1.1

FLP 技术贡献:

- 最终吞吐量达到 62,239 tasks/sec
- 额外性能提升: +3.5% (增益 2,112 tasks/sec)
- 综合性能改进: +15.7%

架构创新必要性 p2.2

明确展示了后量子密码学实现中架构创新的关键作用：

传统方法局限性：

- 未经优化的实现无法满足实际部署需求
- 传统并行化方法存在根本性限制

专门化架构优势：

- 只有通过系统性架构设计才能实现实用级别性能

测量可靠性验证 p3.1

针对审稿意见 p3.1 关于基于剖析的性能模型准确性关切，提供全面验证：

统计可靠性指标：

- 20 次重复测量 + 中位数绝对偏差离群值过滤
- 交叉验证：91.3% 预测准确率 ($\pm 10\%$ 范围内)
- 样本外测试：87.6% 线程数预测准确性

总结

修订进展状态

已完成核心修订:

- 性能分解分析实验成果 ✓
- 分析方法学准确性讨论 ✓
- 审稿意见 p1.1、p2.2 和 p3.1 技术回应 ✓

下周最终任务:

- GPU 硬件级性能剖析工作
- 审稿意见 p1.2、p2.3 和 p3.2 技术回应
- 完成第三篇论文全部修订要求并准备重新提交

总结

老师评语

继续推进完成审稿意见回复

抓紧推进