周报

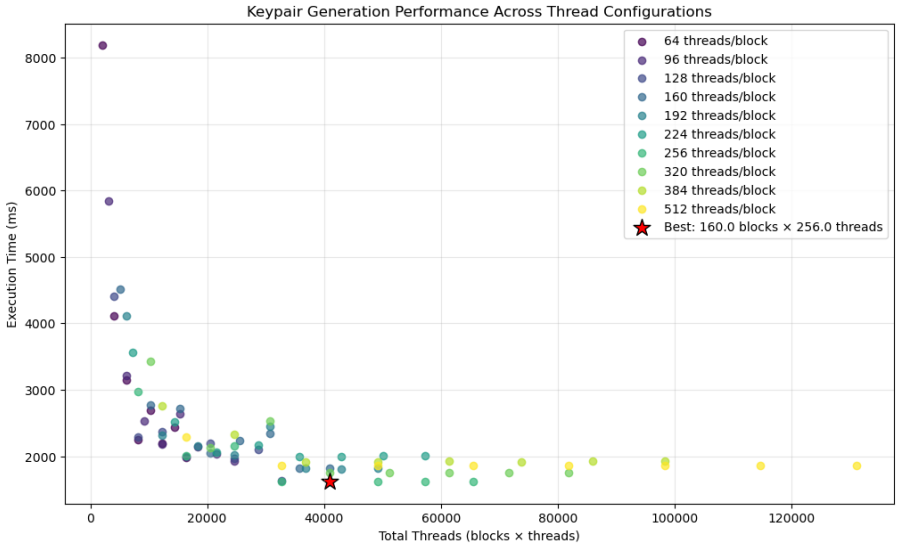
2025 年 3 月 25 日

本周主要工作

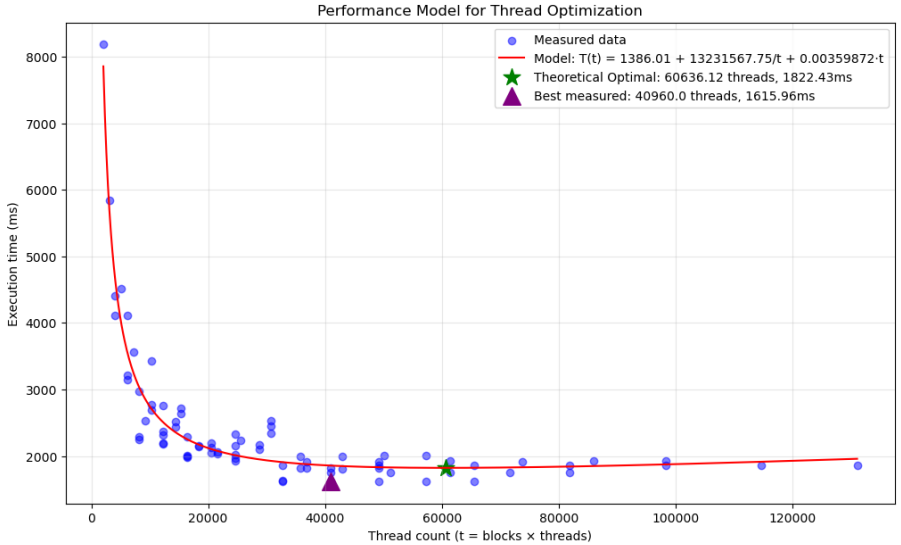
摘要

- 完成自适应线程分配（ATA）方法的实验验证与扩展应用
- 将 ATA 从公钥生成扩展至签名过程，实现 17.4% 性能提升
- 完成包含 ATA 和函数级并行两个核心组件的优化架构图设计

线程数与性能分析



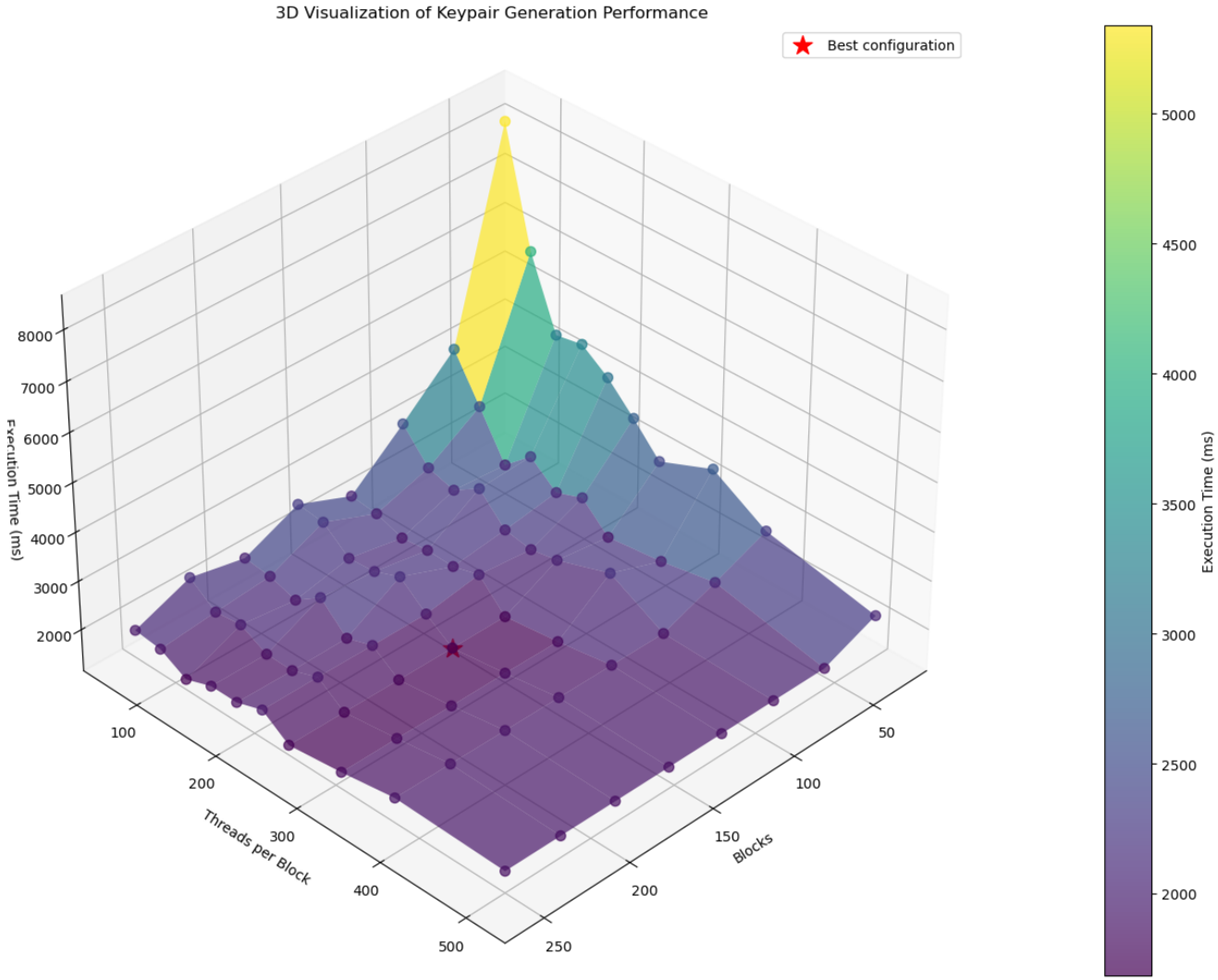
block 和 thread 配置下的性能对比



性能函数拟合曲线

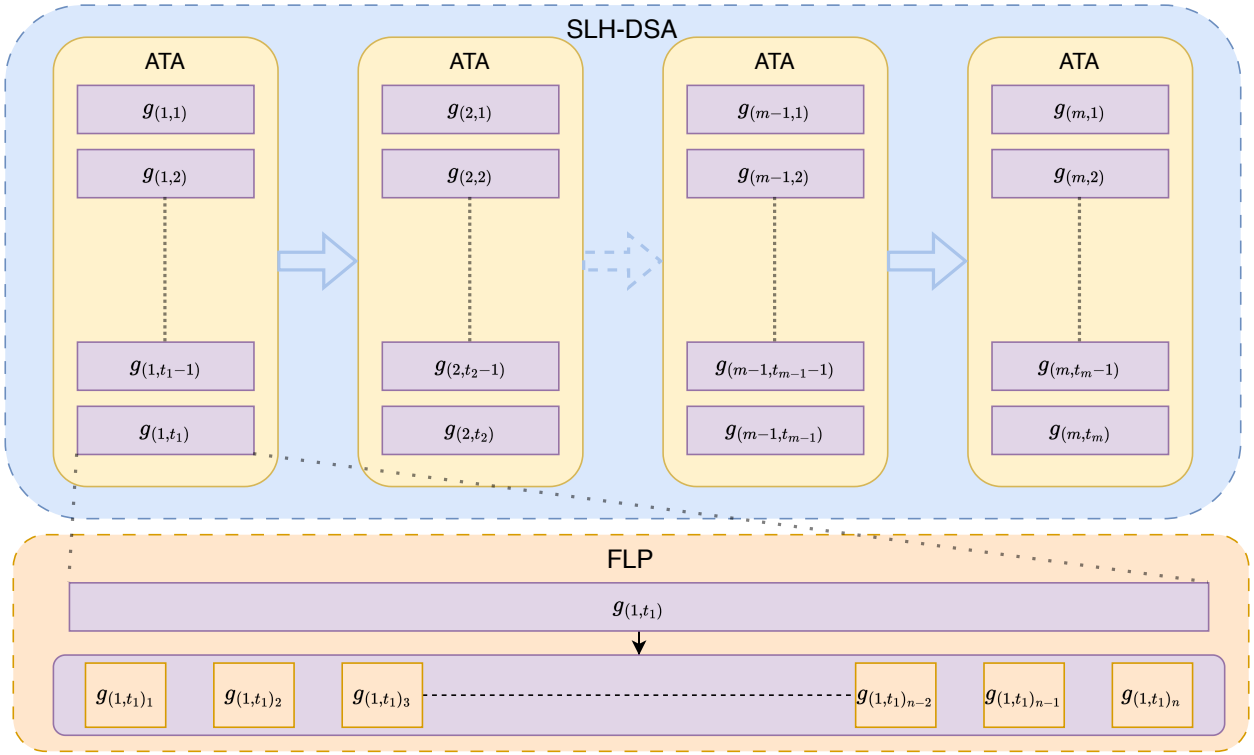
- 系统性测试了 8 种 block 数量 (32-256) 和 10 种 thread 数量 (64-512)
- 通过函数拟合成功预测最优线程配置
- 签名处理时间从 0.0605 秒 [WDC+25] 降至 0.0493 秒，提升 17.4%

Thread 与 Block 配置优化



- 固定总并行度条件下，分析 block 和 thread 比例对性能的影响
- 每个 block 包含 256 个 threads 时达到最佳性能

优化架构设计



- 优化架构：
  - 自适应线程分配（Adaptive Thread Allocation, ATA）
  - 函数级并行（Function-Level Parallelism, FLP）
- 作为论文核心图表，清晰传达优化方法论

老师评语

论文的写作进展慢，还有就是写作语言很多没用书面正式语

参考 trans 短报论文，对写作进行优化

下周计划

1. 开始论文实验章节书写
2. 完善创新点 2，函数级并行优化

参考文献

Ziheng Wang, Xiaoshe Dong, Heng Chen, Yan Kang, and Qiang Wang.
Cuspx: Efficient gpu implementations of post-quantum signature sphincs⁺.
IEEE Transactions on Computers, 74(1):15–28, 2025.