周报

2025 年 4 月 2 日

大纲

1. 论文实验

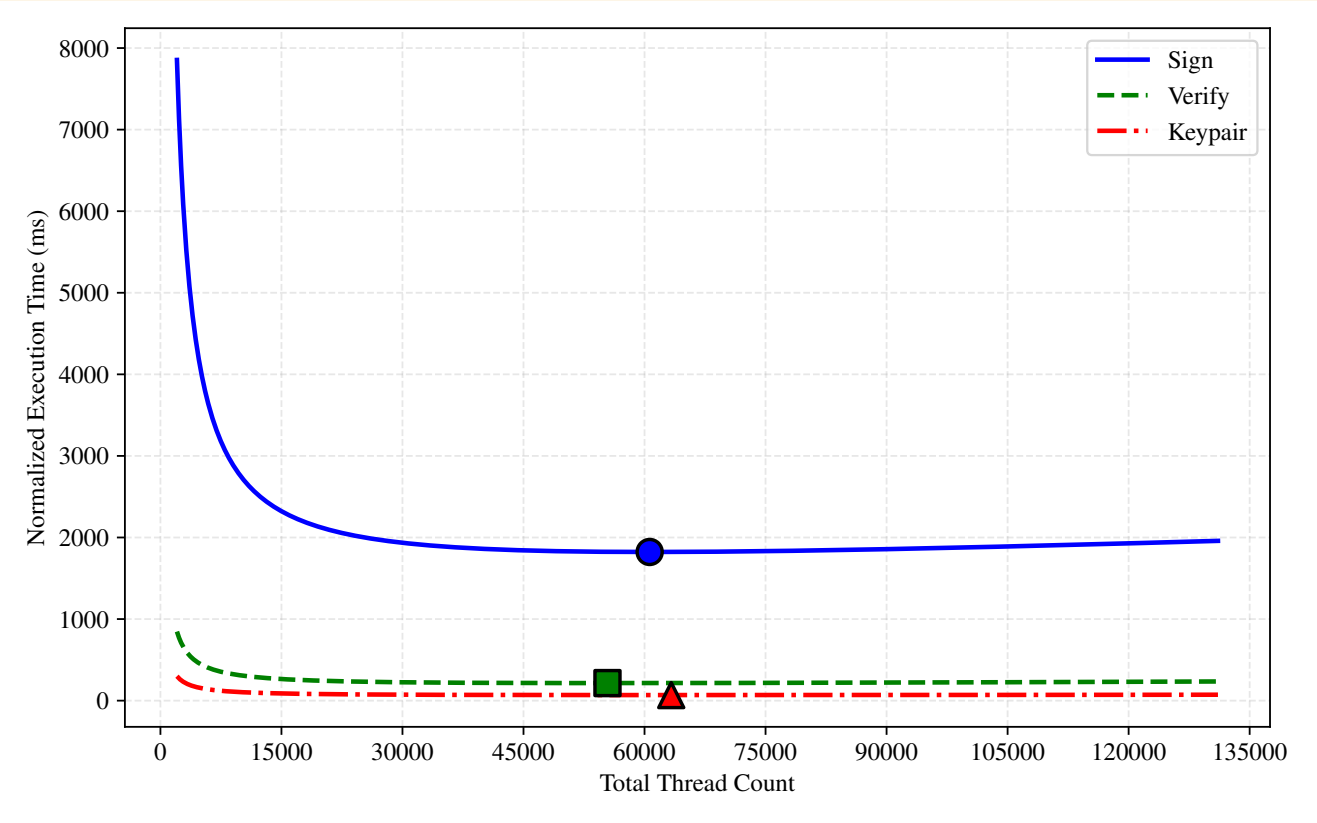
2. 论文写作

自适应线程分配实验

实验结果

相比 [WDC+25] 的基准实现，我们的优化方案：

- 签名生成阶段：性能提升20%
- 在资源密集型操作（如哈希计算）中效果尤为明显



口语化表达修正

语言调整

我们对论文进行了全面的语言风格优化，主要包括：将一般性描述替换为更精确的专业术语，优化句法结构以消除冗余表达，重构段落组织以确保逻辑连贯，采用学术写作规范的被动语态，以及精炼图表说明文字。

```
SLH-DSA is a stateless hash-based signature
scheme that delivers post-quantum security
through a hierarchical certification
structure. The signature generation process
relies on three main components:
SLH-DSA represents a stateless hash-based
signature scheme that provides post-quantum
security through hierarchical certification
architecture. The signature generation
mechanism comprises three fundamental
components:
```

实验章节框架设计

基于 NVIDIA RTX 4090 GPU 的硬件平台配置与 NIST 标准参数集的实验环境设置。

实验章节框架设计

基于 NVIDIA RTX 4090 GPU 的硬件平台配置与 NIST 标准参数集的实验环境设置。

通过精确测量各组件执行时间定量评估 ATA 算法对密码学核心函数的优化贡献。

实验章节框架设计

基于 NVIDIA RTX 4090 GPU 的硬件平台配置与 NIST 标准参数集的实验环境设置。

通过精确测量各组件执行时间定量评估 ATA 算法对密码学核心函数的优化贡献。

与传统串行实现对比评估 FLP 技术在不同安全级别下的加速效果。

实验章节框架设计

基于 NVIDIA RTX 4090 GPU 的硬件平台配置与 NIST 标准参数集的实验环境设置。

通过精确测量各组件执行时间定量评估 ATA 算法对密码学核心函数的优化贡献。

与传统串行实现对比评估 FLP 技术在不同安全级别下的加速效果。

与 NIST 参考代码和最新 GPU 实现进行多维度对比。

实验章节框架设计

基于 NVIDIA RTX 4090 GPU 的硬件平台配置与 NIST 标准参数集的实验环境设置。

通过精确测量各组件执行时间定量评估 ATA 算法对密码学核心函数的优化贡献。

与传统串行实现对比评估 FLP 技术在不同安全级别下的加速效果。

与 NIST 参考代码和最新 GPU 实现进行多维度对比。

在不同安全参数下测试性能变化趋势。

POPE 评估指标

基本操作并行效率 (Primitive Operation Parallel Efficiency)

1. 专门度量密码学算法基本操作 P 上的线程利用率
2. 直接反映并行架构中最小计算单元的利用效率
3. 建立密码学算法特性与并行资源分配策略的直接联系
4. 预测不同安全参数下算法性能的可扩展性

老师评语

你觉得你现在写这篇论文遇到的最大困难是什么？

如何在签名组件实现，并行化不能在提升的情况下，去提升性能？

下周计划

- 完成 POPE 指标实验验证
- 准备完整的实验数据与可视化图表

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.