周报

2025 年 2 月 25 日

摘要

- **SHA256 GPU 实现与性能分析**
- **论文前置知识写作**

SHA256 实验结果

表 1: 不同实现方式的最大吞吐量对比

实现方式	最大吞吐量 (MB/s)	消息大小 (B)	加速比
CPU 单核 [WDC+25]	230.40	131,072	1×
GPU 单核 [WDC+25]	25.39	16,384	0.11×
GPU 并行	478,324.05	1,024	2,076×
GPU 多流	22,923.71	16,384	99×

- GPU 单核性能低于 CPU 单核：执行效率低 + 数据传输开销
- 最优配置 (Grid=128, Block=256)：2076 倍加速比

性能分析

线程配置影响

- Grid=128 匹配 SM 数量最优
- Block=256 在资源平衡点
- 大 Block 导致资源竞争

消息大小影响

- 4B-512B：快速增长期
- 1024B-4096B：峰值性能
- >4096B：性能下降期

关键发现：动态调整线程配置和消息分配具有研究价值，即存在核函数与其并发数量的最优组合，该组合配置下，吞吐量最大。

前置知识写作

SPHINCS$^+$ 组成

- WOTS+：一次性签名方案
- FORS：少次签名方案
- Hypertree：多层 Merkle 树结构

GPU 计算模型

- 硬件：多个 SM，每个包含 CUDA 核心
- 多级存储系统
- CUDA 优化策略

老师评语

继续推进

下周计划

1) 将动态线程配置策略扩展到整个 SPHINCS$^+$ 签名过程
2) 探索 GPU 多流处理技术，进一步提高性能

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.