周报

2025 年 2 月 11 日

摘要

- 论文阅读与分析

论文阅读与分析

[WDC+25] 文中详细阐述了针对 HT 树、FORS 树及 WOTS+ 算法的并行化策略，并依据各组成部分的执行顺序提出了一种分层并行方案，共划分为四个层次。由于各层之间相对独立，该文提出的组合并行策略可根据具体资源情况灵活调整，从而实现更高的并行效率（PE），即 PE=效率/资源。

Merkle Tree 并行化

如图 1 所示，左侧示例展示了最大并行化情形，即将每次 HASH 运算视为独立任务，但由此引入了四次同步操作，导致计算负载不均衡并引发等待现象；而右侧示例则采用最小并行化策略，将所有 HASH 运算合并为两个任务，虽然有效缓解了负载不均问题，但并行度则显著降低。因此，我们计划在这两种策略之间寻求一个合适的 HASH 运算分组数，以实现计算负载与并行度之间的最佳折中，并由此提升 PE。

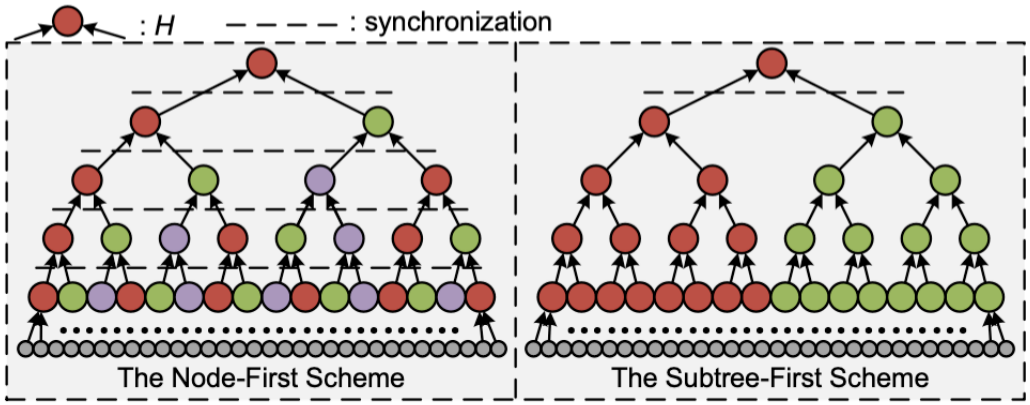

Fig. 2. Two schemes of parallel Merkle tree construction with three threads.

图 1: Merkle Tree 并行化 [WDC+25]

老师评语

阴影标注部分需要更详细说明创新，而不是如此简单，现在的摘要是没有意义的

现确定创新的方向为：更高的并行效率（PE）和签名算法的场景应用，创新手段确定后，再对摘要进行修改。

论文写作基本没有推进??

在精读 [WDC+25] 论文与代码花费太多时间。

下周计划

- 复现 [WDC+25] 实验
- 调整 HASH 运算分组数，提升并行效率 PE

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.