周报-向嘉豪 (2025 年 2 月 10 日)

摘要：

下周计划： 1）GPU 并行化实现 FORS 和 HT 树，2）推进论文写作。

1 论文阅读

本周主要阅读了 [WDC+25]，该文对于如何并行化实现 SPHINCS+ 签名算法进行了深入的研究。其中对签名中的 HT 树、FORS 树、WOTS+ 算法进行了并行化实现，并依据其各组件先后运行的顺序，对其进行分层并行，从上到下一共进行了 4 层的并行化。由于分层后，各层之间的相互独立，因此 [WDC+25] 中可以对各层之间的并行化进行组合，依据具体的资源情况进行选择，从而实现更高的并行效率（PE），i.e. PE= 效率/资源。

这种组合方式下能够获得更高的 PE，但是为能获取到最优的 PE，因此获取一个最优的 PE 为我们创新方向。具体展开来说，以图 1 为例，左侧为最大并行化的情况，其将每次 HASH 运算作为一个任务，同时导致需要四次同步操作，为此导致计算的不平衡性，使计算之间出现等待。而右侧则是最小并行化的情况，其将所有 HASH 运算作为二个任务，减少计算之间的不平衡性，但是其并行度较低。因此我们计划在这两种策略之间，寻取一个中间 HASH 运算的分组数，使得计算之间的不平衡性和并行度达到一个平衡，从而获得更好的 PE。

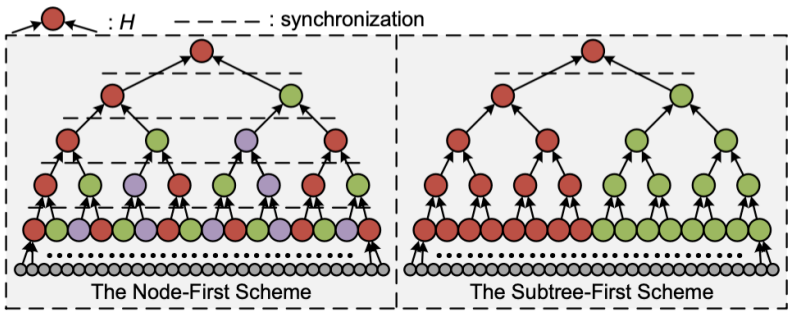

Fig. 2. Two schemes of parallel Merkle tree construction with three threads.

图 1: Merkle Tree 并行化 [WDC+25]

参考文献

[WDC+25] 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.