周报

2025-04-14

大纲

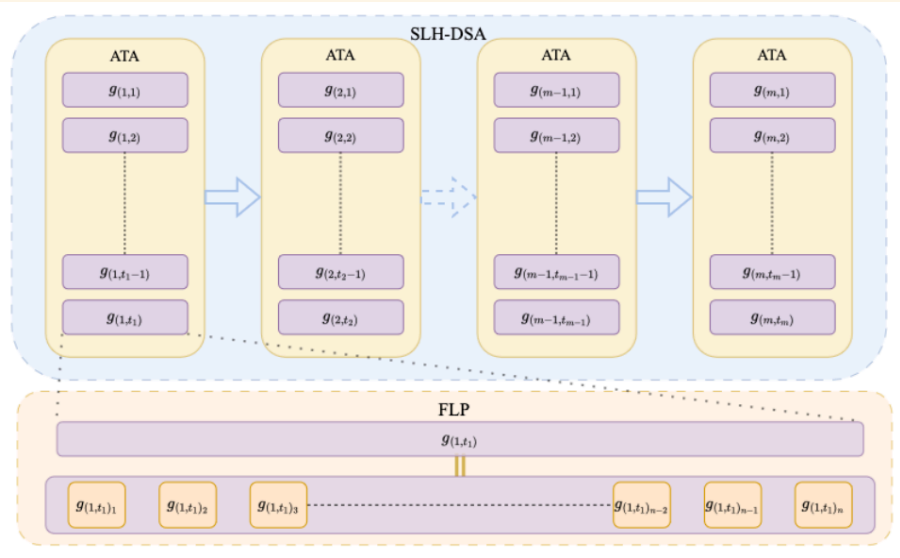
1. 论文写作

2. FLP 写作与实验

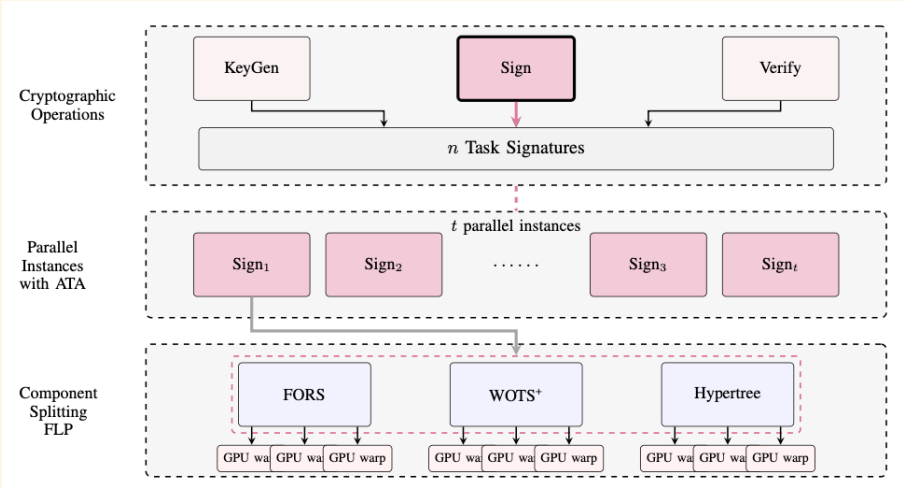
架构图优化

优化内容

- 新版 SLH-DSA 签名流程图结构更简洁明了
- 改进视觉层次与元素关系表达
- 更清晰展示 ATA 与 FLP 之间关系



左：原始流程图



右：改进后流程图

FLP 部分撰写与实验

函数级并行（FLP）

- FLP 为 Thread-Adaptive 架构的重要组成部分
- 主要策略：
  - WOTS$^+$ 并行化：l 个哈希链并发计算
  - FORS 并行化：$k \times 2^a$ 密钥元素并行生成
  - Hypertree 并行化：跨 d 层多 Merkle 树并发构建
- 合理利用合并内存访问与共享内存

FLP 实验结果

签名操作延迟分布（SPHINCS$^+$-128f）

组件	延迟 (ms)	占总时间百分比
WOTS$^+$ Sign	1.857	0.35%
FORS Sign	29.371	5.58%
Hypertree Sign	495.252	94.07%
总签名延迟	526.48	100.00%

- Hypertree 构建占据签名延迟主导地位（94.07%）

老师评语

图 2 过大，一定要小而紧凑，多学学 trans 期刊绘图

继续对图表进行优化

下周工作计划

- 全面检查论文符号一致性与潜在错误
- 进一步优化关键图表和实验结果呈现方式