周报

2025-04-07

大纲

1. 论文实验

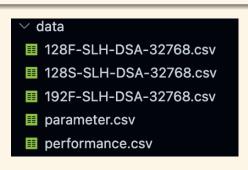
2. 实验章节

实验数据收集

目前还差一个小章节的实验未做完

扩展更多参数集

- 从 SPHINCS+-128F 扩展到 SPHINCS+-128S 和 SPHINCS+-192F
- 收集和分析运行时数据
- 完成性能评估与验证



线程模型与性能分析

线程模型参数与优化分配

通过实验建立的模型参数反映了不同操作在各参数集的计算特性:

- α_i 、 β_i 和 γ_i 反映计算密度与特性
- t*; 根据模型计算出的最优线程数
- 不同安全级别和参数配置需要不同的线程分配策略以达到最佳性能

操作	$lpha_i$	eta_i	γ_i	t_i^*
128F-密钥	52.06	506,000	1.26E-4	63,310
128F-签名	1,386	13,231,567	3.60E-3	60,636
128F-验证	164.72	1,395,012	4.54E-4	55,407
128S-密钥	3,317	32,046,199	7.15E-3	66,929
128S-签名	23,716	248,632,501	6.59E-2	61,419
1285-验证	63.22	484,914	1.44E-4	57,968

SLH-DSA 实现性能比较

性能提升亮点

- 相比于基准实现, 我们的方法在同样硬件下取得性能提升
- 通过自适应线程分配策略优化了 GPU 资源利用率

实现	吞吐量 (任务/秒)				
	公钥生成	签名	验证		
128f [KCS24] 128f [WDC ⁺ 25] 128f [WDC ⁺ 25] [†] 128f 本工作	725,118 (55%) 1,309,136 (100%) 1,435,690 (109.7%) 1,587,849 (121.3%)	44,391 (97%) 45,425 (100%) 53,804 (118.4%) 62,239 (137.0%)	285,681 (81%) 352,333 (100%) 451,883 (128.3%) 502,243 (142.5%)		

老师评语

那个第 1 篇参考文献 1994 年的换成最近的,比如综述论文引用 过这篇的,不要用 20 年前的参考文献

已替换为 20 年后文献

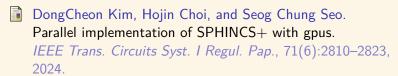
加快推进可投稿

抓紧时间

下周计划

- 完成最后一小章节 FLP 实验
- 对文章图片和段落进行润色

参考文献



Ziheng Wang, Xiaoshe Dong, Heng Chen, Yan Kang, and Qiang Wang.

Cuspx: Efficient gpu implementations of post-quantum signature sphincs < sup>+</ sup>.

IEEE Transactions on Computers, 74(1):15–28, 2025.