周报-向嘉豪 (2025-01-06)

摘要：本周完成了三项主要工作：1）确定了研究方向，选择 NIST 后量子密码标准化项目中的 SPHINCS$^+$ 算法作为实现对象；2）完成了初步技术调研，分析了 SPHINCS$^+$ 中哈希函数的性能瓶颈，测试显示 SHA-256 和 SHAKE256 在不同操作中的延迟范围在 1.6-31.0 微秒之间；3）开始论文写作，确定了题目《Efficient Implementations of SPHINCS$^+$ on GPUs》，并完成了引言部分初稿。通过分析发现，SPHINCS$^+$ 的签名生成过程具有明显的并行计算特性，这为我们利用 GPU 进行优化实现提供了可能。

下周计划：1) 研读 SPHINCS$^+$ 第三轮提交规范及参考实现代码，整理关键数据结构和操作流程. 2) 深入分析 GPU 端并行化策略 [WDC+25].

1 论文阅读

更换实现算法： 鉴于后量子密码标准化进程的重要进展，我们决定将研究重心转向 NIST 后量子密码标准化项目。该项目于 2024 年 8 月 13 日公布了最终标准，包括 CRYSTALS-Dilithium、CRYSTALS-KYBER 和 SPHINCS$^+$ 等算法。在学长的指导下，我们选择了 SPHINCS$^+$ 作为研究对象，这是一个无状态哈希签名方案，由 [BHK+19] 提出。与传统数字签名不同，SPHINCS$^+$ 基于哈希函数构建，能够抵抗量子计算攻击，在后量子密码标准化中具有重要地位。我们计划基于其第三轮提交规范开展优化实现工作。

SPHINCS$^+$ 算法： SPHINCS$^+$ 的签名生成过程包括三个主要步骤：计算消息哈希值，FORS 签名和 HT 签名。其中表 1展示了 SPHINCS$^+$ 中哈希函数的延迟测试结果。其中 H、F 和 Hmsg 分别表示 HT 签名、FORS 签名和 Hmsg 的哈希函数延迟。PRF、PRFmsg 为计算过程中随机数生成所需延迟。为此我们可以从 HT、FORS、Hmsg 和 PRF 四个方面考虑，以求更优的实现方案。

表 1: SPHINCS+-128F-SIMPLE 哈希函数延迟测试（微秒）[WDC+25]

算法	H	F	PRF	PRFmsg	Hmsg
SHA-256	3.2	2.8	1.6	5.9	4.8
SHAKE256	6.9	6.5	5.1	5.2	6.3

2 论文写作

- 我们确定了题目《Efficient Implementations of SPHINCS$^+$ on GPUs》, 并完成了摘要部分的撰写。
- 引言部分阐述了量子计算对现有密码体系的威胁，强调了后量子密码学标准化进程中 SPHINCS$^+$ 作为无状态哈希签名方案的重要地位。结合 SPHINCS$^+$ 计算开销大的特点，我们提出利用 GPU 并行计算能力来加速签名生成过程。

参考文献

[BHK+19] Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. The sphincs$^+$ signature framework. In Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz, editors, *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*, pages 2129–2146. ACM, 2019.

[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.