

周报

向嘉豪

衡阳师范学院

2025 年 1 月 7 日

- 论文阅读：实现算法更换为 SPHINCS⁺
- 论文写作：确定题目, 完成引言部分写作

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 为计算过程中伪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

- 我们确定了**题目**《Efficient Implementations of post-quantum SPHINCS⁺ on GPUs》, (i.e, 老师指导下, 添加后量子算法), 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。



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.



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.

题目中能不能在这个算法修改为后量子算法 sphincs

已添加后量子算法

下周计划

- ① 研读 SPHINCS⁺ 第三轮提交规范及实现代码，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].