

周报向嘉豪 (2025 年 3 月 30 日)

摘要： 本

下周计划： 1) 完成第二阶段算法优化工作 2) 开始撰写实验章节 3) 准备下周的项目进度汇报演示文稿

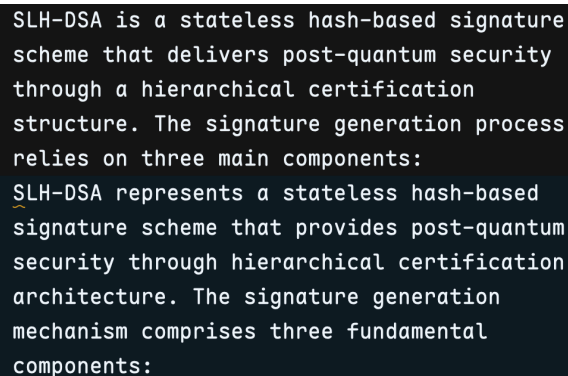
1 工作进展

本节将详细介绍本周的工作进展，包括技术实现、实验分析以及文档编写等方面。[\[WDC+25\]](#)的基准实现相比，我们在签名处理时间上从 0.0605 秒降至 0.0493 秒，实现了 17.4% 的性能提升。

2 论文写作

2.1 口语表达修正

在论文撰写过程中，对文本进行了系统性语言风格调整，以提升学术质量和技术准确性。这些修订主要包括：采用更精确的动词表达；删除冗余短语，构建更紧凑的句子结构；改进段落组织，确保每段具有明确的主题句和支持论点；统一使用被动语态以维持学术客观性；优化图表说明，使解释更加直接明了。图1展示了这类修订的实例，其中将口语化表达如“is”和“main”分别替换为更专业的术语“represents”和“fundamental”，从而增强了文本的学术严谨性。



```
SLH-DSA is a stateless hash-based signature
scheme that delivers post-quantum security
through a hierarchical certification
structure. The signature generation process
relies on three main components:
SLH-DSA represents a stateless hash-based
signature scheme that provides post-quantum
security through hierarchical certification
architecture. The signature generation
mechanism comprises three fundamental
components:
```

图 1: 学术语言风格优化示例

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.