

周报

2025-11-24

本周研究摘要

完成 ML-DSA 签名算法深入分析与 NTT 优化策略研究

- 签名算法结构和计算特征章节撰写：签名流程、Fiat-Shamir with Aborts、NTT 算法伪代码
- 性能瓶颈识别：拒绝采样、NTT 主导(60-70%)、模约减、哈希函数
- 优化策略阐述：汇编优化、延迟约减、预计算

签名算法结构分析

签名流程两层结构：

- Wrapper 函数：上下文验证(255 字节限制)、随机数生成(32 字节)
- 内部签名：Fiat-Shamir with Aborts 范式、拒绝采样循环

拒绝采样机制：

- 采样掩蔽向量 $y \rightarrow$ 计算承诺 $w = A \cdot y \rightarrow$ 推导挑战 c
- 响应向量 $z = y + c \cdot s_1$ 需通过边界检验(阈值 $\gamma_1 - \beta$)
- 期望迭代次数：ML-DSA-44/65/87 分别为 4.25、5.1、3.85 次

NTT 计算特征

NTT 算法结构：

- 环 $R_q = \frac{\mathbb{Z}_{q[X]}}{X^{256} + 1}$, 模数 $q = 8380417$
- 正向 NTT: Cooley-Tukey 蝶形, 本原根 $\zeta = 1753$
- 逆向 NTT: Gentleman-Sande 蝶形, 缩放因子 $f = 256^{-1} \bmod q$

计算复杂度：

- 单次 NTT: $256 \times 8 = 2048$ 次蝶形操作
- 每次蝶形: 1 次模乘、2 次模加减
- NTT 占签名总成本 60-70%

性能瓶颈识别

四个主要瓶颈：

- 拒绝采样：迭代开销，最坏情况>20 次
- NTT 计算主导：60-70% 总计算成本
- 模约减：占 NTT 成本 40%，每次蝶形后执行
- SHAKE-256 哈希：15-20% 签名计算量

优化策略框架

NTT 汇编优化：

- 手工 ARM 汇编：指令级并行、寄存器优化、流水线调度
- UMULL 指令： $32 \times 32 \rightarrow 64$ 位乘法、条件执行消除分支

延迟模约减：

- 跨多个蝶形操作推迟约减、维持系数 $< 2q$ 而非 $< q$
- Montgomery：融合乘-约减操作

预计算策略：

- 秘密向量 s_1 、 s_2 存储为 NTT 表示，旋转因子预计算

总结

下周计划

论文实现优化与结果分析撰写：

- 实现 NTT 汇编优化或延迟模约减策略
- 论文 Results and Analysis 章节撰写

总结

老师评语

继续推进定稿可投

抓紧推进论文和实验