# 周报

2025-12-01

# 本周研究摘要

## 论文 Discussion 章节撰写

- Cryptographic Optimization Implementation 子章节
- NTT 优化：周期降低(320 万→230 万周期)

# 密码学优化实现细节 - NTT 汇编优化

## 手工 ARM 汇编优化

- UMULL 指令：32×32→64 位乘法
- 寄存器分配优化：13 个通用寄存器
- 循环展开因子 2-4、预计算旋转因子

## 性能剖析量化

- 参考 C 实现：320 万周期
- 汇编优化：230 万周期(28.1% 降低)
- 聚合签名延迟降低：20-30%

# 密码学优化实现细节 - 延迟模约减与 Barrett 约减

## 延迟模约减策略

- 维持中间值于宽松边界$[0, 2q)$或$[0, 4q)$
- 延迟约减链跨 2-4 个连续操作

## Barrett 模约减技术

- 预计算$\mu = \lfloor 2^{48}/q \rfloor = 33554431$
- 替代除法操作，基于乘法的约减

# 性能分析与部署权衡 - 计算性能

组合优化技术达到 40-50% 性能改进

## 密钥生成性能

- 100.7-238×开销相对 ECDSA P-256
- 执行时间：151-357 毫秒

## 签名生成与验证

- 签名延迟：657-1150 毫秒(70-122×慢于 ECDSA)
- 验证延迟：416-717 毫秒(26-44×开销相对 ECDSA)

# 总结

# 下周计划

论文实验数据采集与 Results 章节完善:

- MQTT 协议性能实验数据
- Results 章节补充完善

# 老师评语

## 继续推进定稿可投

抓紧推进论文写作