周报

2025-12-08

本周研究摘要

扩展论文 Cryptographic Optimization Implementation 章节

- ARM Cortex-M4 NTT 汇编优化技术详细阐述
- NTT 优化性能汇总表：53.8% 延迟降低(320K→148K 周期)

ARM Cortex-M4 架构特性

ARMv7E-M 架构 Thumb-2 指令集

- 13 个通用 32 位寄存器(R0-R12)
- 三级流水线：取指、译码、执行

硬件乘法指令

- UMULL：单周期 32×32→64 位乘法
- UMLAL：无符号长乘累加
- MLA：乘累加指令

NTT 蝶形操作优化

Cooley-Tukey 蝶形运算

- $a' \leftarrow a + t \cdot \zeta \bmod q$
- $b' \leftarrow a - t \cdot \zeta \bmod q$
- 每 256 点变换执行 2048 次蝶形操作

优化汇编实现

- 7 周期/蝶形 vs 编译 C 代码 18-22 周期
- 61-68% 延迟降低

Montgomery 乘法集成

Montgomery 域高效模算术

- Montgomery 表示：$\tilde{a} = a \cdot R \bmod q, \quad R = 2^{32}$
- 4 周期延迟实现

ARM Cortex-M4 汇编序列

- UMULL 计算$T = \tilde{a} \cdot \tilde{b}$(1 周期)
- MUL 计算$m = T_{lo} \cdot q^{-1} \bmod 2^{32}$(1 周期)
- UMLAL 计算$T' = T + m \cdot q$(1 周期)
- MOV 提取$t = T'/2^{32}$(1 周期)

寄存器分配策略

13 个通用寄存器分区

- 系数寄存器(R0-R7)：8 个蝶形输入/输出
- 旋转因子寄存器(R8)：当前旋转因子
- 常量寄存器(R9-R10)：q^{-1}与q
- 地址寄存器(R11-R12)：数组指针

内存访问优化

- 0.5 次加载+0.5 次存储/蝶形
- vs 朴素实现 3 次加载+2 次存储/蝶形

延迟模约减策略

约减成本占 NTT 计算 35-40%

- 延迟约减维持中间值于$[0, 2q)$或$[0, 4q)$
- 完整约减仅发生于 NTT 阶段边界

约减操作消除

- 4096 次→768 次约减/变换
- 81% 约减操作消除，18-23% 延迟降低

Barrett 约减技术

Montgomery 域外高效模算术

- 预计算$\mu = \lfloor 2^{48}/q \rfloor = 33554431$
- 乘法移位序列替代除法

ARM Cortex-M4 实现

- 6 周期 vs 软件除法 12-18 周期
- 50-67% 约减开销改进

NTT 优化性能汇总

ARM Cortex-M4 168 MHz 周期计数

优化技术	周期	累积改进
参考 C 实现	320,000	基线
汇编蝶形	248,000	22.5%
Montgomery 乘法	198,000	38.1%
延迟约减	172,000	46.3%
4 倍循环展开	156,000	51.3%
指令调度	148,000	53.8%

总结

下周计划

论文完善:

- 完善 Results 章节实验数据
- 补充 Conclusion 章节撰写

老师评语

继续推进，注意时间分配，不要一次只能做一件事，一定要学会并行处理事情

并行规划处理好事项