周报 向嘉豪(2025-12-01)

摘要: 本周完成论文 Discussion 章节撰写，涵盖密码学优化实现细节、计算性能分析强化与部署权衡量化三个核心维度。新增 Cryptographic Optimization Implementation 子章节(84 行代码增量)，详述 NTT 汇编优化在 ARM Cortex-M4 平台达到 28.1% 周期降低(320 万周期→230 万周期)，延迟模约减策略实现 15-25% NTT 延迟改进，Barrett 模约减技术达到 25-35% 约减开销降低。创建 ML-DSA 参数集归一化比较表(ML-DSA-44 作为 1.0×基线)，量化 ML-DSA-65 相对基线呈现 1.30×签名时间、1.37×签名大小、1.45× SRAM 开销，ML-DSA-87 呈现 1.75×签名时间、1.91×签名大小、1.90× SRAM 开销。

下周计划: 1) 实现缺失实验数据采集 2) Results 章节补充完善

1 密码学优化实现细节

完成了 Cryptographic Optimization Implementation 子章节撰写,系统阐述针对 ARM Cortex-M4 平台 ML-DSA 签名验证的三类核心优化技术。NTT 汇编优化通过手工优化 ARM 汇编替代编译器生成代码实现性能突破,利用 UMULL 指令执行 32×32→64 位乘法生成完整乘积无溢出,支持高效模乘法无中间截断。条件执行消除蝶形循环内分支指令降低流水线停顿惩罚,寄存器分配优化维护旋转因子、多项式系数与中间结果于 13 个可用于计算的通用寄存器内最小化存储访问。优化 NTT 实现结构化计算于 256 元素块匹配 Cortex-M4 缓存行特征,循环展开因子 2-4 降低循环开销并通过双发射执行单元利用指令级并行。预计算旋转因子存储于 Flash 存储器消除运行时幂运算,以 2 KB 存储换取消除每 NTT 操作$256 \log_2 256 = 2048$次模幂运算。性能剖析量化汇编优化影响:参考 C 实现 NTT 执行需要 320 万周期于 Cortex-M4 168 MHz,汇编优化实现达到 230 万周期(28.1% 降低),结合逆向 NTT 优化(类似 26-29% 改进),聚合签名延迟降低 20-30% 相对参考实现。

延迟模约减策略通过跨多个算术操作推迟模约减降低约减频率,解决参考实现采用每操作约减维持系数于$[0, q)$边界内产生的 35-40% NTT 计算成本占比问题。延迟约减维持中间值于宽松边界$[0, 2q)$或$[0, 4q)$取决于操作序列深度,实现分析 ML-DSA 算术确立安全延迟约减链。NTT 蝶形操作执行$a + b \bmod q$和$a - b \bmod q$容忍输入系数达$2q - 1$不溢出于 32 位算术(对 ML-DSA 模数$q = 8380417$满足$2 \cdot 2q < 2^{32}$),乘法结果$(a \cdot b) \bmod q$伴随输入界限$2q$产生乘积低于$4q^2 < 2^{64}$,适配 64 位中间表示由 UMULL 生成。延迟约减链跨 2-4 个连续加减操作序列推迟约减然后应用单次约减操作,NTT 阶段执行成对蝶形操作$(w_j, w_{j+n}) \leftarrow (w_j + t, w_j - t)$采用单次约减于两操作后而非每操作约减,减半约减频率。临界路径分析确保系数边界保持于安全范围遍布计算链防止算术溢出。实现达到 15-25% NTT 延迟降低通过延迟约减策略相对每操作约减基线,结合汇编优化累积 NTT 性能改进达 40-50%。

Barrett 模约减技术以基于乘法的方法替代基于除法的模约减解决 ARM Cortex-M4 缺乏硬件整数除法问题,传统$a \bmod q$通过$a - q\lfloor a/q \rfloor$计算需要 12-18 周期软件除法实现产生实质开销。Barrett 约减预计算$\mu = \lfloor 2^{48}/q \rfloor = 33554431$对 ML-DSA 模数$q = 8380417$,32 位值$a$的约减通过近似商计算$\hat{q} = \lfloor (a \cdot \mu)/2^{48} \rfloor$经 32×32 乘法和 48 位右移实现,后续校正步骤$r = a - \hat{q} \cdot q$产生结果r满足$0 \leq r < 2q$,条件减法生成最终约减值$r' = r < q ? r : r - q$。ARM Cortex-M4 实现利用 UMULL 指令执行$(a \cdot \mu)$乘法提取高 32 位作为近似商,后续乘法$\hat{q} \cdot q$与减法采用标准 32 位算术,条件减法采用比较与条件移动指令(CMP、IT、SUB)无分支开销。Barrett 约减集成于 NTT 实

现内替代所有模约减操作,达到 25-35% 约减开销改进相对基于除法方法,优化对签名生成特别有效(数十万次约减操作)但对密钥生成等不频繁操作提供最小收益。

2 性能分析与部署权衡量化

完成了计算性能分析强化、安全-性能权衡量化与部署可行性评估三个子章节的扩展撰写。计算性能测量采用 pqm4 库实现整合多项优化技术,所有报告周期计数反映优化实现利用 NTT 汇编优化(20-30% 延迟降低)、延迟模约减(15-25% NTT 改进)、Barrett 约减模算术(25-35% 开销降低)与预计算旋转因子,组合优化技术达到 40-50% 性能改进相对参考实现,确立 ARM Cortex-M4 部署性能上界。测量量化可达成性能于激进优化下而非基线参考实现。密钥生成性能呈现 100.7-238×计算开销相对 ECDSA P-256 反映固有格基密码复杂度,优化技术对密钥生成操作提供有限改进因其主导于随机多项式采样与矩阵展开而非 NTT 算术。测量执行时间 151-357 毫秒确立设备配置期间不频繁密钥生成可行性,但禁止高频率轮换策略需要次秒密钥派生。签名生成构成 NTT 优化技术主要受益者,每次拒绝采样迭代需要多个正向 NTT 与逆向 NTT 操作用于多项式算术,优化 NTT 实现降低每迭代计算成本 40-50% 直接转换为比例签名延迟降低。然而绝对签名延迟 657-1150 毫秒跨参数集保持 70-122×慢于 ECDSA 尽管激进优化,确立基于签名 IoT 认证基本性能约束。验证操作受益于预计算旋转因子与优化 NTT 实现,达到 26-44×开销相对 ECDSA 对比 71-122×开销用于签名生成,但绝对验证延迟 416-717 毫秒超过次秒界限需要交互式 IoT 应用跨所有参数集。

安全-性能权衡分析章节创建归一化比较表量化 ML-DSA-44/65/87 参数集增量权衡。三个 ML-DSA 参数集呈现量化安全-性能权衡跨计算、存储、协议维度,ML-DSA-44(NIST 安全级别 2,AES-128 等价)达到 657 ms 签名延迟、416 ms 验证延迟、2420 字节签名、22.7 KB 总 SRAM 消耗。ML-DSA-65(级别 3,AES-192 等价)增加这些指标至 853 ms 签名、533 ms 验证、3309 字节签名、32.8 KB SRAM,代表 29.8% 计算开销、36.8% 签名大小增加、44.5% 存储增加相对 ML-DSA-44。ML-DSA-87(级别 5,AES-256 等价)进一步提升至 1150 ms 签名、717 ms 验证、4627 字节签名、43.1 KB SRAM,即 72.3% 计算开销、91.2% 签名大小增加、89.9% 存储增加相对 ML-DSA-44。归一化表展示 ML-DSA-44 作为 1.0×基线,ML-DSA-65 呈现 1.30×签名时间、1.27×验证时间、1.37×签名大小、1.45× SRAM,ML-DSA-87 呈现 1.75×签名时间、1.72×验证时间、1.91×签名大小、1.90× SRAM。对于 5-10 年操作生命周期的 IoT 部署于当前量子计算发展轨迹下,NIST 安全级别 2(ML-DSA-44)提供充分量子抗性伴随最小资源开销。长期基础设施部署(20+年操作生命周期)需要保守安全边际证明 ML-DSA-87 尽管 75-90% 资源开销增加,ML-DSA-65 占据中间位置适合需要 AES-192 等价安全无 ML-DSA-87 最大资源成本的部署。