周报 - 审稿回复

2025-07-15

研究概述

本周研究摘要

本周完成 审稿回复的 P1 和 P3 任务：P1 通过七种 S-box 的实验评估展示 11.7%-86.1% 的优化改进，P3 在相同平台上证明 bitsliced 相比表查找有 22.5% 性能优势。

更新了两个核心性能表格，并规划了 P2 任务的 GIFT-COFB 实验验证。

截至时间：2025 年 7 月 29 日

P1 任务：S-box 优化贡献增强

任务完成情况 【已完成】

针对审稿人对新颖性描述不清的关切，完成了 S-box 优化的综合性实验评估。

核心贡献：开发了一种改进的约束简化方法，提升了单元传播效率而不影响解决方案质量。

S-box 优化性能结果

S-box	Feng et al. (s)	本研究 (s)	改进倍数
PRØST	2.511	2.217	1.13×
SKINNY S_4	8.455	6.399	1.32×
Piccolo	16.875	2.347	7.19×
Keccak	37.005	15.947	2.32×
GIFT	418.715	60.154	6.96×
RECTANGLE	689.812	155.464	4.44×
QARMAv2	4055.519	2101.336	1.93×

P3 任务：性能比较公平性纠正

任务完成情况 【已完成】

解决了审稿人指出的跨不同处理器架构性能比较不公平的问题。

原有比较存在根本性缺陷：不同处理器架构导致的性能差异使得比较结果无意义。

在相同的 STM32L476 平台上实施标准化比较：

- 表查找实现：325.25 CPB 处理单个分组
- bitsliced 方法：252.06 CPB 并行处理两个分组
- 性能优势：22.5%

综合性能评估表

密码	芯片	语言	实现方式	分组数	周期	CPB	Flash (bytes)
QARMAv2	STM32L476	Assembly	Bitsliced	2	10,952	684.50	25,340
QARMAv2	STM32L476	C	Lookup Table	1	16,910	2,113.75	17,220
AES	STM32L476	Assembly	Bitsliced	2	8,066	252.06	25,244
AES [21]	STM32L476	Assembly	Bitsliced	2	8,932	279.12	27,100
AES [23]	STM32L476	C	Lookup Table	1	5,204	325.25	26,616

P2 任务：NIST 轻量级密码适用性验证

任务规划 【进行中】

针对审稿人关于技术对 NIST 轻量级密码标准适用性的问题，计划实施 GIFT-COFB bitsliced 优化实验。

与 Adomnicai et al. (2020) TCHES 的 fixslicing 方法进行对比

应用 OPO 算法和改进的 BGC 模型优化：

- GIFT 的线性层
- 4-bit S-box

验证方法在 NIST LWC 标准上的有效性

选择 GIFT-COFB 的原因

Ascon 的限制：

- 320-bit 状态分为五个 64-bit 字
- 在 32-bit MCU 上 64-bit 字长要求数据跨越多个寄存器
- 严重限制并行计算效率

GIFT-64 的优势：

- 架构更适合 32-bit 平台的 bitsliced 优化
- 能够更好地展示我们方法的实际效果

总结

下周计划

完成 P2 任务：

- 实施 GIFT-COFB bitsliced 优化实验
- 与 fixslicing 方法对比
- 验证技术在 NIST LWC 标准上的适用性

完成编辑意见回复

老师评语

上面这个摘要就要写在邮件正文，要学会利他思想，我知道别人最想知道什么我就按别人的要求写东西，我们现在很多学生是利己做事。

学生下次改正

已修改部分的回复信没写还是没有发给我???

学生想整体修改好后发您