周报 向嘉豪(2025-07-14)

摘要: 本周完成 SecondPaper 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。

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。完成剩余审稿回复。

审稿回复

P1 任务：S-box 优化贡献增强 (完成)

本周完成的 P1 任务显著增强了 S-box 优化的贡献描述，通过实施综合性实验评估来回应审稿人对新颖性描述不清的关切。核心贡献在于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。

实验评估涵盖七种不同的密码 S-box，在受控条件下与现有的 Feng et al. (2024) BGC 方法进行对比。优化时间改进范围从 11.7%（PRØST）到令人瞩目的 86.1%（Piccolo），部分情况下实现了高达 7.19 倍的加速，同时保持完全的功能等价性和相同的门数量。

为促进可重现性研究和进一步发展，完整的 S-box 优化框架已开源发布至 GitHub 仓库 https://github.com/jiahaoxiang2000/sbox-bgc。此举不仅提升了研究的透明度，也为学术界提供了实用的优化工具。

S-box 优化性能比较表

表 1　S-box 优化性能对比：本研究方法相对于 Feng et al. (2024) 的时间改进

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×

关键发现： 平均优化时间改进为 3.19 倍，最显著改进出现在 Piccolo S-box（7.19 倍加速）和 GIFT S-box（6.96 倍加速），所有测试的 S-box 都实现了性能提升，证明了方法的普适性。

P3 任务：性能比较公平性纠正 (完成)

P3 任务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重要问题。原有比较存在根本性缺陷，因为不同处理器架构导致的性能差异使得比较结果无意义。

通过在相同的 STM32L476 平台上实施标准化比较，使用自研的 LCB（Lightweight Cryptography Benchmarking）基准测试框架确保评估一致性。结果显示，表查找实现达到 325.25 CPB 处理单个分组，而 bitsliced 方法通过并行处理两个分组实现 252.06 CPB，证明了 22.5% 的性能优势。

建立了公平的评估基准，突出了 bitsliced 并行处理相对于顺序表查找实现的效率优势，其中跨多个分组分摊计算成本的能力在相同硬件平台上提供了显著的效率增益。

密码实现综合性能评估表

表 2　CTR 模式下密码实现性能评估对比

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
QARMAv2	ESP32S3	C	Lookup Table	1	42,709	5,338.63	140,143
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

性能分析要点： 优化后的 AES bitsliced 实现达到 252.06 CPB，相比基准实现提升 9.7%，主要得益于 ShiftRow 优化将 PPO 操作从 6 个减少到 4 个。在相同 STM32L476 平台上，bitsliced 方法相比表查找实现具有 22.5% 的性能优势，证明了并行处理的有效性。首次实现 QARMAv2 的软件优化，bitsliced 实现相比查找表方法实现 67.6% 的性能提升，为该密码的实用化奠定基础。

P2 任务：NIST 轻量级密码适用性验证 (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，我们计划实施 GIFT-COFB bitsliced 优化实验作为 P2 任务的核心验证。

实验计划： 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 的线性层和 4-bit S-box，验证方法在 NIST LWC 标准上的有效性。

为何选择 GIFT-COFB： Ascon 的 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。相比之下，GIFT-64 的架构更适合 32-bit 平台的 bitsliced 优化，能够更好地展示我们方法的实际效果。