周报 向嘉豪(2025-07-21)

摘要: 本周在审稿回复工作中取得进展。完成 GIFT 实验验证，我们获得了 19.5% 的显著性能提升（114.81 CPB 相比 142.63 CPB 基准），成功完成了 P2 任务中 NIST 轻量级密码适用性的验证工作。同时，我们系统性地回应了编辑提出的四个核心改进点。

目前论文已具备提交的基本条件，所有主要的审稿意见都得到了妥善回应。下周的工作将聚焦于最终的完善和细节优化，确保论文达到发表标准。

下周计划: 审阅和提交第二篇意见， 推进第三篇论文的大修意见回复工作。

GIFT 实验完成

实验背景与目标

本周完成了 P2 任务的核心实验验证 - GIFT-COFB bitsliced 优化实验。该实验旨在回应审稿人关于我们的优化技术对 NIST 轻量级密码标准适用性的质疑，通过具体的实验数据证明方法的广泛适用性。

选择 GIFT-COFB 作为验证目标主要基于架构适配性考量。GIFT-64 的架构设计更适合在 32-bit 平台上进行 bitsliced 优化实现。相比之下，Ascon 算法采用 320-bit 状态划分为五个 64-bit 字的设计，在 32-bit 微控制器平台上实现时，64-bit 字长操作需要数据跨越多个寄存器，这种架构特性显著限制了并行计算的效率。

实验结果与性能分析

通过与 Adomnicai et al. (2020) 方法进行对比，我们的 GIFT bitsliced 实现在 STM32L476 平台上取得了显著的性能提升：

表 1　GIFT-64 性能对比：本研究方法相对于现有 fixslicing 方法的改进

密码	实现方式	分组数	周期	CPB	改进
GIFT	本研究 Bitsliced	2	1,837	114.81	19.5%
GIFT	Adomnicai et al.	2	2,282	142.63	基准

实验取得的关键成果表明，我们的优化方法在多个关键指标上均实现了显著改进。性能提升方面，我们的实现将 CPB 值从基准的 142.63 降低到 114.81，实现了 19.5% 的性能提升。在计算复杂度方面，周期数从 2,282 减少到 1,837，展现了算法的高效性。更重要的是，这些结果验证了 OPO 算法和改进的 BGC 模型在 NIST 轻量级密码标准上的有效性和实用性。

NIST LWC 适用性分析

我们的分析系统性地评估了 NIST 轻量级密码竞赛的主要候选算法。对于适用算法方面，GIFT-COFB 基于 GIFT 分组密码并采用 4-bit S-box 结构，与我们的优化技术完全兼容，可以充分发挥算法的优势。ASCON 算法在某些方面展现了适用性，其 5-bit S-box 结构可以有效应用我们的优化方法，但在 32-bit 微控制器平台上进行 64-bit 操作时存在架构限制。

编辑意见系统性回应

本周完成了对编辑提出的四个核心改进点的系统性回应：

1. 新颖贡献清晰阐述

在 Section III.B 中增强了新颖贡献的阐述，通过对七种不同 S-box 实现进行详细的时序性能比较分析（TABLE IV），系统性地展示了 11.7% 到 86.1% 范围内的优化改进效果。为了促进学术界的可重现性研究和进一步发展，我们将优化框架进行了开源发布。

2. NIST 标准适用性论证

在 Section IV.C.2 中补充了 NIST 标准适用性的论证内容，加入了具体的 GIFT-COFB 实现实验结果，证明了 19.5% 的性能改进效果。同时提供了对 NIST 轻量级密码候选算法适用性的全面分析，从理论和实践两个层面验证了我们方法的广泛适用性。

3. 公平性能比较

针对审稿人指出的性能比较公平性问题，我们修正了实验设计，确保所有性能分析都在相同的 STM32L476 硬件平台上进行。通过标准化的比较环境，我们证明了 bitsliced 方法相比传统的基于表查找的实现方式具有 22.5% 的显著性能优势。

4. 参考文献和写作质量

系统性地提升了论文的写作质量，进行了全面的校对工作。这包括对语法表达的具体修正，确保学术表达的准确性和流畅性。同时更新了参考文献，特别是用更新的 Lee et al. (2022) 研究替换了过时的 GPU 实现相关参考文献，确保引用的时效性和相关性。