周报 - 实验完成与编辑意见回应

2025-07-22

研究概述

本周研究摘要

本周在审稿回复工作中取得进展。完成 GIFT 实验验证，获得了 19.5% 的性能提升（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。

系统性地回应了编辑提出的四个核心改进点，论文已具备提交的基本条件。

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。

实验完成 【已完成】

实验结果与性能分析

与 Adomnicai et al. (2020) 方法进行对比，在 STM32L476 平台上取得显著性能提升：

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

关键成果：

- 性能提升：CPB 值从 142.63 降低到 114.81
- 计算复杂度：周期数从 2,282 减少到 1,837

编辑意见系统性回应 【已完成】

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）
- 展示了 11.7% 到 86.1% 范围内的优化改进效果

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
- 提供了对 NIST 轻量级密码候选算法适用性的分析

3. 公平性能比较

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：

- 标准化的比较环境
- 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
- 消除了跨不同处理器架构比较的不公平性

4. 参考文献和写作质量

系统性地提升了论文的写作质量：

- 全面的校对工作，对语法表达的具体修正
- 确保学术表达的准确性和流畅性
- 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

总结

下周计划

核心任务：

- 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

老师评语

回复信格式一定要按照实验室的通用格式来，不要在这些格式上别出心裁

已按实验室通用格式修改好