周报 - 审稿意见回复工作

2025-07-08

研究概述

本周研究摘要

本周主要完成的审稿意见系统性回复工作。针对编辑和两位审稿人提出的关键问题进行了深入分析和响应。

截至时间：2025 年 7 月 29 日

审稿人 1 意见回复

意见 1：S-box 实现优化描述 【正在进行】

“Unlike the first contribution, the second contribution that aims to optimize the S-box implementation, is not clearly described. In particular, it is unsure which part of III.B is novel, compared to existing work, which requires a more detailed comparison.”

- 初步测试结果：QARMAv2 4-bit S-box 20 个串行排列
  - Feng[24]方法：2101 秒
  - 我们的方法：486 秒
  - 测试环境：100 线程下 cryptominisat 求解

意见 2：NIST 轻量级密码学适用性 【正在进行】

“It seems like the technique is only applicable to certain block ciphers that are similar to AES. How about more recent NIST lightweight cryptography schemes? The authors are encourage to discuss this aspect in detail.”

- 学长建议优先添加 GIFT-COFB 对比实验结果

意见 3：实验比较公平性 【正在进行】

“It is unfair to say that table based implementation is faster than bitsliced implementation by comparing [23] with [21]. They are using a completely different processor, so it is natural to have very different performance. Moreover, availability of registers is also key to the performance of bitsliced implementation, which can be very different for various processor architectures.”

- 在实验章节中添加更公平的比较，确保相同环境下对比[23]和[21]

意见 4 - 语言校对 【已完成】

“This article needs proofreading. Some obvious errors can be found easily. For example, pg. 6 first sentence, it should be ‘An encoding method….’ Ref[12] is also not formatted correctly in the last page.”

- 修正了“A encoding method”到“An encoding method”的语法错误
- 纠正了处理器名称从“Tensilica LX”到“Xtensa LX”的技术准确性问题
- 参考文献[12]的格式已修正，确保符合期刊要求

意见 5 - 参考文献更新 【已完成】

“Reference [8] seems to be old, there are other more recent GPU implementations of bitsliced AES.”

- 已按照审稿人建议更新了相关参考文献
- 使用更新的 GPU 实现研究来替换过时的引用

编辑意见策略

回复策略

“The reviewers’ main concerns revolve around the novelty and contributions of the paper. To address these, please focus on: 【待完成-依赖审稿人 1 所有意见完成】

- Clearly articulating the novel contribution.
- Discussing the applicability of the technique to NIST standards.
- Revising the comparison with table-based implementations to ensure a fair evaluation.

回复策略

- Updating the references and improving the overall writing quality.“

编辑意见是对审稿人 1 各项意见的总结：

策略：先完成审稿人 1 的所有具体意见，然后基于这些具体回复来综合回应编辑的整体关注点。

审稿人 2

意见

“Y”

审稿人 2 没有提出具体意见，我们认为其，接受我们的工作。

下周计划

主要任务

1. 完成审稿人 1 所有意见的详细回复：
   - P1 完善 S-box 编码方法与现有 SAT 方法的对比实验和数据表格
   - P2 扩展 GIFT-COFB 对比实验结果
   - P3 实施[23] [21]公平的性能比较实验，确保相同硬件平台条件
2. 基于审稿人 1 意见完成情况，综合回复编辑的整体关注点

老师评语

要尽全力仔细理解审稿人每句话的真正含义，并认真修改好，确保能录用

全力以赴修改好审稿人意见