周报 向嘉豪(2025-07-07)

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。重点突破在于 S-box 编码方法创新性的明确阐述和 NIST 轻量级密码学标准适用性讨论的扩展。完成了语言校对和参考文献更新工作，审稿人意见 4 和 5 已全部完成。当前正在推进审稿人意见 1、2、3 的详细回复，包括与现有 SAT 方法的实验对比、轻量级密码算法适用性分析以及公平性实验设计。通过初步实验验证，我们的方法在 QARMAv2 4-bit S-box 优化上相比 Feng 等人的方法实现了 4.3 倍的性能提升。

本周计划

1. 完成审稿人 1 所有意见的详细回复：
   - 完善 S-box 编码方法与现有 SAT 方法的对比实验和数据表格
   - 扩展 NIST 轻量级密码学标准适用性讨论
   - 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

回复审稿意见

编辑意见

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

编辑提出的主要关注点包括新颖性阐述、NIST 标准适用性、实验比较公平性和整体写作质量。由于编辑意见实际上是对审稿人 1 各项意见的总结，因此我们的策略是先完成审稿人 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 1

审稿人 1 对论文的两项技术贡献给予了积极评价，但指出了几个需要改进的重要问题：

审稿人意见 1： “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.” 【正在进行】

目前，我们初步测试了 Feng[24]和我们的方法在 QARMAv2 4-bit S-box 20 个串行排列上的时间分别是 2101 和 486 秒，测试环境为 100 线程下 cryptominisat 求解。 数据完善后，我们将在实验章节添加结果数据表，同时在第二章中添加 SAT 的相关背景介绍。

审稿人意见 2： “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.” 【正在进行】

添加讨论章节，包括对 Ascon、Elephant、ISAP 等入围算法的适用性分析。去详细解释最优排列排序算法如何应用于不同的结构，以及 S-box 优化技术如何适配 5 位、8 位等不同位宽的变化。

审稿人意见 3： “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.” 【正在进行】

此处审稿人指出的是通过[23]与[21]的对比，不能说明比特切片下 AES 算法比表实现要慢的结论。而我们的核心在于，对现有比特切片实现的优化，因此该问题不是对我们工作的直接批评，而是对现有文献的比较方式，提出了质疑。我们将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]。

审稿人意见 4： “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.” 【已完成】

语言质量的全面提升通过系统性校对得以实现。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]的格式也已修正，确保符合期刊要求。

审稿人意见 5： “Reference [8] seems to be old, there are other more recent GPU implementations of bitsliced AES.” 【已完成】

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。

审稿人 2

审稿人 2 对论文给予了积极评价，表示接受我们的工作。