周报 向嘉豪(2025-10-20)

摘要: 本周完成第二篇论文 R2 小修审稿意见 Point 2 与 Point 3 核心修订任务。针对 QARMAv2 基准选择疑问(Point 2)，在第 IV-C2 节性能分析部分添加明确基准选型说明，阐述查找表基准作为首个软件位切片 QARMAv2 实现对比标准的合理性。完成全部编辑性修订(Point 3)，修正 Sec. II-C 术语错误、Fig. 1 上标标记、Ref [23]格式问题，补充 Table VI 组件分类注释。更新审稿意见回复文档，提供 Point 2 与 Point 3 详细修订说明。截至目前已完成 R2 修订 5 项任务中的 2 项，余下完成安全性分析(Point 1)、图表质量提升(Point 4)、Default/Baksheesh 密码评估(Point 5)。投稿截止时间:10 月 30 日。

下周计划: 1) 完成 Point 1 安全性分析章节撰写，添加位切片恒定时间特性与侧信道防护说明。 2) 提升 Table 1 与 Figure 4 视觉质量，转换矢量图格式确保可读性。 3) 评估 Default/Baksheesh 密码实现可行性，确定基准测试或未来工作方案。 4) 完成审稿意见回复文档全部 Response 部分撰写。 5) 最终稿件校对与提交准备工作。

1 编辑性修订完成(Point 3)

术语错误修正 完成 Sec. II-C 术语修正，将“trivial forms”替换为“transformations”，准确反映线性与非线性变换技术描述。该修正提升论文技术术语准确性，避免读者误解。修改通过`\revised{}`宏标记蓝色高亮，便于审稿人识别修订内容。

图表标记统一 修正 Fig. 1 图注中上标标记错误，将b_j^i统一为b_i^j，确保与符号表定义一致。修订后标记表述为“b_i^j表示第j个块的第i位”，消除原有混淆。该修正强化论文符号体系一致性，提升可读性。

参考文献格式 更新 Ref [23]参考文献格式，将“riscvOVPsim”规范化为“RISC-V OVPsim”，符合 RISC-V 基金会官方命名规范。该修正体现学术严谨性，确保引用格式专业性。

表格组件说明 为 Table VI 添加脚注，明确“Others”组件包含数据移动与轮密钥异或操作。脚注内容:“Data movement and round key XOR”，消除审稿人关于组件分类疑问。该补充强化性能分析透明度，便于读者理解周期开销分配。

文献与专有名词 验证参考文献[6]、[7]、[22]、[23]无重复条目，确认全部 25 条引用唯一性。术语一致性决策:保持“bitslicing”单词写法，遵循密码学文献[21]、[22]、[23]惯例。

2 QARMAv2 基准选择说明(Point 2)

2.1 Baseline 阐述

对比标准缺失 审稿人 Point 2 指出 QARMAv2 查找表基准选择需明确说明。根本原因在于 QARMAv2 原始论文未提供软件性能评估，本工作提出首个软件位切片 QARMAv2 实现。文献中不存在可直接对比的位切片实现，需选择合适软件基准建立性能参照。

查找表基准合理性 在 Sec. IV-C2 性能分析段落添加基准选型原理阐述，说明查找表方法代表分组密码常规软件实现策略。添加内容:“性能评估采用查找表实现作为基准，因文献中不存在可直接对比的位切片 QARMAv2 实现。查找表方法代表分组密码常规软件实现策略，为评估资源受限平台位切片优势提供有意义基准。”该补充长度 2 句话，遵循简洁修订原则。

Response 撰写 在 response 中为 Point 2 撰写详细回复说明，包含 4 项要点:(1)本工作提出首个软件位切片 QARMAv2 实现，原工作专注硬件无软件性能评估;(2)不存在可直接对比的位切片实现;(3)查找表方法代表常规软件实现策略;(4)QARMAv2 硬件导向设计特性利于位切片。回复引用添加内容原文，以蓝色高亮展示修订位置。

3 修订进度与下周重点

3.1 当前进度总结

截至 10 月 20 日，R2 小修 5 项任务完成 2 项(40% 进度)。已完成任务:Point 2 QARMAv2 基准说明、Point 3 编辑性修订。待完成任务:Point 1 安全性分析(需添加位切片恒定时间特性与侧信道防护说明)、Point 4 图表质量提升(Table 1 格式优化、Figure 4 矢量化)、Point 5 Default/Baksheesh 密码基准测试(需评估实现可行性)。

3.2 时间规划

投稿截止时间 10 月 30 日，余下 10 天计划用 6 天完成 3 项核心任务。Point 1 安全性分析预计 1-2 天(文献调研、段落撰写、引用整合)。Point 4 图表优化预计 1-2 天(TikZ/Matplotlib 重绘、格式调整)。Point 5 密码评估预计 2 天(实现可行性分析、基准测试或未来工作方案确定)。审稿意见回复文档完善与稿件最终校对预计 1 天。余下 4 天作为缓冲时间应对突发问题，确保按时提交高质量修订稿件。