# 周报

2025-10-20

# 本周研究摘要

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

- QARMAv2 基准选择疑问(Point 2)：添加基准选型说明
- 全部编辑性修订(Point 3)：术语修正、图表标记、参考文献格式

# R2 修订进度概览

已完成：2/5 项任务(40% 进度)

- Point 2：QARMAv2 基准说明
- Point 3：编辑性修订

待完成：3 项核心任务

- Point 1：安全性分析
- Point 4：图表质量提升
- Point 5：Default/Baksheesh 密码评估

截止：10 月 30 日

# 编辑性修订完成(Point 3)

术语错误修正：Sec. II-C “trivial forms” → “transformations”

图表标记统一：Fig. 1 图注上标 $b_j^i \to b_i^j$，确保符号一致性

参考文献格式：Ref [23] “riscvOVPsim” → “RISC-V OVPsim”

表格组件说明：Table VI 添加脚注，明确“Others”包含数据移动与轮密钥 XOR

# QARMAv2 基准选择说明(Point 2)

问题根源：QARMAv2 原始论文未提供软件性能评估，本工作为首个软件位切片实现

回复：在 Sec. IV-C2 添加基准选型原理阐述

- 查找表方法代表分组密码常规软件实现策略
- 文献中不存在可直接对比的位切片 QARMAv2 实现
- 为评估资源受限平台位切片优势提供有意义基准

# 总结

# 下周计划

- Point 1 安全性分析
- Point 4 图表质量提升
- Point 5 密码评估
- 审稿回复与校对

预计 10-26 号完成

# 老师评语

## 认真修改，到这步千万别拒稿了

仔细认真修改