周报

2025-10-27

本周研究摘要

本周完成第二篇论文 R2 小修全部修订任务并成功提交

- 安全性分析章节(Point 1)：新增 Security Considerations 子章节
- 图表质量提升(Point 4)：Table 1 优化与全部图表矢量化
- 2025 年 10 月 26 日成功提交 R2 修订版本

安全性分析章节完成(Point 1)

章节定位：在 Sec. IV-C3 新增“Security Considerations”子章节

恒定时间执行特性：

- 位切片实现固有的恒定时间与恒定流特性
- 引用[25] Aldaya et al., TCHES 2019

门级掩码优势：

- 引用[26] Balasch et al., CHES 2015
- 相比查找表实现更系统化且开销更低

图表质量全面提升(Point 4)

Table 1 格式优化:

- 增加行间距避免内容拥挤
- 采用左对齐描述列增强视觉舒适度
- 扩展列间水平间距至 2em 消除视觉混淆

DrawIO 矢量图转换:

- 全部 5 幅图表(Fig. 1-5)重新绘制为 PDF 矢量格式
- 满足 IEEE 出版质量标准
- 任意缩放下保持清晰度

图表质量全面提升(Point 4 续)

字体大小提升:

- 统一将全部图表字体从 35px 提升至 45px
- 28.6% 增幅显著增强可读性
- 符合 IEEE 会刊图表规范

冗余元素清理:

- 优化画布尺寸移除不必要空白
- Fig. 5 移除重复位置框
- 强化核心置换变换逻辑表达

总结

下周计划

推进第四篇论文写作与实验

pqm4 移植：完成 ARM Cortex-M4 平台适配与功能验证

MQTT 原型：实现载荷签名系统，测量协议级传输开销

老师评语

继续推进第 4 篇论文写作工作, 报告一定要有详细下周计划

继续推进论文写作