周报

2026-01-26

本周研究摘要

完成第四篇小论文精简工作，篇幅从 15 页压缩至 7 页

完成硕士学位论文第三章 CRAFT 密码 FPGA 高效实现撰写

第四篇小论文精简

删除 514 行冗余内容，新增 174 行精炼表述，精简幅度约 50%

- Related Work：删除过多历史背景介绍，聚焦研究空白
- 算法描述：简化优化技术实现细节，保留核心算法结构
- 实验方法：合并重复测量方法说明，减少统计方法冗余描述

精简后核心贡献表述更清晰，提升论文可读性与投稿竞争力

第三章 CRAFT 密码 FPGA 高效实现

首次在 FPGA 平台上实现 CRAFT 轻量级密码

- CRAFT 算法：64 位明文、128 位密钥、64 位杂凑，轮函数含列混合、字节置换、S 盒
- 串行架构：数据通路宽度从 64 位降为 4 位，S 盒数量由 16 降为 1
- 展开架构：每周期执行 2 轮函数，16 周期完成加密

基于 SAT 求解器优化 S 盒，采用 4 个 MOAI1 门、3 个 MAOI1 门、1 个 AND3 门

实现结果与资源评估

在 Artix-7、Kintex-7、Spartan-7 三种 FPGA 平台进行测试

- 串行架构面积较迭代架构减少 10.16%
- 展开架构最大吞吐率提升 40.53%
- 单比特能耗降低 47.89%

S 盒优化方案面积较现有方案减少 28.9%

总结

下周计划

- 修改第四篇小论文
- 继续撰写第四章：面向 32 位处理器的 SPN 密码比特切片低延迟实现

老师评语

15 页到 7 页又少了，一般 9 到 12 页左右，不低于 9 页

后续补充提升核心创新点