周报

2026-01-19

本周研究摘要

硕士学位论文第一章绪论与第二章基础知识撰写完成

采用 IEEE Trans 模板 第四篇小论文，制定论文长度优化方案

第一章绪论撰写

包括选题背景及研究意义、国内外研究现状和研究内容三个部分

- 选题背景：SPN 结构密码在物联网和云计算环境中的应用需求
- 国内外研究现状：轻量级密码硬件实现、比特切片软件实现、GPU 并行实现
- 研究内容：CRAFT 密码 FPGA 实现、SPN 比特切片优化、AES GPU 并行优化

第二章基础知识撰写

系统介绍 SPN 密码基本原理、软件实现技术和硬件实现技术

- SPN 密码原理：S 盒变换、线性变换、AES-128 四个基本操作
- 软件实现：查找表实现、比特切片实现、SIMD 向量化实现
- 硬件实现：ASIC/FPGA 平台、迭代/串行/展开架构

以 AES-128 为例详细分析 SubBytes、ShiftRows、MixColumns、AddRoundKey

小论文长度优化

当前篇幅约 942 行，需精简约 15%(139 行)以满足 IEEE Trans 10-12 页要求

- Related Work：精简约 12 行，聚焦研究空白
- ML-DSA 算法描述：精简约 28 行，保留核心结构
- 实现架构：精简约 24 行，合并重复内容
- 自适应协议：精简约 20 行，删除冗余示例
- 实验与结果：精简约 55 行，合并表格与分析

总结

下周计划

- 继续撰写第三章：面向资源受限环境的 CRAFT 密码 FPGA 高效实现
- 完善第四篇小论文，按优化方案精简篇幅

老师评语

第 3 篇小论文精简到不超过 13 页，最好就是 12 页以内，简洁表达是现在所有写作均要求的，包括国家自然科学基金申报都作了硬性规定页数限制 trans 论文免费页数实际就是他们希望一篇论文的长度，一般不得超过期免费长度 2 页

精简到 12 页内