周报 向嘉豪(2026-01-26)

摘要: 本周完成第四篇小论文的精简工作，将论文篇幅从 15 页压缩至 7 页，删除 514 行冗余内容并新增 174 行精炼表述。同时完成硕士学位论文第三章面向资源受限环境的 CRAFT 密码 FPGA 高效实现的撰写工作。第三章系统阐述了 CRAFT 算法的结构与规范，提出串行与展开两种 FPGA 优化实现架构，利用 SAT 求解器优化 S 盒实现使面积减少 28.9%，并在 Artix-7、Kintex-7、Spartan-7 三种 FPGA 平台上进行了全面的性能评估。

下周计划: 1) 修改第四篇小论文 2) 继续完成第四章面向 32 位处理器的 SPN 密码比特切片低延迟实现的撰写工作

1 第四篇小论文精简

完成了第四篇小论文的篇幅精简工作，将论文从原有的 15 页压缩至 7 页，以满足期刊投稿要求。本次修改删除了 514 行冗余内容，新增 174 行精炼表述，整体精简幅度约为 50%。精简工作遵循 AGENTS.md 中定义的写作规范，在保留核心贡献和关键实验结果的前提下，对以下部分进行了重点压缩：Related Work 部分删除了过多的历史背景介绍，聚焦于本研究填补的具体空白；算法描述部分简化了优化技术的实现细节，保留核心算法结构的完整性；实验方法部分合并了重复的测量方法说明，减少了统计方法的冗余描述。

精简后的论文结构更加紧凑，核心贡献的表述更为清晰。通过删除冗余的部署配置示例和过度详细的性能分析，使论文能够在有限篇幅内完整呈现研究的创新点和实验验证结果，提升了论文的可读性和投稿竞争力。

2 硕士学位论文撰写

2.1 第三章 CRAFT 密码 FPGA 高效实现

完成了第三章面向资源受限环境的 CRAFT 密码 FPGA 高效实现的撰写工作，该章节包括 CRAFT 算法结构与规范、FPGA 优化实现方法和实现结果与资源评估三个主要部分。本章首次在 FPGA 平台上实现了 CRAFT 轻量级密码，提出串行与展开两种架构分别优化面积与吞吐率。

CRAFT 算法结构与规范部分详细描述了 CRAFT 作为轻量级可调块密码的基本特性，包括 64 位明文、128 位密钥和 64 位杂凑的输入输出规范。轮函数由列混合、字节置换和 S 盒三部分组成，其中列混合采用自反矩阵实现加解密复用，S 盒为 4 位输入输出的非线性变换。

FPGA 优化实现方法部分提出了两种架构设计。串行架构将数据通路宽度从 64 位降为 4 位，通过复用硬件资源降低面积，S 盒数量由 16 降为 1，并采用时钟门控技术降低能耗。基于 SAT 求解器的 S 盒优化采用 GEC 编码方案，最终方案采用 4 个 MOAI1 门、3 个 MAOI1 门和 1 个 AND3 门，面积较现有方案减少 28.9%。展开架构每周期执行 2 轮函数，可在 16 个周期内完成加密，相比迭代架构的 32 周期实现吞吐率翻倍。

实现结果与资源评估部分在 Artix-7、Kintex-7、Spartan-7 三种 FPGA 平台上进行了全面测试。实验结果表明，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%。性能评估指标包括 FF、LUT、Slice 等面积指标，以及最大吞吐率、100MHz 下吞吐率、单位 Slice 吞吐率等吞吐率指标，同时对动态功耗、静态功耗和能耗进行了详细分析。