周报 向嘉豪(2026-01-19)

摘要: 本周完成硕士学位论文第一章绪论与第二章基础知识的撰写工作，并采用 IEEE Trans 模板完成第四篇小论文撰写。第一章论述了 SPN 结构密码在物联网和云计算环境中的应用需求，明确了 CRAFT 密码 FPGA 实现、SPN 密码比特切片优化和 AES GPU 并行优化三个研究方向；第二章以 AES-128 为例阐述了 SubBytes、ShiftRows、MixColumns 和 AddRoundKey 的设计原理，并系统介绍了查找表、比特切片、SIMD 向量化等软件实现技术和迭代架构、串行架构、展开架构等硬件实现技术。 小论文完成“ML-DSA Digital Signatures in Resource-Constrained MQTT Environments”的 IEEE Trans 格式撰写，研究 ML-DSA 后量子签名在资源受限 MQTT 环境中的集成与评估，提出了自适应安全级别选择协议。由于论文篇幅过长(约 942 行)，制定了论文长度优化方案，精简约 15%(139 行)以满足 IEEE Trans 10-12 页要求。

下周计划: 继续完成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，同时完善第四篇小论文。

1 硕士学位论文撰写

1.1 第一章绪论撰写

完成了论文第一章绪论部分的撰写工作，该章节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主要部分。选题背景部分阐述了 SPN 结构密码在现代分组密码设计中的主流地位及其在物联网安全领域的应用需求，分析了物联网设备资源受限性与安全需求复杂性之间的矛盾，以及数据中心和云计算平台面临的高吞吐量密码学挑战。研究意义部分从理论意义和实际应用价值两个维度进行了论述，理论意义涵盖硬件实现理论、软件实现理论和并行计算理论三个层面，实际应用价值涉及物联网安全、嵌入式系统安全和云计算数据中心三个领域。

国内外研究现状部分从轻量级密码硬件实现、比特切片密码软件实现和 GPU 并行密码实现三个方向对相关研究进行了系统综述。轻量级密码硬件实现部分涵盖了 PRESENT、LED、Midori、GIFT、CRAFT 等密码的设计与实现进展，比特切片密码软件实现部分介绍了从 Biham 提出的比特切片技术到针对 32 位处理器的优化方法，GPU 并行密码实现部分分析了 AES 算法在 GPU 平台上的并行优化特性。研究内容部分明确了论文的三个主要研究方向：面向资源受限环境的 CRAFT 密码 FPGA 高效实现、面向 32 位处理器的 SPN 密码比特切片低延迟实现、以及面向 GPU 的 AES 算法线程自适应并行优化实现。

1.2 第二章基础知识撰写

完成了第二章 SPN 结构密码的软硬件优化实现基础知识的撰写工作，该章节系统介绍了 SPN 密码基本原理、软件实现技术和硬件实现技术三个方面的理论基础。在 SPN 密码基本原理部分，从数学角度形式化定义了 S 盒变换和线性变换，给出了 S 盒比特函数、S 盒变换、线性变换和线性变换矩阵的严格数学定义。以 AES-128 为例详细分析了 SubBytes、ShiftRows、MixColumns 和 AddRoundKey 四个基本操作的设计原理与实现方式，阐述了 SPN 结构通过替代层和线性层的协同作用实现 Shannon 混淆和扩散原理的安全机制。

软件实现技术部分介绍了查找表实现、比特切片实现和 SIMD 向量化实现三种主要技术路线。查找表实现通过预先计算的输入输出映射关系将运行时计算转换为内存访问操作，比特切片技术通过将密码操作映射到位级布尔运算利用处理器的位并行性同时处理多个数据分组，SIMD 向

量化技术通过宽位向量寄存器进一步提升比特切片实现的并行度。硬件实现技术部分介绍了ASIC 和 FPGA 两类平台，详细阐述了迭代架构、串行架构和展开架构三种实现架构的特点与适用场景，分析了 S 盒的查找表方法和逻辑门电路方法，以及线性层比特置换和矩阵乘法的硬件实现优化策略。

2 第四篇小论文撰写

完成了题为“ML-DSA Digital Signatures in Resource-Constrained MQTT Environments”的 IEEE Trans 格式论文撰写工作。该论文研究 ML-DSA 后量子数字签名算法在资源受限物联网环境中的集成与性能评估，针对 MQTT 协议提出了自适应安全级别选择协议。论文的主要贡献包括三个方面：提出了根据设备资源状态、消息关键性和操作上下文动态选择 ML-DSA 参数集的自适应安全级别选择协议，相比固定最高安全配置降低了 23-31% 的平均计算开销；在 ARM Cortex-M4 微控制器上进行了 ML-DSA 签名操作的周期精确测量，量化了三种标准化参数集的执行延迟和吞吐量；评估了 MQTT 发布-订阅工作流中的端到端延迟和消息大小开销。

第四篇小论文当前篇幅过长(约 942 行)，需按 IEEE Trans 要求精简至 10-12 页。建议精简约 139 行(约 15%)，重点保留核心贡献、自适应协议设计和实验结果。

- **Related Work 部分**: 精简约 12 行，删除部分背景历史介绍，聚焦本论文填补的研究空白
- **ML-DSA 算法描述部分**: 精简约 28 行，简化优化技术细节，保留核心算法结构描述
- **实现架构部分**: 精简约 24 行，合并硬件平台与软件架构描述，删除重复内容
- **自适应协议部分**: 精简约 20 行，删除冗余的部署配置示例，保留核心机制
- **实验方法部分**: 精简约 15 行，合并测量方法描述，减少重复的统计方法说明
- **结果分析部分**: 精简约 40 行，合并相似表格，删除部分过度详细的性能分析