周报

2025-12-22

本周研究摘要

ML-DSA 论文全文内容精炼与学术表达优化

Introduction 章节优化

内容精炼：

- 消除冗余强调副词（“fundamentally” → 直接陈述）
- 避免主观程度判断（“severe/prohibitive” → “degradation/overhead”）

贡献陈述重构为可测量技术指标：

- Computational Performance：周期级测量，ARM Cortex-M4 168 MHz
- Memory Utilization：Flash/Stack/SRAM 峰值量化
- Protocol Integration：端到端延迟与消息开销评估

Related Work 章节改进

学术表达规范化：

- 消除冗余连接词（“While...have undergone” → 直接陈述）
- 明确研究空白（“IoT-specific protocols remain underexplored”）

技术准确性提升：

- 性能数据量化（“order-of-magnitude throughput reductions”）
- 参数格式统一（“1.38–1.51”标准化表示）

ML-DSA Algorithm 章节优化

技术参数精确化：

- 拒绝采样迭代次数：建立参数集直接对应（4.25/5.1/3.85）
- 密钥尺寸：标准化单位表示（1.3–4.9,KB）

算法描述简化：

- 采用直接算法引用方式
- 确定性签名变体表述压缩
- NTT 性能瓶颈描述精简（2.5–3.0 million cycles）

总结

下周计划

- 完善 Results 章节实验数据分析
- **1 月初 博士申请复试**

老师评语

现在就要根据拟投期刊风格与格式去写了

已初步修改