周报 - 大论文三个核心章节翻译

2025-09-09

本周研究摘要

本周完成大论文三个核心论文章节中文翻译工作：

- 第三章 CRAFT 算法实现：串行架构面积减少 10.16%，展开架构吞吐量提升 40.53%
- 第四章 32 位处理器 SPN 密码：指令数减少 64.3%，BGC 编码加速 3.19 倍，AES 和 QARMAv2 性能分别改进 9.7% 和 67.6%
- 第五章 GPU SLH-DSA 并行架构：实现 62,239 签名/秒，性能提升 1.16 倍

第三章：CRAFT 密码算法高效实现

FPGA 实现架构优化：

- 串行架构：面积减少 10.16%
- 展开架构：吞吐量提升 40.53%

S 盒优化技术创新：

- SAT 求解器 + GEC 编码优化
- 硬件实现效率提升

第四章：32 位处理器 SPN 密码 Bitsliced 实现

置换优化算法突破：

- 指令数减少 64.3%
- 增强 BGC 编码：性能加速 3.19 倍

性能验证成果：

- AES 算法：性能改进 9.7%
- QARMAv2 算法：性能提升 67.6%

第五章：GPU SLH-DSA 线程自适应优化

核心技术创新：

- Thread-Adaptive Allocation (ATA)
- Function-Level Parallelization (FLP)

性能成果验证：

- 62,239 签名/秒 处理能力
- 性能提升 1.16 倍 先进性改进

总结

下周计划

- 第四篇论文撰写工作 继续推进
- 大论文摘要和目录 完善

老师评语

你这那有第 4 篇论文的内容报告??

本周主要完成小论文翻译，下周重点推进第四篇论文撰写工作