周报 向嘉豪(2025-09-08)

摘要: 本周完成大论文三个核心论文章节中文翻译。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。

下周计划: 1) 继续第四篇论文的撰写工作。 2) 开展后翻译阶段工作，包括全面技术审查、章节间逻辑整合、术语标准化统一，以及大论文最终稿的质量保障工作。

1 大论文 三个核心章节翻译

1.1 第三章：CRAFT 密码算法高效实现方法研究

本周完成了第三章的全面中文翻译工作，该章节系统性阐述了 CRAFT 轻量级密码算法的高效实现方法研究。翻译内容涵盖了 FPGA 平台上的串行和展开架构实现方案，以及基于 SAT 求解器和 GEC 编码的 S 盒优化技术。通过精确的技术术语转换和学术语言规范化，确保了中文版本完整保持了原有的技术深度和研究贡献。

FPGA 实现架构翻译 系统性翻译了串行架构和展开架构两种不同的 FPGA 实现方案。串行架构的翻译重点强调了其在硬件资源占用方面的优化特性，通过详细的中文技术描述展现了 10.16% 的面积减少效果。展开架构的翻译则着重体现了并行处理能力的增强，准确传达了 40.53% 的吞吐量提升这一关键性能指标。

S 盒优化技术的中文表述 完成了基于 SAT 求解器和 GEC(Gray Equivalence Class)编码的 S 盒优化方法的专业翻译。这一部分的翻译工作特别注重了密码学专业术语的准确性，确保了技术概念在中文语境下的精确传达。GEC 编码优化策略的中文阐述清晰地展现了该技术在硬件实现中的创新价值。

1.2 第四章：32 位处理器上 SPN 密码的 Bitsliced 低延迟实现

第四章的翻译工作聚焦于 32 位处理器平台上 SPN(Substitution-Permutation Network)密码的 Bitsliced 实现技术。该章节的中文翻译全面涵盖了置换优化算法、增强 BGC 编码技术，以及在 AES 和 QARMAv2 算法上的具体性能改进成果。翻译过程中特别注重了技术实现细节的准确传达和性能指标的量化表述。

置换优化算法的技术突破 完成了置换优化算法部分的深度翻译，该算法实现了 64.3% 的指令数减少这一显著成果。中文翻译准确传达了该算法在 32 位处理器环境下的技术创新性，特别是在指令级优化方面的突破性贡献。通过精确的技术语言转换，确保了算法的核心思想和实现策略在中文版本中的完整体现。

增强 BGC 编码性能提升 系统性翻译了增强 BGC 编码技术及其 3.19 倍的性能加速效果。这一部分的翻译工作特别关注了编码技术的理论基础和实际应用效果的平衡表述，确保中文读者能够准确理解该技术的创新点和实用价值。BGC 编码在 S 盒实现中的优化作用通过详细的中文技术描述得到了充分展现。

AES 和 QARMAv2 性能验证 完成了 AES 算法 9.7% 性能改进和 QARMAv2 算法 67.6% 性能提升的详细翻译工作。这一部分的中文表述重点强调了实验验证的严谨性和结果的可信度，通过准确的性能指标翻译展现了研究工作的实际应用价值。

1.3 第五章：GPU 上 SLH-DSA 的线程自适应优化并行架构

第五章的翻译工作涵盖了后量子密码学领域的 GPU 加速实现技术，重点阐述了 SLH-DSA(Stateless Hash-based Digital Signature Algorithm)的线程自适应分配(ATA)和函数级并行化(FLP)优化策略。该章节的中文翻译完整保持了后量子密码学的技术严谨性和 GPU 并行计算的专业深度。

线程自适应分配技术的创新翻译 系统性完成了 Thread-Adaptive Allocation(ATA)技术的中文翻译，该技术是实现 GPU 高效并行计算的核心创新。翻译工作特别注重了自适应分配机制的技术原理阐述，确保中文读者能够准确理解该技术在 GPU 资源优化中的关键作用。ATA 技术与传统并行策略的对比分析通过详细的中文技术描述得到了充分体现。

函数级并行化策略实现 完成了 Function-Level Parallelization(FLP)技术的专业翻译，该技术进一步增强了 GPU 并行计算的效率。FLP 技术的中文表述重点强调了其在后量子密码算法中的特殊适用性，以及与 ATA 技术结合时产生的协同优化效果。通过精确的技术术语转换，确保了该技术在中文学术语境下的准确传达。

性能验证和先进性对比 系统性翻译了 62,239 签名/秒的性能成果和 1.16 倍的先进性改进指标。这一部分的中文翻译特别注重了性能评估方法的严谨性表述和对比实验的公正性说明。通过详细的性能数据翻译和技术对比分析，充分展现了研究工作在后量子密码 GPU 加速领域的贡献价值。