周报 向嘉豪(2025-07-28)

摘要: 本周完成三项核心工作。7 月 25 日完成第二篇论文审稿回复和提交，回应编辑和审稿人所有关切。完成省级项目结题报告撰写，围绕 5 篇论文（1 篇已发表，2 篇审稿中，2 篇合作）总结密码算法优化研究成果。深入研读第三篇论文大修意见，明确性能分解分析、算法背景补充、工具验证增强三个改进方向。

下周计划: 集中精力回应第三篇论文的大修意见，重点完成 性能分解分析和 GPU 性能剖析，补充算法实现细节和相关背景介绍。

第二篇论文审稿回复最终提交

审稿回复完成情况

7 月 25 日完成了第二篇论文《Low-Latency Implementation of Bitsliced SPN-Cipher on IoT Processors》的最终审稿回复和提交工作。经过系统性的修订，我们成功回应了编辑和审稿人提出的所有核心关切。

编辑关注的四个主要问题均已得到充分解决：新颖贡献清晰阐述 通过 Table IV 展示了 7 种 S 盒的详细时序对比；NIST 标准适用性论证 通过 GIFT-COFB 实验验证了 19.5% 的性能提升；公平性能比较 修正了跨平台比较问题，证明了 22.5% 的性能优势；参考文献和写作质量 进行了全面的校对和更新。

项目结题材料完成

围绕 5 篇论文编写省级项目结项报告：

已发表论文 1 篇：

- 《Efficient implementations of CRAFT cipher for Internet of Things》(Computers and Electrical Engineering, 2024)

审稿中论文 2 篇：

- 《Low-Latency Implementation of Bitsliced SPN-Cipher on IoT Processors》(IEEE Transactions on Computers, R2 阶段)
- 《Thread-Adaptive: High-Throughput Parallel Architectures of SLH-DSA on GPUs》(IEEE Computer Architecture Letters, R1 阶段)

合作论文 2 篇：

- 《Optimizing label correlation in deep learning-based side-channel analysis》(Microelectronics Journal, 2025)
- 《Tripm: a multi-label deep learning SCA model for multi-byte attacks》(International Journal of Machine Learning and Cybernetics, 2025)

第三篇论文大修意见研读

审稿意见核心关切

深入研读了第三篇论文《Thread-Adaptive: High-Throughput Parallel Architectures of SLH-DSA on GPUs》的大修意见，明确了三位审稿人的核心关切和改进方向。

审稿人 1（小修建议） 主要关注性能分解分析的细化。要求提供线程分配优化和函数级并行的具体贡献分解，以及 GPU 计算和内存利用率的详细剖析数据。这需要我们补充更精细的性能测量和分析框架。

审稿人 2（拒稿建议） 指出了算法背景介绍不足的问题。主要关切包括：SLH-DSA 算法细节缺乏、数据流和架构设计动机不明确、硬件级评估工具使用不足。需要大幅补充算法实现细节和使用 NVIDIA Nsight 等专业分析工具。

审稿人 3（大修建议） 强调了分析模型的完整性问题。指出性能模型的剖析精度损失讨论不足，内存影响分析缺失，特别是在大规模应用场景下的内存含义需要深入探讨。

改进策略制定

基于审稿意见分析，制定了系统性的改进策略：

性能分解分析强化： 需要实现更细粒度的性能测量框架，分别量化 ATA 和 FLP 技术的具体贡献，提供 GPU 利用率、缓存行为、占用率等详细指标。

算法背景补充： 大幅扩展 SLH-DSA 算法的技术细节介绍，包括 WOTS+、FORS、Hypertree 等核心组件的工作原理，以及我们的并行化设计动机和实现细节。

工具验证增强： 集成 NVIDIA Nsight Compute 等专业 GPU 性能分析工具，提供硬件级的执行分析和优化验证，增强技术贡献的可信度。