

周报 向嘉豪(2025-08-04)

摘要: 本周专注于第三篇论文《Thread-Adaptive: High-Throughput Parallel Architectures of SLH-DSA on GPUs》的大修回复工作。成功完成了三项关键修订任务，包括**新颖性贡献阐述**、**术语精确性修正**和**SLH-DSA 算法细节回应**。完成了对审稿意见 1.3、1.4 和 2.1 评论的详细响应，明确区分了我们的架构创新与现有工作的差异。当前需要集中精力完成两项重要的实验性工作：性能分解分析和 GPU 性能剖析实验。

下周计划: 完成第三篇论文剩余的实验性修订要求，重点实施**性能分解分析实验**和**GPU 硬件级性能剖析**，使用 NVIDIA Nsight 工具获取详细的计算和内存利用率数据，完善审稿意见 2.2、2.3 和 3.1、3.2 评论的技术回应。

1 第三篇论文审稿回复进展

1.1 已完成修订任务总结

本周在第三篇论文的修订工作中取得了显著进展，成功完成了计划中五项任务的前三项核心修订工作。这些已完成的任务均属于无需额外实验的理论分析和内容完善类别，为后续的实验性工作奠定了坚实基础。

任务 1: SLH-DSA 算法细节补充（已完成） 针对审稿意见 2.1 提出的算法背景不足问题，我们提供了全面的技术回应。考虑到期刊的 4 页篇幅限制，我们在回复中明确说明了论文重点关注架构创新和性能优化技术，而非算法本身的密码学细节。我们引导读者参考 FIPS 205 官方标准获取详细的算法规范，同时在修订版本中增强了方法介绍的技术背景和实现脉络。

任务 2: 新颖性贡献明确阐述（已完成） 这是本次修订工作的重点任务，回应了审稿意见 1.3 和 2.1 关于技术贡献区分度的核心关切。我们系统性地重新组织了第 III.B 节的内容结构，使用蓝色标记清晰区分了我们的原创性贡献与现有工作的基础技术。具体而言，在 WOTS+ 并行化方面，我们突出了针对超树结构的战略性共享内存缓冲区利用技术；在 FORS 并行化中，强调了树构建过程中的优化共享内存缓冲区聚合中间根节点的创新方法；在超树并行化领域，详细阐述了我们独特的半并行方法，采用四节点组合的分层执行策略，相比于现有工作的双节点方法实现了更高的内存效率和更低的同步开销。

任务 3: 术语精确性修正（已完成） 响应审稿意见 1.4 的精确性建议，我们将论文中的“理论最优线程数”统一修正为“经验确定的最优线程数”。这一术语调整更准确地反映了我们通过实证性能建模和线程数量扫描实验获得最优配置的科学方法，避免了对纯理论分析的误导性表述。

2 待完成实验性修订要求

2.1 性能分解分析需求

审稿意见 1.1、2.2 和 3.1 的评论集中指向一个核心技术问题：需要提供我们提出的自适应线程分配和函数级并行两种技术的独立性能贡献分析。当前的表格 II 展示了线程分配优化的单独效果，而表格 III 呈现的是聚合结果，审稿人要求我们量化每种方法对整体性能提升的具体贡献度。

这项工作需要我们设计和实施细粒度的性能测量框架，分别禁用和启用不同的优化技术，通过对照实验准确测量各技术分量的性能影响。同时需要包含分析计算负载特征的剖析结果，支撑我们关于 SLH-DSA 算法计算需求的技术论断。此外，还需要深入讨论基于剖析的性能模型可能存在的精度损失和应用局限性。

2.2 GPU 硬件级性能剖析要求

审稿意见 1.2、2.3 和 3.2 强调了硬件级评估的重要性，特别要求使用 NVIDIA Nsight Compute 等专业 GPU 性能分析工具获取详细的计算和内存利用率指标。这项工作需要我们多个维度深入分析 GPU 执行特征：计算单元利用率分析需要展现不同 SLH-DSA 组件在 GPU 多处理器上的负载分布情况；缓存行为和占用率分析要求深入研究内存访问模式对 GPU 缓存层次结构的影响；端到端执行分解需要提供完整的计算流水线分析。

内存影响分析是另一个重要维度，特别是在大规模应用场景下的可扩展性含义。我们需要提供详细的内存需求分析，包括不同参数集下的内存使用模式，以及内存瓶颈对整体性能的制约效应。这些数据将为我们的架构设计决策提供坚实的硬件层面验证。

3 下阶段工作策略

基于当前的修订进展和剩余任务的技术要求，下周的工作将集中于实验性验证和数据收集。首要任务是构建性能分解分析的实验框架，通过系统性的消融研究量化各优化技术的独立贡献。这需要我们重新组织代码结构，支持选择性地启用或禁用特定的优化模块。

GPU 性能剖析工作将采用 NVIDIA Nsight Compute 作为主要分析工具，结合 NVIDIA Visual Profiler 进行补充验证。我们将从计算密集度、内存带宽利用率、指令吞吐量、缓存命中率等多个维度全面分析我们的实现效果。特别需要关注不同 SLH-DSA 组件（WOTS+、FORS、Hypertree）的硬件资源利用特征差异，以及我们的优化技术对这些特征的改善效果。

通过这些深入的实验分析，我们预期能够为审稿人提供令人信服的技术验证，展现我们的架构创新在理论分析和实际性能之间的一致性，最终完成这篇重要论文的修订工作。