周报 向嘉豪 (2025 年 4 月 28 日)

摘要： 本周主要完成了论文的修订定稿与IEEE 期刊投稿准备工作。论文方面, 对 Thread-Adaptive: Optimized Parallel Architectures of SLH-DSA on GPUs 进行了系统性优化，明确了线程自适应分配架构与函数级并行方法的技术细节，完善了实验数据与性能分析。投稿准备方面，已按照IEEE TCAS-II期刊要求完成了 Cover Letter 撰写、文档整理与格式规范化等工作。

下周计划： 1) 论文校正与投稿

1 论文修正和投稿准备

1.1 论文修正

本周对论文 Thread-Adaptive: Optimized Parallel Architectures of SLH-DSA on GPUs 进行了最终修订与完善，主要内容包括：对论文架构的核心贡献进行了更清晰的阐述。将三层并行优化架构的描述进行了精炼，包括自适应线程分配（ATA）与函数级并行（FLP）两个关键技术点。自适应线程分配技术通过建立精确的性能模型，为每个密码操作精确校准最佳线程配置，有效平衡了并行计算与同步开销。函数级并行方法将密码操作分解为细粒度计算任务，实现了更高效的资源利用。这两项技术的结合显著提升了 SLH-DSA 在 GPU 平台上的执行性能。

完善了实验数据与性能分析部分。通过系统性的对比实验，明确了在SHA2-128f 参数集下，本方案实现了62,239 次/秒的签名吞吐量，较 Wang 等人的方案提升了 1.15 倍。针对不同参数集的扩展实验表明，对于计算密集型的 SHA2-128s 参数集，吞吐量提升达到了 1.33 倍。

优化了学术表达方式与技术术语。减少了列表环境的使用，改为更连贯的段落叙述，提升了论文的学术性与可读性。精确定义了技术术语，如 small（s）和 fast（f）操作模式的明确解释，增强了论文的专业性。文中图表也进行了优化，增加了签名延迟分布的可视化分析，为读者提供更直观的性能对比。

1.2 期刊投稿准备

完成了面向IEEE Transactions on Circuits and Systems Part II: Express Briefs的投稿准备工作：撰写了专业的Cover Letter。信中系统阐述了论文的三个主要贡献：自适应线程分配框架、函数级并行架构以及全面的性能评估。强调了本研究与期刊范围的高度契合性，特别是在密码硬件实现（DCS120B0）与密码架构（DCS120A5）两个领域。详细说明了研究成果的创新性与实用价值，突出了在量子安全密码学领域的前沿贡献。

按照期刊严格要求整理了投稿材料。IEEE TCAS-II 对篇幅有严格限制——内容部分4.5 页，参考文献0.5 页，总计 5 页。针对此要求，对论文格式进行了专门调整，确保参考文献单独占据最后半页。创建了完整的提交清单，包括主文稿 PDF、LaTeX 源文件压缩包、利益冲突声明等所有必要文件。