周报

2025-04-28

大纲

1. 论文修正

2. 期刊投稿准备

论文修正与完善

核心贡献优化

- 明确阐述了两个关键技术点：
  - 自适应线程分配（ATA）：建立精确性能模型，平衡并行计算与同步开销
  - 函数级并行（FLP）：将密码操作分解为细粒度任务，提高资源利用率
- 优化学术表达方式，减少列表环境，转为连贯段落
- 完善技术术语定义（如 small 和 fast 操作模式）

实验数据与性能分析

性能突破

- SHA2-128f 参数集下，签名吞吐量达62,239 次/秒
- 较现有方案（[WDC+25]）提升1.15 倍
- 对计算密集型 SHA2-128s 参数集，性能提升1.33 倍

可视化增强

- 增加签名延迟分布的可视化分析
- 优化图表表达，提供更直观的性能对比

IEEE TCAS-II 投稿准备

Cover Letter 撰写

强调三个主要贡献：

- 自适应线程分配框架
- 函数级并行架构
- 全面的性能评估

突出与期刊研究领域契合点：

- 密码硬件实现（DCS120B0）
- 密码架构（DCS120A5）

投稿材料准备

期刊要求与调整

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

调整：

- 格式精确调整，确保参考文献单独占据最后半页
- 创建完整提交清单（主文稿 PDF、LaTeX 源文件、利益冲突声明等）

老师评语

摘要的前半部分语言在仔细斟酌一下，并不出彩

学习好的文章，进行修改

参考文献最后一篇格式不正确，也可以考虑替换

已替换

本周计划

- 仔细修改论文

参考文献


Ziheng Wang, Xiaoshe Dong, Heng Chen, Yan Kang, and Qiang Wang.
Cuspx: Efficient gpu implementations of post-quantum signature sphincs⁺.
IEEE Transactions on Computers, 74(1):15–28, 2025.