周报——向嘉豪（2024 年 12 月 31 日）

向嘉豪

衡阳师范学院

2024 年 12 月 31 日

摘要

1. 复现 [LSSH22] 的实验
2. 完善论文写作，初步确定题目

实验复现与结果

在 RTX 4090 平台上复现 [LSSH22] 实验

作者通过数据表示方式的重排降低了线程间等待，并对部分轮密钥的预计算，使 AES 的并行效率提升。使用其实现对 1GB 消息加密，吞吐量可达 3057 Gbps，较 [LSSH22] 中 RTX 3080 平台 (1489 Gbps) 提升近一倍，说明了硬件平台对整体性能的关键影响。表 1呈现了当下的实验结果。

表 1: 基于 GPU 的 AES CTR 模式实现性能对比

实现	吞吐量 (Gbps)	硬件平台	发表年份
[HMKG19]	1,478	Tesla V100	2019
[LSSH22]	1,489	RTX 3080	2022
本文复现	3,057	RTX 4090	—

论文写作进展

论文题目《High Throughput Implementation of AES on GPUs》，(其中 AES 算法需要替换), 并完成了引言与摘要部分的写作

引言突出对称加密在大规模数据传输场景（如数据中心与 5G 网络）实现高吞吐的紧迫需求，同时结合 GPU 并行计算的潜力，对现有研究的局限性与挑战进行概述。后续将在论文中重点介绍 bitslicing 与线程调度的优化方法。

参考文献 I

Omid Hajihassani, Saleh Khalaj Monfared, Seyed Hossein Khasteh, and Saeid Gorgin.
Fast AES implementation: A high-throughput bitsliced approach.
IEEE Trans. Parallel Distributed Syst., 30(10):2211–2222, 2019.

Wai-Kong Lee, Hwa Jeong Seo, Seog Chung Seo, and Seong Oun Hwang.
Efficient implementation of aes-ctr and aes-ecb on gpus with applications for high-speed frodokem and exhaustive key search.
IEEE Transactions on Circuits and Systems II: Express Briefs, 69:2962–2966, 2022.

老师评语

不要用 AES，建议用最新顶刊或顶会的一个密码算法（最好是别人没做过的）

寻找一个新的密码算法

本周计划

1. 继续深入阅读 [LSSH22] 的 GPU 实现代码
2. 寻找最新顶会或顶刊的密码算法