周报-向嘉豪 (2024-12-30)

摘要：围绕 GPU 加速下 AES 实现的实验与论文写作开展工作。通过阅读 [LSSH22] 并复现其在 RTX 4090 环境下的实验设置，我们成功获得了对 1GB 消息加密可达 3057 Gbps 的速度。同时，我们也初步确定了论文的题目《High Throughput Implementation of AES on GPUs》，并对引言部分进行了初步写作。

下周计划：1）仔细阅读 [LSSH22] 的代码，和 [HMKG19] 论文，2）继续论文写作，思考我们优化实现的方案。

1 论文实验

本周主要对 [LSSH22] 一文进行了细致的阅览与实验复现。作者在该文中通过对数据表示方式的重新排列，去除了线程间运行的等待时间，并预计算部分轮密钥，从而有效提升 AES 的并行效率。我们依照其公开的实验配置在 RTX 4090 平台上进行测试时，针对 1GB 消息加密达到了 3057 Gbps，相较 [LSSH22] 原文在 RTX 3080 中测得的 1489 Gbps 提升近一倍。我们推测，硬件平台的性能差异在其中发挥了主导性作用。表 1展示了现阶段的实验结果。我们之后的目标是将吞吐量提升至 3057 Gbps 以上。

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	—

2 论文写作

我们初步确定了题目《High Throughput Implementation of AES on GPUs》，并对引言与摘要写作。引言部分强调了 AES 在大规模数据传输（如数据中心、5G 网络等）环境下实现高吞吐的紧迫需求，结合 GPU 大规模并行计算的潜能性，对当前研究的差距和挑战进行初步分析。为解决传统软件与扩展指令架构在 Gbps 到 Tbps 量级数据吞吐范围内的局限性，我们计划在论文中集中展示 bitslicing 技术与线程调度方法的优化思路，以缓解缓存未命中和线程阻塞对性能的影响。

参考文献

[HMKG19] 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.

[LSSH22] 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.