周报——向嘉豪（2024 年 12 月 24 日）

向嘉豪

衡阳师范学院

2024 年 12 月 24 日

本周主要工作

- 第二篇投稿
- 第三篇论文背调

第二篇投稿

在准备投稿的过程中，研究了 *Computer* 期刊的选题方向与投稿要求，并完成了针对最合适 Topic 的初步匹配。由于个人 Biography 信息不全导致稿件被退回，我们已补充完成该部分并再次提交，以期进入下一轮审查。

第三篇论文背调

在第三篇论文的背景调研中，我们考察了安全性、性能与成本三者间的关联，并针对不同安全等级与性能需求分析了软硬件加速方案。结论显示：若在高度安全的同时追求更高性能，则对应硬件加速；若严格控制成本，则性能相对较低，多采用纯软件实现。针对中等成本与中等性能，软硬件结合能够在绿色、蓝色区域之外形成平衡（红色区域）。

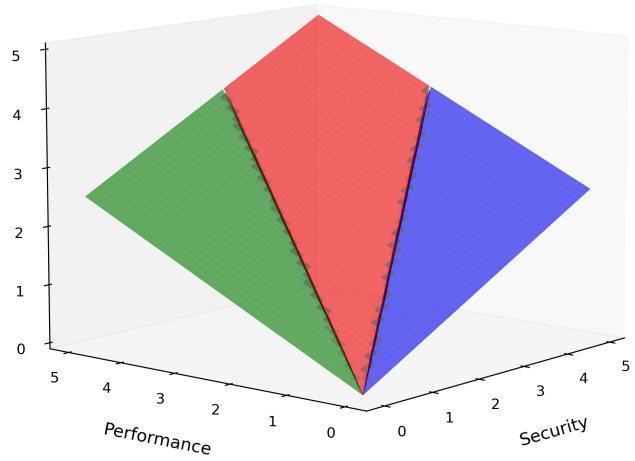

图 1: 安全性、性能和成本的关系

Related Work: GPU-Based Cipher Implementations (Part I)

Paper Name	**Year**	**Publication**
Speed Record of AES-CTR and AES-ECB Bit-Sliced Implementation on GPUs	2024	IEEE EMBEDDED SYSTEMS LETTERS
Optimized GPU Implementation and Performance Analysis of HC Series of Stream Ciphers	2012	Information Security and Cryptology
High Throughput Implementation of Post-quantum Key Encapsulation and Decapsulation on GPU for IoT Applications	2021	IEEE Transactions on Services Computing
Fast AES Implementation – A High-Throughput Bitsliced Approach	2019	IEEE Transactions on Parallel and Distributed Systems

表 1: Summary of GPU-based cipher implementations (Part I)

Related Work: GPU-Based Cipher Implementations (Part II)

Paper Name	Year	Publication
Efficient Implementation of AES-CTR and AES-ECB on GPUs With Applications for High-Speed FrodoKEM and Key Search	2022	IEEE Transactions on Circuits and Systems II: Express Briefs
ACE-HoT–Accelerating an Extreme Amount of Symmetric Cipher Evaluations for High-Order Avalanche Tests	2023	International Conference on Cryptology and Information Security

表 2: Summary of GPU-based cipher implementations (Part II)

其中，我们可以仿写“IEEE Transactions on Circuits and Systems II: Express Briefs”，中 5 页的短报。注：CHSE 也有 GPU 实现工作，但多是为 AI 模型服务的同态加密方向，与大论文无相关性。

老师评语

写作思路正确，我就是看的哪几篇期刊论文，然后在这几篇论文基础上就瞄定这个期刊主题写作

写完第 3 篇后，可以思考点原始创新，如密码困难待解问题或现在大家公开提出的问题如何突破

写完大论文的三篇后，向原始创新方向思考。

本周计划

- 复现和优化 AES 的 GPU 实现