周报-向嘉豪（2024 年 12 月 10 日）

向嘉豪

衡阳师范学院

2024 年 12 月 10 日

摘要

本周主要工作

- **论文修订**
- **投稿准备**

论文修订与规范化

针对 IEEE 期刊的格式要求，我们对论文进行了修订，主要包括以下方面：

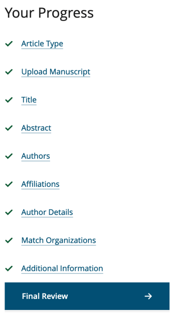
1. **符号体系规范化**：
   - 引入了 `amssymb` 数学符号库，解决了特殊数学符号（如 $\ggg$）的显示问题。
   - 对全文的数学公式和符号进行了统一规范，确保符号使用的一致性和准确性。
2. **参考文献完善**：
   - 补充了参考文献中缺失的页码范围和期刊卷号等信息。

投稿准备工作

我们按照 IEEE 计算机学会的出版指南，系统地完成了投稿准备工作：

1. **熟悉投稿流程**：
   - 深入研究了 IEEE Author Portal 系统（见图1a），详细了解投稿的每个步骤。
2. **撰写投稿信**：
   - 按照期刊要求，撰写了投稿信（见图1b），突出论文的创新性和研究意义。
3. **选择合适期刊**：
   - 考虑到 *IEEE Transactions on Information Forensics and Security* 偏重理论研究，经导师指导，决定将论文投向 *IEEE Transactions on Computers*。

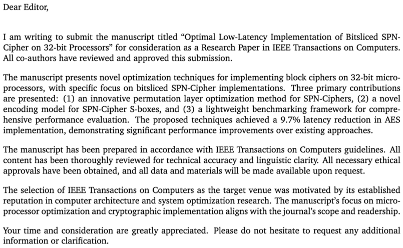
投稿材料



Your Progress

- ✓ Article Type
- ✓ Upload Manuscript
- ✓ Title
- ✓ Abstract
- ✓ Authors
- ✓ Affiliations
- ✓ Author Details
- ✓ Match Organizations
- ✓ Additional Information

(a) IEEE Author Portal 投稿流程



Dear Editor,

I am writing to submit the manuscript titled “Optimal Low-Latency Implementation of Bitsliced SPN-Cipher on 32-bit Processors” for consideration as a Research Paper in IEEE Transactions on Computers. All co-authors have reviewed and approved this submission.

The manuscript presents novel optimization techniques for implementing block ciphers on 32-bit microprocessors, with specific focus on bitsliced SPN-Cipher implementations. Three primary contributions are presented: (1) an innovative permutation layer optimization method for SPN-Ciphers, (2) a novel encoding model for SPN-Cipher S-boxes, and (3) a lightweight benchmarking framework for comprehensive performance evaluation. The proposed techniques achieved a 9.7% latency reduction in AES implementation, demonstrating significant performance improvements over existing approaches.

The manuscript has been prepared in accordance with IEEE Transactions on Computers guidelines. All content has been thoroughly reviewed for technical accuracy and linguistic clarity. All necessary ethical approvals have been obtained, and all data and materials will be made available upon request.

The selection of IEEE Transactions on Computers as the target venue was motivated by its established reputation in computer architecture and system optimization research. The manuscript’s focus on microprocessor optimization and cryptographic implementation aligns with the journal’s scope and readership.

Your time and consideration are greatly appreciated. Please do not hesitate to request any additional information or clarification.

(b) 投稿信示例

图 1: 论文投稿材料准备

老师评语

去看下拟投稿期刊论文，对自己的论文再提升一下

依据该期刊 2020 年收录《Efficient Software Implementation of Ring-LWE Encryption on IoT Processors》软件实现优化论文，对论文进行修改。

本周计划

完善论文