周报-向嘉豪 (2024-12-09)

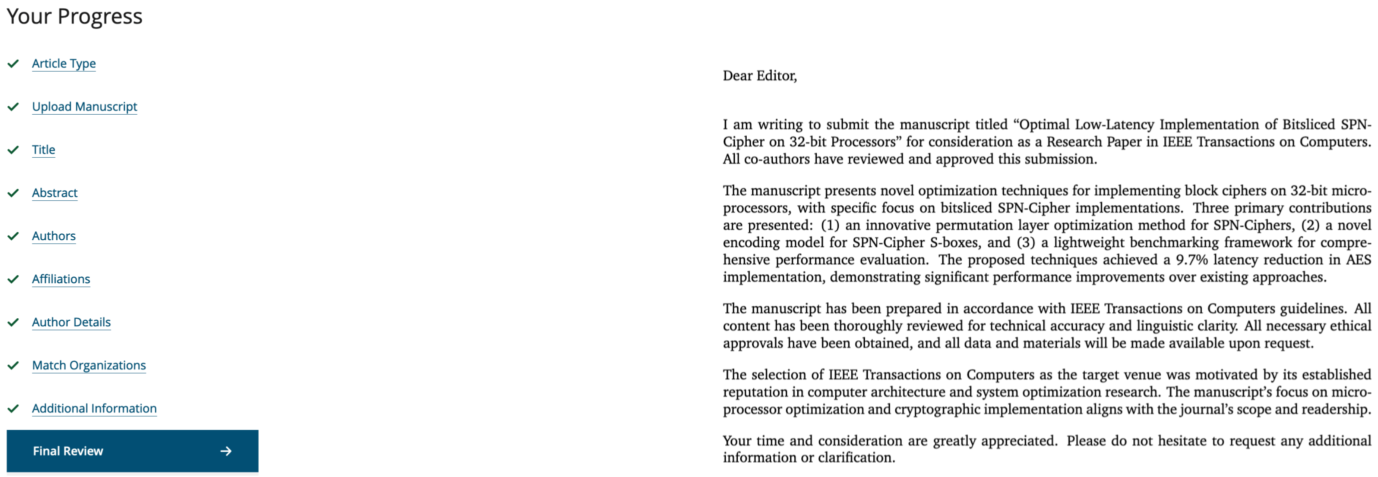
Abstract: 本周工作主要聚焦于论文的最终修订与投稿准备工作。在论文修订方面，我们完成了以下工作：1）通过引入 amssymb 数学符号库，规范了全文的数学公式与符号体系；2）完善了参考文献的基础信息，确保符合 IEEE 引用规范。在投稿准备方面：1）基于 IEEE 计算机学会出版指南完成了投稿材料准备；2）深入研究 IEEE Author Portal 系统，熟悉了投稿流程；3）经过审慎考虑，决定将论文投向 IEEE Trans. on Computers。
下周计划: 1）完成 IEEE Trans. on Computers 的在线投稿

0.1 论文修订与规范化

针对 IEEE 期刊格式要求，我们对论文进行了系统性修订。在符号体系方面，通过引入 amssymb 数学符号库，解决了特殊数学符号（如 $\ggg$）的显示问题。同时，对全文的数学公式和符号进行了统一规范。在文献引用方面，我们完善了所有参考文献的基础信息，包括补充缺失的页码范围和期刊卷号，确保符合 IEEE 引用规范。

0.2 投稿准备工作

基于 IEEE 计算机学会出版指南（`https://www.computer.org/publications/author-resources`），我们完成了投稿材料的系统性准备工作。通过深入研究 IEEE Author Portal 系统（见图 1a），我们熟悉了完整的投稿流程，并按要求撰写了投稿信（见图 1b）。考虑到研究内容的性质以及 IEEE Trans. on Info. Forensics and Security 偏重理论性研究的特点，经老师指导后，决定将论文投向 IEEE Trans. on Computers。目前，所有投稿材料均已完备，即将开始投稿程序。



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.

(a) 投稿流程

(b) 投稿 cover letter

图 1: 论文投稿材料准备