周报——向嘉豪（2024 年 12 月 17 日）

向嘉豪

衡阳师范学院

2024 年 12 月 17 日

摘要

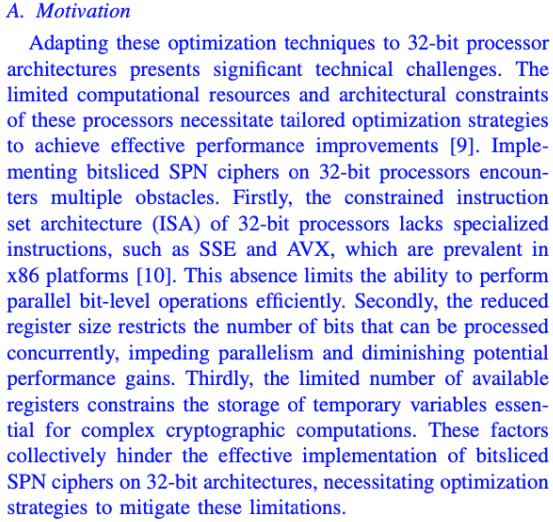
本周主要工作

- 摘要的修改与完善
- 实验章节的改进

摘要的修改与完善

在参考了 *IEEE Transactions on Computers* 中相关文献 [LAKS20] 后，我们对论文摘要进行了细致的调整：

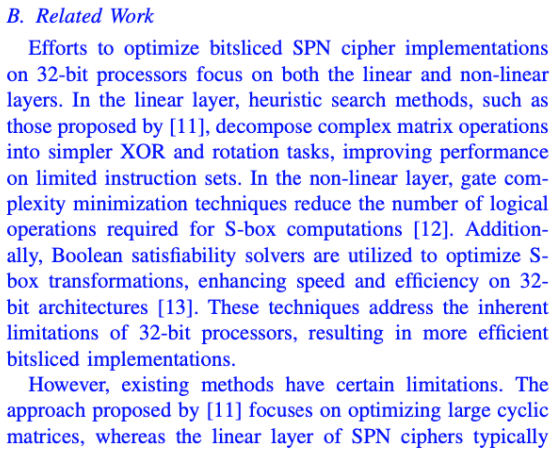
1. 将摘要细分为多个小节，新增“动机”和“相关工作”两个部分。
2. 在“动机”部分（见图1a），详细阐述了研究问题的重要性和必要性。
3. 在“相关工作”部分（见图1b），对现有研究进行了系统综述，明确了本研究的创新点和贡献。



A. Motivation

Adapting these optimization techniques to 32-bit processor architectures presents significant technical challenges. The limited computational resources and architectural constraints of these processors necessitate tailored optimization strategies to achieve effective performance improvements [9]. Implementing bitsliced SPN ciphers on 32-bit processors encounters multiple obstacles. Firstly, the constrained instruction set architecture (ISA) of 32-bit processors lacks specialized instructions, such as SSE and AVX, which are prevalent in x86 platforms [10]. This absence limits the ability to perform parallel bit-level operations efficiently. Secondly, the reduced register size restricts the number of bits that can be processed concurrently, impeding parallelism and diminishing potential performance gains. Thirdly, the limited number of available registers constrains the storage of temporary variables essential for complex cryptographic computations. These factors collectively hinder the effective implementation of bitsliced SPN ciphers on 32-bit architectures, necessitating optimization strategies to mitigate these limitations.

(a) 动机部分



B. Related Work

Efforts to optimize bitsliced SPN cipher implementations on 32-bit processors focus on both the linear and non-linear layers. In the linear layer, heuristic search methods, such as those proposed by [11], decompose complex matrix operations into simpler XOR and rotation tasks, improving performance on limited instruction sets. In the non-linear layer, gate complexity minimization techniques reduce the number of logical operations required for S-box computations [12]. Additionally, Boolean satisfiability solvers are utilized to optimize S-box transformations, enhancing speed and efficiency on 32-bit architectures [13]. These techniques address the inherent limitations of 32-bit processors, resulting in more efficient bitsliced implementations.

However, existing methods have certain limitations. The approach proposed by [11] focuses on optimizing large cyclic matrices, whereas the linear layer of SPN ciphers typically

(b) 相关工作部分

图 1: 摘要部分的修改

实验章节的改进

为了提高实验部分的完整性和学术规范性，我们进行了以下改进：

1. 提供了实验测试的开源链接，方便他人重复实验并验证结果。
2. 将表格格式由 IEEE 默认样式改为 [LAKS20] 中使用的三线表，提升了表格的美观性和可读性。
3. 增加了对实验结果的深入分析和解释（见图2a），补充了非 SPN 结构的密码算法实现（见图2b），更充分地展示了研究成果。

AES Performance Analysis. The proposed AES bitsliced implementation achieves a CPB of 252.06, demonstrating superior efficiency compared to the implementation in [21], which yields 279.12 CPB. The primary improvement arises from the ShiftRow optimization, which reduces the number of Permutation Primitive Operations (PPOs) from six to four. PPOs are computationally expensive on IoT processors; thus, reducing their number significantly enhances performance.

An interesting observation is that AES implementations using lookup tables can outperform bitsliced implementations. For instance, the RISC-V based FE310-G000 implementation proposed in [23] exhibits better performance than the bitsliced implementation in [21]. This advantage is attributed to the use of precomputed tables that merge the S-box and MixColumn operations, leading to faster execution. However, these large tables consume more memory space, and the performance may not be consistent across different platforms due to variations in memory architecture.

(a) 实验结果分析

Additional results for non-SPN block cipher implementations within the LCB framework are presented in Table VI, providing further insights into low-latency block cipher performance on IoT devices. These results establish a comparative baseline for future research aiming to develop efficient cryptographic implementations suitable for resource-constrained environments.

TABLE VI
NON-SPN BLOCK CIPHER IMPLEMENTATIONS IN CTR MODE

Cipher	Size (bytes)	Cycles	CPB	Flash (bytes)
WARP‡	8	27,642	3,455.25	11,520
WARP	8	31,177	3,897.12	11,204
SIMON	8	1,655	206.87	11,232
LLLWBC	8	53,166	6,645.75	12,164

‡ Lookup Table implementation

(b) 非 SPN 结构算法实现

图 2: 实验章节的改进

参考文献 I


Zhe Liu, Reza Azarderakhsh, Howon Kim, and Hwajeong Seo.
Efficient software implementation of ring-lwe encryption on iot processors.
IEEE Trans. Computers, 69(10):1424–1433, 2020.

老师评语

确定好可以投稿

好的

本周计划

- 完成论文的最终校正和投稿。
- 开始筹备第三篇的工作。