周报-向嘉豪 (2024-11-11)

Abstract: 本周完成了线性层的重构。为深入理解线性层的优化方法，我们对 [LP24] 进行了系统性分析。实验结果表明，循环矩阵在 AES 中的应用效果未达预期。基于此发现，我们将研究重点转向线性层中置换操作的优化，主要包括以下三个方面：结构优化、算法改进和 OPO 算法优化。
下周计划: 1）完善 AES 算法实现的实验工作。

0.1 线性层优化算法分析

线性层的初始状态表示为 $((x_1), 1)$，其中代价函数定义为 $Cost(x) = weight(x)$，表示输入向量 x 的汉明权重。优化过程采用递归方法，通过状态转移实现代价函数的单调递减。基本转移规则包含以下两类：

$$x_i = 1 \lll r : ((x_1, \ldots, x_i, \ldots, x_v), v) \to ((x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_v), v-1) \tag{1}$$

$$x_i = x_j \lll r : ((x_1, \ldots, x_i, \ldots, x_v), v) \to ((x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_v), v-1) \tag{2}$$

进一步分析表明，算法采用了三种核心转移策略：

$$x_i = a \oplus (a \ggg r) \oplus b, \quad a = x_i \wedge (x_i \lll r), \quad a \wedge (a \ggg r) = 0 :$$
$$((x_1, \ldots, x_i, \ldots, x_v), v) \to ((x_1, \ldots, a, \ldots, x_v, b), v+1) \text{ 或} ((x_1, \ldots, a, \ldots, x_v), v) \tag{3}$$

$$x_i = x_i \oplus (x_j \lll r), \quad i \neq j : ((x_1, \ldots, x_i, \ldots, x_v), v) \to ((x_1, \ldots, x_i \oplus x_j \lll r, \ldots, x_v), v) \tag{4}$$

$$x_i = a \oplus b, \quad x_j = (a \ggg r) \oplus c : ((x_1, \ldots, x_i, \ldots, x_j, \ldots, x_v), v) \to ((x_1, \ldots, b, \ldots, c, \ldots, x_v, a), v+1) \tag{5}$$

0.2 AES 线性层优化实现

基于 [AP21] 的研究，我们分析了切片 AES 线性层 $L = MP$ 的结构特征。其中 M 为 128×128 矩阵，P 为 128×128 单位置换矩阵。M 具有显著的分块特征：

$$M = \begin{pmatrix} M_0 & 0 & 0 & 0 \\ 0 & M_0 & 0 & 0 \\ 0 & 0 & M_0 & 0 \\ 0 & 0 & 0 & M_0 \end{pmatrix}, \quad \text{其中} \quad M_0 = \begin{pmatrix} M_{00} & M_{01} & M_{02} & M_{03} \\ M_{03} & M_{00} & M_{01} & M_{02} \\ M_{02} & M_{03} & M_{00} & M_{01} \\ M_{01} & M_{02} & M_{03} & M_{00} \end{pmatrix} \tag{6}$$

0.3 优化效果分析

对 AES 第一个寄存器的 M 矩阵在 interleaved 形式下进行分析，其可表示为 4×8 矩阵 M_i：

$$M_i = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{7}$$

通过实验验证，我们发现：

- 向量 $x_i = 01111010$ 可实现最优分解：$x_i = a \oplus (a \ggg r) \oplus b$

- 参数取值：$a = 0101000$，$r = 3$，$b = 0010000$
- interleaved 形式下，$Cost(a) = 2$，理论上可减少 33% 的 XOR 操作

然而，实验结果表明，当转换回标准形式时，仍需 4 次 XOR 操作。这一现象揭示了 [LP24] 优化方法的局限性：仅在 XOR 操作次数超过 4 次时才能体现实质性优势

0.4 论文撰写

本周研究表明，循环矩阵在 AES 应用中的效果未达预期。基于这一发现，我们将研究重心转向线性层中置换操作的优化，主要包含以下三个方面：

结构优化: 为提高论文的逻辑性和可读性，我们重新组织了内容结构：首先引入置换操作的基本概念和理论基础，其次详细阐述置换操作的优化方法，最后展示在实际应用中的优化效果。

算法改进: 在 split 和 merge 操作的设计中，我们基于两个核心思想进行优化：切片并行, 通过数据分割提高计算效率，引出 merge; 动态规划, 采用自底向上的优化策略，引出 split。

OPO 算法优化: 我们对原有的 OPO（Optimal Permutation Operation）算法进行了改进：引入贪心递归策略，保证算法收敛性，优化分解与合并过程，确保获得全局最优解。

参考文献

[AP21] Alexandre Adomnicai and Thomas Peyrin. Fixslicing aes-like ciphers new bitsliced AES speed records on arm-cortex M and RISC-V. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(1):402–425, 2021.

[LP24] Gaëtan Leurent and Clara Pernot. Design of a linear layer optimised for bitsliced 32-bit implementation. *IACR Trans. Symmetric Cryptol.*, 2024(1):441–458, 2024.