

周报-向嘉豪 (2024-11-11)

Abstract: 本周主要工作为线性层部分重写。

1 线性层重构与优化分析

为深入理解线性层的优化方法，本研究对 [LP24] 进行了系统性分析。由于原文对线性层的描述相对简略，我们通过源代码分析补充了关键实现细节。

1.1 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：

$$x_i = 1 \lll r : ((x_1, \dots, x_i, \dots, x_v), v) \rightarrow ((x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_v), v-1) \quad (1)$$

$$x_i = x_j \lll r : ((x_1, \dots, x_i, \dots, x_v), v) \rightarrow ((x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_v), v-1) \quad (2)$$

进一步分析表明，算法采用了三种核心转移策略：

$$x_i = a \oplus (a \ggg r) \oplus b, \quad a = x_i \wedge (x_i \lll r), \quad a \wedge (a \ggg r) = 0 :$$

$$((x_1, \dots, x_i, \dots, x_v), v) \rightarrow ((x_1, \dots, a, \dots, x_v, b), v+1) \text{ 或 } ((x_1, \dots, a, \dots, x_v), v) \quad (3)$$

$$x_i = x_i \oplus (x_j \lll r), \quad i \neq j : ((x_1, \dots, x_i, \dots, x_v), v) \rightarrow ((x_1, \dots, x_i \oplus x_j \lll r, \dots, x_v), v) \quad (4)$$

$$x_i = a \oplus b, \quad x_j = (a \ggg r) \oplus c : ((x_1, \dots, x_i, \dots, x_j, \dots, x_v), v) \rightarrow ((x_1, \dots, b, \dots, c, \dots, x_v, a), v+1) \quad (5)$$

1.2 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：

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

1.3 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 ：

$$M_i = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad (7)$$

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

参考文献

- [AP21] Alexandre Adomnicaï 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.