周报-向嘉豪 (2024-11-11)

Abstract: 本周主要工作为线性层部分重写。

1 线性层部分重写

为了深入理解线性层的优化方法，我们研究了 [LP24]。由于 [LP24] 中对线性层的描述较为简略，我们结合其提供的源代码进行了详细分析。

1.1 学习 [LP24] 源码

未优化的线性层最初表示为：$((x_1), 1)$，其代价函数为：$Cost(x) = weight(x)$，即 x 的汉明距离。随后，作者采用递归方法，根据不同条件进行状态转移，确保代价函数逐步收敛。终止条件如下：

$$\begin{aligned} x_i = 1 \lll r &: ((x_1, \ldots, x_i, \ldots, x_v), v) \to ((x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_v), v-1) \\ x_i = x_j \lll r &: ((x_1, \ldots, x_i, \ldots, x_v), v) \to ((x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_v), v-1) \end{aligned}$$

每次转移后，代价函数的取值降低。然而，作者未对选择这些转移条件的原因进行说明。我们认为，作者采用了启发式方法，无法保证优化结果为最优。具体的转移条件如下：

$$\begin{aligned} & x_i = a \oplus (a \ggg r) \oplus b, \quad a = x_i \wedge (x_i \lll r), \quad a \wedge (a \ggg r) = 0: \\ & \quad ((x_1, \ldots, x_i, \ldots, x_v), v) \to ((x_1, \ldots, a, \ldots, x_v, b), v+1) \text{ or } ((x_1, \ldots, a, \ldots, x_v), v) \\ & x_i = x_i \oplus (x_j \lll r), \quad i \neq j: ((x_1, \ldots, x_i, \ldots, x_v), v) \to ((x_1, \ldots, x_i \oplus x_j \lll r, \ldots, x_v), v) \\ & x_i = a \oplus b, \quad x_j = (a \ggg r) \oplus c: ((x_1, \ldots, x_i, \ldots, x_j, \ldots, x_v), v) \to ((x_1, \ldots, b, \ldots, c, \ldots, x_v, a), v+1) \end{aligned}$$

1.2 AES 线性层的优化

AES 线性层 $L = MP$, M 为 128×128 的矩阵，P 为 128×128 的单位置换矩阵。其中 M 表示为

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

$$M_{00} = \begin{pmatrix} 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 1&0&0&0&1&0&0&0 \\ 1&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 1&0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0&0 \end{pmatrix} \quad M_{01} = \begin{pmatrix} 1&1&0&0&0&0&0&0 \\ 0&1&1&0&0&0&0&0 \\ 0&0&1&1&0&0&0&0 \\ 1&0&0&1&1&0&0&0 \\ 1&0&0&0&1&1&0&0 \\ 0&0&0&0&0&1&1&0 \\ 1&0&0&0&0&0&1&1 \\ 1&0&0&0&0&0&0&1 \end{pmatrix}$$

$$M_{02} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad M_{03} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

其中 P 表示为, 其中 E 为 8×8 单位矩阵:

$$P = \begin{pmatrix}
E & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & E & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & E & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & E \\
0 & 0 & 0 & 0 & E & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & E & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & E & 0 \\
0 & 0 & 0 & E & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & E & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & E & 0 & 0 \\
0 & 0 & E & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & E & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & E & 0 & 0 & 0 \\
0 & E & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & E & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & E & 0 & 0 & 0 & 0
\end{pmatrix}$$

$$L = \begin{pmatrix}
M_{00} & 0 & 0 & 0 & 0 & M_{01} & 0 & 0 & 0 & 0 & M_{02} & 0 & 0 & 0 & 0 & M_{03} \\
M_{03} & 0 & 0 & 0 & 0 & M_{00} & 0 & 0 & 0 & 0 & M_{01} & 0 & 0 & 0 & 0 & M_{02} \\
M_{02} & 0 & 0 & 0 & 0 & M_{03} & 0 & 0 & 0 & 0 & M_{00} & 0 & 0 & 0 & 0 & M_{01} \\
M_{01} & 0 & 0 & 0 & 0 & M_{02} & 0 & 0 & 0 & 0 & M_{03} & 0 & 0 & 0 & 0 & M_{00} \\
0 & 0 & 0 & M_{03} & M_{00} & 0 & 0 & 0 & 0 & M_{01} & 0 & 0 & 0 & 0 & M_{02} & 0 \\
0 & 0 & 0 & M_{02} & M_{03} & 0 & 0 & 0 & 0 & M_{00} & 0 & 0 & 0 & 0 & M_{01} & 0 \\
0 & 0 & 0 & M_{01} & M_{02} & 0 & 0 & 0 & 0 & M_{03} & 0 & 0 & 0 & 0 & M_{00} & 0 \\
0 & 0 & 0 & M_{00} & M_{01} & 0 & 0 & 0 & 0 & M_{02} & 0 & 0 & 0 & 0 & M_{03} & 0 \\
0 & 0 & M_{02} & 0 & 0 & 0 & 0 & M_{03} & M_{00} & 0 & 0 & 0 & 0 & M_{01} & 0 & 0 \\
0 & 0 & M_{01} & 0 & 0 & 0 & 0 & M_{02} & M_{03} & 0 & 0 & 0 & 0 & M_{00} & 0 & 0 \\
0 & 0 & M_{00} & 0 & 0 & 0 & 0 & M_{01} & M_{02} & 0 & 0 & 0 & 0 & M_{03} & 0 & 0 \\
0 & 0 & M_{03} & 0 & 0 & 0 & 0 & M_{00} & M_{01} & 0 & 0 & 0 & 0 & M_{02} & 0 & 0 \\
0 & M_{01} & 0 & 0 & 0 & 0 & M_{02} & 0 & 0 & 0 & 0 & M_{03} & M_{00} & 0 & 0 & 0 \\
0 & M_{00} & 0 & 0 & 0 & 0 & M_{01} & 0 & 0 & 0 & 0 & M_{02} & M_{03} & 0 & 0 & 0 \\
0 & M_{03} & 0 & 0 & 0 & 0 & M_{00} & 0 & 0 & 0 & 0 & M_{01} & M_{02} & 0 & 0 & 0 \\
0 & M_{02} & 0 & 0 & 0 & 0 & M_{03} & 0 & 0 & 0 & 0 & M_{00} & M_{01} & 0 & 0 & 0
\end{pmatrix}$$

参考文献

[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.