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：

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

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：

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

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.