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

为了学习对线性层优化的写作手法，我们对 [LP24] 进行学习，由于 [LP24] 对其线性层的描述过于简洁，因此我们结合其提供的源代码对其进行学习。

1.1 学习 [LP24] 源码

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.