Encoding countermeasure - sBoxLayer and pLayer

- The implementation of sBoxLayer and pLayer are based on four 16×64 lookup tables, $T0, T1, T2, T3$.
- Let $\boldsymbol{x} = x_3x_2x_1x_0$ be an element in $\mathbb{F}_2^4$.
- We write

$$\mathsf{SB}(x_3x_2x_1x_0) = x_3^s x_2^s x_1^s x_0^s.$$

Definition of $T0$ is as follows:

$$\begin{array}{rcl} T0 : C & \rightarrow & C \times C \times C \times C \\ \texttt{encode}(x_3x_2x_1x_0) & \mapsto & \texttt{encode}(000x_3^s), \texttt{encode}(000x_2^s), \texttt{encode}(000x_1^s), \texttt{encode}(000x_0^s) \end{array}$$