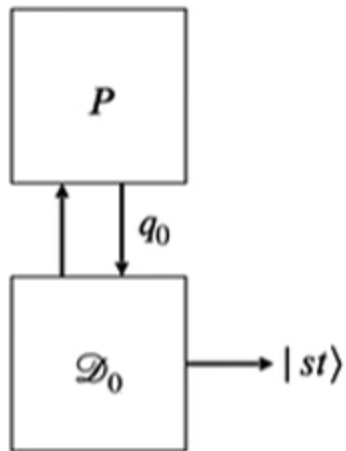


Phase 1:



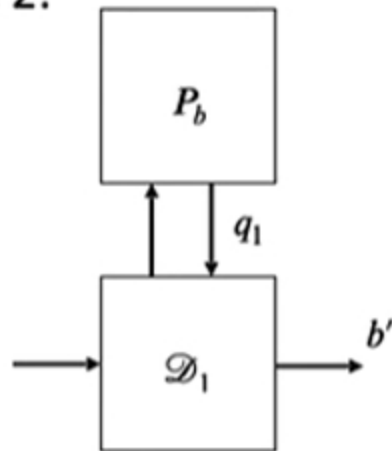
$$P_0 = P$$

$$P_1 = P \circ \text{swap}_{s_0, s_1} = \begin{cases} P(s_0) & \text{if } x = s_1 \\ P(s_1) & \text{if } x = s_0 \\ P(x) & \text{otherwise} \end{cases}$$

Phase 2:

$$\begin{aligned} b &\stackrel{\$}{\leftarrow} \{0,1\} \\ s_0 &\stackrel{\$}{\leftarrow} \{0,1\}^n \\ s_1 &\stackrel{\$}{\leftarrow} \{0,1\}^n \end{aligned}$$

$$(|st\rangle, s_0, s_1)$$



\mathcal{D} wins if $b = b'$