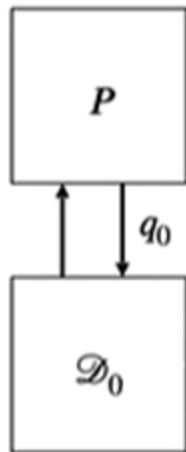
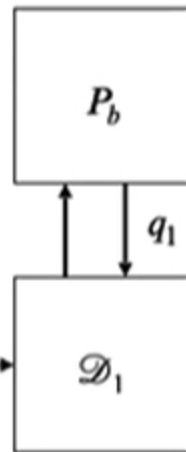


Phase 1:



$$\begin{aligned} b &\stackrel{s}{\leftarrow} \{0,1\} \\ \hat{s} &\leftarrow D \\ s_0 &= \tau \circ P(\hat{s}) \\ s_1 &= f(s_0) \end{aligned}$$

Phase 2:



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

$$(|st\rangle, D, \tau)$$

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

$$\begin{aligned} \tau &\in F \subset S_{2^n} \\ f &\text{ involution.} \end{aligned}$$

b'