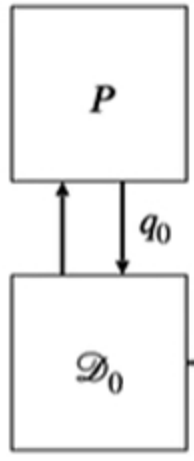
Phase 1:



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

$b \xleftarrow{\$} \{0,1\}$

$\hat{s} \leftarrow D$

$s_0 = \tau \circ P(\hat{s})$

$s_1 = f(s_0)$

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

$\tau \in F \subset S_{2^n}$

f: involution.

Phase 2:

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