① SKE is correct $\iff \forall_{k} \in K, \forall_{m} \in M: \Pr[\mathrm{Dec}(k, \mathrm{Enc}(k,m)) = m] = 1$.

Set $\lambda = 2$, $k = 01$, $m = 10$. Then $\mathrm{Dec}(k, \mathrm{Enc}(k,m)) = 00$ but $m = 10$.

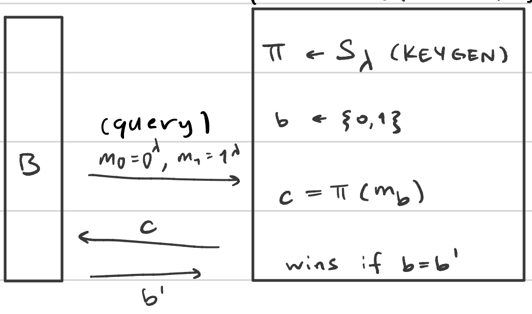
So, there exists a key and message such that $\mathrm{Dec}(k, \mathrm{Enc}(k,m)) \neq m \Rightarrow \Pr[\mathrm{Dec}(k,\mathrm{Enc}(k,m)) = m] \neq 1$

② Permutation π is applied to the indices of the given message $\Rightarrow$ message is shuffled.

(1) $\mathrm{Dec}(k, \mathrm{Enc}(k,m)) = \mathrm{Dec}(k, \pi(m)) = \pi^{-1}(\pi(m)) = (\pi^{-1} \circ \pi)(m) = \mathrm{Id}(m) = m$.

Black-box that has access to both $L_{OTS\text{-}0}$ and $L_{OTS\text{-}1}$

(2)


B
(query)
$m_0 = 0^\lambda$, $m_1 = 1^\lambda$
c
b'
$\pi \leftarrow S_\lambda$ (KEYGEN)
$b \leftarrow \{0,1\}$
$c = \pi(m_b)$
wins if $b = b'$

where $b' = \begin{cases} 0 & \text{if } c = 0^\lambda \\ 1 & \text{if } c = 1^\lambda \end{cases}$ as part of the strategy of B.

$$\Pr[b = b'] = \Pr[b = b' \cap \overset{\text{i.e. } b=0}{L_{OTS\text{-}0}}] + \Pr[b = b' \cap \overset{\text{i.e. } b=1}{L_{OTS\text{-}1}}]$$

$$= \underbrace{\Pr[0 = b' \mid L_{OTS\text{-}0}]}_{1} \underbrace{\Pr[L_{OTS\text{-}0}]}_{\frac{1}{2}} + \underbrace{\Pr[1 = b' \mid L_{OTS\text{-}1}]}_{1} \underbrace{\Pr[L_{OTS\text{-}1}]}_{\frac{1}{2}} = 1$$

Recall: For any event A and B, $\Pr(A \cap B) = \Pr(A|B)\Pr(B) = \Pr(B|A)\Pr(A)$.

③ (1) $\mathrm{Dec}(k, \mathrm{Enc}(k,m)) = \mathrm{Dec}(k, k \oplus m) = k \oplus (k \oplus m) = m$

(2) $m = 111$ & $k[i] \leftarrow B_{0.75} \Rightarrow c[i] = 1$ with prob. 0.75 and $c[i] = 0$ w. prob. 0.25

- $\Pr[k = 000] = (0.75)^3 \Rightarrow \Pr[c = 111] = (0.75)^3$
- $\Pr[k = 100] = \Pr[010] = \Pr[001] = (0.75)^2 (0.25)$

  $\Rightarrow \Pr(c = 011) = \Pr[101] = \Pr[110] = (0.75)^2 (0.25)$
- $\Pr[k = 110] = \Pr[101] = \Pr[011] = (0.75)(0.25)^2$

  $\Rightarrow \Pr[c = 001] = \Pr[010] = \Pr[100] = (0.75)(0.25)^2$
- $\Pr[k = 111] = (0.25)^3 \Rightarrow \Pr[c = 000] = (0.25)^3$

(3) $\Pr[B \circ L_{OTS\text{-}Real} = 1] = \Pr[\mathrm{Enc}(k,m) = m] = \Pr[k \oplus m = m] = \Pr[k = 000] = (0.75)^3$

$\Pr(B \circ L_{OTS\text{-}Rand} = 1] = \Pr[c = m] = 1/8$

(4) $L_{OTS\text{-}Real} \equiv L_{OTS\text{-}Rand}$ if for every $m \in M$, $c \in C$ $\Pr[c = \mathrm{Enc}(k,m) \mid k \leftarrow \mathrm{keygen}()] = 1/|c|$.

By part (3), we know that for $m = 111$, $c = 111$, this is not the case.

(5) Optimal strategy is that B outputting 1 when $c = 111, 110, 101,$ or 011 because all this ciphertexts occur with higher probability in the real world compared to random one.