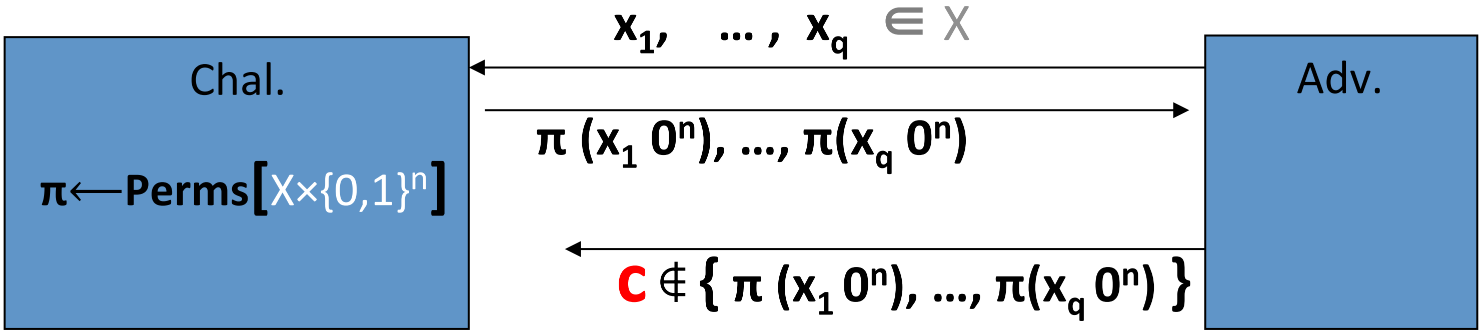
Let (E, D) be a secure PRP. $E: K \times (X \times \{0,1\}^n) \longrightarrow X \times \{0,1\}^n$

Thm: $1/2^n$ is negligible ⇒ PRP-based enc. provides DAE

Proof sketch: suffices to prove ciphertext integrity



$x_1, \ \dots, \ x_q \in X$

Chal.

$\pi \leftarrow \mathrm{Perms}[X \times \{0,1\}^n]$

$\pi(x_1 0^n), \dots, \pi(x_q 0^n)$

$c \notin \{\pi(x_1 0^n), \dots, \pi(x_q 0^n)\}$

Adv.

But then $\Pr[\ \mathrm{LSB}_n(\ \pi^{-1}(c)\ ) = 0^n\ ] \leq 1/2^n$