

Security

Step 2 is tight: $\forall A \exists B: \text{PRP}_{\text{adv}}[A, E] = \text{PRP}_{\text{adv}}[B, E']$

Intuition: \forall sets $Y \subseteq X$, applying the transformation to a random perm. $\pi: X \rightarrow X$

gives a random perm. $\pi': Y \rightarrow Y$

Step 1: same security as Luby-Rackoff construction

(actually using analysis of Patarin, Crypto'03)

note: no integrity