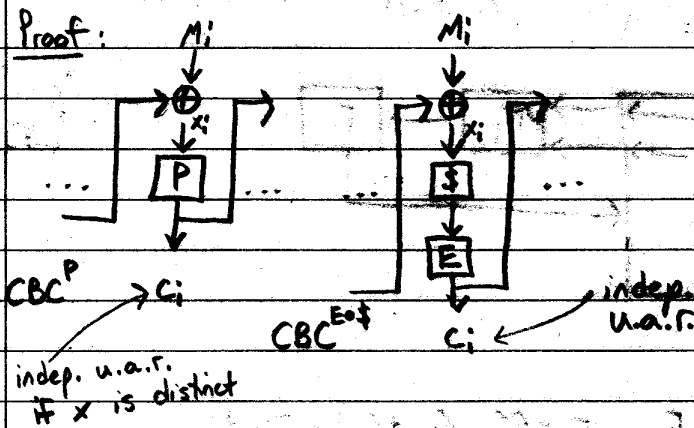


Lemma: $CBC^{E \circ f}$ and CBC^P , $P \leftarrow \text{Perms}$ are $(t, q, \frac{\epsilon}{2^{n-1}})$ indistinguishable

Proof:



So, $CBC^{E \circ f} \stackrel{t, q}{\approx} CBC^P$ as long as x is distinct
 By same argument as before,
 $CBC^{E \circ f} \stackrel{t, q}{\approx} CBC^P$

Lemma: CBC^E and CBC^P , $P \leftarrow \text{Perms}$ are (t, q, ϵ) indistinguishable if E is a (t, q, ϵ) PRP

Proof: Suppose A can distinguish CBC^E and CBC^P . Then, $B^A = A \circ CBC^{\text{perm}}$ can distinguish E and P .

running time of $B =$ running time of $A +$ CBC operations

Thm: $CBC^E \stackrel{t, q}{\approx} CBC^{E \circ f}$, i.e. CBC^E is (t, q, ϵ) R-or-R secure (if E is a (t, q, ϵ) PRP)

Proof: $CBC^E \stackrel{t, q}{\approx} CBC^P \stackrel{t, q}{\approx} CBC^{E \circ f}$

Alternative Definitions of Security

Def: $\Pi_i(x_0, x_1) = x_i$

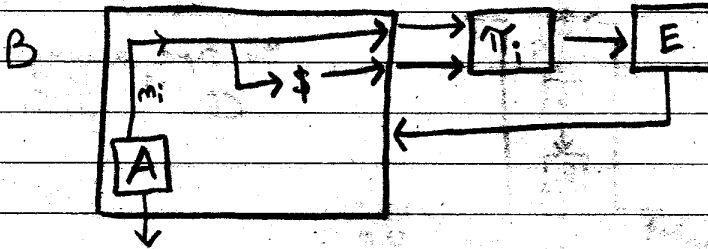
Def: (Left Right (LR) security) E is (t, q, ϵ) LR secure if $E_{x_0} \circ \Pi_0 \stackrel{t, q}{\approx} E_{x_1} \circ \Pi_1$

Thm: E is (t, q, ϵ) R-or-R secure iff E is (t, q, ϵ) LR secure
 queries must be for pairs of equal length

Proof: $LR \Rightarrow R\text{-or-}R$ (by contrapositive)

Suppose A can (t, q, E) $R\text{-or-}R$ break E .

Then let $B \stackrel{E \cdot \pi_i}{=} A \stackrel{E \cdot \pi_i \cdot (\cdot, \$(\cdot))}{=}$



$$E \cdot \pi_0 \cdot (\cdot, \$(\cdot)) = E, \quad E \cdot \pi_1 \cdot (\cdot, \$(\cdot)) = E \cdot \$$$

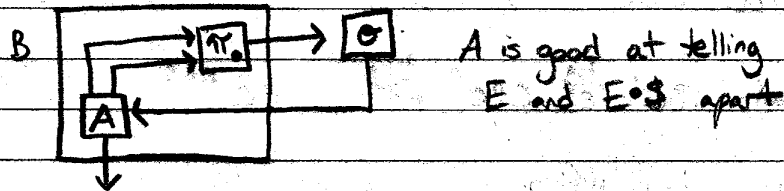
So, B can $(t + O(q), q, E)$ LR break E .

$R\text{-or-}R \Rightarrow LR$ (direct proof)

$$(t, q, E) R\text{-or-}R \Rightarrow \begin{cases} E \stackrel{+2}{\leq} E \cdot \$ \\ E \cdot \pi_0 \stackrel{+2}{\leq} E \cdot \$ \cdot \pi_0 \end{cases} \quad \text{if } |m_0| = |m_1|$$

and $E \cdot \pi_0 \stackrel{+2}{\leq} E \cdot \$ \cdot \pi_0$

if A distinguishes $E \cdot \pi_0$ and $E \cdot \$ \cdot \pi_0$.



$$\stackrel{+2}{\leq} E \cdot \$ \cdot \pi_0 = E \cdot \$ \cdot \pi_1 \neq |m_0| = |m_1|$$

By transitivity, $E \cdot \pi_0 \stackrel{+2}{\leq} E \cdot \pi_1$

Semantic Security

Oracle $E_k \circ S_b$

$S_b(M)$

$m \leftarrow^{\$} M$

$m' \leftarrow^{\$} M$

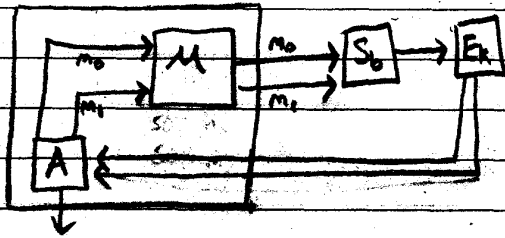
return $\Pi_b(m, m')$

$$\text{Adv } A = \left| \Pr [A^{E_k \circ S_0} = (f, f(m_1, m_2, \dots, m_n))] - \Pr [A^{E_k \circ S_1} = (f, f(m_1, m_2, \dots, m_n))] \right|$$

↙ given ciphertext of messages
← given garbage

Then Semantic Security is equivalent to LR security

Proof Semantic \Rightarrow LR (by contrapositive)



turn each single query into two