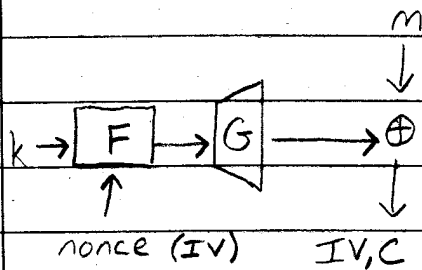
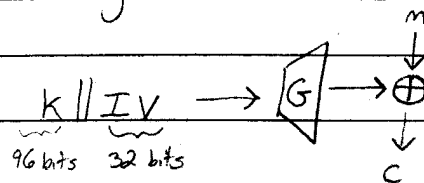


# Stream Ciphers

09/20



## A wrong construction



Is this a PRF  
ie.  $F(k, n) = G(k || n)$ ?

Suppose  $G: \{0, 1\}^{96} \rightarrow \{0, 1\}^L$  is PRF

Let  $G(x) = G'(\text{first}_{96}(x))$

$G: \{0, 1\}^{128} \rightarrow \{0, 1\}^L$

$G$  is a PRG

$F$  is not a PRF because the following  $A$  will break  $F$

$A: y_1 = \mathcal{O}(0)$  oracle

$y_2 = \mathcal{O}(1)$

return  $y_1 = y_2$

$A$  is a  $(3, 2, 1 - 2^{-t})$ -distinguisher

3 steps 2 queries

probability of success

for  $F$  and  $R$

A function  $F$  is a  $(t, q, \epsilon)$  PRF  $\forall A$  running in time  $t$  with  $q$  queries to its oracle  $\mathcal{O}$  (where  $\mathcal{O} = F_k$  or  $R$ )

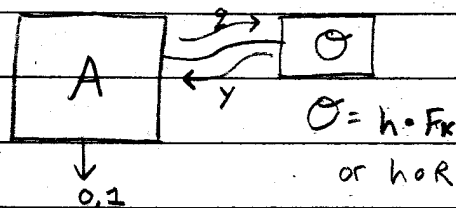
$\text{Adv } A = |P_r [A^{F_k} = 1; k \leftarrow \text{keys}]$

$- P_r [A^R = 1; R \leftarrow \text{Funcs}] | \leq \epsilon$

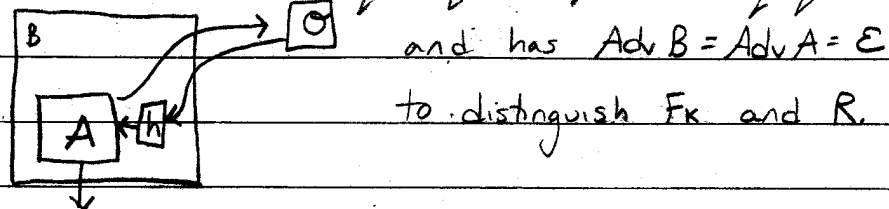
Lemma (DPI PRFs) If  $F$  is a  $(t, q, \epsilon)$  PRF and  $h$  is any function, then  $h \circ F$  is  $(t - O(q), q, \epsilon)$  indistinguishable from  $h \circ R$ .

Proof (by contrapositive)

Suppose  $A$  distinguishes  $h \circ F$  and  $h \circ R$  in time  $t - O(q)$  with  $q$  queries, and with probability  $\epsilon$ .



Then,  $B$  runs in  $t - O(q) + O(q) = t$ , makes  $q$  queries,



and has  $\text{Adv } B = \text{Adv } A = \epsilon$  to distinguish  $F_k$  and  $R$ .

G.e.  $U_q$  is a probability distribution on  $\{0, 1\}^q$

$U_L$  is a probability distribution on  $\{0, 1\}^L$

$F$  is a probability distribution on

$\text{Funcs} (\{0, 1\}^q \rightarrow \{0, 1\}^L)$

$F: \text{keys} \times \{0, 1\}^q \rightarrow \{0, 1\}^L$

$R$  is a uniform distribution on  $\text{Funcs} (\{0, 1\}^q \rightarrow \{0, 1\}^L)$

Def: Probability distributions  $D_1, D_2$  on  $\text{Funcs}(x \rightarrow y)$

are  $(t, q, \epsilon)$  computationally indistinguishable if

$\forall A$  running in time  $t$  and making at most  $q$  queries

$$\text{Adv } A = \left| \Pr[A \stackrel{F}{=} 1; F \stackrel{\$}{\leftarrow} D_1] - \Pr[A \stackrel{F}{=} 1; F \stackrel{\$}{\leftarrow} D_2] \right| \leq \epsilon$$

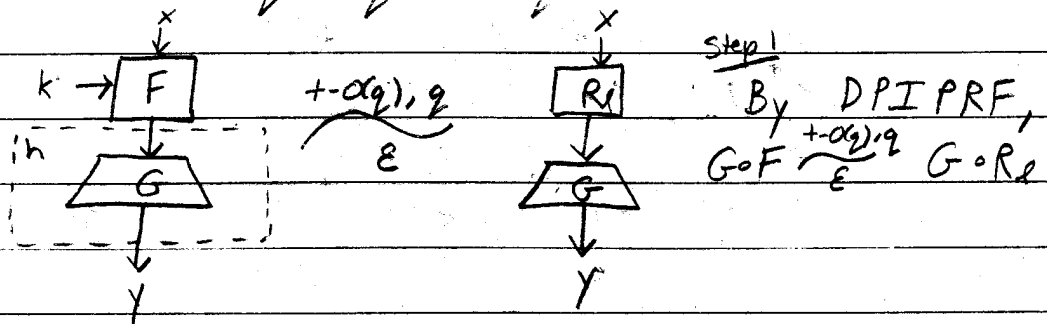
Lemma If  $D_1 \stackrel{t, q}{\approx} \epsilon_1} D_2$  and  $D_2 \stackrel{t, q}{\approx} \epsilon_2} D_3$ , then  $D_1 \stackrel{t, q}{\approx} \epsilon_1 + \epsilon_2} D_3$

Proof same as general proof of transitivity for prob. dist.

Thm: If  $F$  is a  $(t, q, \epsilon)$  PRF and  $G$  is a

$(t, \epsilon')$  PRG, then  $G \circ F$  is a

$(t + O(q), q, \epsilon + q\epsilon')$  PRF



step 2  
 $G \circ R_k \approx R_k$

Hybrid Argument: Let  $T_i(x_j) = \begin{cases} R_k(x_j) & \text{if } j < i \\ G \circ R_k(x_j) & \text{otherwise} \end{cases}$

$T_1 = G \circ R_k$   
 $T_{q+1} = R_k$  (for adversaries making at most  $q$  queries)

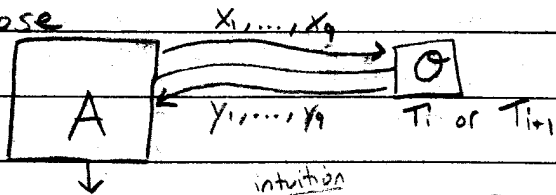
Note:  
 assume all queries to  $\mathcal{O}$  are distinct

$$T_1 \stackrel{t, q}{\approx} \epsilon'} T_2 \stackrel{t, q}{\approx} \epsilon'} T_3 \stackrel{t, q}{\approx} \epsilon'} \dots \stackrel{t, q}{\approx} \epsilon'} T_{q+1}$$

Lemma  $T_i \xrightarrow[\epsilon']{+t, q} T_{i+1}$  since  $G$  is  $(t, \epsilon')$  PRG

Proof (by contrapositive)

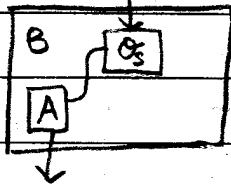
Suppose



intuition

Only useful query is  $x_1$

$s$  is an  $L$ -bit string  
 $S = G \circ U_L$  or  $U_L$



$$\text{where } O_s(x_j) = \begin{cases} R_L(x_j) & j < i \\ S & j = i \\ G \circ R_L(x_j) & j > i \end{cases}$$

(If  $S$  was chosen according to  $U_L$ )

If  $S \xleftarrow{s} U_L$ , then  $O_s = T_{i+1}$

$S \xleftarrow{s} G \circ U_L$ , then  $O_s = T_i$

So,  $\text{Adv } B = \text{Adv } A = \epsilon'$  at breaking  $G$

$B$  runs in  $t$  time, so  $T_i \xrightarrow[\epsilon']{+t, q} T_{i+1}$

$$G \circ F \xrightarrow[\epsilon']{+t, q} G \circ R_L = T_1 \xrightarrow[\epsilon']{+t, q} T_2 \xrightarrow[\epsilon']{+t, q} \dots \xrightarrow[\epsilon']{+t, q} T_{g+1}$$

By transitivity,  $G \circ F \xrightarrow[\epsilon + g\epsilon']{+t, q} R_L$