¡HM:

$F'_k(x) = F_{F_k(0^n)}(x)$ $\quad F = \{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$

PRF Family is a PRF Family

Proof: Define the following experiments.

H_0: $F'_k(x) = F_{F_k(0^n)}(x)$ $\quad k \leftarrow U_n$

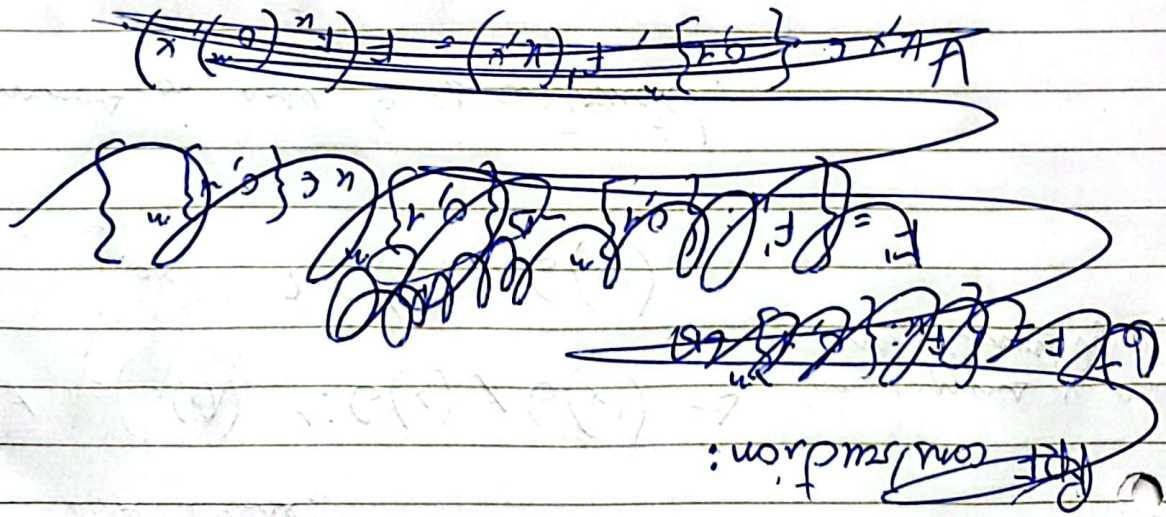
H_1: $F'_k(x) = F_z(x)$ $\quad z \leftarrow U_n$

H_2: $F'_k(x) = R'(x)$ $\quad R' \leftarrow R(\lambda, n, n)$

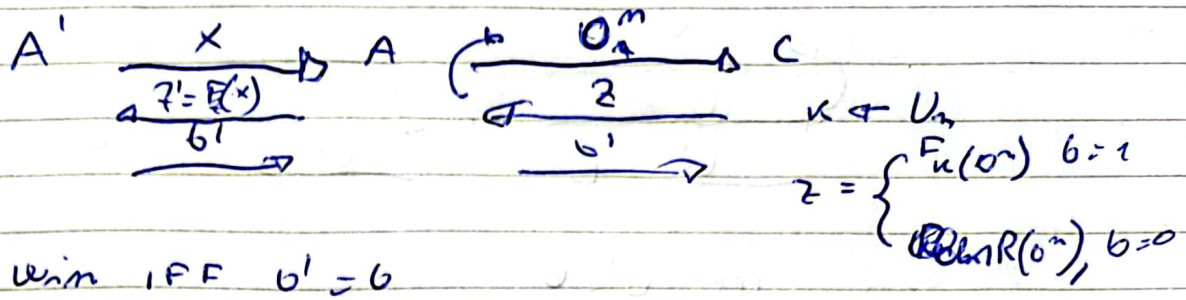
now we need to prove that $H_0 \approx_c H_1 \approx_c H_2$

$\boxed{H_0 \approx_c H_1}$

Suppose not, $\exists$ PPT A': $Pr\left[A'(z)=1 \mid z = F_k(0^n)\right] - Pr\left[A'(z)=1 \mid z \leftarrow U_n\right] \geq negl(\lambda)$



then we can build a reduction against PRF F.



win IFF $b' = b$

$$Pr\left[A'(z)=1 \mid z = f_k(0^n)\right] = Pr\left[Game_{A,F}^{PRF}(\lambda,0)=1\right]$$

$$Pr\left[A'(z)=1 \mid z \leftarrow U_n\right] = Pr\left[Game_{A,F}^{PRF}(\lambda,1)=1\right]$$

$$Pr\left[Game_{A,F}^{PRF}(\lambda,0)=1\right] - Pr\left[Game_{A,F}^{PRF}(\lambda,1)=1\right] \geq \frac{1}{Bly}$$

↓

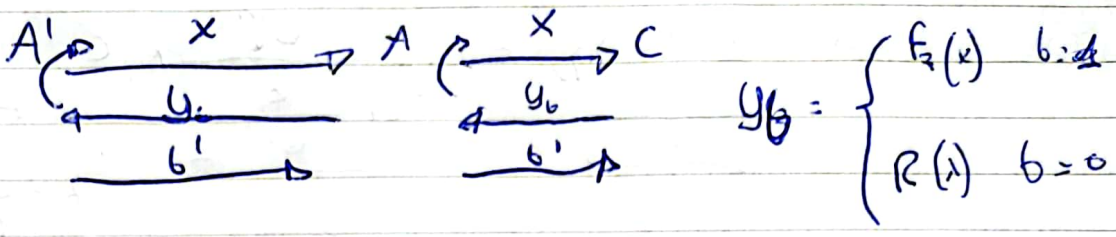
IMPOSSIBLE due to PRF security of $c \Rightarrow H_0 \tilde{\approx}_c H_1$

$H_1 \tilde{\approx}_c H_2$

Suppose not, $\exists$ PPT A' : $Pr\left[A'(z)=1 \mid z \leftarrow U_m\right] -$

$- Pr\left[A'(z)=1 \mid z = R(\lambda, \sim, m)\right]$

Then we can built a reduction against PRF F



A' win IFF $b' = b$

$$\left.\begin{aligned} Pr[A' \text{ win} \mid b=1] &= Pr\left[GAME^{PRF}_{A,F}(\lambda, 0) = 1\right] \\ Pr[A' \text{ win} \mid b=0] &= Pr\left[GAME^{PRF}_{A,F}(\lambda, 1) = 1\right] \end{aligned}\right\}$$

$$Pr\left[GAME^{PRF}_{A,F}(\lambda,0) = 1\right] - Pr\left[GAME^{PRF}_{A,F}(\lambda,1) = 1\right] \geq \frac{1}{poly.}$$

impossible due to PRF $\Rightarrow H_1 \overset{c}{\approx} H_1$

So $H_1 \overset{c}{\approx} H_2 \overset{c}{\approx} H_3 \Rightarrow$ F is a PRF family.

THM:

$\Pi = (Kgen, Sig, Vorfy)$

$\Pi' = (Kgen, Sign', Vorfy')$ over $m \in \{0,1\}^n$

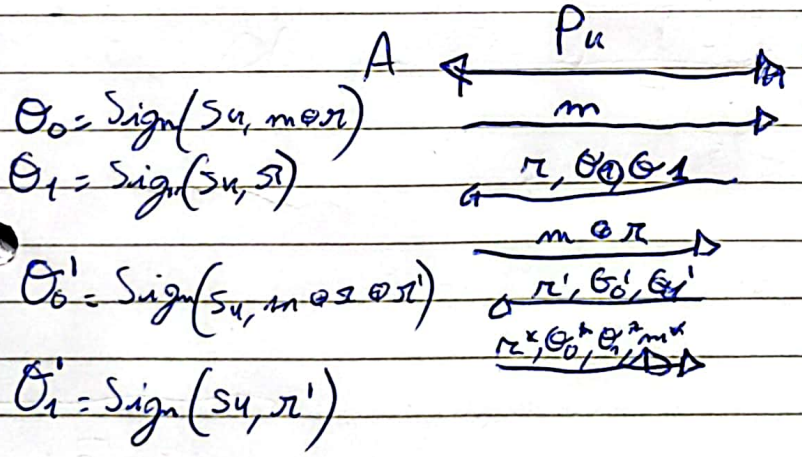
$Sign'(Sk, m) = (r, Sign(Sk, m \oplus r), Sign(Sk, r))$ for $r \leftarrow \{0,1\}^n$

$Vorfy'(Pk, m, (r, \sigma_0, \sigma_1)) = (Vorfy(Pk, m \oplus r, \sigma_0)) \wedge (Vorfy(Pk, r, \sigma_1))$

Π is UF-CMA?

~~Suppose not, $\exists$ PPT $\mathcal{A}$: $\mathcal{A}$~~

Proof:



2. Prove that nor PRG is secure against unbounded A.

$G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$ is a PRG with stretch $\ell : \ell(\lambda) > 0$ if

$$GAME^{PRG}_{A,G}(\lambda, 0) \approx_c GAME^{IRG}_{A,G}(\lambda, 1)$$

$$GAME^{IRG}_{A,G}(\lambda, b)$$

A $\xrightarrow{z}$ C

$\xrightarrow{b' = \{0,1\}}$

$$z = \begin{cases} G(s), & s \leftarrow \{0,1\}^\lambda \quad b = 0 \end{cases}$$

~~G is a PRF~~

~~$G'(s) = G(s) \| (0^{n-|s|})$ is PRF?~~

$G'(s) = (x \oplus y, u, v) \quad (x,y) = G(s) \quad (u,v) \; G(y)$

We need to prove the following are indistinguishable.

H_0: $G'(s) = (x \oplus y, u, v)$

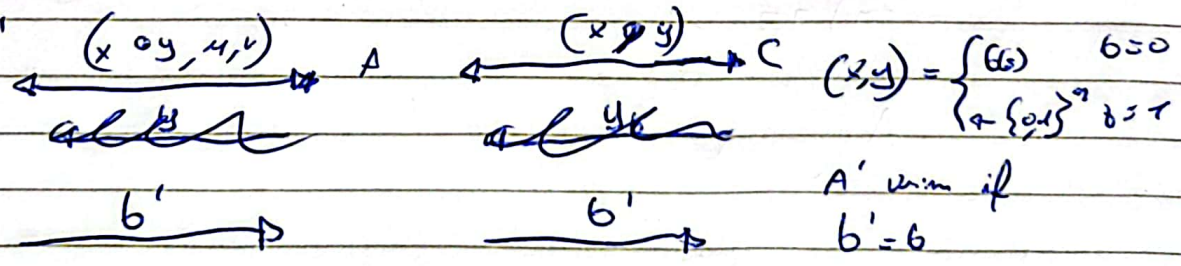
H_1: $G'(s) = (x \oplus y, u, v) \quad (x,y) \leftarrow \{0,1\}^{2n} \quad (u,v) = G(y)$

H_2: $G'(s) = (x \oplus y, u, v) \quad (x,y) \leftarrow \{0,1\}^{2n} \quad (u,v) \leftarrow \{0,1\}^{2n}$

$H_0 \approx_c H_1$

Suppose not $\exists$ PPT A' : $\Pr[A' \text{ win} \mid (x,y) \leftarrow H_0] - \Pr[A' \text{ win} \mid (x,y) \leftarrow H_1] \geq \text{negl}(\lambda)$

Then we can build reduction against PRG G:



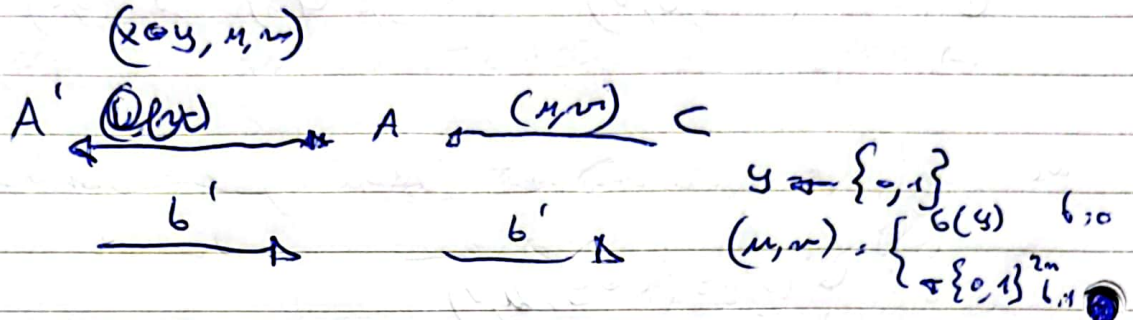
$\Pr[A' \text{ wins} \mid b=0] = \Pr[\text{GAME}^{PRG}_{A,G}(\lambda, 0) = 1]$

$\Pr[A' \text{ wins} \mid b=1] = \Pr[\text{GAME}^{PRG}_{A,G}(\lambda, 1) = 1]$ $\Big\} \geq \frac{1}{\text{Poly}}$

$\Rightarrow$ IMPOSSIBLE

$H_1 \approx_c H_2$

suppose not, $\exists$ PPT A' : $\Pr[A' \text{ wins} \mid (u,v) \leftarrow H_1] - \Pr[A' \text{ wins} \mid (u,v) \leftarrow H_2] \geq \frac{1}{poly}$



A' wins if $b' = b$

$\Pr[A' \text{ wins} \mid b=0] - \Pr[A' \text{ wins} \mid b=1] =$

$\Pr[\text{GAME}^{PRG}_{A,G}(\lambda,0)=1] - \Pr[\text{GAME}^{PRG}_{A,G}(\lambda,1)=1] \geq \text{negl}(\lambda)$

impossible due to PRG

$H_1 \approx_c H_2$

So G' is a PRG

G'' is a PRG:

In order to prove that, we need to prove that the following are indistinguishable.

$H_0 = (x, y \oplus u, v)$ $(x,y) = G(s)$ $(u,v) = G(y)$

$H_1 = \;''$ $(x,y) \leftarrow \{0,1\}^{2n}$ $(u,v) \leftarrow \{0,1\}^{2n} = G(1)$

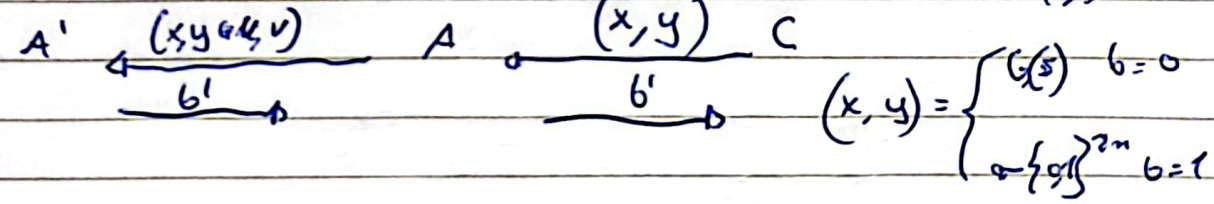
$H_2 = \;''$ $(x,y) \leftarrow \{0,1\}^{2n}$ $(u,v) \leftarrow \{0,1\}^{2n}$

$\boxed{H_0 \approx_c H_1}$

Suppose not, $\exists$ PPT A': $Pr[A'(x,y \oplus u, v) = 1 \mid (x,y) \leftarrow H_0] -$

$Pr[A'(x, y \oplus u, v) = 1 \mid (x,y) \leftarrow H_1] \geq negl$

then we can built a reduction from PRG G



A' win iff $b' = b$

$Pr[A' \text{ wins} \mid b=0] = Pr[GAME^{PRG}_{A,G}(\lambda, 0) = 1]$

$Pr[A' \text{ wins} \mid b=1] = Pr[GAME^{PRG}_{A,G}(\lambda, 1) = 1]$

$Pr[GAME^{PRG}_{A,G}(\lambda,0) = 1] - Pr[GAME^{PRG}_{A,G}(\lambda,1) = 1] \geq negl(\lambda)$ → impossible due to PRG

!

$H_0 \approx_c H_2$

$H_1 \tilde{\approx}_c H_2$

Assume not, $\exists$ PPT A': $\Pr\left[A'(x, y \oplus u, v) \mid (u,v) \leftarrow G(y)\right]$

$$- \Pr\left[A'(x, y \oplus u, v) \mid (u,v) \leftarrow \{0,1\}^{2n}\right] \geq \frac{1}{p(n)}$$

then we can built a reduction from PRG G:

$A' \xrightarrow{(x, H \oplus u, v)} A \xrightarrow{(u,v)} G$ $\quad$ $y \in \{0,1\}^n$

$A' \xrightarrow{b'}$ $\quad$ $A \xrightarrow{b'}$

$$(u,v) = \begin{cases} G(x) & b=0 \\ \leftarrow \{0,1\}^{2n} & b=1 \end{cases}$$

A' wins iff $b' = b$

$$\left.\begin{aligned} \Pr\left[A' \text{ wins} \mid b=0\right] &= \Pr\left[G\text{-}AHC^{PRG}_{A,G}(\lambda, 0) = 1\right] \\ \Pr\left[A' \text{ wins} \mid b=1\right] &= \Pr\left[G\text{-}AHC^{PRG}_{A,G}(\lambda, 1) = 1\right] \end{aligned}\right\} \; 1^e - 2^a \geq \text{negl}$$

impossible due to PRG.

Therefore A' can't exist and $H_1 \tilde{\approx}_c H_1$

So G'' is a PRG

Def. $\Pi^* = (Enc^*, Dec^*)$

Enc: $k^* = (k', k'')$ in input and returns $c^* = (r, c', c'')$

r on $\{0,1\}^n$

$c' = f_{k'}(r) \oplus m$

$c'' = Tag_{k''}(c')$

Dec: $k^* = (k', k'')$ $c^* = (r, c', c'')$ and output m

$m = F_{k'}(r) \oplus c'$

iff $Tag_{k''}(c') = c''$

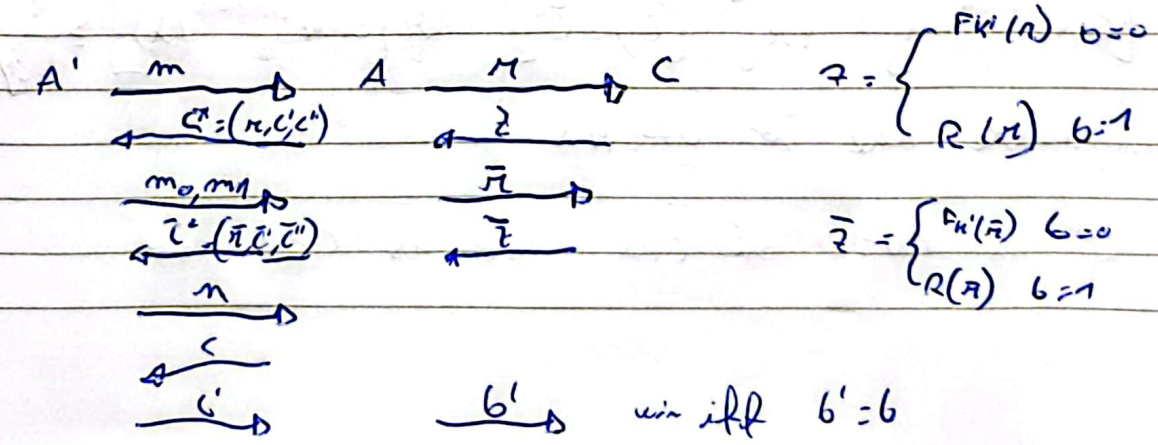
Prove Π^* CCA ?

Proof: We need to prove that Π is CPA and AUTH.

Π' is CPA

Assume not; $\exists$ PPT A': $Pr[CAME^{CPA}_{A',\Pi'}(\lambda, 0) = 1] - Pr[CAME^{CPA}_{A',\Pi'}(\lambda, 1) = 1] \geq negl(\lambda)$

Then we can build a reduction from against PRF



$\Pr[\text{win} \mid b=0] = \Pr[\text{GAME}]$

$\Pr[\text{GAME}^{\text{CPA}}_{\Pi,\mathcal{A}}(\lambda,0)=1] = \Pr[b'=0 \mid z=F_k(r)] = \Pr[\text{GAME}^{\text{ORF}}_{\mathcal{A},F}(\lambda,0)]$

$\quad\quad (\lambda,1) \quad\quad\quad\quad\quad\quad \mid z=R(\bar{r})] = \quad\quad (\lambda,1)]$

$1^a - 2^a \geq \text{negl}(\lambda)$ → impossible due to PRF

↓

Π^* is CPA secure

Π^* IS AUTH

Assume not, then $\exists$ PPT $\mathcal{A}'$: $\Pr[\text{Game}^{\text{AUTH}}_{\mathcal{A}',\Pi^*}(\lambda)=1] \geq 1$

then we can built a reduction from UF-CMA

$\mathcal{A}'$ —m→ $\mathcal{A}$ —c'→ C

$c^* = (r, c', c'')$ ←c''—

$\bar{c}^* = (r, \bar{c}', \bar{c}'')$ ←$(\bar{c}', \bar{c}'')$— win iff $(\bar{c}') \notin \{\bar{c}\}$ and $\log_k(\bar{c}') = \bar{c}''$

$\Pr[\text{GAME}^{\text{AUTH}}_{\mathcal{A}',\Pi^*}=1] = \Pr[\log(\bar{c}') = \bar{c}''] = \Pr[\text{GAME}^{\text{UFCMA}}_{\mathcal{A},\Pi}(\lambda)] \geq \frac{1}{\text{poly}}$

impossible due to UFCMA

Π^* is AUTH and CPA so is CCA too.