__DEF__ : Let $\Pi = (Enc, Dec)$ be a SKE scheme.
Then, we say Π is ONE-TIME COMP. SECURE if $\forall$ PPT $\mathcal{A}$:

$$GAME^{one\text{-}time}_{\Pi,\mathcal{A}}(\lambda, 0) \approx_c GAME^{one\text{-}time}_{\Pi,\mathcal{A}}(\lambda, 1)$$

$GAME^{one\text{-}time}_{\Pi,\mathcal{A}}(\lambda, b)$

this is Alice and Bob

$$\mathcal{A}(1^\lambda) \xrightarrow{\quad m_0, m_1 \in \mathcal{M} \quad} C(1^\lambda)$$

$$K \in \mathcal{K}$$

$$\xleftarrow{\quad c \quad} \quad c = Enc(K, m_b)$$

$$\xrightarrow{\quad b \in 0,1 \quad}$$

only one cyphertext, this is why it's called onetime

__EX__ : Show that perfect secrecy is equivalent to the above definition where "$\approx_c$" is replaced by "$\equiv$" and $\mathcal{A}$ is all powerful

Let $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda + \ell}$ be a PRG and set

$n(\lambda) = \lambda + \ell(\lambda)$.

Consider $\Pi = (Enc, Dec)$

$$Enc(K, m) = G(K) \oplus m; \quad m \in \{0,1\}^n$$

$$K \in \{0,1\}^\lambda$$

$$\mathrm{Dec}(k, c) = G(k) \oplus c \qquad c \in \{0,1\}^n$$

THM Assume G is a secure PRG, then above

Π IS ONE-TIME COMP. SECURE

(if you can break the encryption, you can break the PRG)

The proof is based on the HYBRID ARGUMENT

LEMMA Let $X = \{X_\lambda\}_{\lambda \in \mathbb{N}}$, $Y = \{Y_\lambda\}_{\lambda \in \mathbb{N}}$, $Z = \{Z_\lambda\}_{\lambda \in \mathbb{N}}$

If $X \approx_c Y$ and $Y \approx_c Z$, then $X \approx_c Z$

PROOF: For all PPT distinguishers $\mathcal{D}$:

must prove that this $\leq \varepsilon$

$$\left| \Pr[\mathcal{D}(X_\lambda) = 1] - \Pr[\mathcal{D}(Z_\lambda) = 1] \right|$$

$$= \left| \Pr[\mathcal{D}(X_\lambda) = 1] - \Pr[\mathcal{D}(Y_\lambda) = 1] + \right.$$

$$\left. + \Pr[\mathcal{D}(Y_\lambda) = 1] - \Pr[\mathcal{D}(Z_\lambda) = 1] \right|$$

this is ε bc $X \approx_c Y$

$$\leq \left| \Pr[\mathcal{D}(X_\lambda) = 1] - \Pr[\mathcal{D}(Y_\lambda) = 1] \right| +$$

this is ε bc $Y \approx_c Z$

$$\left| \Pr[\mathcal{D}(Y_\lambda) = 1] - \Pr[D(Z_\lambda) = 1] \right|$$

$$\leq \varepsilon_1(\lambda) + \varepsilon_2(\lambda) \quad \text{for } \varepsilon_1(\lambda), \varepsilon_2(\lambda) = \mathrm{negl}(\lambda)$$

$$\leq \mathrm{negl}(\lambda)$$

EX: Let $X^{(i)} = \{X_\lambda^{(i)}\}_{\lambda \in \mathbb{N}}$ and assume that

$\forall i \in [q]$ with $q(\lambda) = poly(\lambda)$ it holds that

$$X^{(i)} \approx_c X^{(i+1)} \Rightarrow X^{(i)} \approx_c X^{(q)}$$

PROOF (Thm): Consider the original game for Π.

$$GAME_{\Pi,A}^{one\text{-}time}(\lambda, b)$$

$$A(1^\lambda) \xrightarrow{\quad m_0, m_1 \in \mathcal{M} \quad} C(1^\lambda)$$

$$K \in \mathcal{K}$$

$$\xleftarrow{\quad c \quad} \quad c = G(k) \oplus m_b$$

$$\xrightarrow{\quad b \in 0,1 \quad}$$

$HYB_{\Pi,A_b}(\lambda, b)$ is a mental experiment, where the $\mathcal{C}$ doesn't pick K but a random $z \leftarrow \$ \{0,1\}^n$,

and $c = z \oplus m_b$ (it's the one-time pad)

Now, by PERFECT SECRECY,

bc we're using OTP

$$\{Hyb(\lambda, 0)\}_{\lambda \in \mathbb{N}} \equiv \{Hyb(\lambda, 1)\}_{\lambda \in \mathbb{N}}$$

Next, we show that

CLAIM: For all $b \in \{0,1\}$,

$$\left\{ \mathrm{GAME}^{\text{one-time}}_{\Pi,\mathcal{A}}(\lambda,b) \right\}_{\lambda\in\mathbb{N}} \approx_c \left\{ \mathrm{Hyb}_{\Pi,\mathcal{A}}(\lambda,b) \right\}_{\lambda\in\mathbb{N}}$$

Then, the theorem follows by HYBRID ARGUMENT:

$$\begin{aligned}
\mathrm{GAME}^{\text{one-time}}_{\Pi,\mathcal{A}}(\lambda,0) &\approx_c \mathrm{Hyb}_{\Pi,\mathcal{A}}(\lambda,0) \\
&\equiv \mathrm{Hyb}_{\Pi,\mathcal{A}}(\lambda,1) \\
&\approx_c \mathrm{GAME}^{\text{one-time}}_{\Pi,\mathcal{A}}(\lambda,1)
\end{aligned}$$

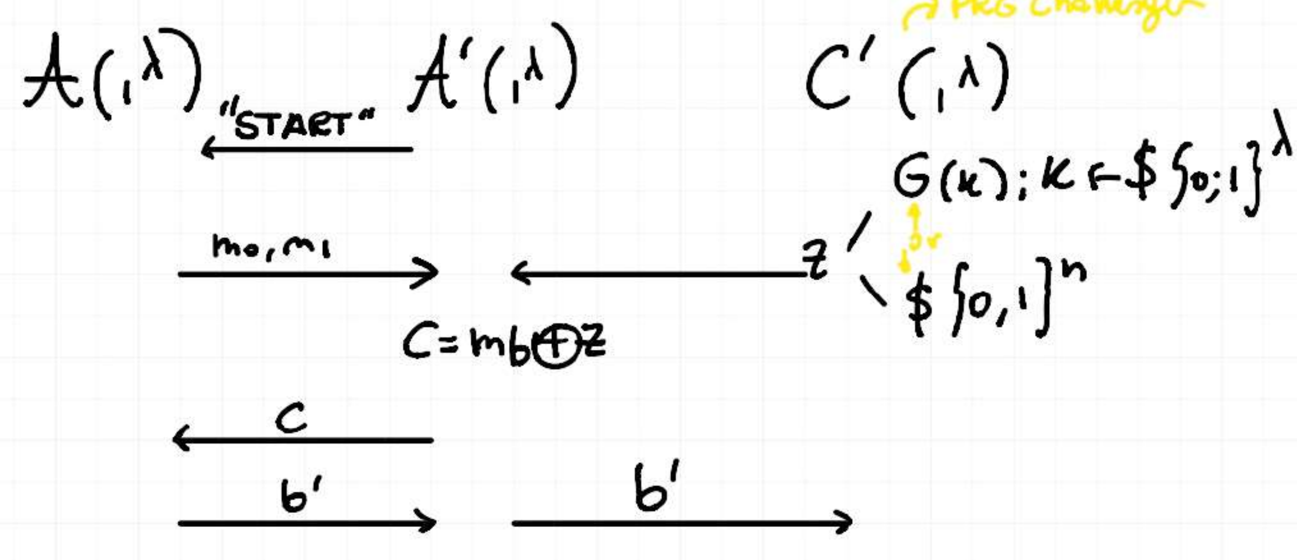
<u>PROOF</u> (claim): Fix $b\in\{0,1\}$. Assume

$\nexists$ PPT $\mathcal{A}$ s.t. → there exists no $\mathcal{A}$ that can distinguish GAME from Hyb

$$\left| \Pr\left[\mathrm{GAME}^{\text{one-time}}_{\Pi,\mathcal{A}}(\lambda,b)=1\right] - \Pr\left[\mathrm{Hyb}_{\Pi,\mathcal{A}}(\lambda,b)=1\right] \right|$$

$$\geq \frac{1}{\mathrm{poly}(\lambda)}$$ → probability not negligible

Then we build a REDUCTION, i.e. a PPT $\mathcal{A}'$ that breaks PRG w.p. $1/\mathrm{poly}(\lambda)$.



Analysis: $\Pr[\mathcal{A}'(1^\lambda, z) = 1 : z = G(k); k \leftarrow \$ \{0,1\}^\lambda]$

$$= \Pr[\mathcal{A}(1^\lambda) = 1 : c = G(k) \oplus m_b ; k \leftarrow \$ \{0,1\}^\lambda]$$

$$= \Pr[\mathrm{GAME}^{\text{one-time}}_{\Pi,\mathcal{A}}(\lambda, b) = 1]$$

Similarly, $\Pr[\mathcal{A}'(1^\lambda, z) = 1 : z \leftarrow \$ \{0,1\}^n]$

$$= \Pr[\mathcal{A}(1^\lambda) = 1 : c = z \oplus m_b ; z \leftarrow \$ \{0,1\}^n]$$

$$= \Pr[\mathrm{Hyb}_{\Pi,\mathcal{A}}(\lambda, b) = 1]$$

$$\Rightarrow \Pr[\mathcal{A}'(1^\lambda, z) = 1 : z = G(k); k \leftarrow \$ \{0,1\}^\lambda]$$
$$- \Pr[\mathcal{A}'(1^\lambda, z) = 1 : z \leftarrow \$ \{0,1\}^n]$$
$$= \big| \Pr[\mathrm{GAME}^{\text{one-time}}_{\Pi,\mathcal{A}}(\lambda, b) = 1]$$
$$- \Pr[\mathrm{Hyb}(\lambda, b) = 1] \big| \geq 1/\mathrm{poly}(n)$$

PLAN :

1) OWFs $\Rightarrow$ PRGs
2) What about MANY cyphertexts?

OWFs $\Rightarrow$ PRGs

Q: Unpredictability vs. Pseudorandomness

Given $y = f(x)$ for $x \leftarrow \$ \{0,1\}^n$, what info about x is hard to compute?

Of course the whole x is hard to compute, but what about a specific bit of x?

<u>DEF</u>: Let $f: \{0,1\}^n \to \{0,1\}^n$ be a OWF.

We say that $h: \{0,1\}^n \to \{0,1\}$ is a HARD-CORE PREDICATE for f if: $\forall$ PPT $\mathcal{A}$

$$\Pr[\mathcal{A}(1^\lambda, y) = h(x) : \substack{x \leftarrow \$ \{0,1\}^n \\ y = f(x)}] \leq \text{negl}(\lambda) + \tfrac{1}{2}$$

<u>EX</u>: Show that there is no single $h: \{0,1\}^n \to \{0,1\}$ that is HARD-CORE for ALL OWFs $f: \{0,1\}^n \to \{0,1\}^n$

<u>THM</u> (Goldreich - Levin, 1989)

Let $f: \{0,1\}^n \to \{0,1\}^n$ be a OWF.

Define $g(x,r) = (f(x), r)$ for $r \in \{0,1\}^n$

Then g is a OWF and

$$h(x,r) = \langle x, r \rangle = \sum_{i=1}^{n} x_i \cdot r_i \bmod 2$$

is HARD-CORE for g

EX Prove that g is a OWF if f is a OWF.

DEF We say that h is HARD-CORE for f if

$$(f(U_n), h(U_n)) \approx_c (f(U_n), U_1)$$

$h(x)$ is unpredictable and undistinguishable from true random

FACT The two DEFs above are equivalent

This suggests SIMPLE construction of PRG with stretch $\ell = 1$

$$G(s) = f(s) \| h(s)$$

EX Prove that above PRG is secure so long as $f: \{0,1\}^n \to \{0,1\}^n$ is a ONE-WAY PERMUTATION (OWP)

EX Let $G: \{0,1\}^\lambda \to \{0,1\}^{\lambda+1}$,

$$G': \{0,1\}^{\lambda+1} \to \{0,1\}^{\lambda+\ell} \text{ with } \ell > 2$$

be secure PRGs. Then

$$G^*(s) = G'(G(s)) \text{ is a PRG.}$$