EXERCISES

1) Prove or refute: (Enc, Dec) vs PERFECTLY SECRET wt for all M over $\mathcal{M}_1$ all $c_0, c_1 \in \mathcal{C}$

$$Pr[C = c_0] = Pr[C = c_1]$$

$$C = Enc(K, M); \quad K \equiv U$$

Is there Π s.t. wt vs PERFECTLY SECRET but does not satisfy the above.

Let $c = k \oplus m$. Define $c' = c \| b$

$$\Pr[b = 0] = 1/4$$

$$\Pr[b = 1] = 3/4$$

Prove still perfectly secret (same proof of OTP)

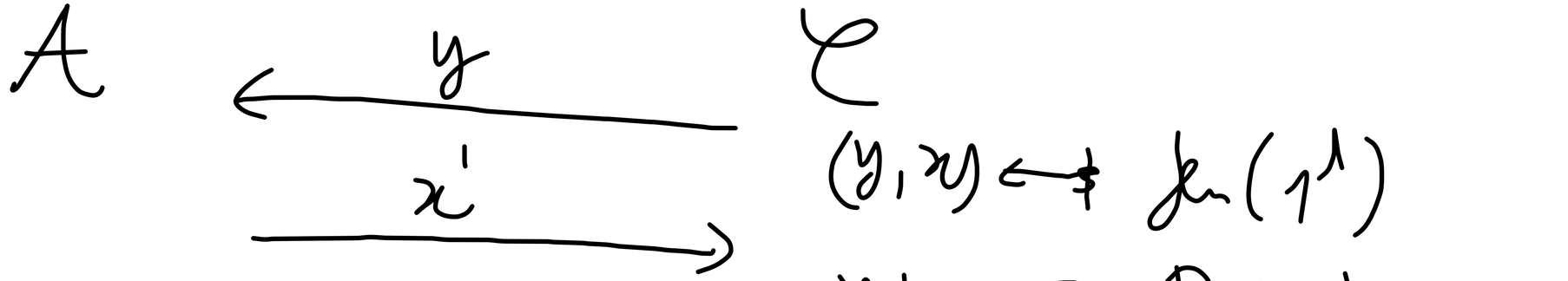
but now CTXs are more likely to ~~start~~ end with 1

2) A ONE-WAY PUZZLE for a relation

$R : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ ns

a PT algo $\mathrm{Sen}(1^\lambda)$ s.t. $(x,y) \leftarrow\!\$\ \mathrm{Sen}(1^\lambda)$ s.t. $R(x,y)=1$.

and moreover $\forall$ PPT A:



$\Pr[\mathrm{win}] \leq \mathrm{negl}$.

Prove: It is equivalent to OWF.

<u>OWF => Puzzles</u>. The relation: $R(x,y)=1 \iff f(x)=y$.

$Gen(1^\lambda)$: $x \leftarrow \{0,1\}^\lambda$

$y = f(x)$

Finding x' s.t. $R(x',y)=1$ is the same as inverting f.

<u>Puzzles => OWF</u>. $Gen(1^\lambda) \to (x,y)$ s.t. $R(x,y)=1$

$f(\cdot) = ???$; $f(r)$: $Gen(1^\lambda; r)$ ← FIX RANDOMNESS to r!

$= (x,y)$

Output y.

3) Let $G: \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ a PRG.

Show G ns by itself a OWF.

By reduction: $\exists$ PPT A_{OWF} s.t.

$$Pr\left[G(x') = y : x \leftarrow\$ \{0,1\}^\lambda ;\ x' \leftarrow\$ A_{OWF}(y)\right]$$

$$y = G(x)$$

A_{OWF} $\xleftarrow{\ y\ }$ $\mathcal{C}_{OWF}$ $x \leftarrow\$ \{0,1\}^\lambda$

$\xrightarrow{\ x'\ }$ $y = G(x)$

WIN: $G(x') = y$

$\geq 1/poly$

A_{OWF} A_{PRG} $\mathcal{C}_{PRG}$

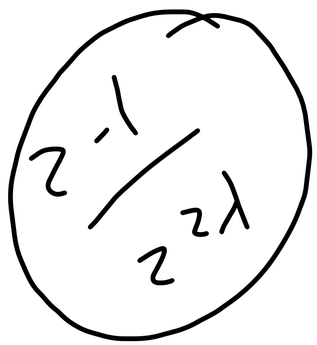
z ⟵ z ⟵ z ⟵ $G(x)$ / UNIFORM over $\{0,1\}^{2\lambda}$

x' ⟶ If $G(x') = z$ then $b'=1$ Else $b'=0$ ⟶ b'

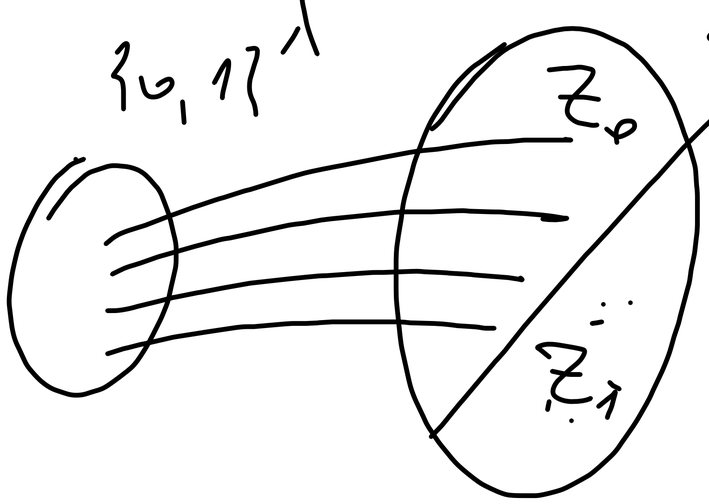
Need: $\left| Pr[b'=1 : z = G(x); x \leftarrow\$ \{0,1\}^{\lambda}] - Pr[b'=1 : z \leftarrow\$ \{0,1\}^{2\lambda}] \right| \geq 1/poly$

$$\Pr[b'=1 : z = G(x),\ x \leftarrow\!\$ \{0,1\}^\lambda] \geq 1/\text{poly}$$

$$\Pr[b'=1 : z \leftarrow\!\$ \{0,1\}^{2\lambda}]$$



$= 2^{-\lambda}$



with prob: $2^{-\lambda}$

$$= 2^{-\lambda} \cdot \Pr[b'=1 : z \leftarrow\!\$ V_{2\lambda}, z \in Z_0]$$

$$\pm 0 \quad \leq 2^{-\lambda} \cdot \Rightarrow |1 \cdot - \cdot| \geq \frac{1}{\text{poly}} - 2^{-\lambda}$$

$$= 1/\text{poly}$$

$$\Pr[b'=1 : z \leftarrow\!\$\, U_{2\lambda}]$$

$$= \Pr[z \in Z_0] \cdot \Pr[b'=1 : z \leftarrow U_{2\lambda} \mid z \in Z_0]$$
$$+ \Pr[z \in Z_1] \cdot \Pr[b'=1 : z \leftarrow\!\$\, U_{2\lambda} \mid z \in Z_1]$$

$= 2^{-1}$

Ex. What if $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+1}$?

*) Let $F_k(x)$ be a PRF. Consider: $\hookrightarrow \in \{0,1\}^n$

(i) $F'_k(x) = F_k(0\|x) \,||\, F_k(1\|x)$ ✓

$\hookrightarrow \in \{0,1\}^{n-1}$

(ii) $F'_k(x) = F_k(0\|x) \,||\, F_k(x\|1)$ ✗

Is F' a PRF?

(ii) Consider $x = 0^{n-1}$ and $x' = 0^{n-2}\|1$

$F'_k(x) = F_k(0^n) \,||\, F_k(0^{n-1}\|1)$

$F'_k(x') = F_k(0^{n-1}\|1) \,||\, F_k(0^{n-2}\|1^2)$