Exercises

*) Alternative definition of perfect secrecy: $\Pi = (Enc, Dec)$ is PS iff $\forall$ M over $\mathcal{M}$, every $c_0, c_1 \in \mathcal{C}$:

$$Pr[C = Enc(K, M) = c_0]$$
$$= Pr[C = Enc(K, M) = c_1].$$

Is this equivalent to our definition?

No. Counterexample: Take the one-time pad; $Enc(k, m) = k \oplus m$.

Consider $Enc'(k, m) = b \| k \oplus m$

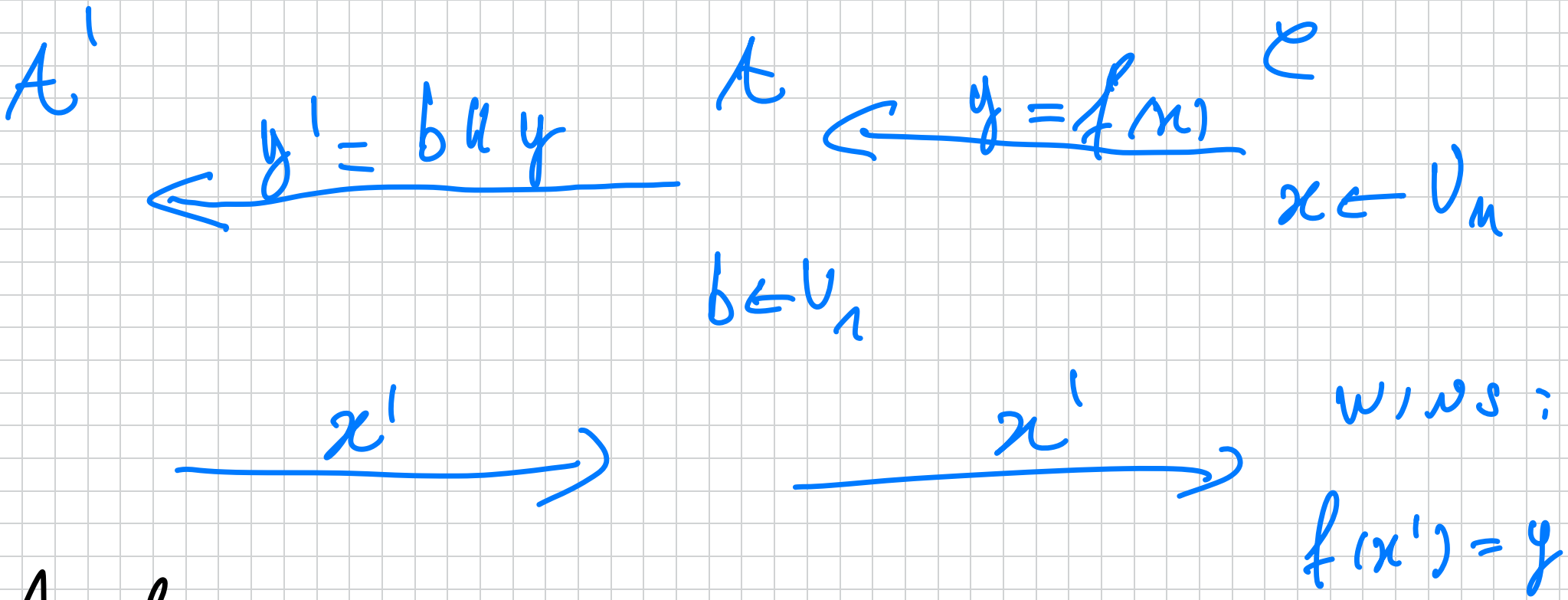
where b is a bit and it is biased (e.g. $\Pr[b=0] = 3/4$).

$\Rightarrow (Enc', Dec')$ is still PS under our definition. But CTxs starting with $b=0$ are more likely than those starting with $b=1$.

*) Assume $f : \{0,1\}^n \to \{0,1\}^n$ is a PRF. Show that $f' : \{0,1\}^m \to \{0,1\}^{m+1}$ s.t.

$$f'(x) = x[1] \,\|\, f(x)$$

is also owf. By reduction:



Analysis:

$$Pr[A \text{ wins}] \geq Pr[b = x_{[1]}] \cdot Pr[A' \text{ wins}]$$

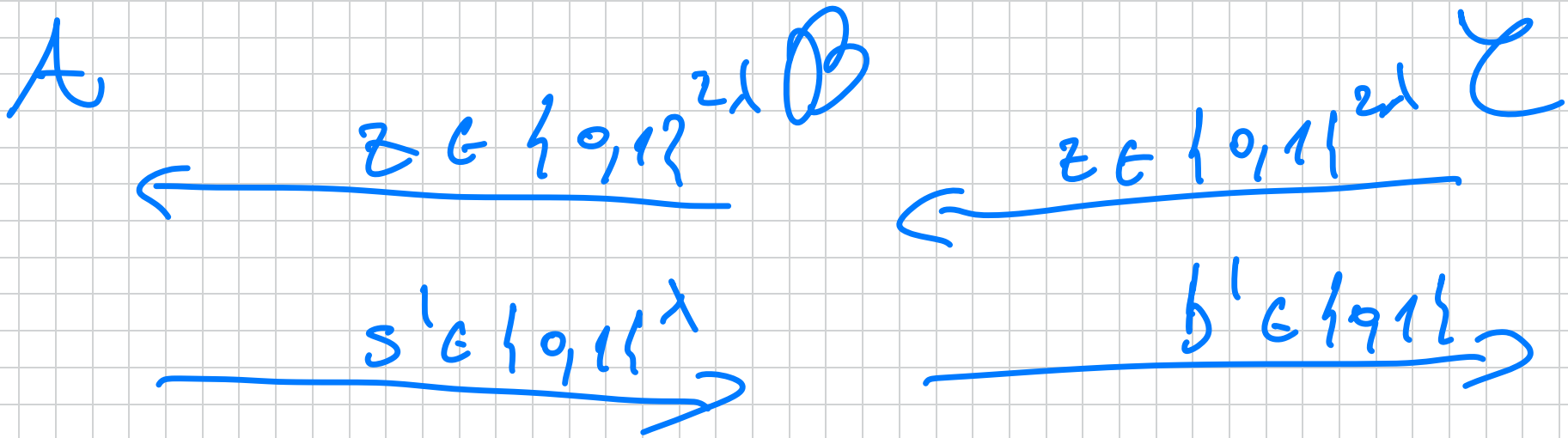
$$= \frac{1}{2} \cdot \frac{1}{poly} \geq \frac{1}{poly}$$

*) Let $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a PRG.
Show that G is also a OWF.

By reduction: $\exists$ PPT A s.t.

$$\Pr[z = G(s') : s \leftarrow U_\lambda;\ z = G(s)\ s' \leftarrow A(z)] \geq 1/\text{poly}$$

But all PPT $\mathcal{B}$ breaking PRG



If $G(s') = z$

$b' = 1$

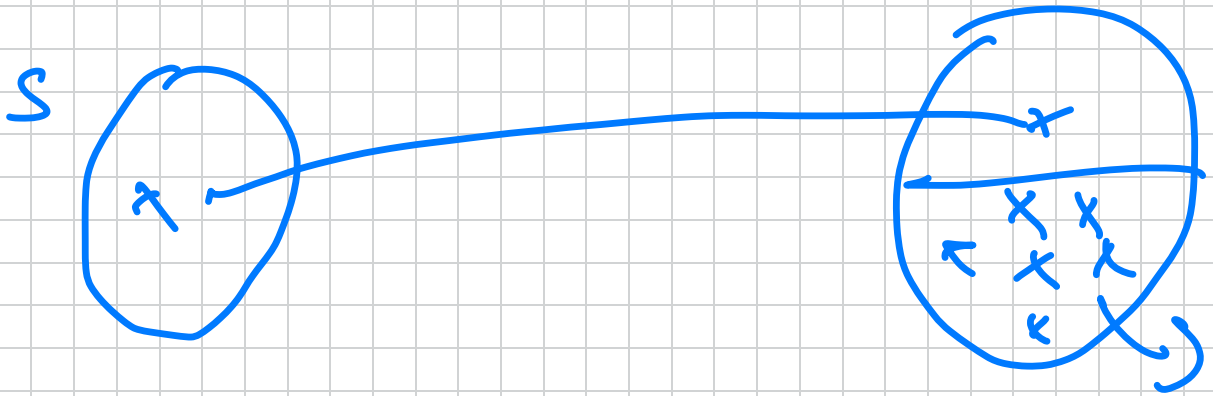
Else,

$b' = 0$

Analysis:

$$\Pr[\, b' = 1 : z = G(s);\ s \leftarrow U_\lambda \,] \geq \frac{1}{poly}$$

$$\Pr[b' = 1 : z \leftarrow N_{2\lambda}] \leq 2^{-\lambda}$$



At most 2^{λ} values in $\{0,1\}^{2\lambda}$ have a pre-image

$$\frac{2^{\lambda}}{2^{2\lambda}} = 2^{-\lambda}$$

*) Variants of this:

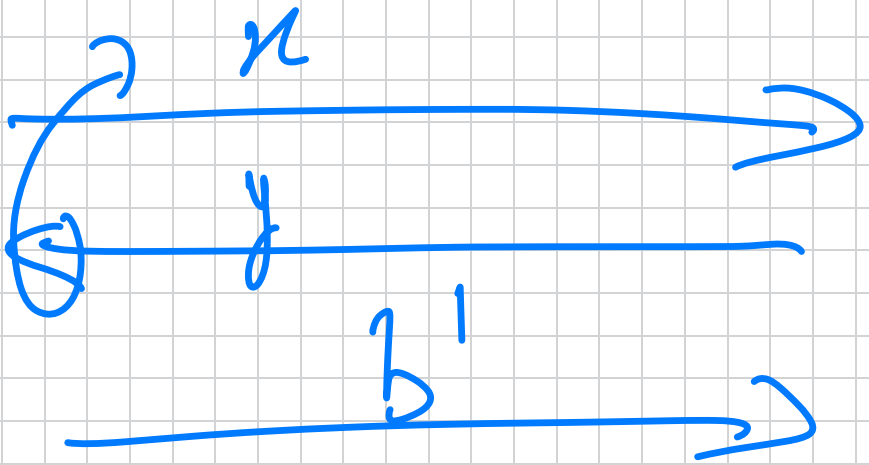
No $G : \{0,1\}^{\lambda} \to \{0,1\}^{\ell}$ can be secure

exists UNBOUNDED PRF Advs.

Also: $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+1}$ as a OWF.

*) No PRF is secure against UNBOUNDED Advs.

A



C

REAL | RAND

$y = F_K(x)$ | $y = R(x)$

$x \leftarrow U_\lambda$ | R RANDOM TABLE

A knows entire table:

$\exists\ k \in \{0,1\}^\lambda$ s.t. $\forall\ x,\ y = f_k(x)$.

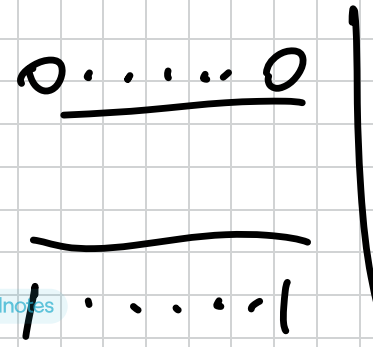
If yes, $b' = 1$

Else $b' = 0$

Analysis: $\Pr[\ b' = 1 : \text{REAL}\ ] = 1$

$\Pr[\ b' = 1 : \text{RAND}\ ] \leq \text{negl}(\lambda)$.

tables consistent with some key : 2^λ



input length: n

output length: m

length of table : $n \cdot 2^n$

# of tables : $2^{n \cdot 2^n}$

$$n(\lambda) = \text{poly}(\lambda)$$

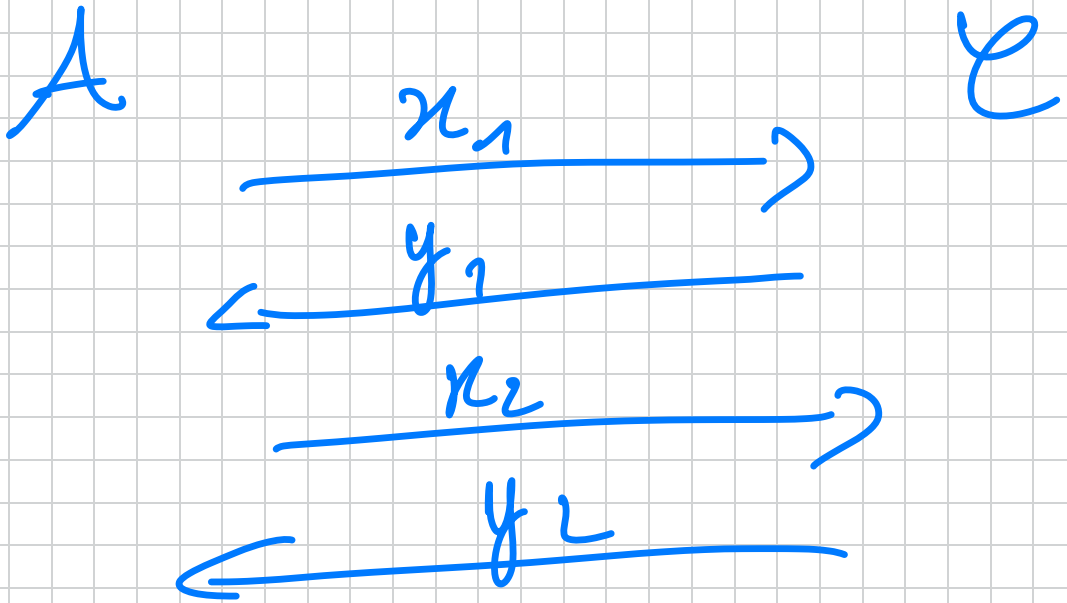
$$2^{\lambda} / 2^{n \cdot 2^n} \equiv \text{negl}(\lambda).$$

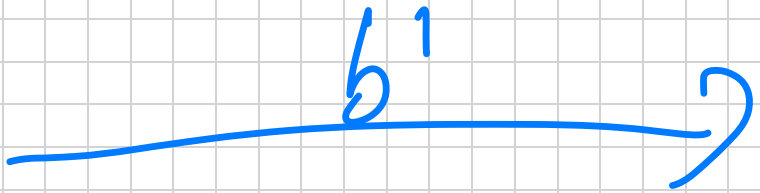
*) Secure or not : $F_K(x) = G'(K) \oplus x$

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

G' ≡ G truncated to λ bits.

$$F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$$





If $y_1 \oplus y_2 = x_1 \oplus x_2$

$b' = 1$

Else $b' = 0$

$\Pr[\, b' = 1 : \text{REAL} \,] = 1$

$\Pr[\, b' = 1 : \text{RAND} \,] = 2^{-\lambda}$

*) Secure or not: $F'_k(x) = F_x(k)$

for SECURE PRF $F: \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$

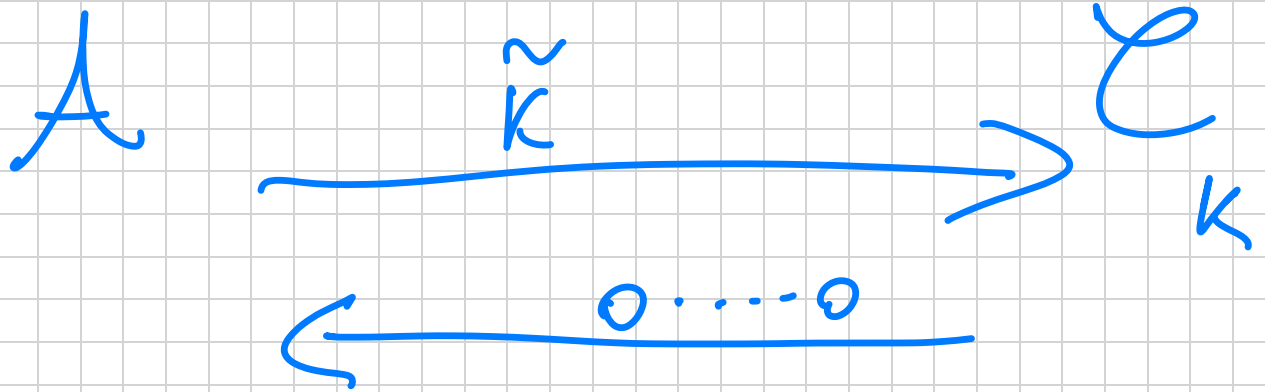
No. Why? Because F requires a random key. Need to show $\exists\ \tilde{F}$ a secure PRF s.t. F' ALWAYS BROKEN when using $\tilde{F}$.

For instance, $\tilde{F}$ could have a BAD key $\tilde{k}$ s.t. $\tilde{F}_{\tilde{k}}(x) = 0^\lambda \quad \forall\ x \in \{0,1\}^\lambda$

$\tilde{F}_k(x) = F_k(x) \quad \forall\ x,\ k \neq \tilde{k}$

Now: $\tilde{F}$ still a PRF. Because the event $\tilde{K} = k$ happens w.p. $2^{-\lambda}$ in the PRF def.

$F'_K(x) = \tilde{F}_x(K)$ is NOT a PRF



REAL: 0 ... 0 w.p. 1

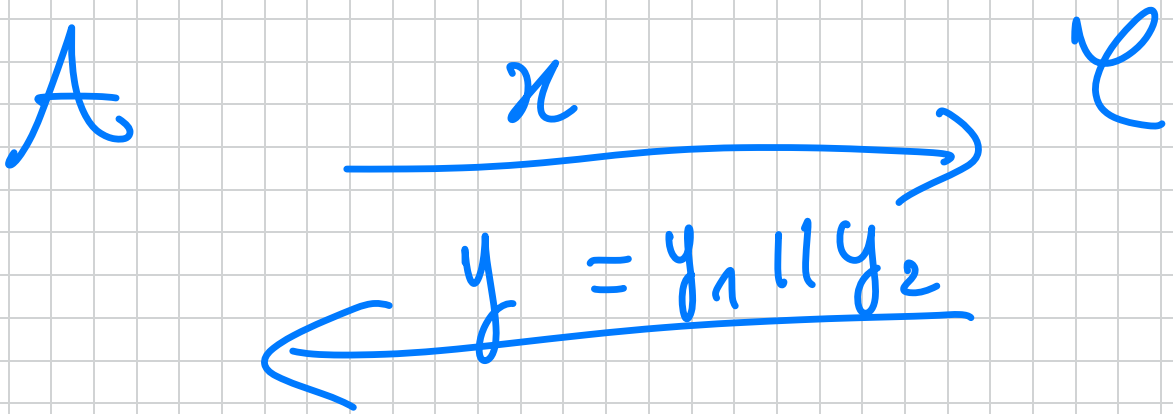
RAND: 0 ... 0 w.p. $2^{-\lambda}$

*) Show that ∃ UF-CMA MAC s.t. it is not by itself a PRF.

E.g., $Tag_K(m) = f_K(m) \| f_K(m)$

1) UF-CMA? Yes. Same proof as we did in class.

2) PRF? No.



$b' = 1$ IFF

$y_1 = y_2$

REAL: $y_1 = y_2$ ALWAYS.

$b' = 1$ w.p. 1

RAND: $y = R(x)$

$y \in U_{2^\lambda}$; $y = y_1 \| y_2$

$y_1 = y_2$?

*) Let Tag_1, Tag_2 be MACs. We know that at least one of them is UF-CMA, but not which one.

Show how to construct Tag that is UF-CMA using both Tag_1, Tag_2.