EXERCISES

*) Prove or refute: An SKE scheme is PERFECTLY SECRET if and only if: $\forall$ M over $\mathcal{M}$, $\forall$ $c_0, c_1 \in \mathcal{C}$

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

(i)

$$C = Enc(K, M)$$

K is UNIFORM.

Recall PERFECT SECRECY:

(NN) $\Pr[M = m] = \Pr[M = m \mid C = c]$

On the one hand, it seems (N) $\Rightarrow$ (NN).

Does (NN) $\Rightarrow$ (N)? In other words,

if a scheme is PERFECTLY SECRET is

it necessary that all CTXs are equally

likely? Not true: Here is a counter

example: Consider $\overline{\Pi} = (\overline{Enc}, Dec)$

s.t. $\overline{Enc}(K, m) = 0 \| m \oplus K$

and $\overline{Dec}(K, b \| c) = c \oplus K$

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

Now, take $c_1 \in C$ to be $1 \| \bar{C}$ and c_0 to be $0 \| C$. Then:

$$Pr[C = c_0] \neq Pr[C = c_1].$$

m

*1 Do This at home: Prove that an SKE Π is PERFECTLY SECRET if and only if $\forall$ adversaries (UNBOUNDED):

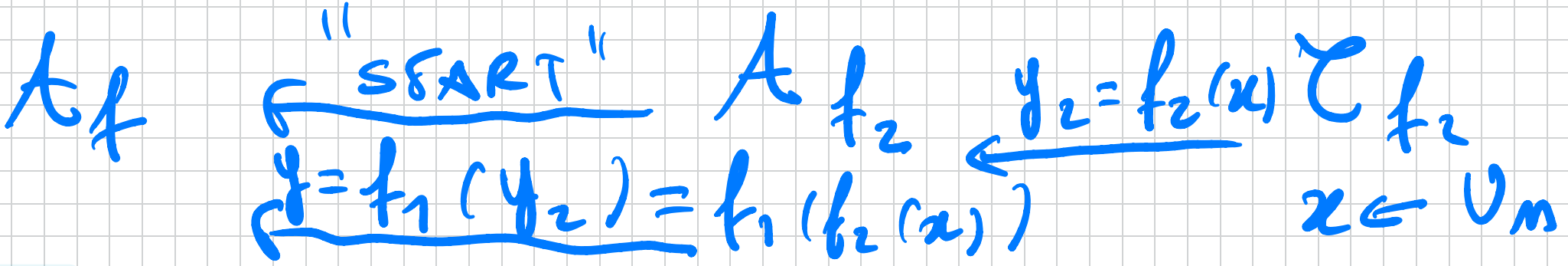
$$\text{GAME}^{\text{one-time}}_{\Pi,\mathcal{A}}(\lambda,0) \equiv \text{GAME}^{\text{one-time}}_{\Pi,\mathcal{A}}(\lambda,1)$$

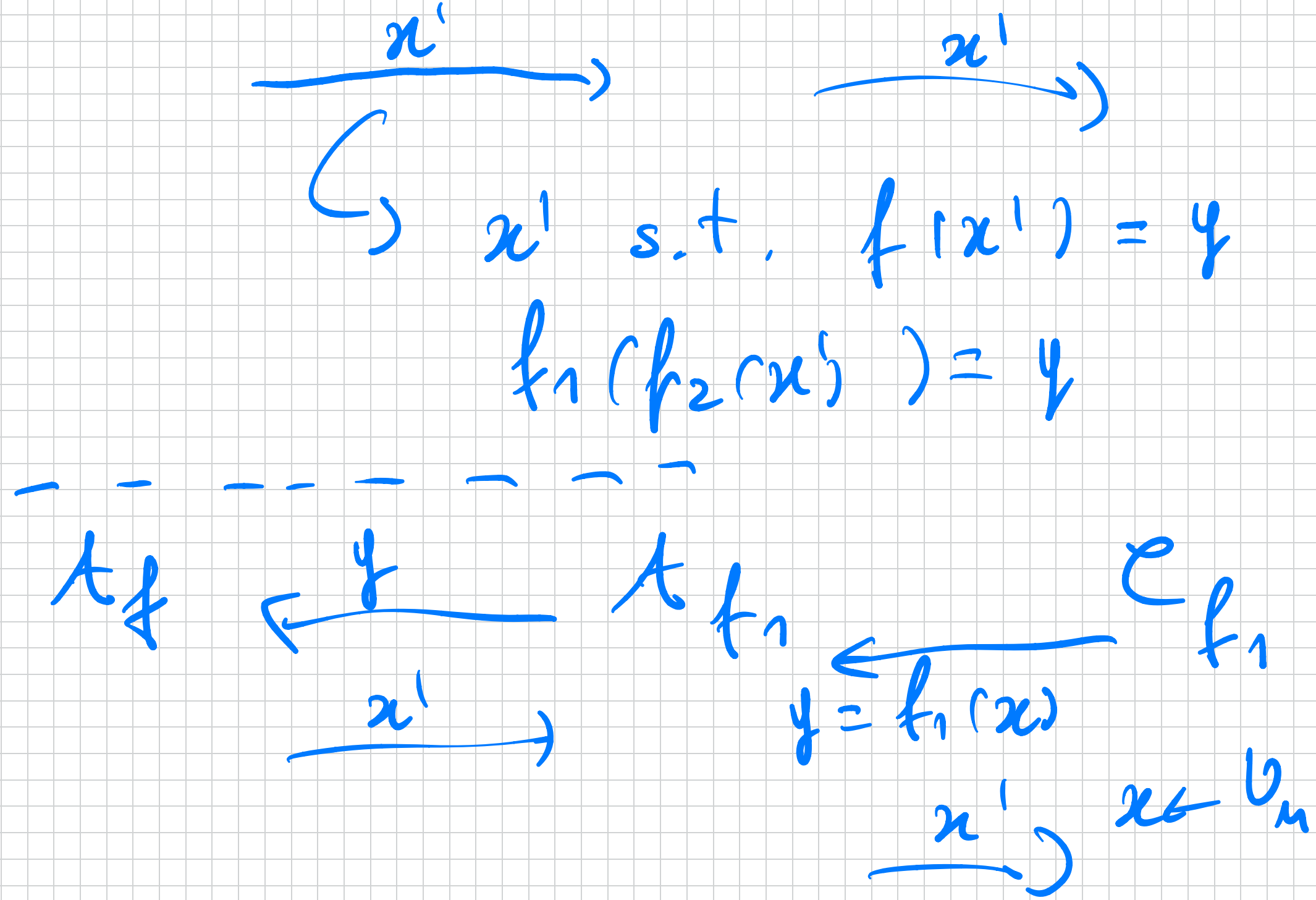
*) We are given $f_1 : \{0,1\}^n \to \{0,1\}^n$ and $f_2 : \{0,1\}^n \to \{0,1\}^n$ and we know at least one is a OWF.

Design f a OWF using f_1, f_2.

Proposal: $f(x) = f_1(f_2(x))$

Try to make the reduction:





Problem: $f_1(U_n)$ might have different distribution than $f_1(f_2(U_n))$

Counter example:

Let $f_2(x) = 0^n \quad \forall \; x \in \{0,1\}^n$

Let $f_1(x) = \begin{cases} f'(x) & \text{if } x \neq 0^n \\ 0^n & \text{if } x = 0^n \end{cases}$

f' is ANY OWF.

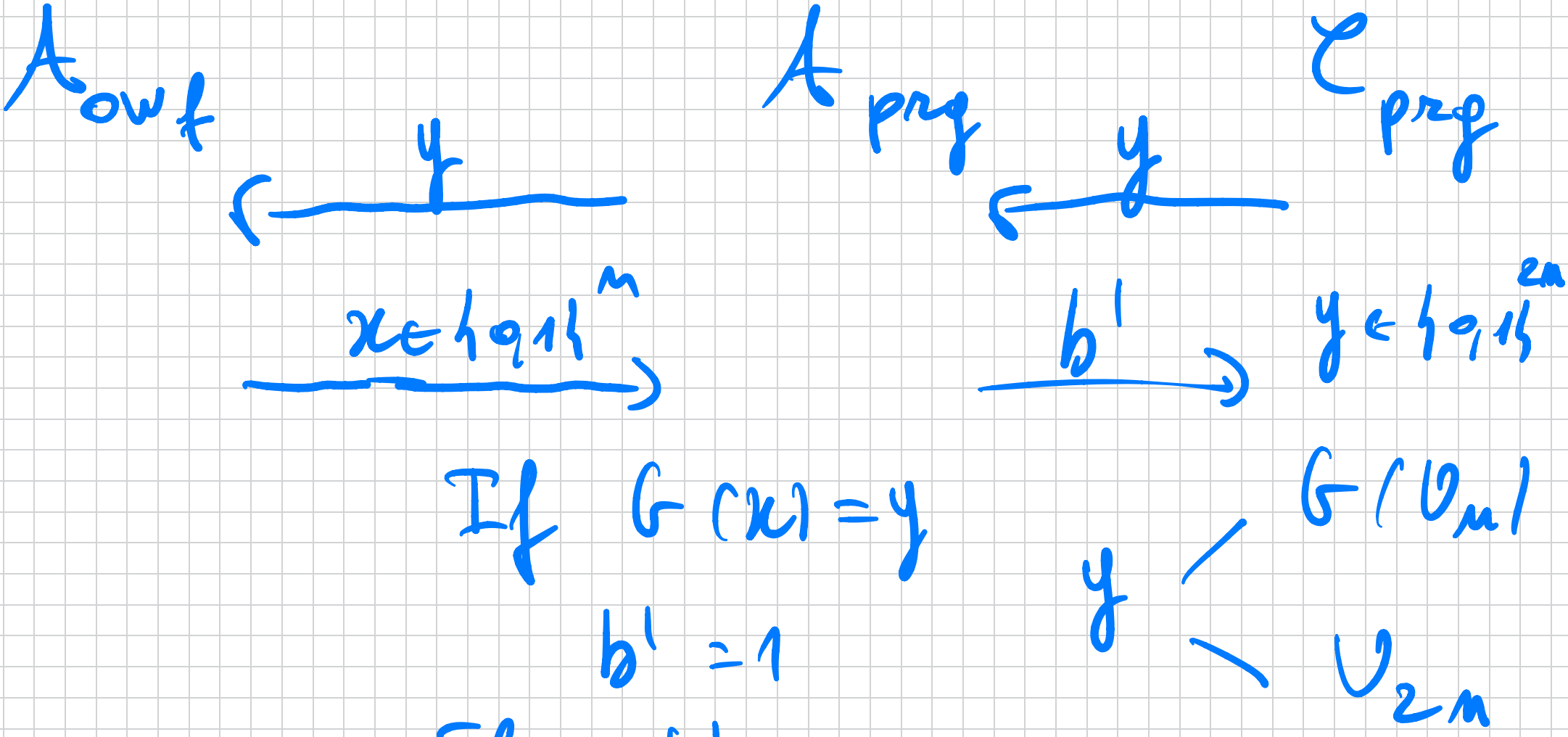
Another attempt:

$$f(x_1 \| x_2) = f_1(x_1) \| f_2(x_2)$$

$$f : \{0,1\}^{2n} \to \{0,1\}^{2n}$$

This works! Work out at home.

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



$$\Pr[\, b' = 1 : y = G(U_n) \,] \geq \varepsilon(n)$$

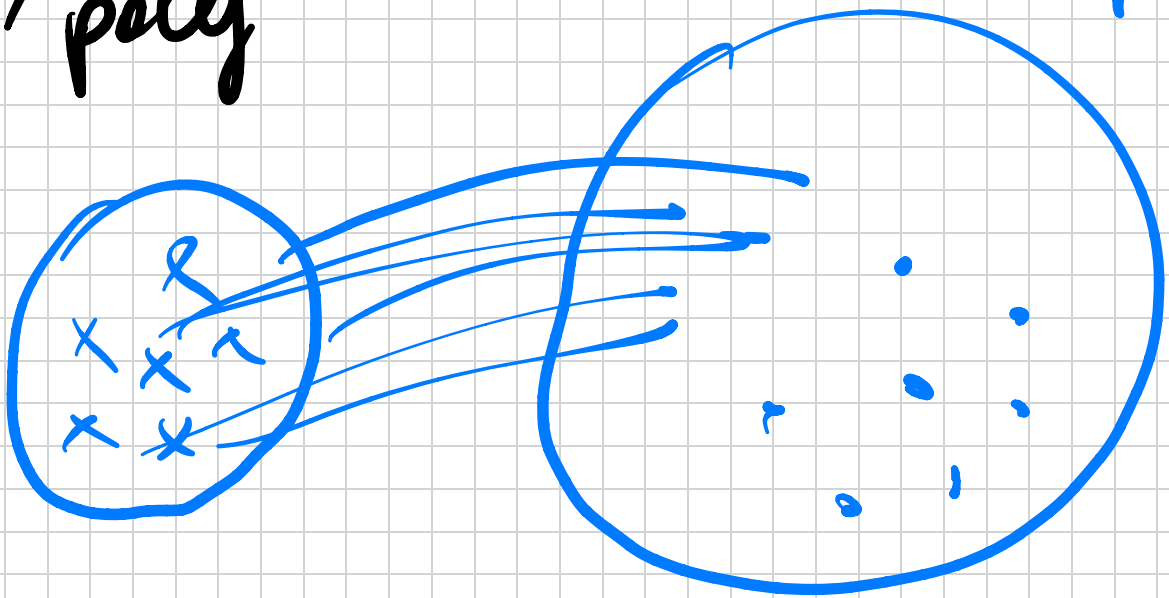
$$\Pr[\, b' = 1 : y \leftarrow U_{2n} \,] \leq \frac{2^n}{2^{2n}} = 2^{-n}$$

$$\varepsilon(n) = \Pr[\, A(G(U_n)) \text{ wins} \,]$$

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

$\{0,1\}^{2n}$

$\{0,1\}^n$



*) Let $F_k'(x) = F_k(0\|x) \| F_k(x\|1)$

Assume $F_k : \{0,1\}^n \to \{0,1\}^n$ a PRF

$$F_k' : \{0,1\}^{n-1} \to \{0,1\}^{2n}$$

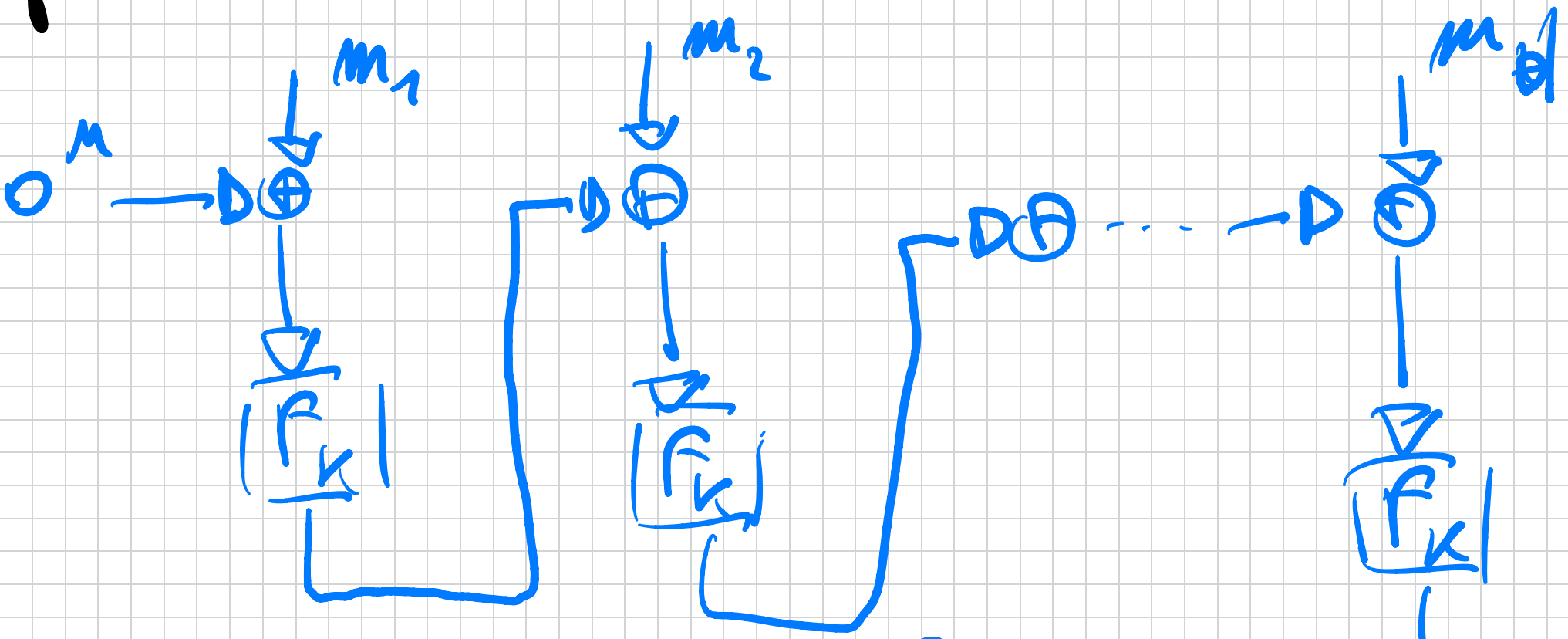
Is F' a PRF? No. Look:

$$F_k'(0^{n-1}) = F_k(0^n) \| F_k(0^{n-1}\|1)$$

$$F_k'(0^{n-2}\|11) = F_k(0^{n-1}\|1) \| F_k(--)$$

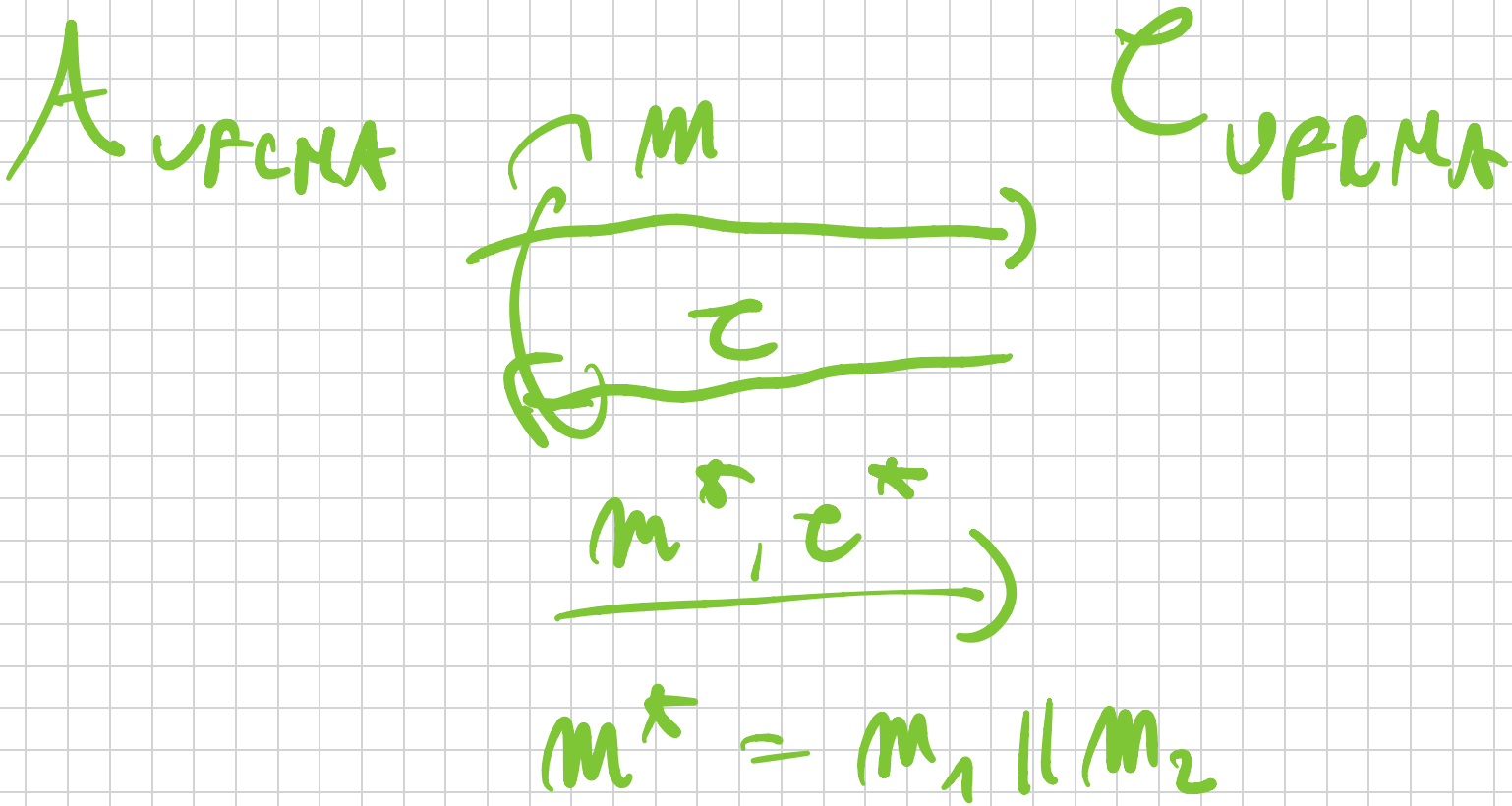
This gives immediately a DISTINGUISHER.

*) Show CBC-MAC is not UFCMA for VIL.



$CBC\text{-}MAC_k(m_1) = F_k(m_1) = c_1$

$CBC\text{-}MAC_k(m_1 \| m_2) = F_k(F_k(m_1) \oplus m_2)$



$$m^* = m_1 \| m_2$$

The queries: $m_1 \rightarrow c_1 = f_k(m_1)$

$$c_1 \oplus m_2 \rightarrow c^* = f_k\left(f_k(m_1) \oplus m_2\right)$$

*) Let $F = \{F_k\}$ be a PRP.

Define (Enc, Dec) s.t.

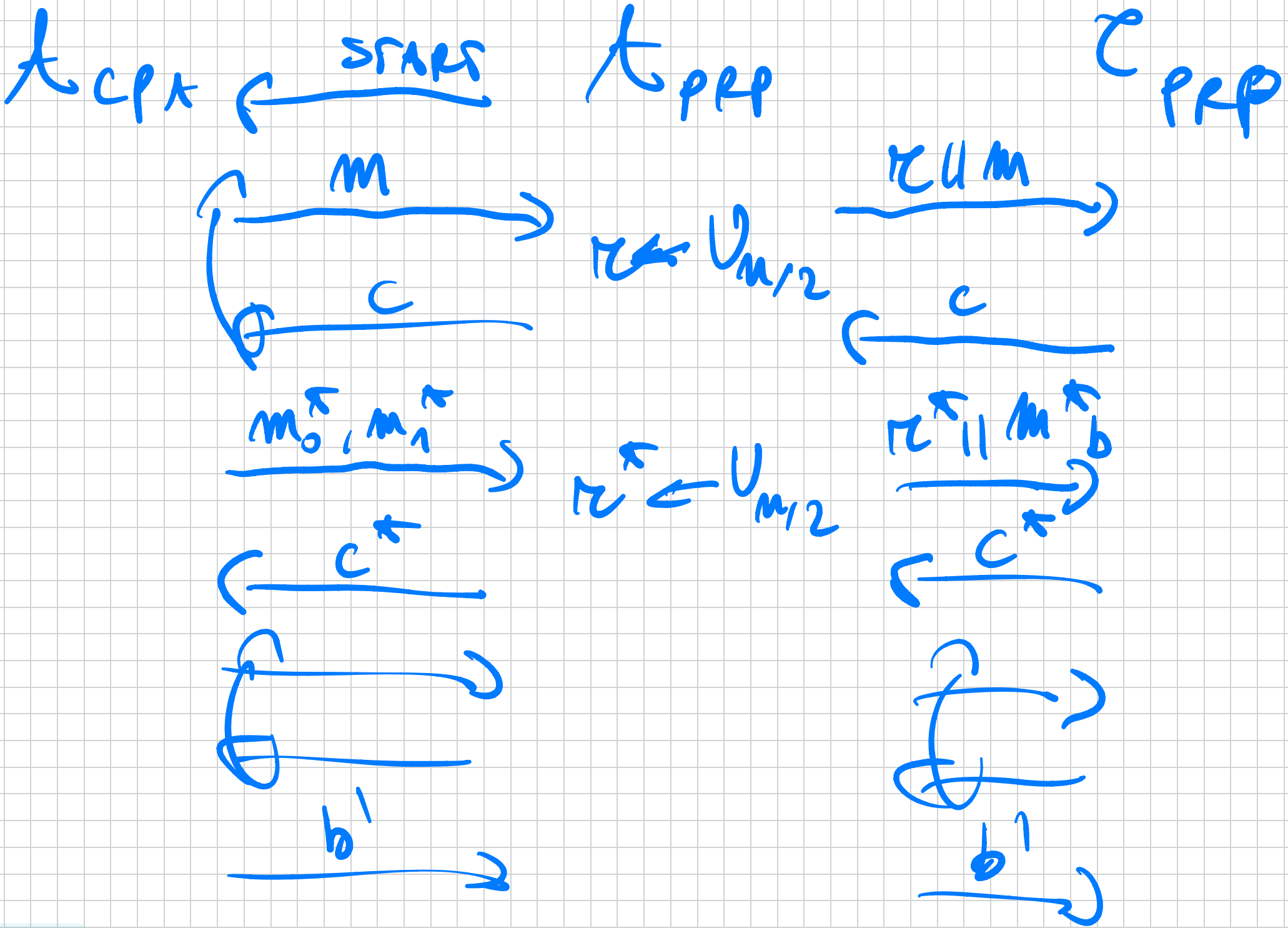
$$Enc(k, m) = F_k(r \| m)$$

$$r \leftarrow U_{n/2} \quad m \in \{0,1\}^{n/2}$$

$Dec(k, c)$ outputs m s.t.

$$r \| m = F_k^{-1}(c)$$

Prove it is CPA secure.



$G(\lambda, b)$: The CPA game with bit $b \in \{0,1\}$

$H(\lambda, b)$: The CPA game with $f_k \to R$ a RANDOM PERMUTATION

By the above reduction:

$\Rightarrow$ $G(\lambda, b) \stackrel{c}{\approx} H(\lambda, b)$ $\forall$ $b \in \{0,1\}$

$$G(\lambda, 0) \simeq_c H(\lambda, 0)$$

$$G(\lambda, 1) \simeq_c H(\lambda, 1)$$

$$H(\lambda, 0) \simeq_s H(\lambda, 1)$$

In $H(\lambda, b)$: $c^* = R(\pi^* \| m_b^*)$

The squeezers (CPA): $c_i = R(\pi_i' \| m_i')$

BAD: The event that π^* equals one of the π_i's.

Consider running on $\overline{BAD}$ $C^{\uparrow}$ uniform.

$$\Rightarrow \#(\lambda, 0) \approx \#(\lambda, 1)$$

$$\Pr[BAD] \leq q(\lambda) \cdot 2^{-n/2}$$

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

$= \#$ CPA queries.