

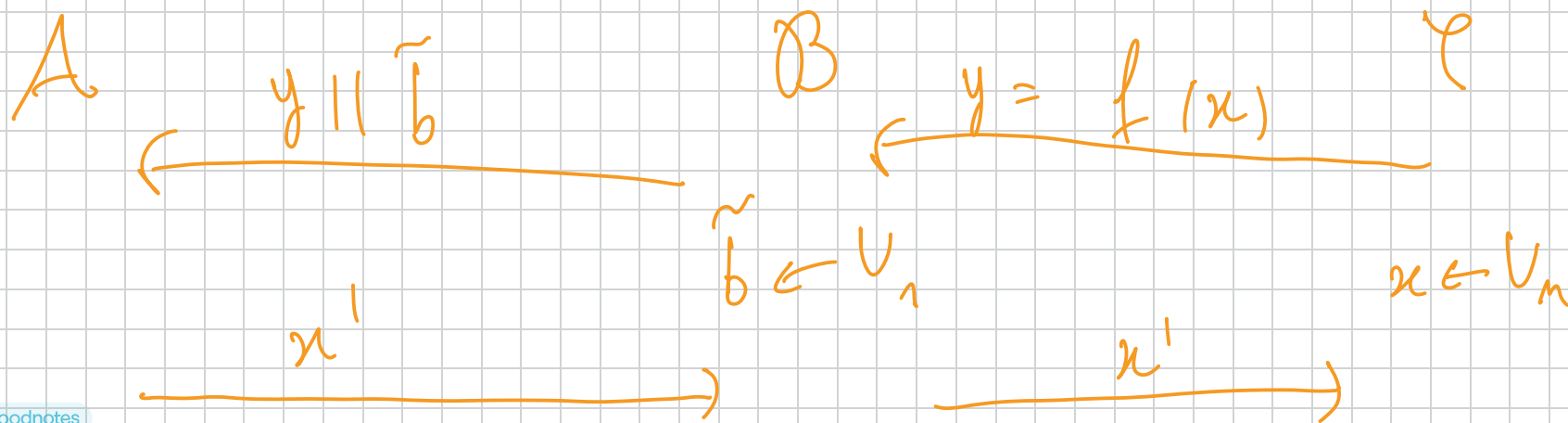
$$f_{BA0}(x) = f(x) \parallel h(x)$$

Clearly, $h(\cdot)$ not hard-core for f_{BA0} .

Why f_{BA0} is still a wff?

Suppose not: $\exists$ ppt A that wins $\text{Game}_{f_{BA0}}^{\text{wff}}(1)$
w. p. $\geq 1/\text{poly}(1)$ - (d.k. non-negligible).

Then, we are going to construct ppt B s.t. B breaks f .



$$\Pr[B \text{ wins}] = \frac{1}{2} \cdot \Pr[A \text{ wins}]$$

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

The next best thing: $\forall f \exists h$,

THM. Let $f: \{0,1\}^m \rightarrow \{0,1\}^m$ be a OWF. Consider

$$g: \{0,1\}^{2m} \rightarrow \{0,1\}^{2m} \text{ s.t. } g(x, r) = f(x) || r \quad \forall x, r \in \{0,1\}^m$$

Then g is a OWF and

$$h(x, r) = \langle x, r \rangle = \sum_{j=1}^m x_j r_j \bmod 2$$

is hard-core for g .

$$x = (x_1, \dots, x_m)$$

$$r = (r_1, \dots, r_m)$$

Intuition: Assume $\exists$ a very good adversary, that ALWAYS computes $h(x, r)$ given $g(x, r) \neq r$.

Then, we could easily get x from:

$$h(x, e_1) = \langle x, e_1 \rangle = \langle x, 10 \dots 0 \rangle = x_1$$

$\vdots$

$\vdots$

$$\langle x, e_m \rangle = \langle x, 0 \dots 0 1 \rangle = x_m$$

The general proof is harder because A wins only w.p. $1/poly$ over random choice of r .

Let's apply PRGs so that we can beat Shannon. Consider:

$$Enc(k, m) = G(k) \oplus m \quad m, c \in \{0, 1\}^{2^n}$$

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

$$G: \{0,1\}^n \rightarrow \{0,1\}^{2n}$$

The key is short: Shorter than the message!

Note: This is still one-time secure. In other words, given

$$c_1 = G(k) \oplus m_1; \quad c_2 = G(k) \oplus m_2$$

$$\Rightarrow c_1 \oplus c_2 = m_1 \oplus m_2$$

We need to understand how to define computational security of SKE.

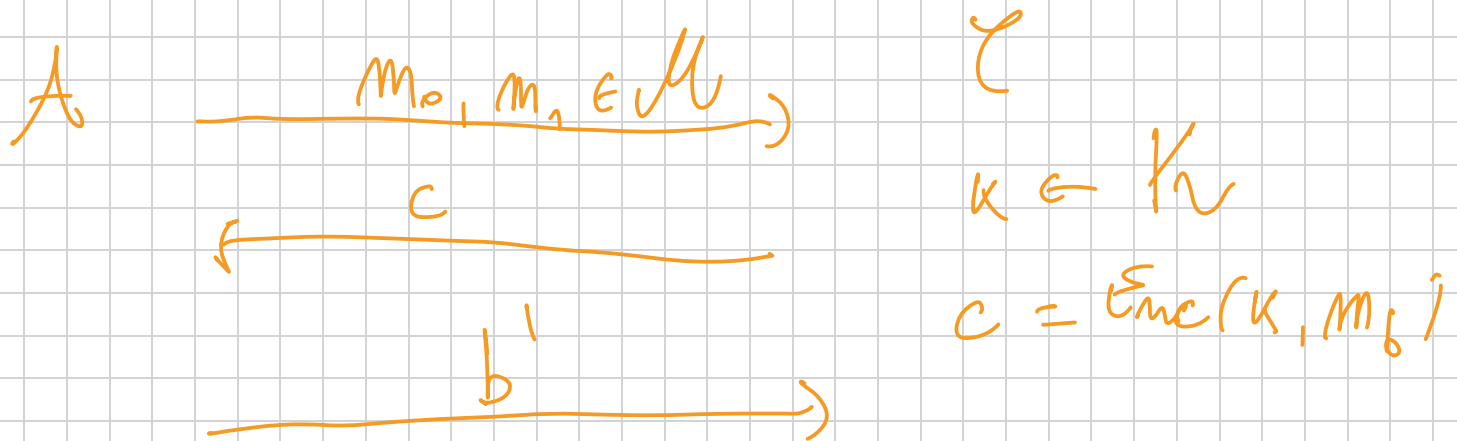
$$\text{Perf of secrecy: } \forall m_0, m_1, \text{Enc}(K, m_0) \stackrel{?}{=} \text{Enc}(K, m_1)$$

$\Rightarrow$ No even UNBOUNDED A can tell them apart!

Def A scheme $\Pi = (\text{Enc}, \text{Dec})$ is one-time computationally secure if:

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

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



Security checks:

- Above definition implies $\Rightarrow$ hard to compute k .

Remark: $\text{Enc}(k, m) = m$ also satisfies the

property that K is hard to compute!

- Also hard to compute m .
- But then also, first bit of m , second bit, ...

THM Assuming G is a PRG, the above defined SKF is one-time computationally secure.

Proof. Common proof technique: GAME HOPPING. We start

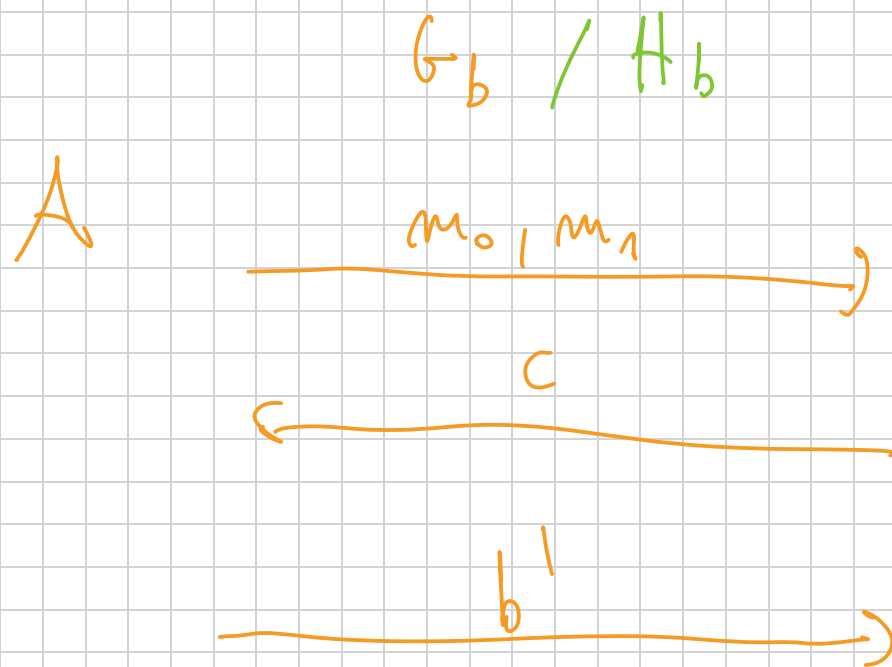
with

$$\text{GAME}_{\Pi, A}^{\text{one-time}}(\lambda, 0) \equiv G_0$$

$$\text{GAME}_{\Pi, A}^{\text{one-time}}(\lambda, 1) \equiv G_1$$

We need to show $G_0 \approx_c G_1$. We introduce

two further games: H_0



$$k \leftarrow \{0,1\}^n; \quad z \leftarrow U_{2n}$$

$$c_b = G(k) \oplus m_b$$

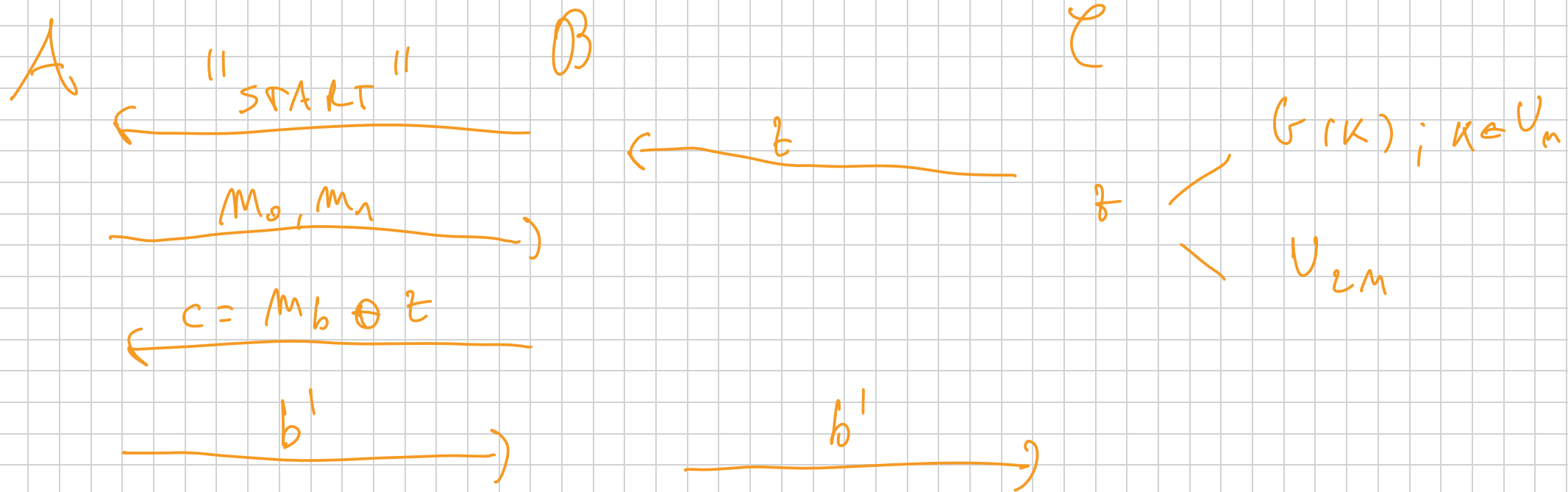
$$c_b = z \oplus m_b$$

Note : $H_0 \equiv H_1$. This follows by perfect secrecy of OTP.

So, it remains to show $G_b \approx_c H_b$. Then:

$$G_b \approx_c H_b \equiv H_1 \approx_c G_1$$

Assume not : $\exists$ PPT A telling apart G_b/H_b
 (for any $b \in \{0,1\}$) w.p. $1/\text{poly}$.



perfect randomness:

$$Pr[B \Rightarrow 1 : z \leftarrow G(k)] =$$

$$Pr[A \Rightarrow 1 : \text{nm } G_b]$$

$$Pr[B \Rightarrow 1 : z \leftarrow U_{2m}] =$$

$$Pr[A \Rightarrow 1 : \text{nm } H_b]$$

