Recap from last lecture: OWF => PRG with stretch $\ell(\lambda) = poly(\lambda)$.

Today: Let's apply what we have learned to SKE. Simple idea:

$$Enc(K, m) = G(K) \oplus m = c$$

$$Dec(K, C) = G(K) \oplus c = m.$$

$K \in \{0,1\}^\lambda$, but $m \in \{0,1\}^{1+\ell}$ for ANY $\ell = poly$.

But what does it mean for the above SKE to be (computationally) secure?

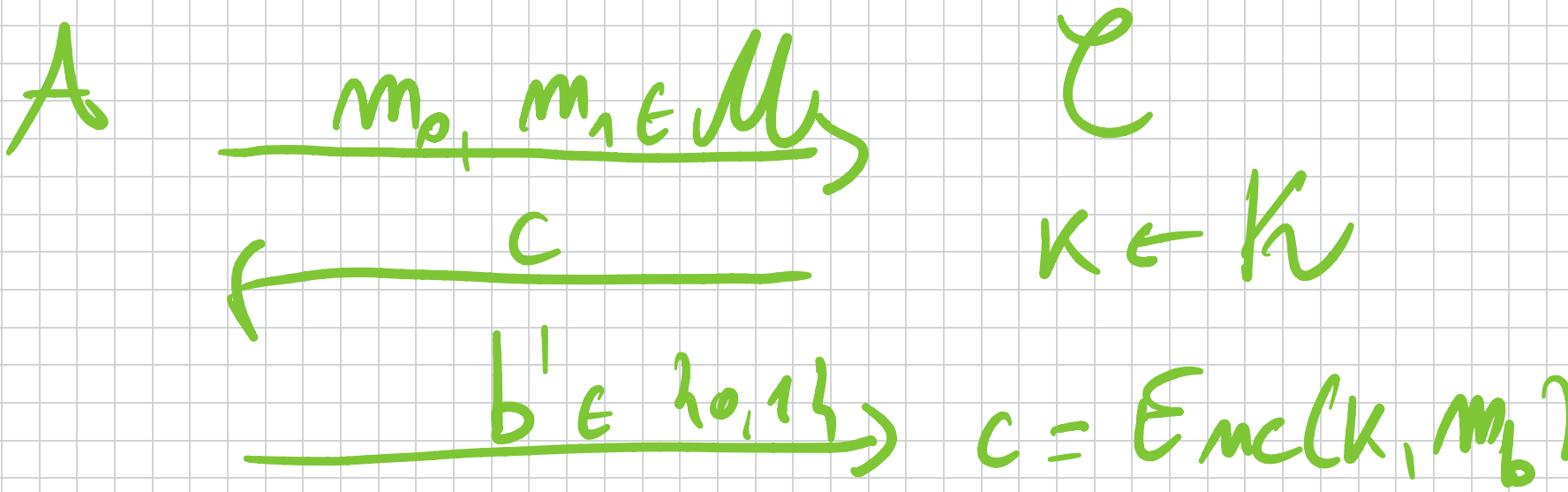
Let's define first a simple notion; this is just a warm-up.

Def Let $\Pi = (Enc, Dec)$ be a SKE.

We say Π is ONE-TIME COMPUTATIONALLY SECURE if:

$$GAME^{1\text{-time}}_{\Pi,A}(\lambda,0) \overset{c}{\approx} GAME^{1\text{-time}}_{\Pi,A}(\lambda,1)$$

$\text{GAME}^{1\text{-TIME}}_{\Pi,A}(\lambda, b)$



Recall, this means:

$$\left| Pr[b' = 1 : \text{GAME}^{1\text{-TIME}}_{\Pi,A}(\lambda, 0)] - Pr[b' = 1 : \text{GAME}^{1\text{-TIME}}_{\Pi,A}(\lambda, 1)] \right| \leq negl(\lambda)$$

Why obf. is good? Because, it captures natural properties every secure SKE should have:

- It should be hard to compute the secret key.
- It should be hard to compute the message.
- It should be hard to compute the 1st bit of the msg.

On the negative side, this notion is one-time (i.e. 1 key, 1 msg).

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

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

If I know, $c_1, c_2, m_1 \rightarrow$ I know m_2.

Apart from this, consider again Π s.t.

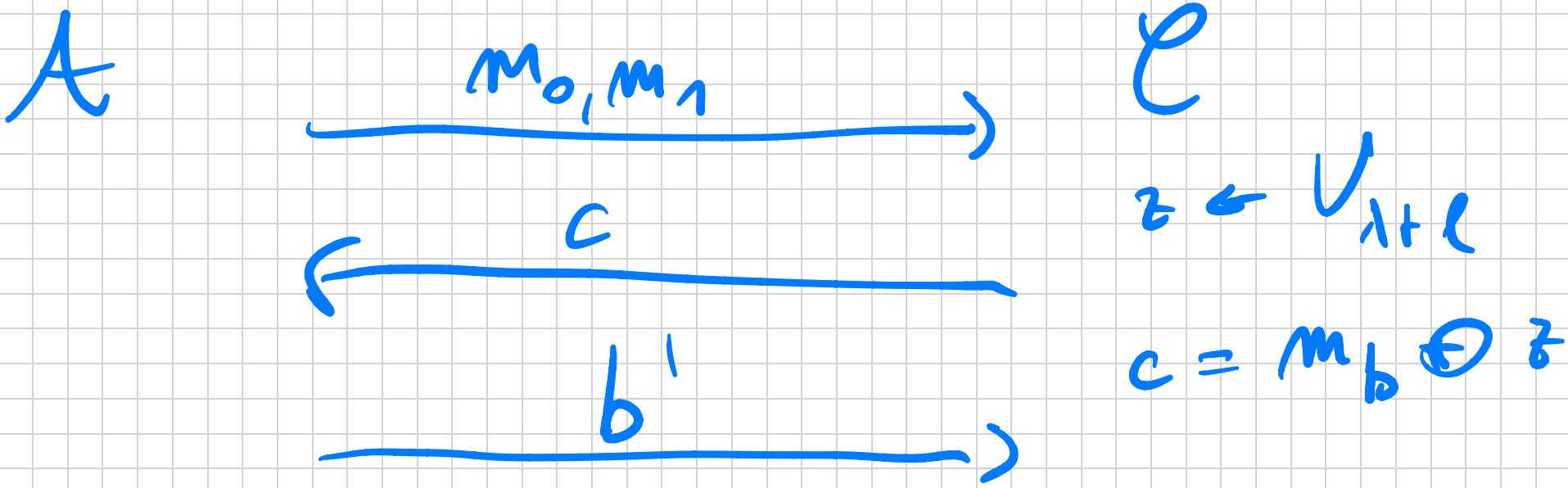
$$Enc(k, m) = G(k) \oplus m$$

$$Dec(k, c) = G(k) \oplus c$$

THM If G is a PRG, the above Π is one-time comp. secure.

Proof. Starting with the original experiment $\text{EAVE}(\lambda, b) \equiv \text{EAVE}^{1\text{-time}}_{\Pi,A}(\lambda, b)$

Consider $\text{HYB}(\lambda, b)$:



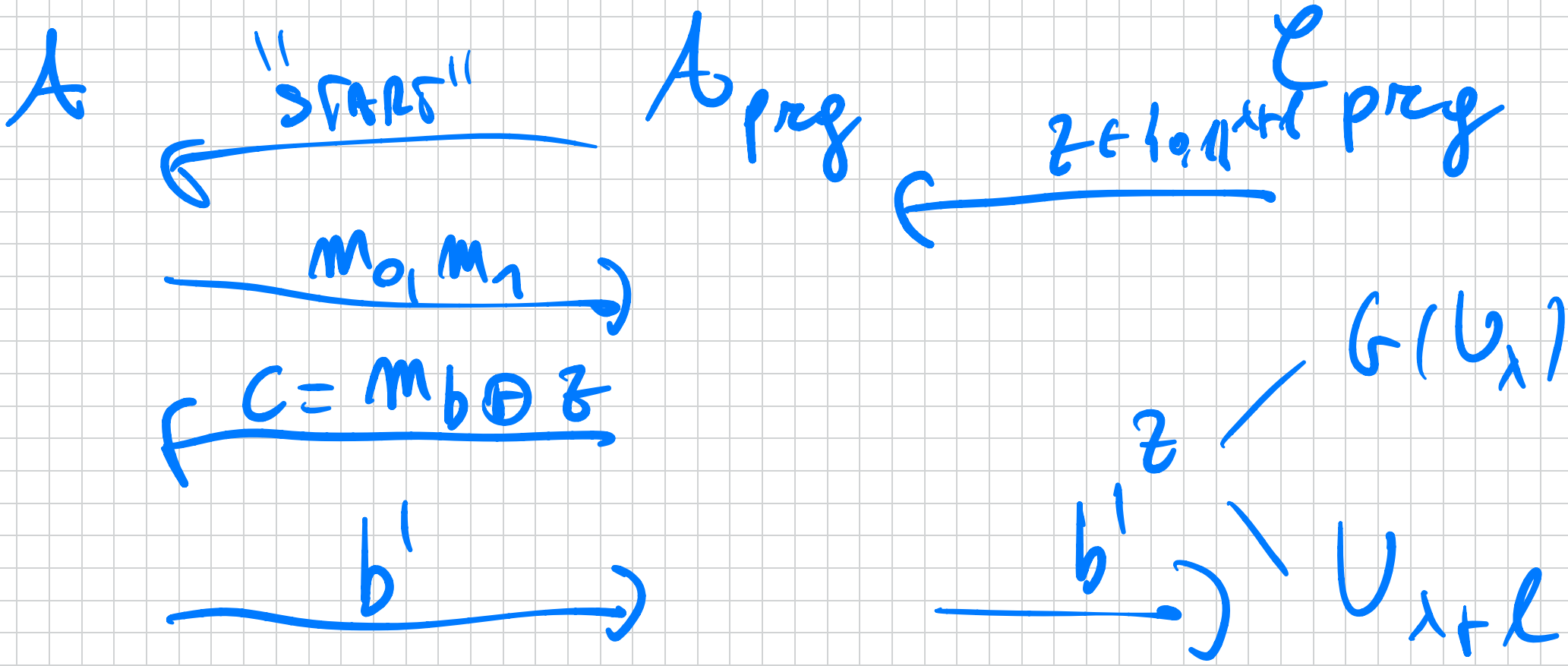
Easy to see: $HYB(\lambda,0) \equiv HYB(\lambda,1)$ because the distribution of c is uniform and independent of b.

On the other hand: $GAME(\lambda,b) \approx_c HYB(\lambda,b)$ $\forall\ b \in \{0,1\}$. By reduction: assume $\exists$ PPT A s.t.

$$\left| Pr[GAME(\lambda,b)=1] - Pr[HYB(\lambda,b)=1] \right|$$

for some $p(\lambda) = poly(\lambda)$ $\geq 1/p(\lambda)$

Then, build PPT A_{prg} against G:



By assumption:

$$\Pr[b' = 1 : z \leftarrow G(U_\lambda)] =$$

$$= \Pr[b' = 1 : G_{\lambda}^{\pi_0}(\lambda, b)]$$

$$\Pr[b' = 1 : z \leftarrow U_{\lambda+\ell}]$$

$$= \Pr[b' = 1 : H^{\pi_0}(\lambda, b)]$$

$$\Rightarrow \left| \Pr[b' = 1 : z \leftarrow G(U_\lambda)] - \Pr[b' = 1 : z \leftarrow U_{\lambda+\ell}] \right| \geq 1/p(\lambda)$$

$$\Rightarrow \quad \mathrm{GARS}(\lambda, 0) \simeq_c \mathrm{HYB}(\lambda, 0)$$

$$\equiv \mathrm{HYB}(\lambda, 1)$$

$$\simeq_c \mathrm{GARS}(\lambda, 1)$$

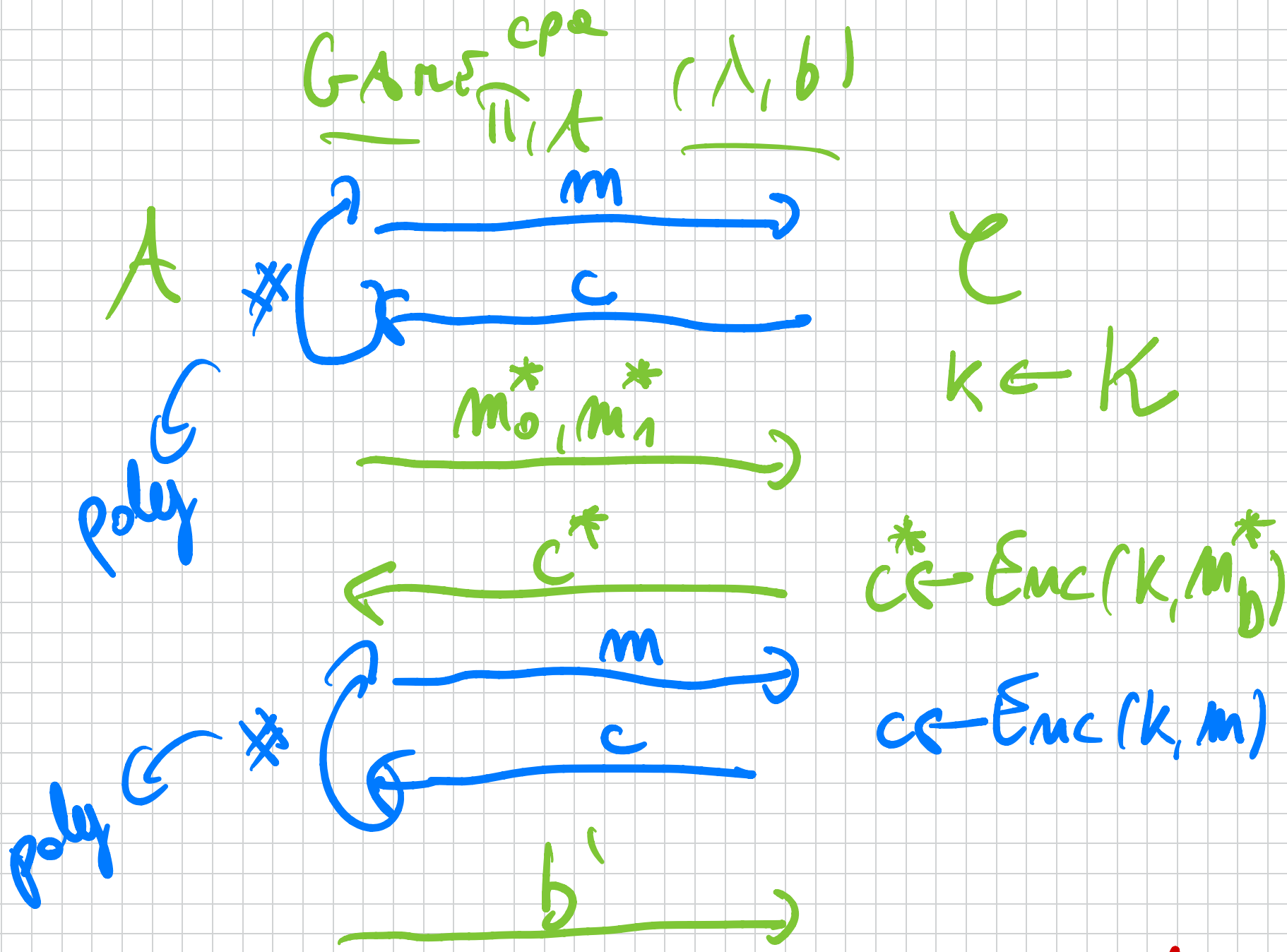
$$\Rightarrow \mathrm{GARS}(\lambda, 0) \simeq_c \mathrm{GARS}(\lambda, 1) \quad \square$$

Our next goal : Chosen-plaintext attack (CPA) security.

Def Let $\Pi = (Enc, Dec)$ be a SKE.

We say Π is CPA-secure if :

$$G^{cpa}_{\Pi,A}(\lambda, 0) \overset{c}{\approx} G^{cpa}_{\Pi,A}(\lambda, 1)$$



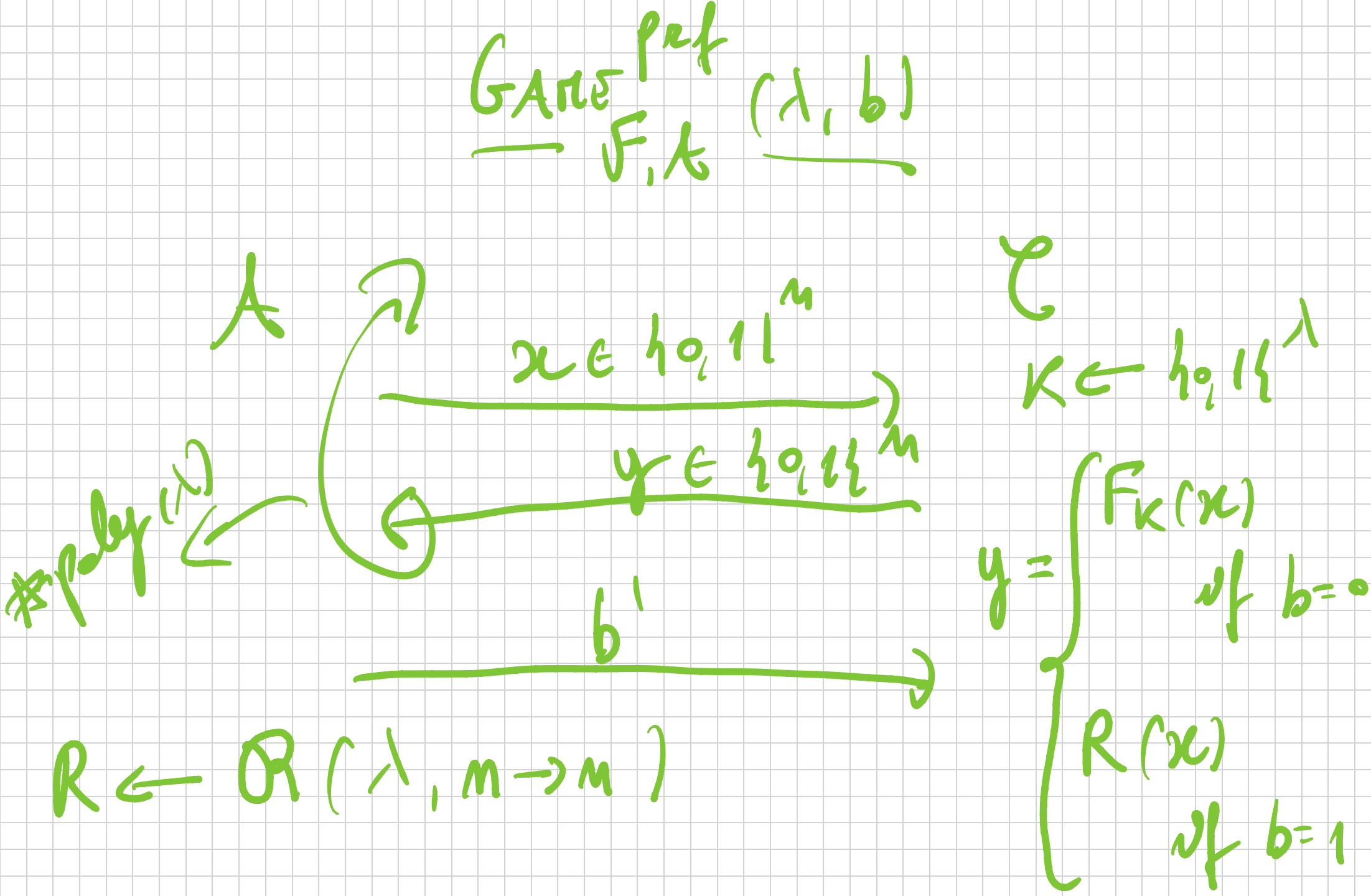
Observe: No DETERMINISTIC SKE can achieve this!

Sanity check: previous scheme is NOT CPA-secure!

We need a new tool: PSEUDORANDOM FUNCTION. Let's start with the definition.

Def A family $F = \{f_k : \{0,1\}^n \to \{0,1\}^m\}$ (with $k \in \{0,1\}^\lambda$) is a PRF if:

$$\text{GAME}^{\text{prf}}_{F,A}(\lambda, 0) \overset{c}{\approx} \text{GAME}^{\text{prf}}_{F,A}(\lambda, 1).$$



Note: R is not efficiently computable as it takes exponential space to store it. $F(k, x)$ instead is efficiently computable for all k, x.

Plan:

- Build a PRF.
- Use it to get CPA secure SKE and more!

How to build a PRF:

- Practice: Many examples like DES, AES, ... (Actually, those are not just PRFs, they are PRPs — namely, they are invertible given K.)
- Theory: OWFs ⇒ PRGs ⇒ PRFs ⇒ PRPs.

We will cover one construction of PRFs:
The GGM Tree. Basically, it is a proof
that PRGs $\Rightarrow$ PRFs. Here it is:
Let $G: \{0,1\}^n \to \{0,1\}^{2n}$ s.t.

$$G(x) = (\underbrace{G_0(x)}_{n \text{ bits}}, \underbrace{G_1(x)}_{n \text{ bits}})$$

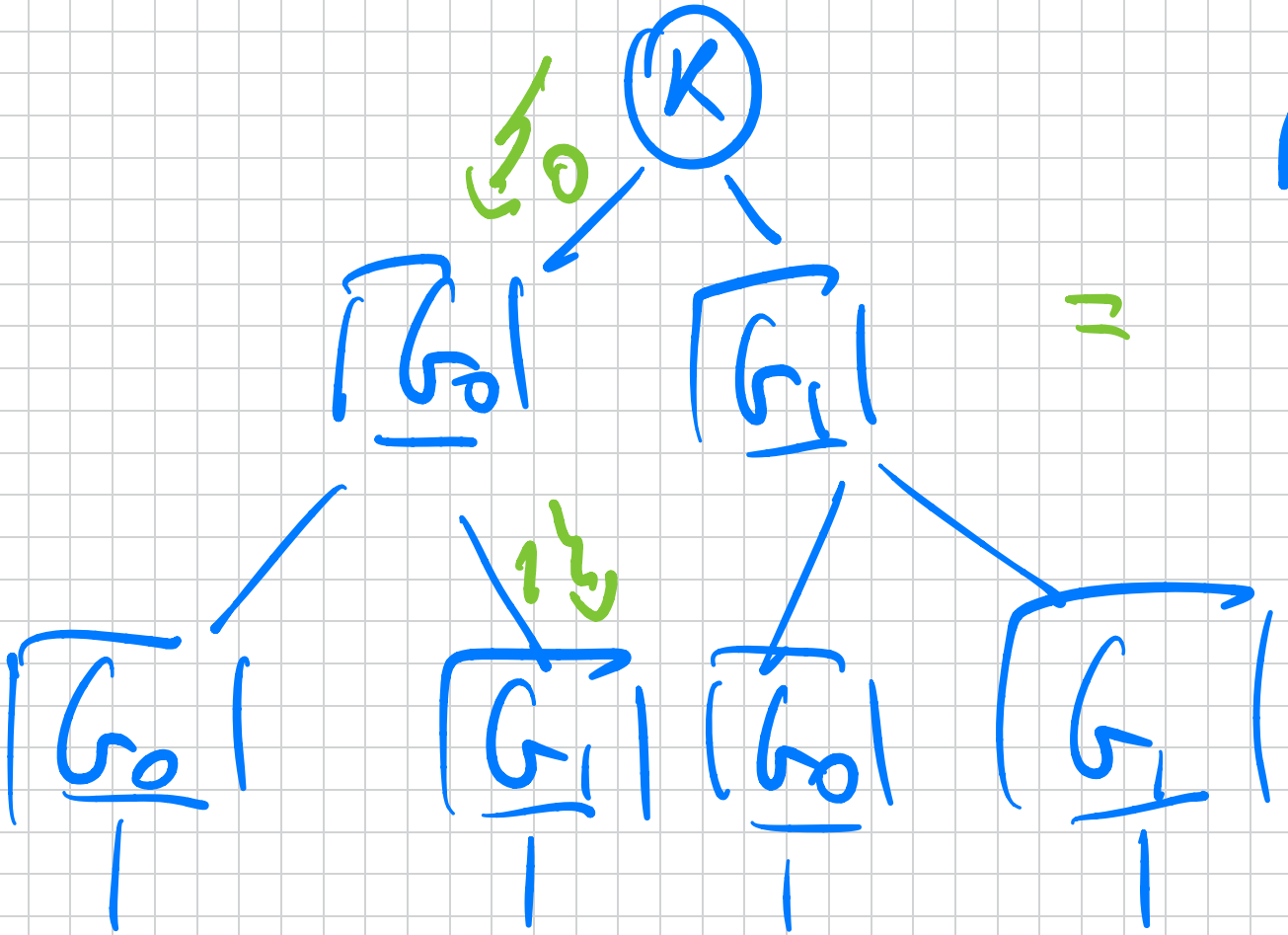
We can

Think of G as $F(K, x)$ for $x \in \{0,1\}$

x	y
0	$G_0(K)$
1	$G_1(K)$

$\approx_c$

x	y
0	\$
1	\$



$$F(K, 01) = G_1(G_0(K))$$

$$y = F_K(01)$$

In general:

$$F_K(x) = G_{x_m}(G_{x_{m-1}}(\cdots G_{x_2}(G_{x_1}(K))\cdots))$$

Thm If G is a PRG then above $F = \{f_k\}$ is a PRF.

For the proof we will need two lemmas.

Lemma If $G: \{0,1\}^n \to \{0,1\}^{2n}$ is a PRG, then for any $t(\lambda) = poly(\lambda)$:

$$(G(k_1), \ldots G(k_t)) \stackrel{c}{\approx} (U_{2n}, \ldots, U_{2n})$$

$$k_1, \ldots k_t \leftarrow U_n$$

Next, given $F_k' : \{0,1\}^{n-1} \to \{0,1\}^n$ be a PRF. Then, define

$$F_k(x,y) = G_x(F_k'(y))$$

$$x \in \{0,1\}, \quad y \in \{0,1\}^{n-1}$$

LEMMA If $\{F_k'\}$ is a PRF, then $\{F_k\}$ is also a PRF.