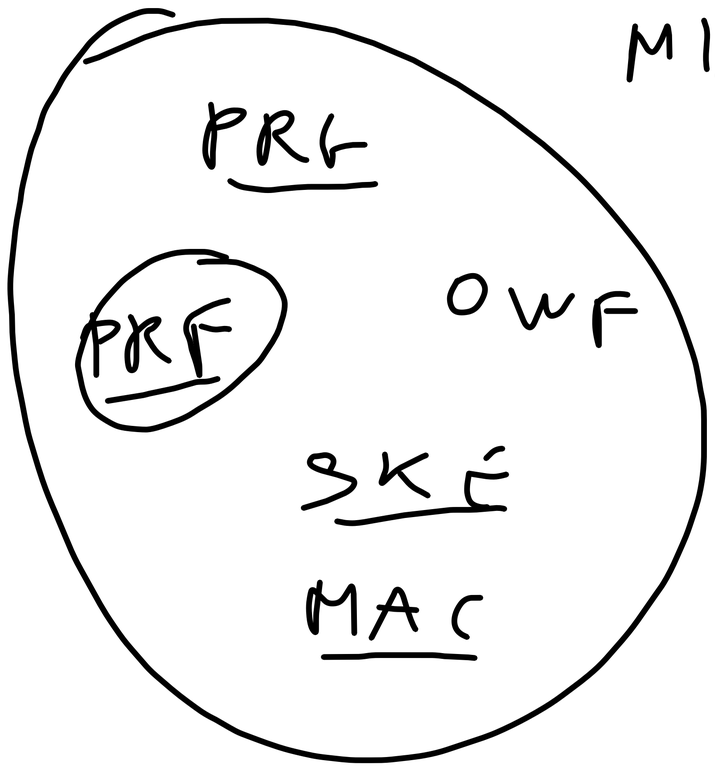
MINICRYPT

The world in which OWFs exist.



MINICRYPT

THEORY

PRACTICE

AES

(PRF)

$G(s) = ?$

Plan:

1) PRG $\Rightarrow$ SKE

2) OWF $\Rightarrow$ PRG

First thing: What's secure encryption?

1) No PPT A can compute k!

$Enc(k, m) = m$ (w.p. $\geq negl(\lambda)$.)

2) No PPT A can compute m

(w.p. $\geq 1/poly(\lambda)$)

Still, A could learn $m[1] \leftarrow$ first bit of m

3) A (PPT) learns nothing about m

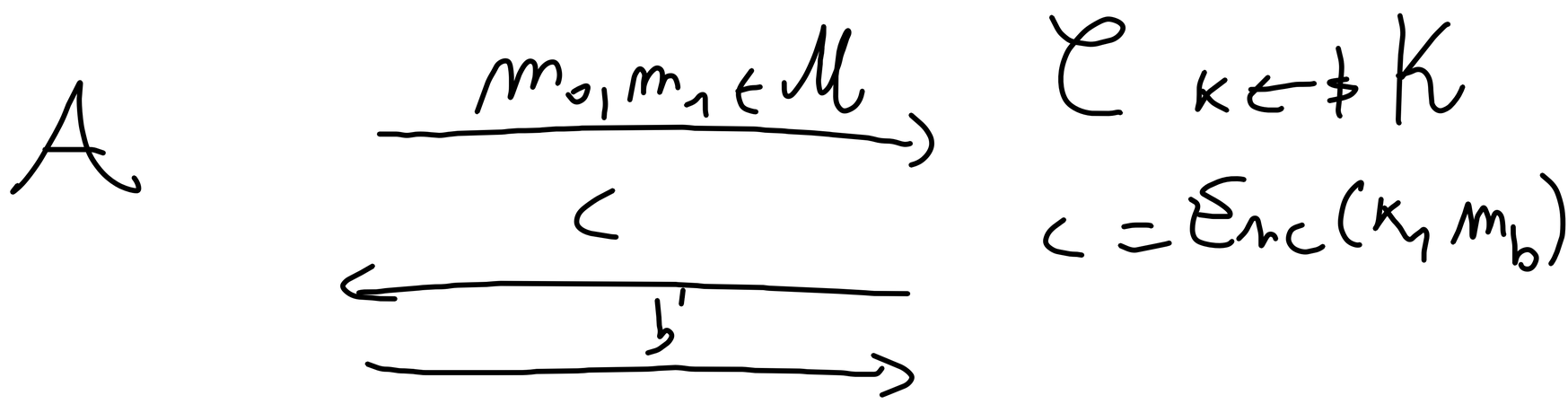
(besides what's known about m)

(3) can be done, but results in complex def. GOLDWASSER + MICALI give simpler equivalent definition.

DEF (ONE-TIME SEC. SKE). $\Pi = (Enc, Dec)$ is ONE-TIME COMP. SECURE if:

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

GAME (λ, b):



DEF $\Rightarrow$ (1). Assume not; $\exists$ PPT A' that given c outputs k. Then construct PPT A:

- Pick any m_0, m_1
- Receive c; run A' on c get k.
- Let $m = Dec(k, c)$
- Output $b' = \tilde{b}$ iff $m = m_{\tilde{b}}$

$\Pr[b' = 1 \mid b = 0$ in the game$] = 0$

$\Pr[b' = 1 \mid b = 1$ " " " $] = 1$

Construction: Let $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$ be a PRG. Consider $\Pi = (Enc, Dec)$:

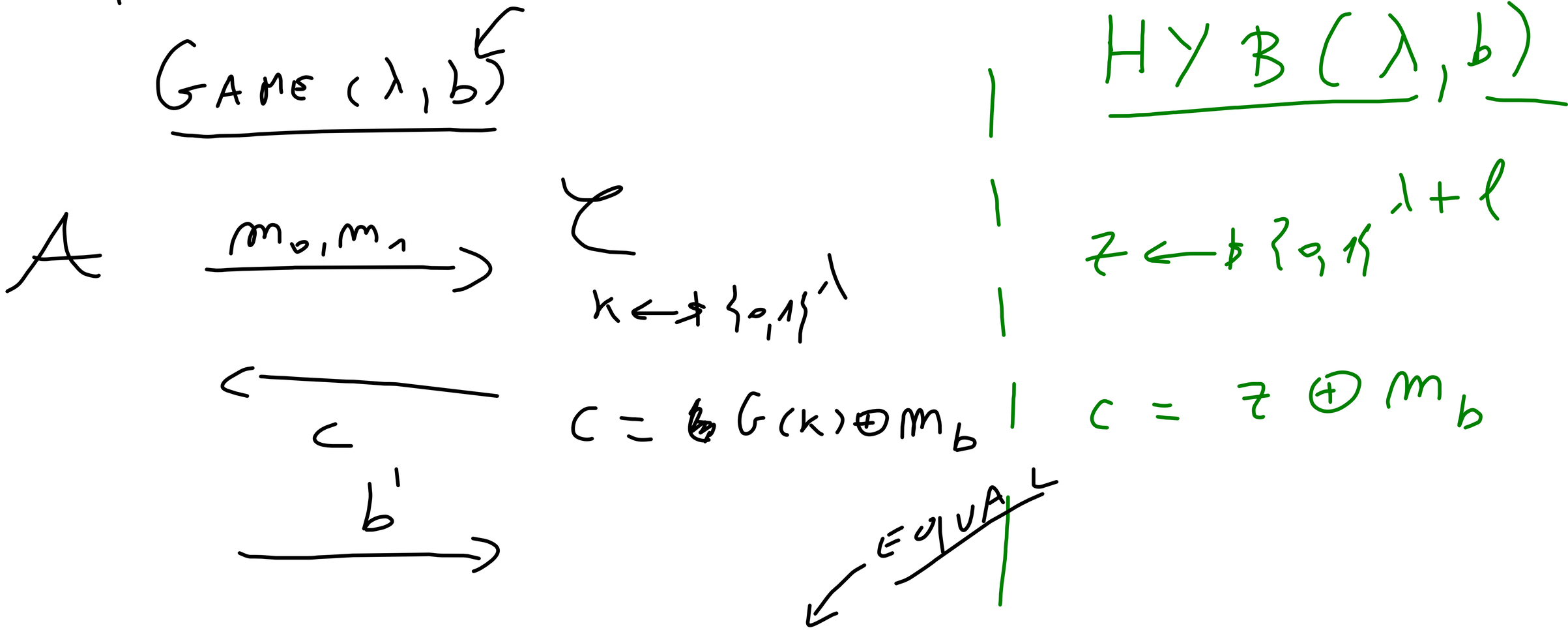
- $Enc(k, m) = G(k) \oplus m$

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

Note $|k| = \lambda$; $|m| = \ell + \lambda$ $(\ell > 0)$

T+M. If G is a PRG, Π is ONE-TIME COMP. SECURE.

Proof. Start with:



LEMMA. $HYB(\lambda, 0) \equiv HYB(\lambda, 1)$.

Proof. By PERFECT SECRECY c is uniform. of m_{enc} thus of b. ☒

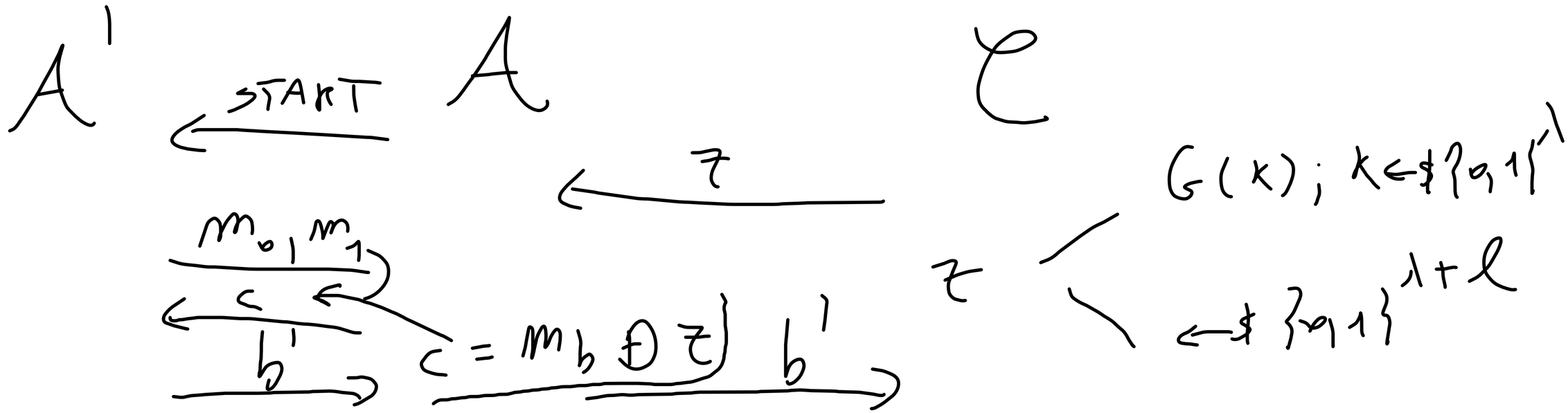
LEMMA - $\text{GAME}(\lambda, b) \approx_c \text{HYB}(\lambda, b)$

Fix $b \in \{0,1\}$. $\forall\, b = 0, 1$.

Proof. Let A' be PPT s.t.

$$\left| \Pr[\text{GAME}_{A'}(\lambda, b) = 1] - \Pr[\text{HYB}_{A'}(\lambda, b) = 1] \right| \geq \frac{1}{\text{poly}(\lambda)}$$

Consider reduction A against G:



$$\Pr[b'=1 : z = G(k),\ k \leftarrow\$ \{0,1\}^\lambda] = \Pr[\text{GAME}^{prg}(\lambda,0)=1]$$

$$= \Pr[b'=1 : c = G(x) \oplus m_b,\ k \leftarrow\$ \{0,1\}^\lambda] = \Pr[\text{GAME}(\lambda,b)=1]$$

$$\Pr[b'=1 : z \leftarrow\$ \{0,1\}^{\lambda+\ell}] = \Pr[\text{GAME}^{prg}(\lambda,1)=1]$$

$$= \Pr[b'=1 : c = z \oplus m_b,\ z \leftarrow\$ \{0,1\}^{\lambda+\ell}] = \Pr[\text{HYB}(\lambda,b)=1]$$

$$\Rightarrow \left| \Pr[\text{GAME}^{prg}(\lambda,0)=1] - \Pr[\text{GAME}^{prg}(\lambda,1)=1] \right| \geq 1/poly \quad \lightning$$

$$\Rightarrow \text{GAME}(\lambda,0) \approx_c \text{HYB}(\lambda,0) \equiv \text{HYB}(\lambda,1) \approx_c \text{GAME}(\lambda,1)$$