OPIS : JR3PE3ZJ

EXERCISES

*) We have seen that every PRF is a VMAC. UF-CMA

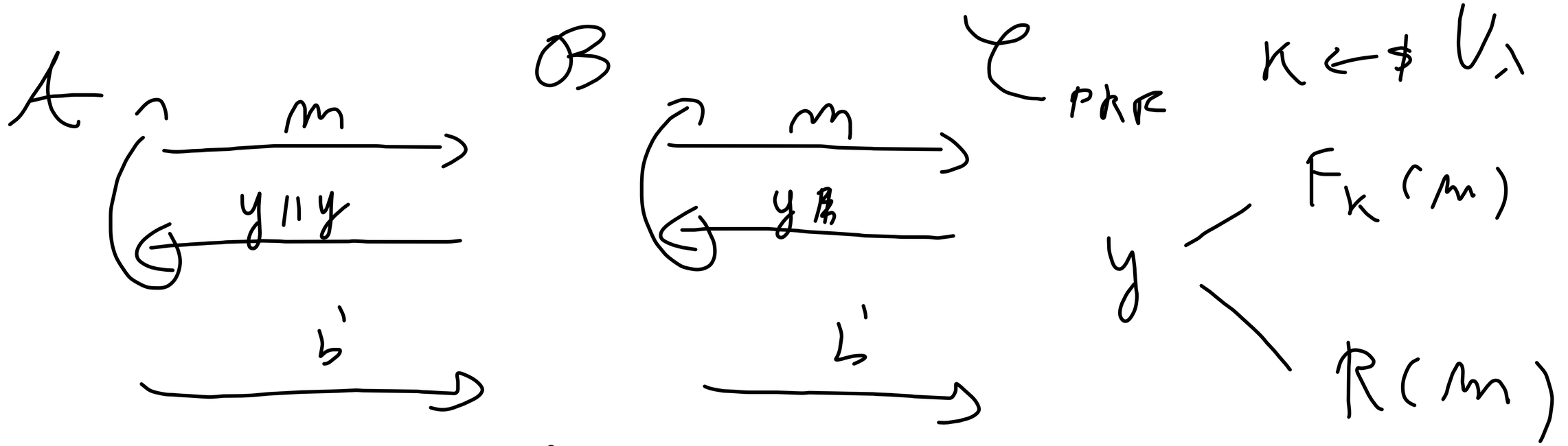
Show the converse is NOT true.

E.g., $Tag(k, m) = F_k(m) \| F_k(m)$

PRF $\Rightarrow$ UF-CMA but Tag not a PRF.

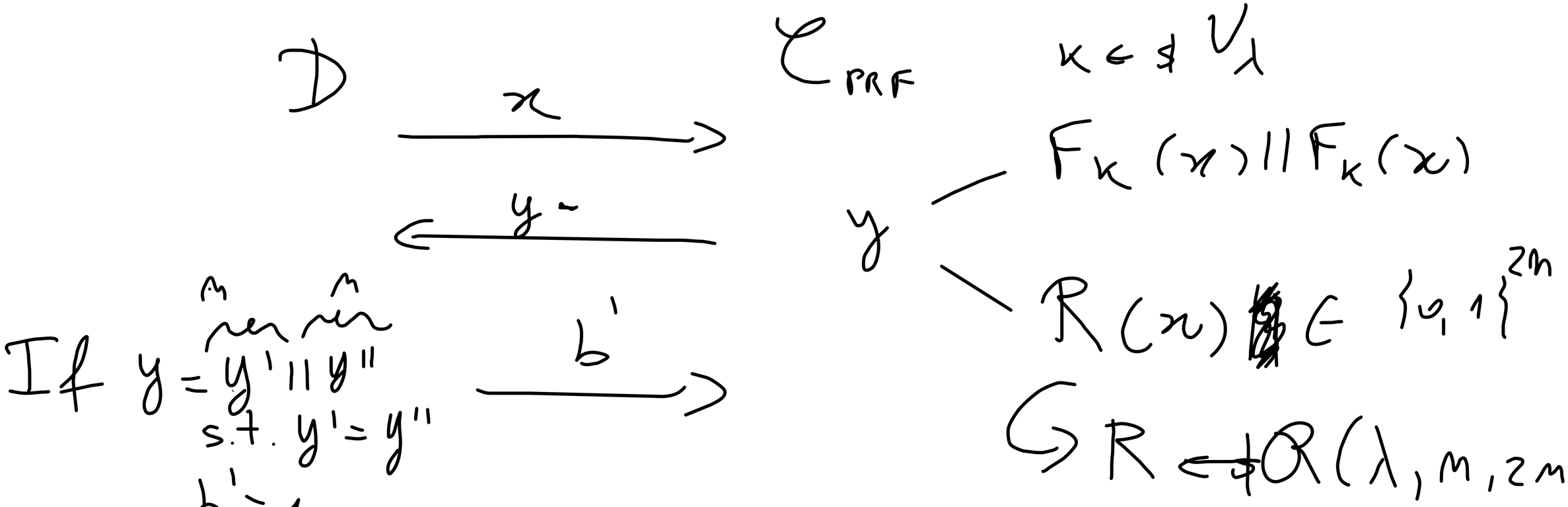
PRF $\Rightarrow$ UF-CMA. Do Hybrid s.t. F_k replaced with $R \leftarrow\$ \mathcal{R}(\lambda, n, m)$.

$G^{ufcma}(\lambda) \approx_c H(\lambda)$.



$Pr[H(\lambda)=1] \leq negl(\lambda)$ because NO ADV can guess $R(m^*)$ w.p. better than 2^{-n}.

Toy not a PRF. Here is my PPT $\mathcal{D}$:



*) We are given Tag_1, Tag_2 s.t. one of them is UF-CMA but we don't know which.

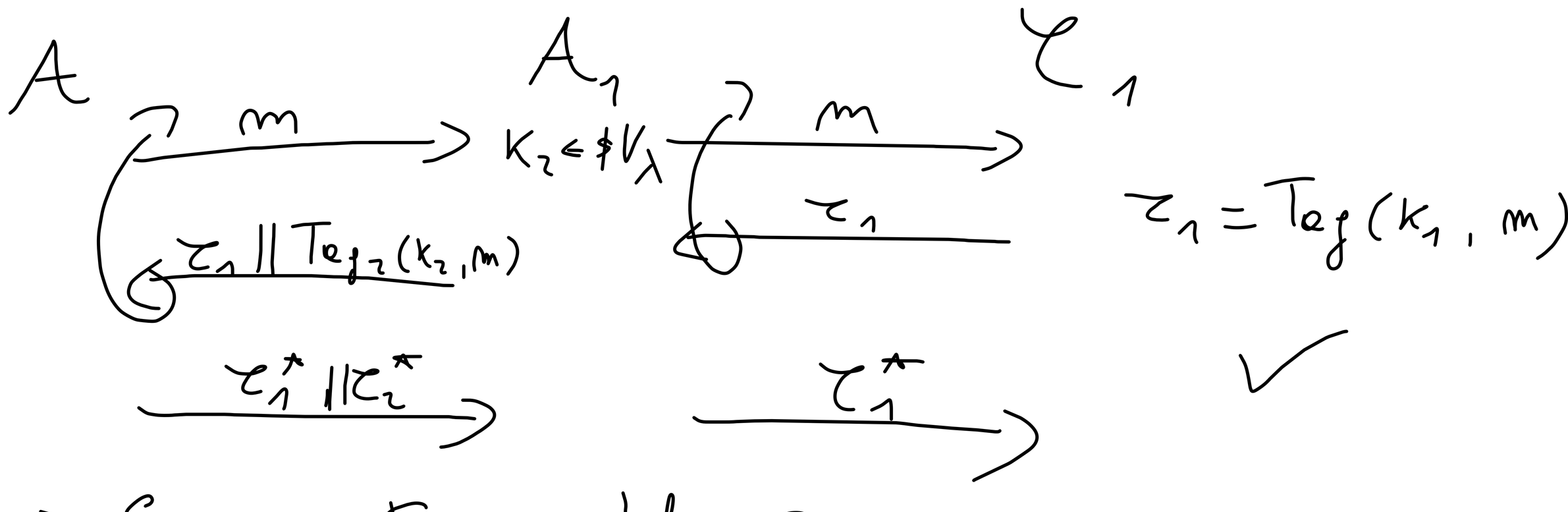
Build a UF-CMA Tag using Tag_1, Tag_2.

$$Tag_{K_1,K_2}(m) = Tag_2(K_2, Tag_1(K_1, m))$$

It works, but restricted to domain of Tag_2 = Range of Tag_1

$$Tag_{K_1,K_2}(m) = Tag_1(K_1, m) \,||\, Tag_2(K_2, m)$$

Assume Teg_1 vs UFCMA (the other case vs SAME)



*) Some question with PRFs G_1, G_2.

$G_2, G_1 : \{0,1\}^λ \to \{0,1\}^{λ+ℓ}$

$$G(s) = G_1(s_1) \oplus G_2(s_2)$$

$$s = \underbrace{s_1}_{*\lambda} \| \underbrace{s_2}_{\lambda} \cdot \qquad G : \{0,1\}^{2\lambda} \to \{0,1\}^{\lambda+\ell}$$

*) $F_k(x) = \underbrace{G'(k)}_{\ell} \oplus x \in \{0,1\}^{\lambda}$ $\qquad \ell > \lambda$

$G : \{0,1\}^{\lambda} \to \{0,1\}^{\lambda+\ell}$ $\qquad G'(s) = G(s)|_{\lambda}$

$\hookrightarrow$ PRG. $\qquad x_1 \to y_1$ $\qquad \hookrightarrow$ TRUNCATES

$x_2 \to y_2$ $\qquad$ to λ.

$y_1 \oplus y_2 = x_1 \oplus x_2$

Is $F_k \in PRF$?

*) $F_k(\cdot)$ a PRF.

$F'_k(x) = \overline{F_x(k)}$. Is it a PRF?

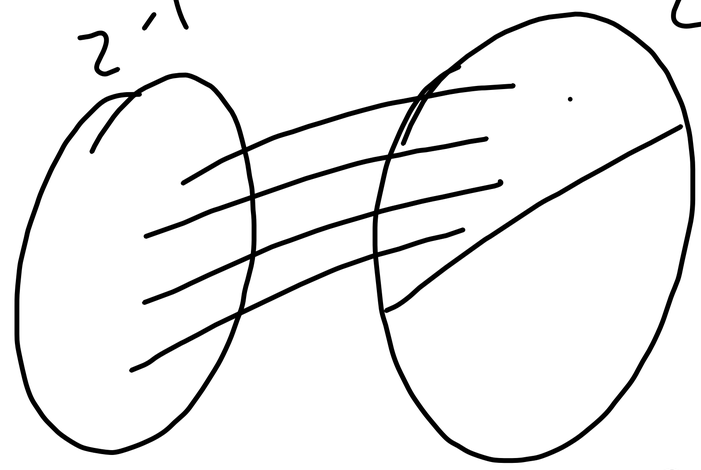
Observation: $F_k(\cdot)$ could be insecure for a BAD key, but still a PRF

E.g. $F''_k(x)$ is a PRF

$$F_k(x) = \begin{cases} 0^\lambda & \text{if } k = 0^\lambda \\ F'_k(x) & \text{otherwise} \end{cases}$$

*) Show that NO PRG/PRF can be secure against UNBOUNDED ADV.

PRG: $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$



EXP TIME

A ⟵ z ⟵ C

Try to find s s.t. $z = G(s)$

If yes $b'=1$

Else $b'=0$

$z \leftarrow G(s)$ ⟶ b' ⟶ $\Pr_s[b'=1 : z=G(s)] = 1$

$\Pr_z[b'=1 : z \leftarrow \$ V_{2\lambda}] = 2^{-\lambda}$

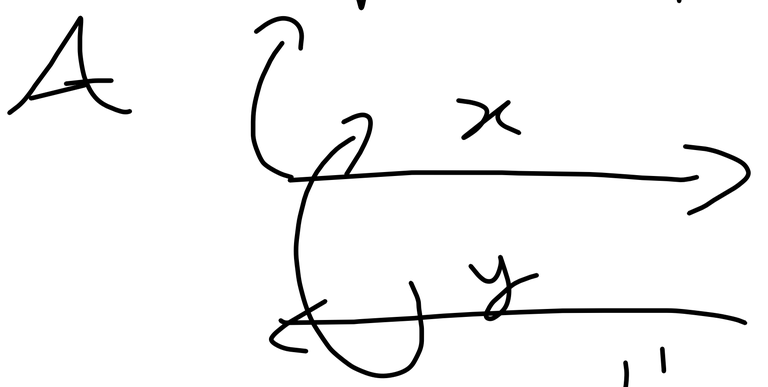
$z \leftarrow V_{2\lambda}$

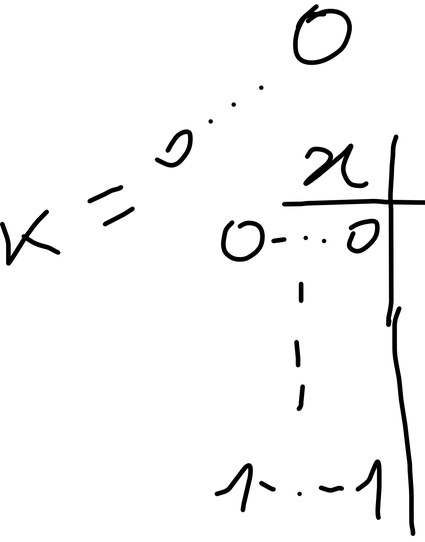
$\frac{2^\lambda}{2^{2\lambda}} = \frac{1}{2^\lambda}$

$2^\lambda - 1$

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

$\forall x \in \{0,1\}^n$



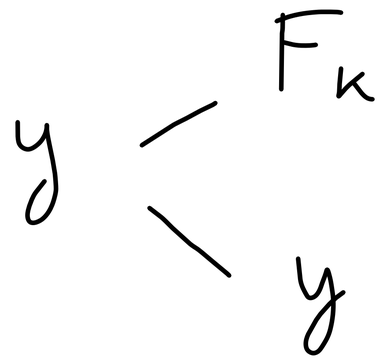


$k = 0^{\cdots}$

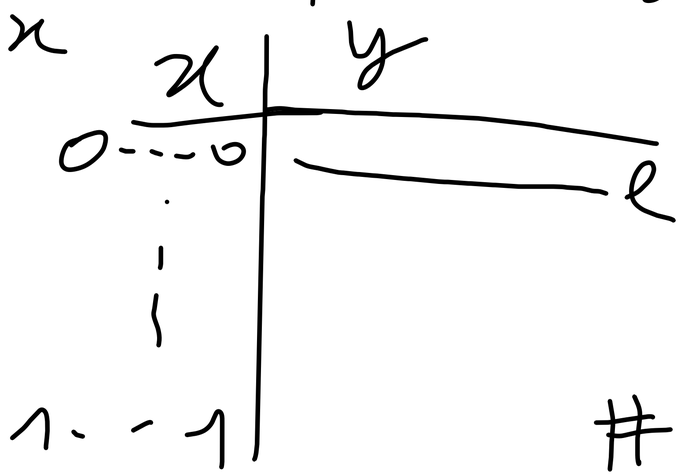
If $\exists k$ s.t. $F_k(x) = y \quad \forall x$

$b' = 1$

Else $b' = 0$



tables $F_k(x) = y = 2^{\lambda}$



$(2^n \cdot \ell)$

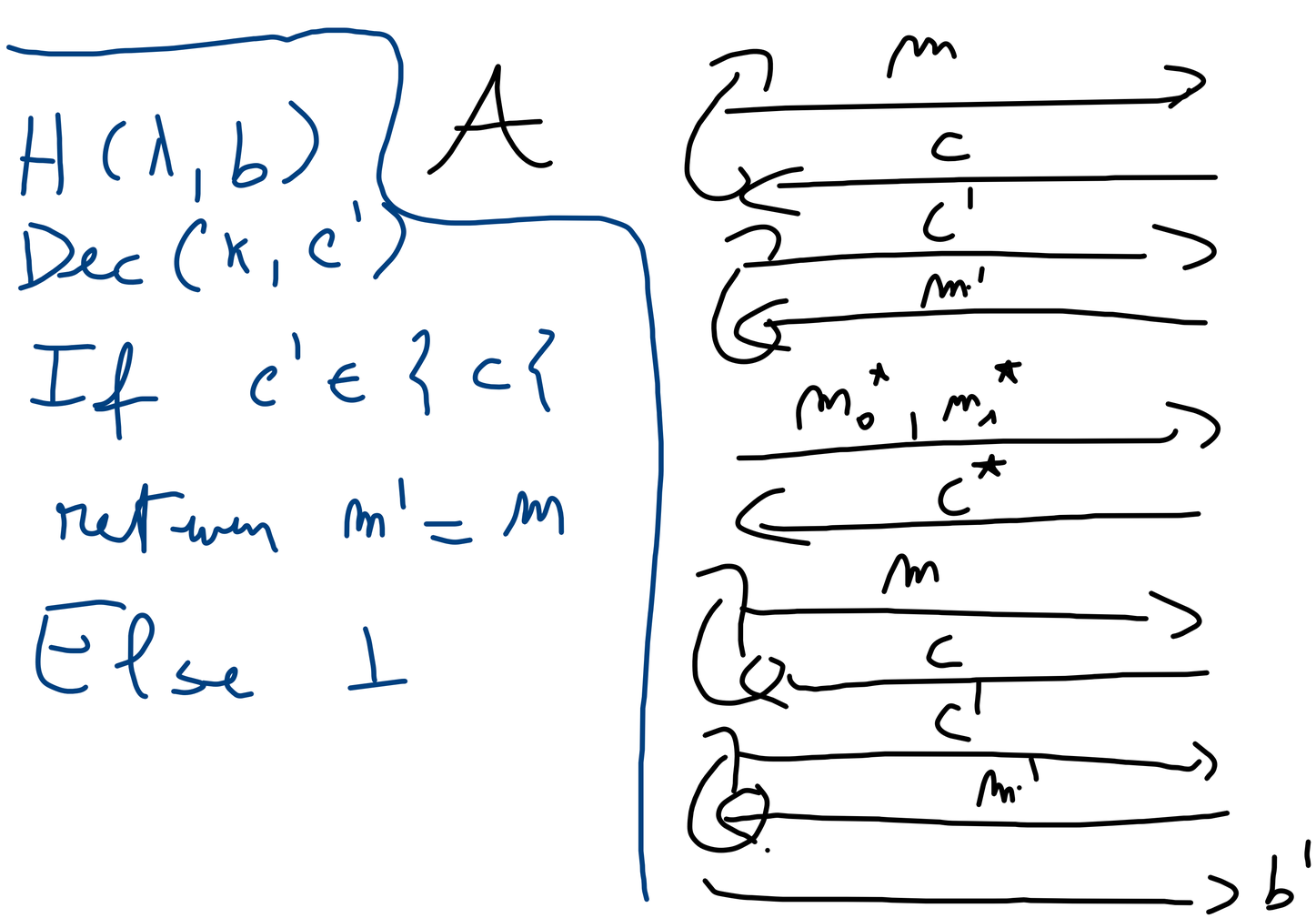
2

# of R(·) tables

*) Let Π be on $S \times \mathcal{E}$.

CPA + AUTH $\Rightarrow$ CCA.

Proof. Start with $G(\lambda, b) \equiv G_{AME}^{cca}(\lambda, b)$



LEMMA. $G(\lambda, b) \approx_c H(\lambda, b) \quad \forall\, b.$

A $\quad A_{AUTH}$ $\quad \mathcal{C}_{AUTH}$.

$\hookrightarrow$ Assume A can find $c' \notin \{c\}$ (FRESH)

s.t. $Dec(k, c') \neq \perp$.

LEMMA $H(\lambda, 0) \approx_c H(\lambda, 1)$

A_{CCA} $\quad A_{CPA}$ $\quad \mathcal{C}_{CPA}$

⋮