CCA SECURITY

Recap: We know CPA security can be achieved from OWF (for FIL, VIL). assuming SHARED Key.

Two missing things:

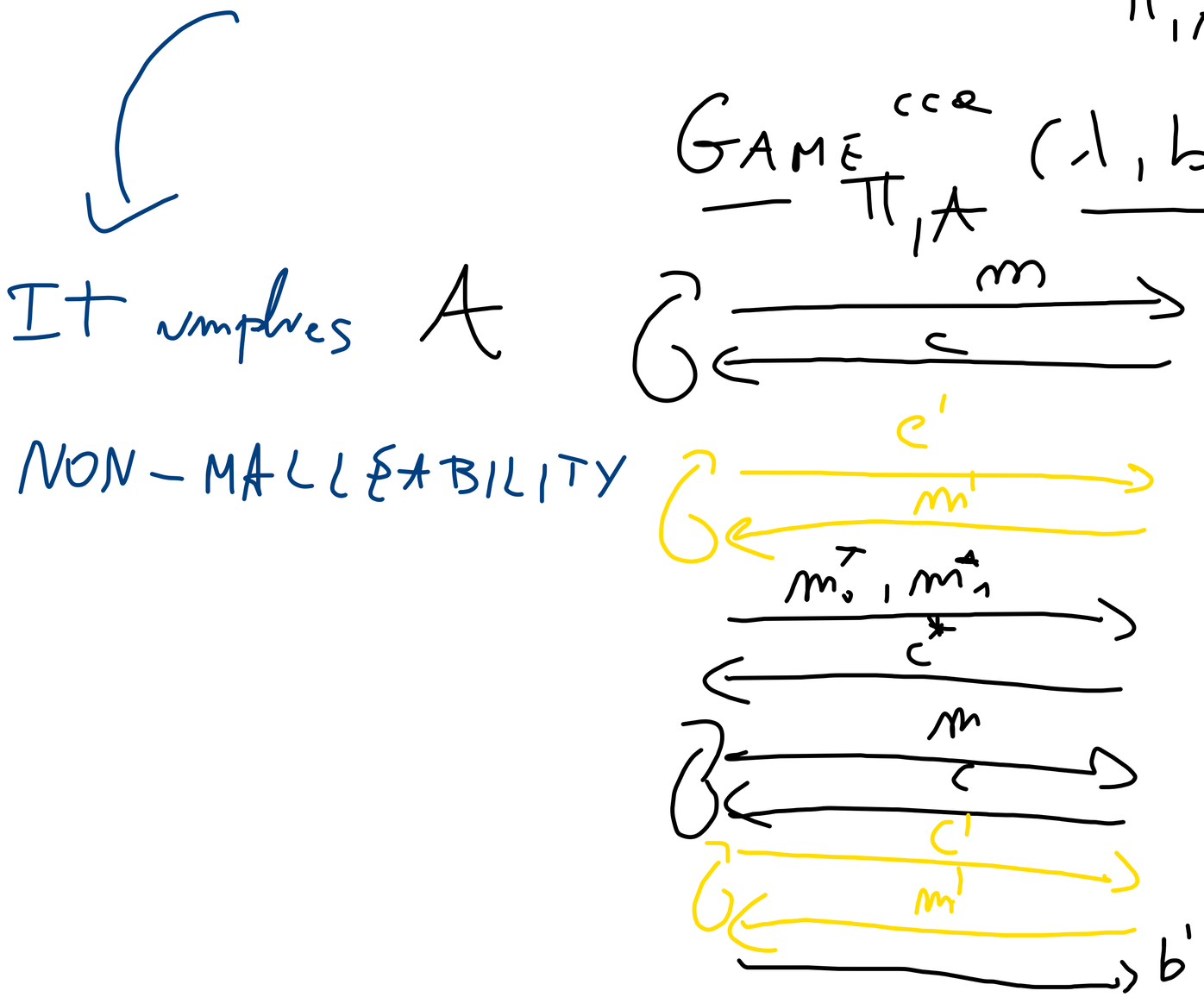
1) Do both at the same time. ✓

2) Real-world block ciphers (DES, AES, ...).

DEF (CCA) $\Pi = (Enc, Dec)$ ns

CCA-secure if $GAME^{cca}_{\Pi,A}(\lambda,0) \approx_c GAME^{cca}_{\Pi,k}(\lambda,1)$

$GAME^{cca}_{\Pi,A}(\lambda,b)$:



$c \leftarrow\$ Enc(k, m)$

$c^* \leftarrow\$ Enc(k, m_b)$

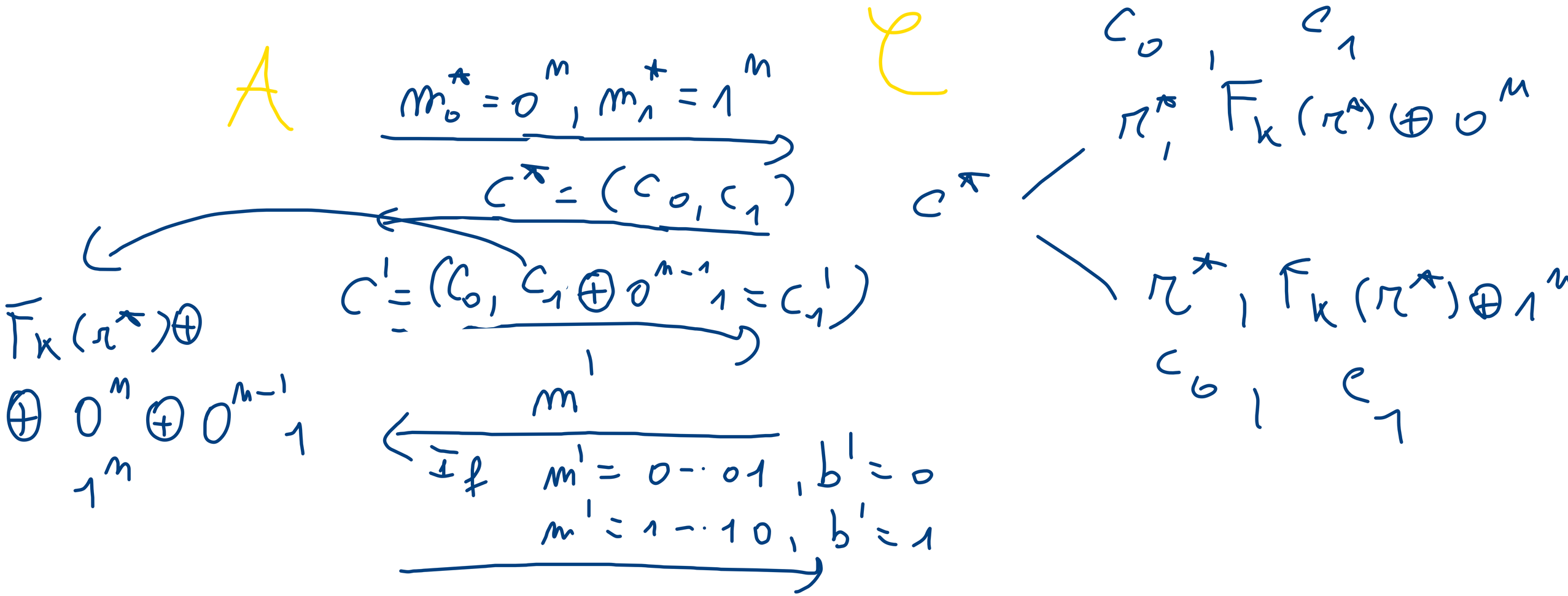
$m' = Dec(k, c')$

$(c' \neq c^*)$

Ex. $C = (K, F_k(r) \oplus m)$ NOT CCA

(Same for CBC, OFB, CFB, CTR).

Here is my adversary:

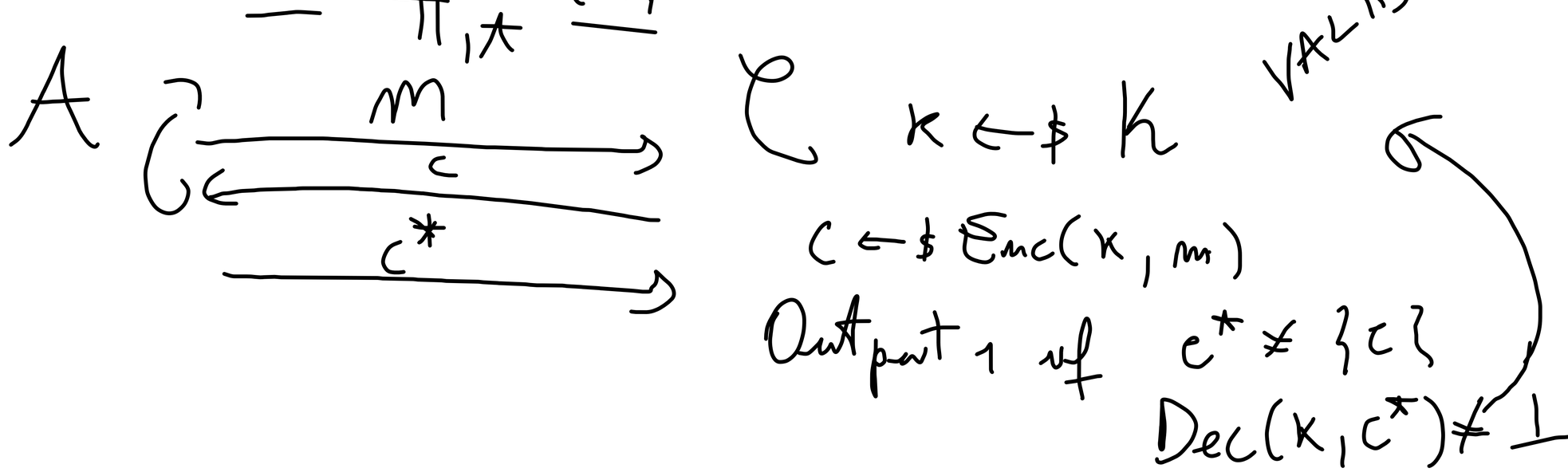


Simple recipe to get CCA:

- CPA + AUTH ← authenticity

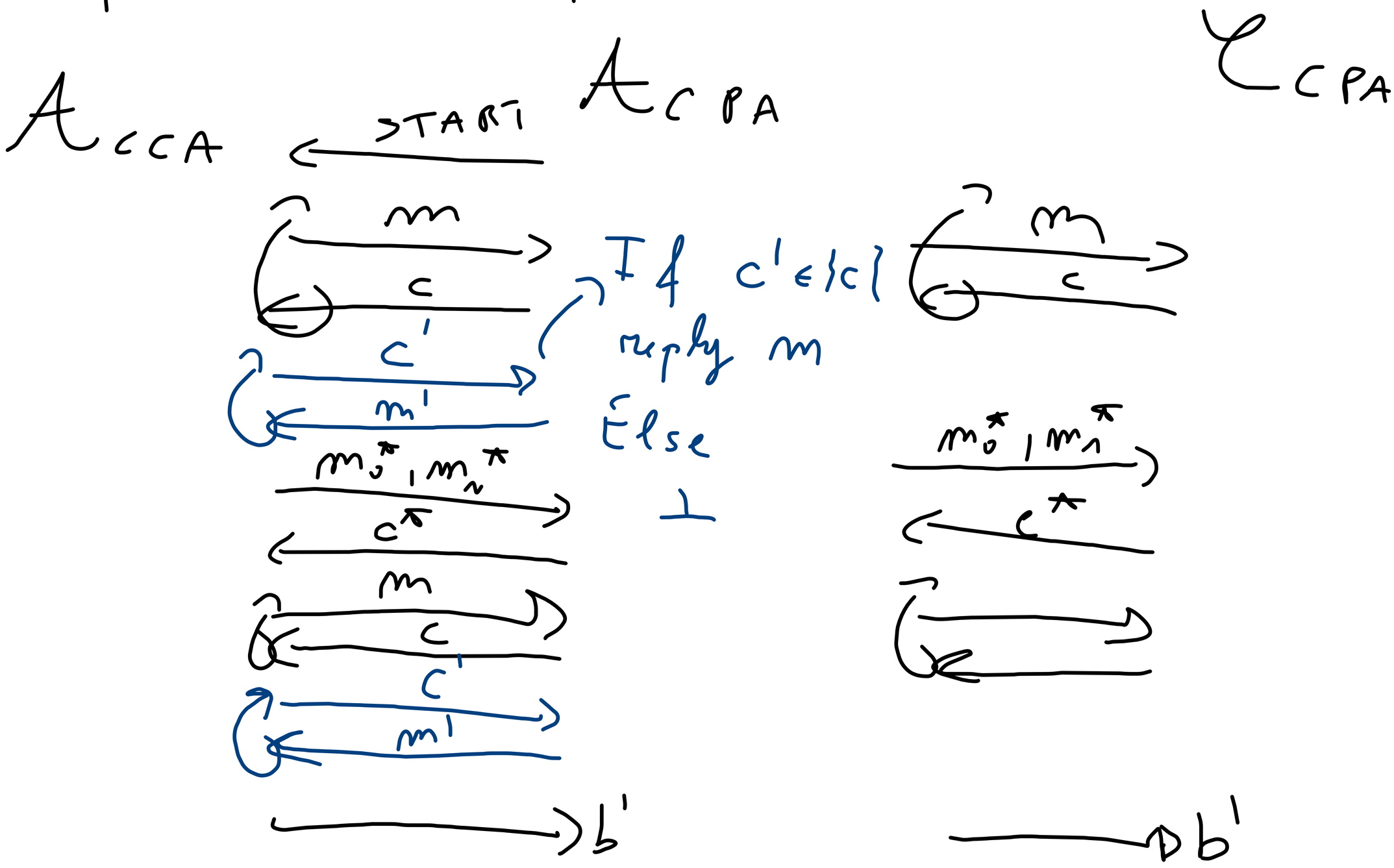
DEF (AUTH) $\Pi = (Enc, Dec)$ satisfies AUTH if $\forall$ PPT A: $Pr[GAME^{auth}_{\Pi,A}(\lambda)=1] \leq negl(\lambda)$.

$GAME^{auth}_{\Pi,A}(\lambda)$



THM CPA + AUTH $\Rightarrow$ CCA.

Proof. Sketch of reduction:



Q: How to get CPA + AUTH?

Combine encryption with message auth?

1) $C \leftarrow\$ Enc(k_1, m)$

$\tau = Tag(k_2, m)$. $c' = (C, \tau)$ ENC-AND-AUTH

Never do it! Not secure for very

Combination of CPA Enc + UFCMA Tag.

Intuition: Tag could leak info about msg!

$\overline{Tag}(x, m) = m[0] \,||\, Tag(k, m) = \overline{\tau}$

↳ UFCMA

2) $\tau = Tag(k_2, m)$

AUTH-THEN-ENC

$C \leftarrow\$ Enc(k_1, m \| \tau)$

Not good. There is BAD combination
that does NOT work.

TLS uses it (that combination is SECURE).

3) $\begin{cases} C \leftarrow\$ Enc(k_1, m) ; \tau = Tag(k_2, C) \\ Enc'(k', m) \quad C' = (C, \tau). \quad k' = (k_1, k_2) \end{cases}$

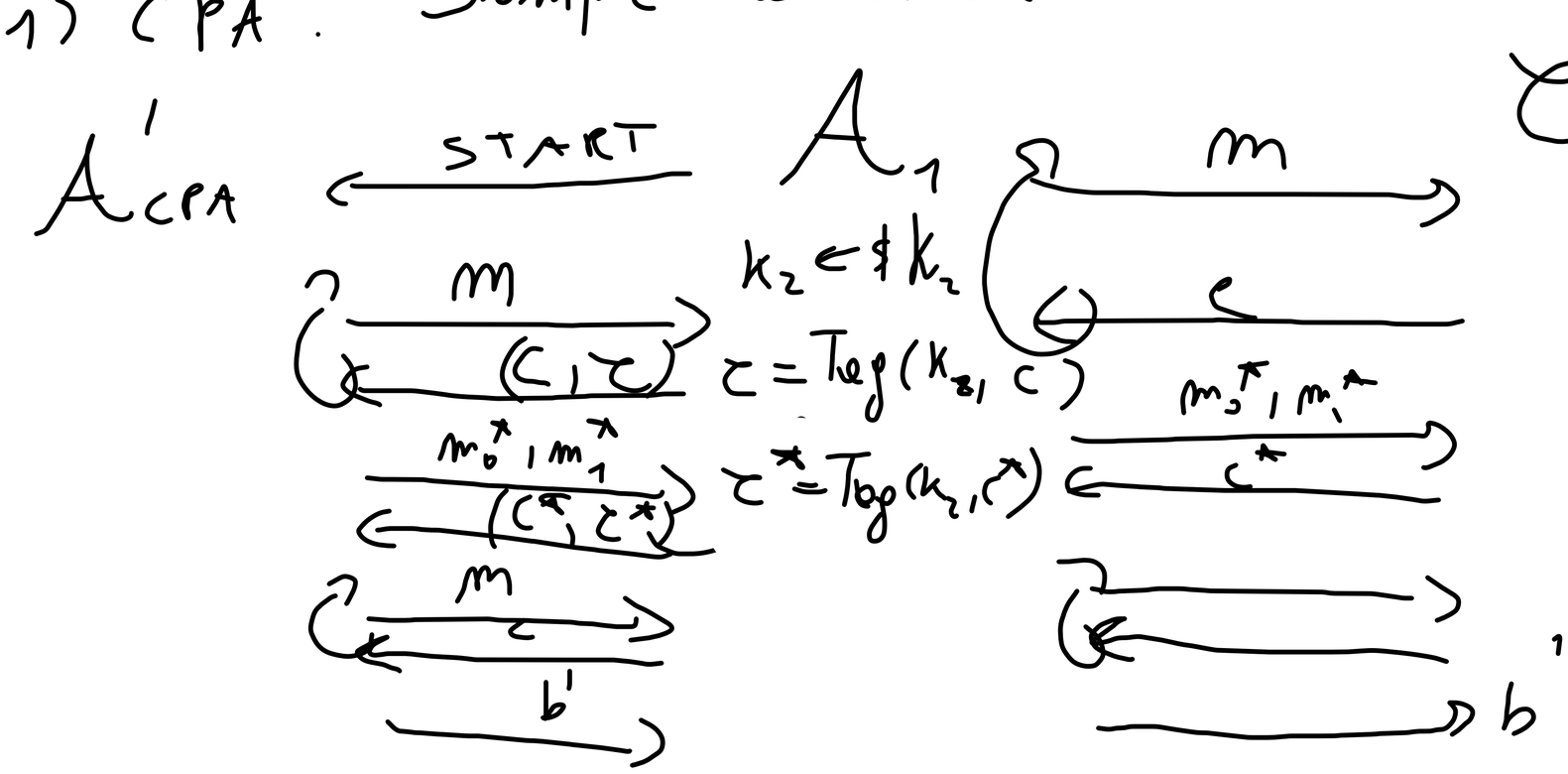
ENC-THEN-AUTH

$Dec'(k', (C, \tau))$: If $\tau \neq Tag(k_2, C)$ output $\perp$
Else output $Dec(k_1, C)$.

THM. If $\Pi_1 = (Enc, Dec)$ is CPA secure and $\Pi_2 = (Tag)$ is UFCMA (one-time tags!) then $\Pi' = $ ENC-THEN-AUTH is CCA secure.

Proof. By previous THM we must prove CPA + AUTH.

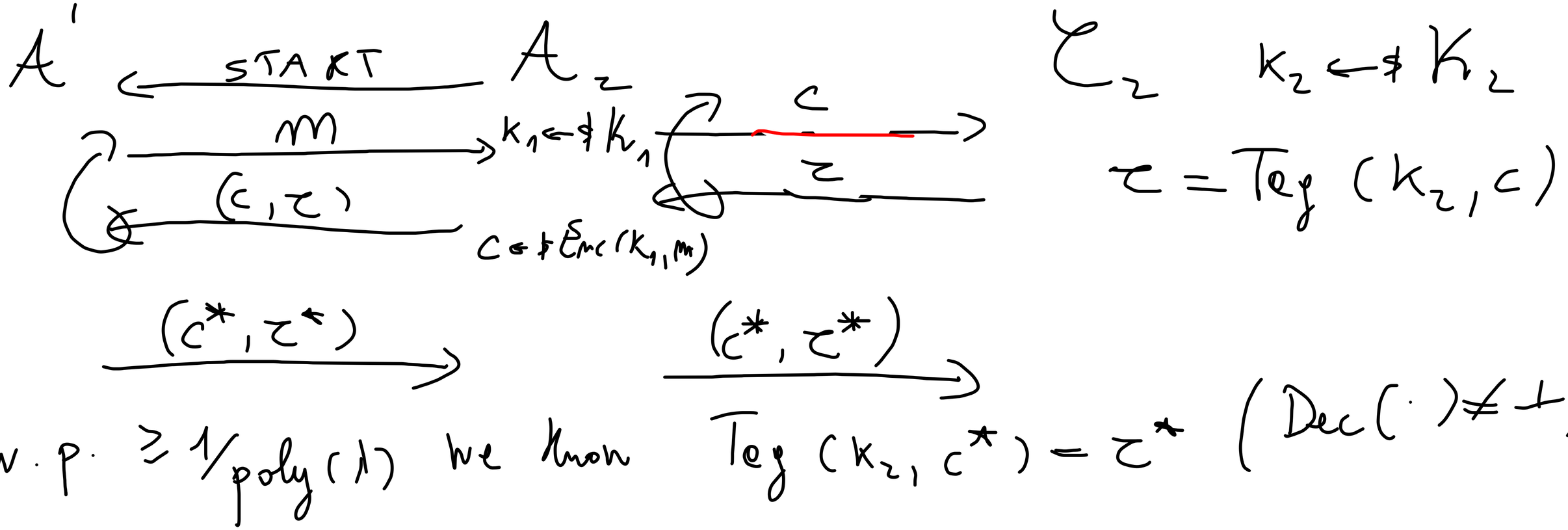
1) CPA. Simple reduction:



2) AUTH. Assume not $\Rightarrow \exists$ PPT A' such that

$$\Pr\left[\text{GAME}^{\text{auth}}_{\Pi', A'}(\lambda) = 1 \right] \geq 1/\text{poly}(\lambda).$$

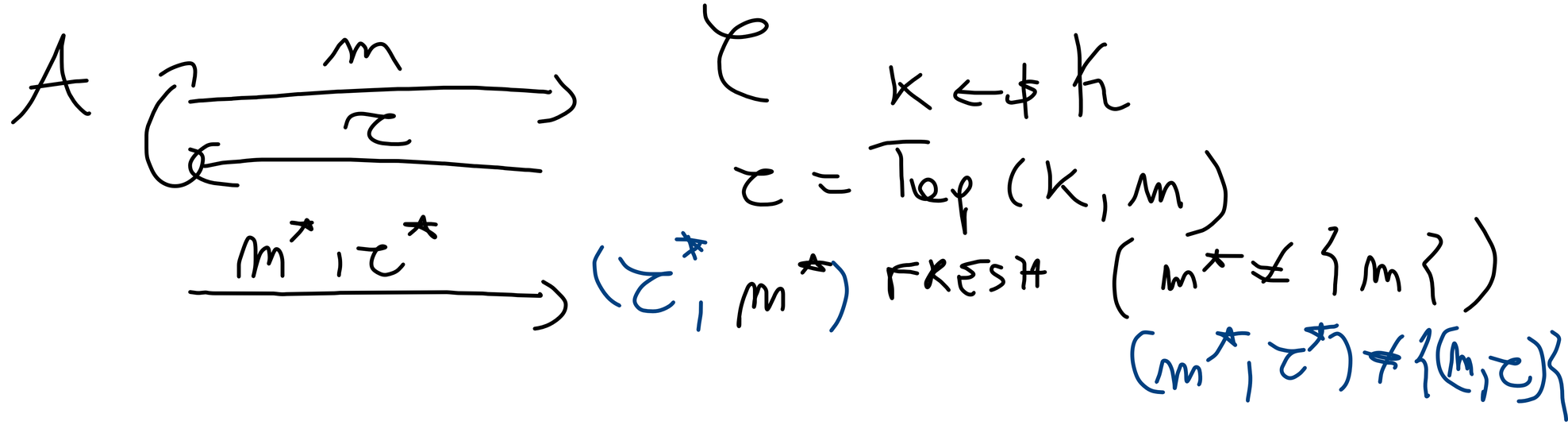
Construct PPT A_2 against UFCMA:



We know that $(c^*, \tau^*) \neq \{(c, \tau)\}$

but we need that $c^* \neq \{c\}$ to break UF-CMA. But if the tags are unique whenever (c^*, τ^*) is FRESH so is c^*. ▨

Ex. Define STRONG UF-CMA:



Prove: STRONG UFCMA $\Rightarrow$ UFCMA

UFCMA $\not\Rightarrow$ STRONG UFCMA