By itself H_{CBC} is not an UF-CPA MAC for VIL.

On the other hand, $F(H_{CBC})$ is directly secure for VIL.

What is left for symmetric crypto:

- Combining encryption and authentication.
- Pseudorandom permutations and block ciphers designed in the real world.

start with the first, also called

NON-MALLEABILITY.

Malleability: The ability to take some ctx C (of which I don't know the ptx), and change it to $\tilde{C} \neq C$ s.t. what's inside $\tilde{C}$ is related to the original ptx.

Concrete application: Sealed AUCTIONS.

Unfortunately, what we have seen so

for us MALLEABLE. For example:

$$c = (c_0, c_1) = (r, F_k(r) \oplus m)$$

$$r \leftarrow U_n$$

Thus us CPA secure. I can flip a bit of m!

$$\tilde{c} = (c_0, c_1 \oplus 10\cdots0)$$

$$\Rightarrow F_k(r) \oplus (m \oplus 10\cdots0)$$

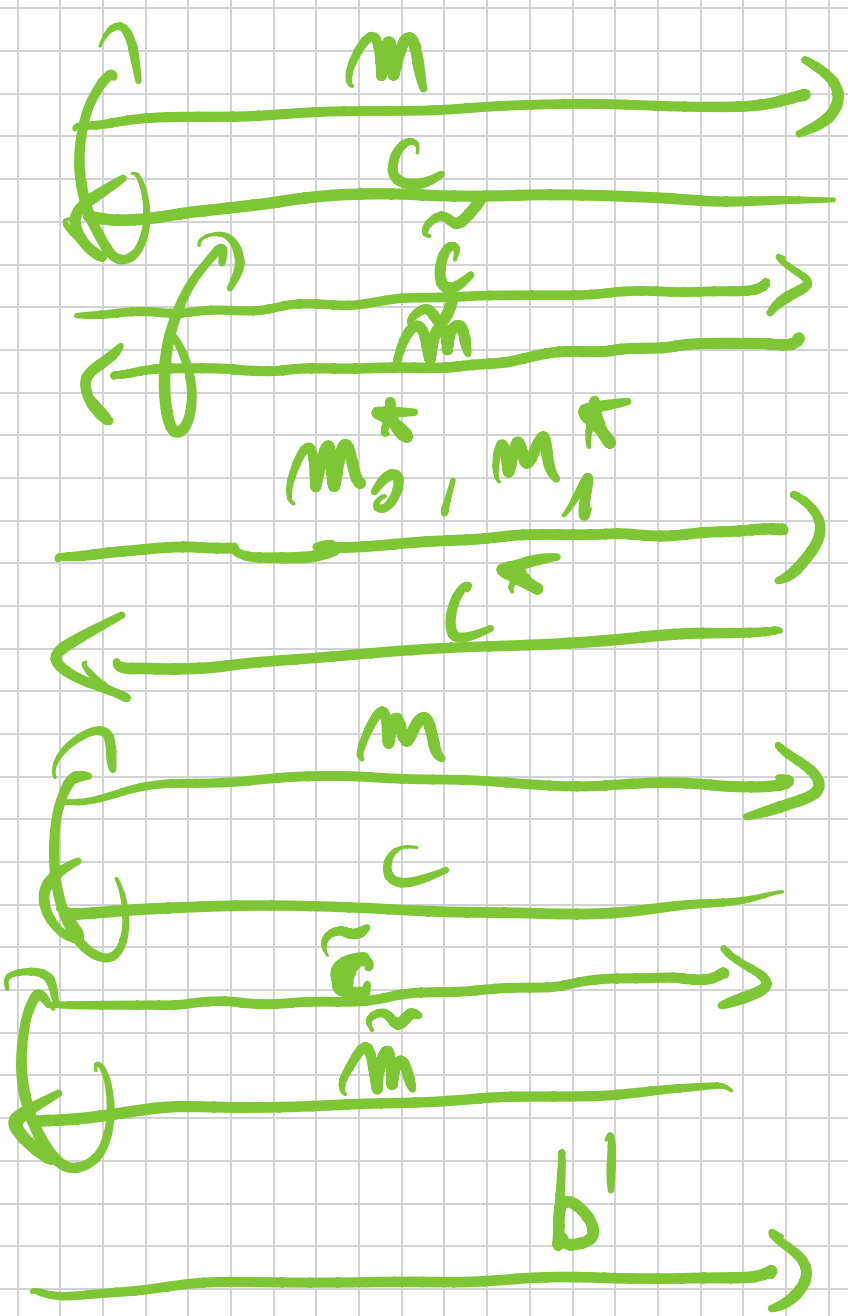
What is the definition of non-malleability? Chosen-ciphertext Attacks (CCA) security.

DEF $\Pi = (Enc, Dec)$ is CCA secure if

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

$\mathrm{Game}^{cca}_{\Pi,A}(\lambda, b)$

A



$\mathcal{C}$

$K \leftarrow \mathcal{K}$

$c \leftarrow \mathrm{Enc}_K(m)$

$c^* \leftarrow \mathrm{Enc}_K(m_b^*)$

$\tilde{m} = \mathrm{Dec}_K(\tilde{c})$

$(\tilde{c} \neq c^*.)$

We will give a general recipe for CCA-secure SKE. In particular, the following two properties will imply all!:

- CPA security.

- Authenticity: The ability to create a VALID CT $\tilde{c}$ without knowing the secret key K.

VALID means $\mathrm{Dec}(K, \tilde{C}) \neq \perp$

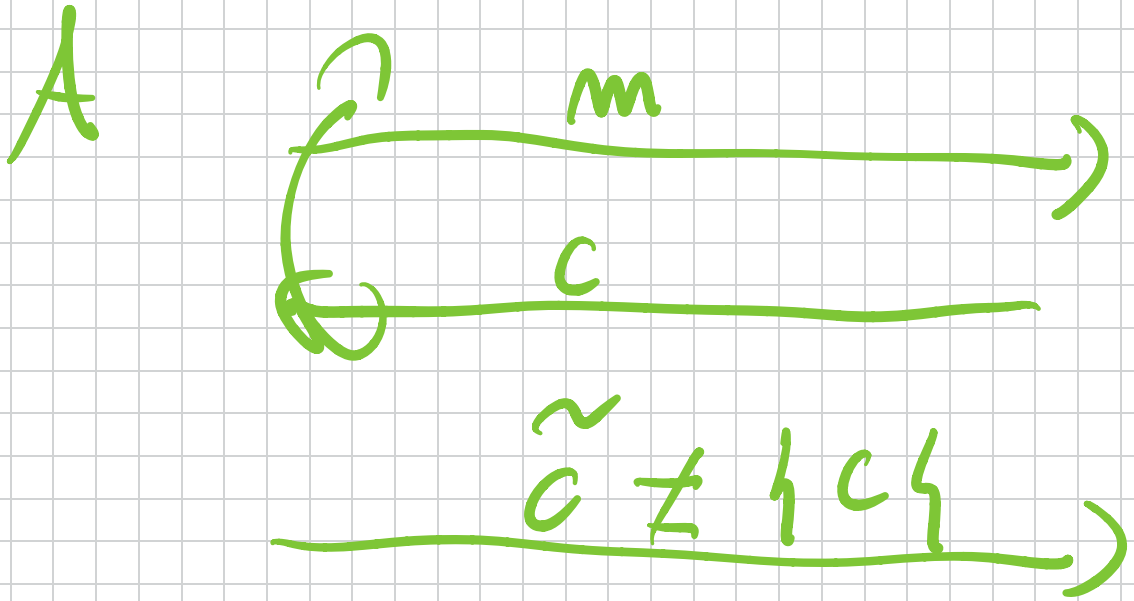
where $\perp$ is a special symbol.

DEF Π satisfies AUTH if $\forall$

PPT A:

$$\Pr\left[\mathrm{GAME}^{\mathrm{auth}}_{\Pi,A}(\lambda) = 1\right] \leq \mathrm{negl}(\lambda)$$

$G_{AMS}^{euf\text{-}cma}$ Π, A (λ)



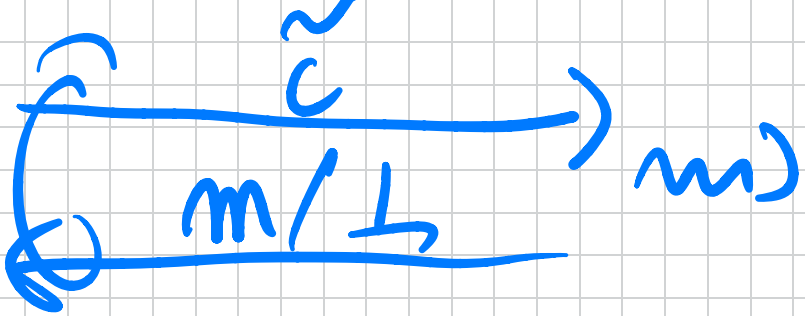
$\text{If } Dec_K(\tilde{c})$

THM CPA + AUTH $\Rightarrow$ CCA.

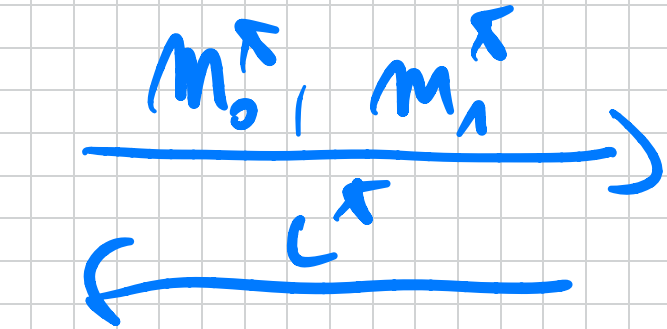
Proof. We will only give a sketch.

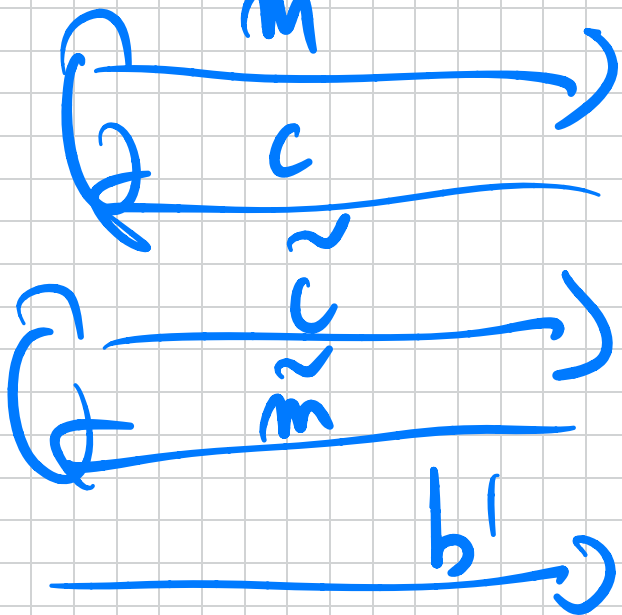
Natural idea: Make a reduction from CPA to CCA security.

A_{CCA} A_{CPA} C_{CPA}



If $\tilde{c} \in \{(m, c)\}$
return m
Else $\perp$





This suggests we should move to a hybrid $H(\lambda, b)$:

- Identical to the CCA game but upon input $\tilde{c}$ (a decryption query) does not return $Dec(K, \tilde{c})$.

Instead: If $\tilde{c} \in \{c\}$ vs the output of $\forall$ a previous enc. query m, return m else $\perp$.

By the above reduction Γ_0 cPA:

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

It remains to prove:

$$G(\lambda, b) \approx_c H(\lambda, b).$$

$$\| \|$$

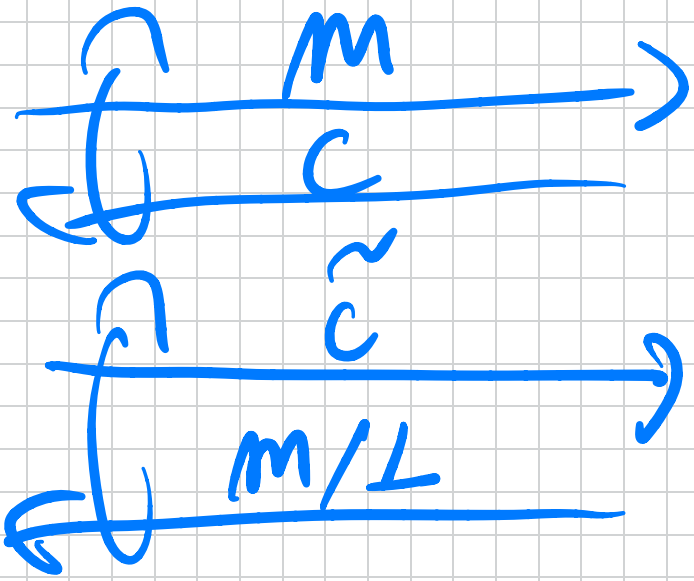
$$\text{Game}_{\Pi, A}^{\text{CCA}}$$

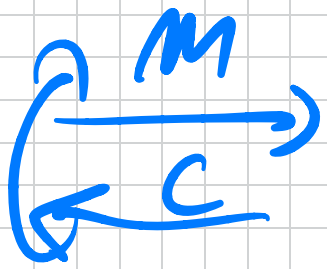
Let Bad be the event that A makes a decryption query $\tilde{c} \neq c$

s.t. $Dec(k, \tilde{c}) \neq \perp$.

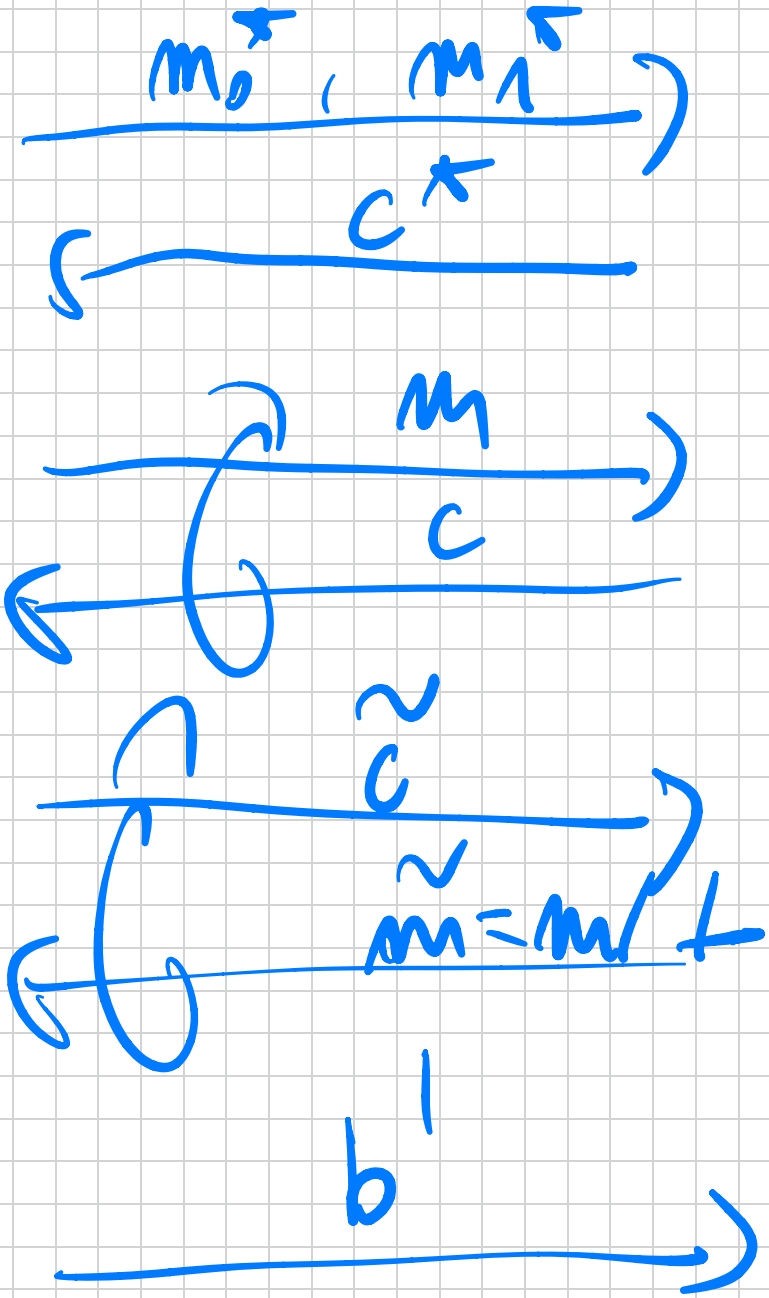
Conditioning on $\overline{BAD}$ $G(\lambda, b) \equiv H(\lambda, b)$. $\Rightarrow$ we just need to prove $Pr[BAD] \leq negl(\lambda)$.

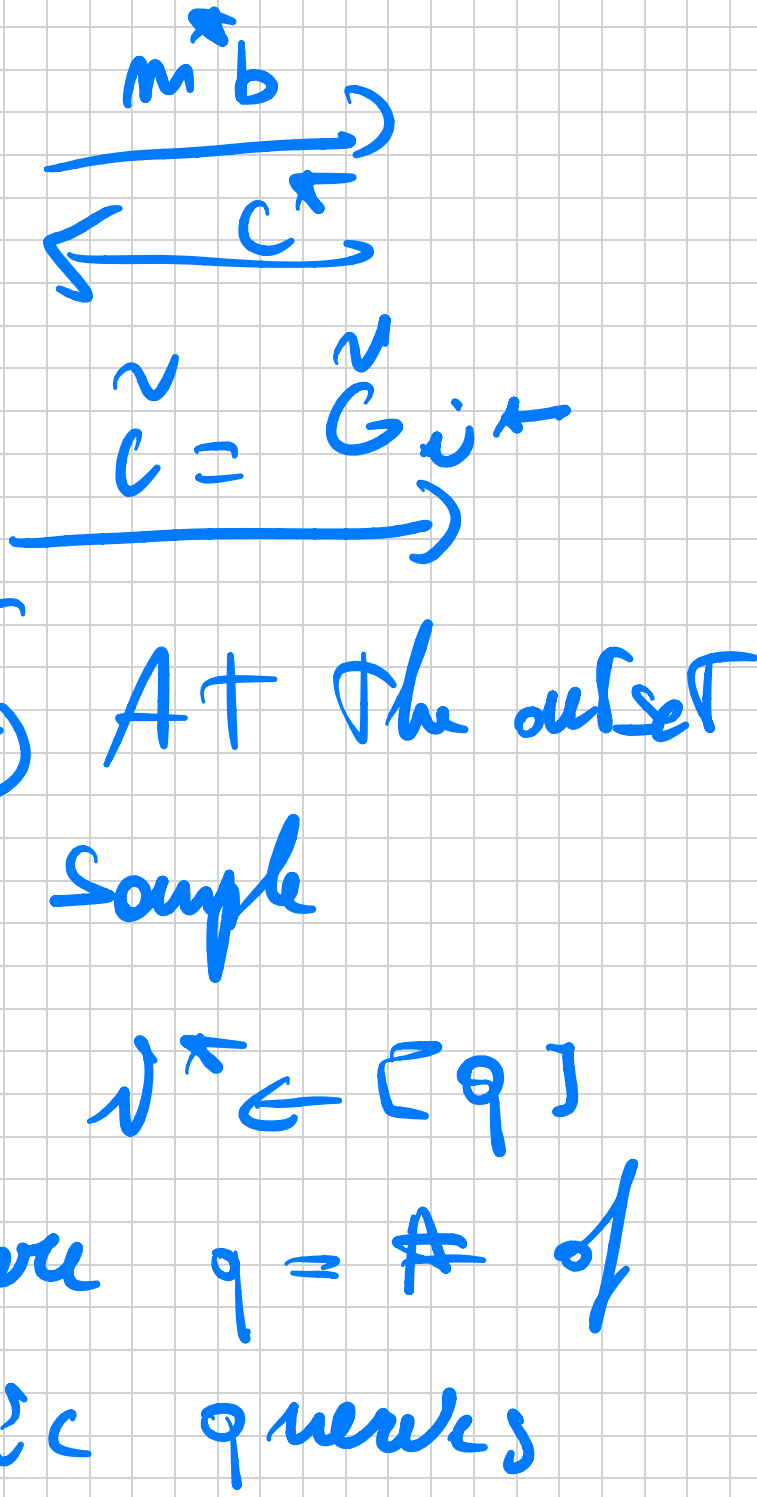
A_{CCA} A_{AUX} C_{AUX}





w.) AS BEFORE





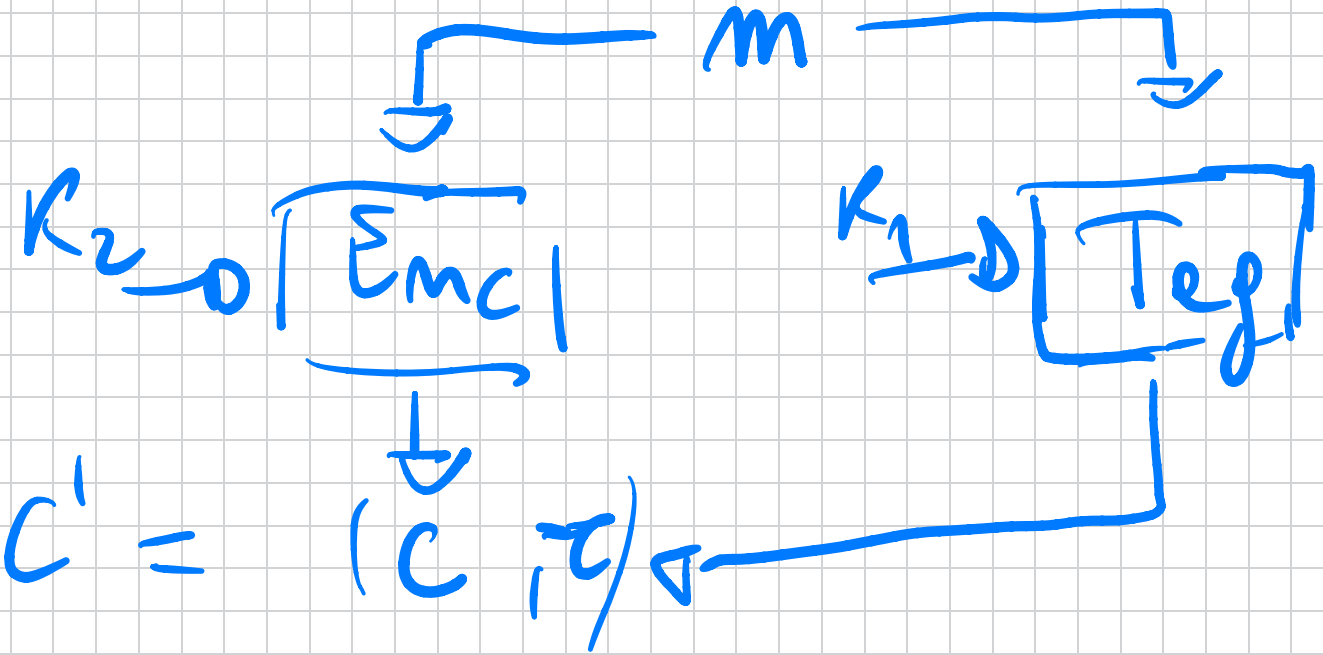
$$\Pr[A_{\text{AUTH WINS}}] \geq \frac{1}{q} \cdot \Pr[A \text{ can produce a valid}]$$

$$\geq \frac{1}{\text{poly}(\lambda)} \cdot \text{non-negligible}$$

Next natural thing is to obtain CPA + AUTH from CPA secure + UF-CMA MACs.

There are several ways to do it:

→ Encrypt-and-MAC.



Exercise: In general, MT does not work. Not CPA secure in general.

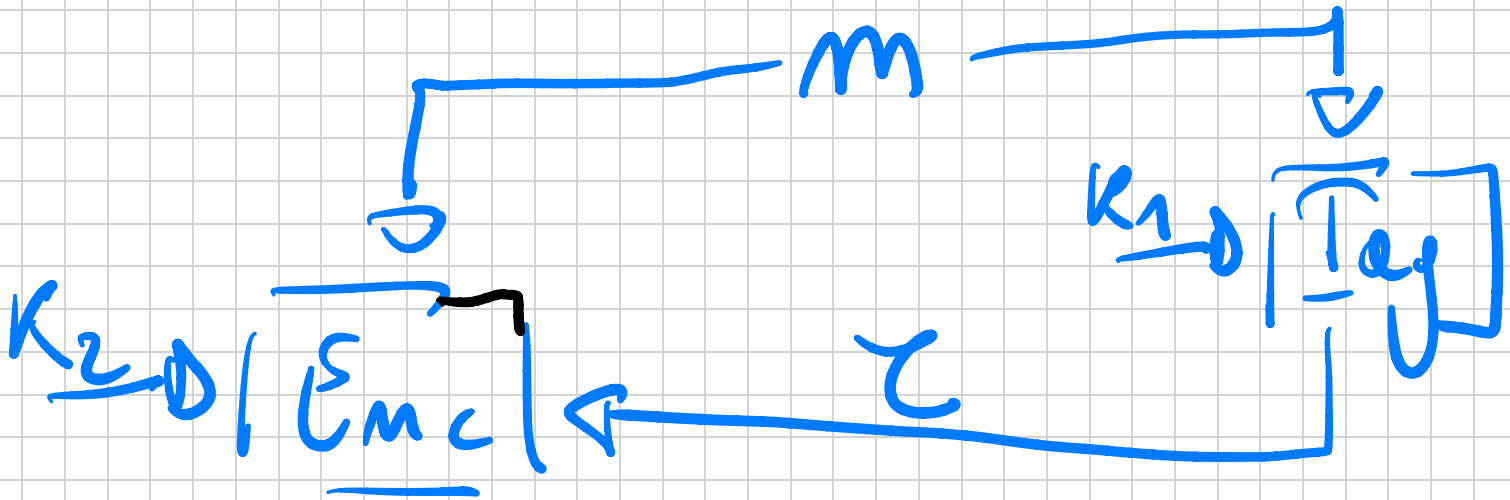
Example: a bad $Tag(K, m) = m[0] \| \tau$

where $\tau = Tag(K, m)$.

↳ VERIFY

Mac-then-Enc

—)



Exercise: It doesn't work in general. TLS does not regardless.

Look: $c' = Enc(k_2, m \| \tau)$

↳ CPA secure.

There exists BAD $\overline{Enc}(k, m) =$

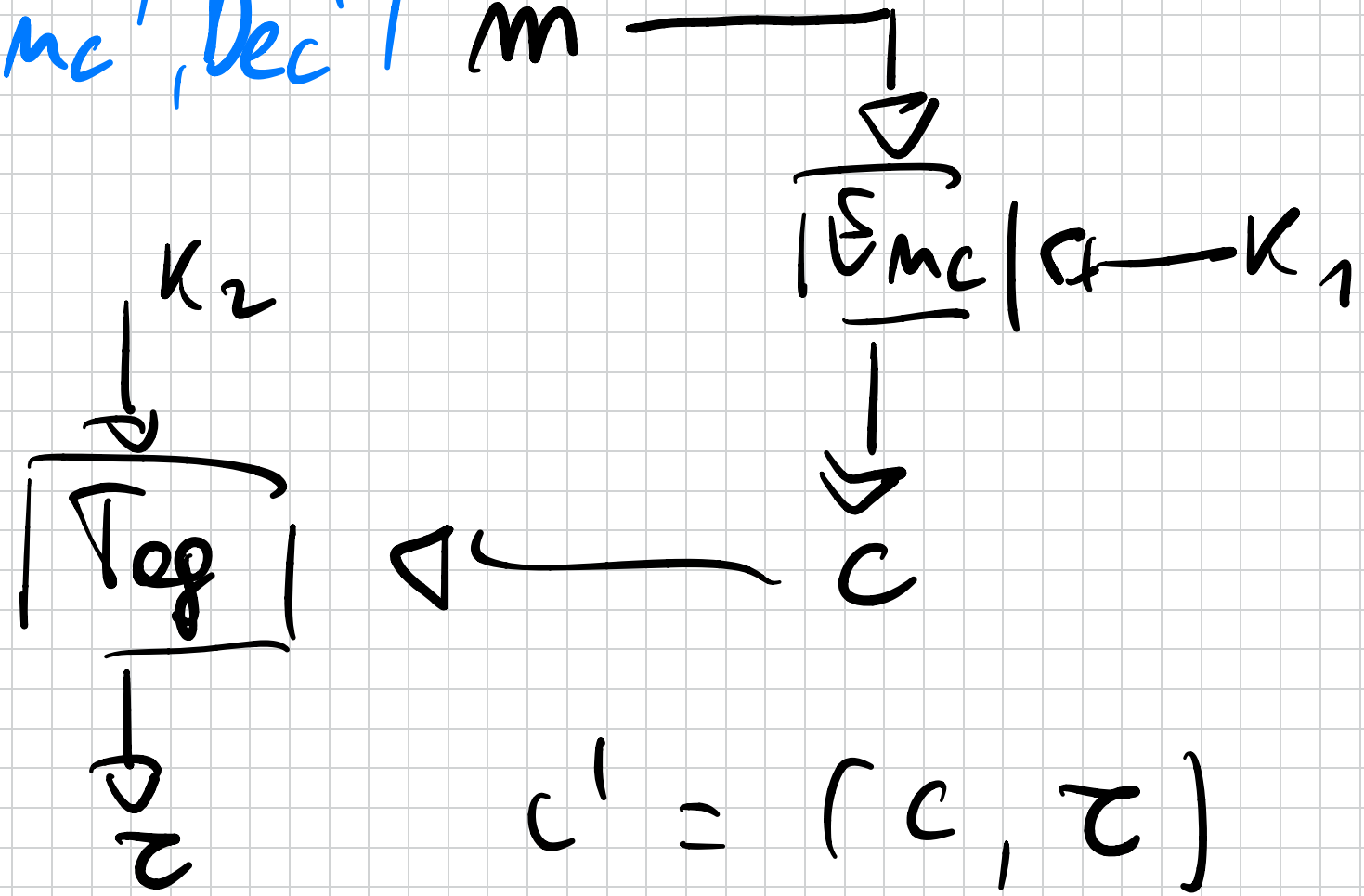
$= 0 \| Enc(k, m)$

↳ CPA secure

$Dec(k, c')$ just ignores first bit.

→ Encrypt - and - MAC

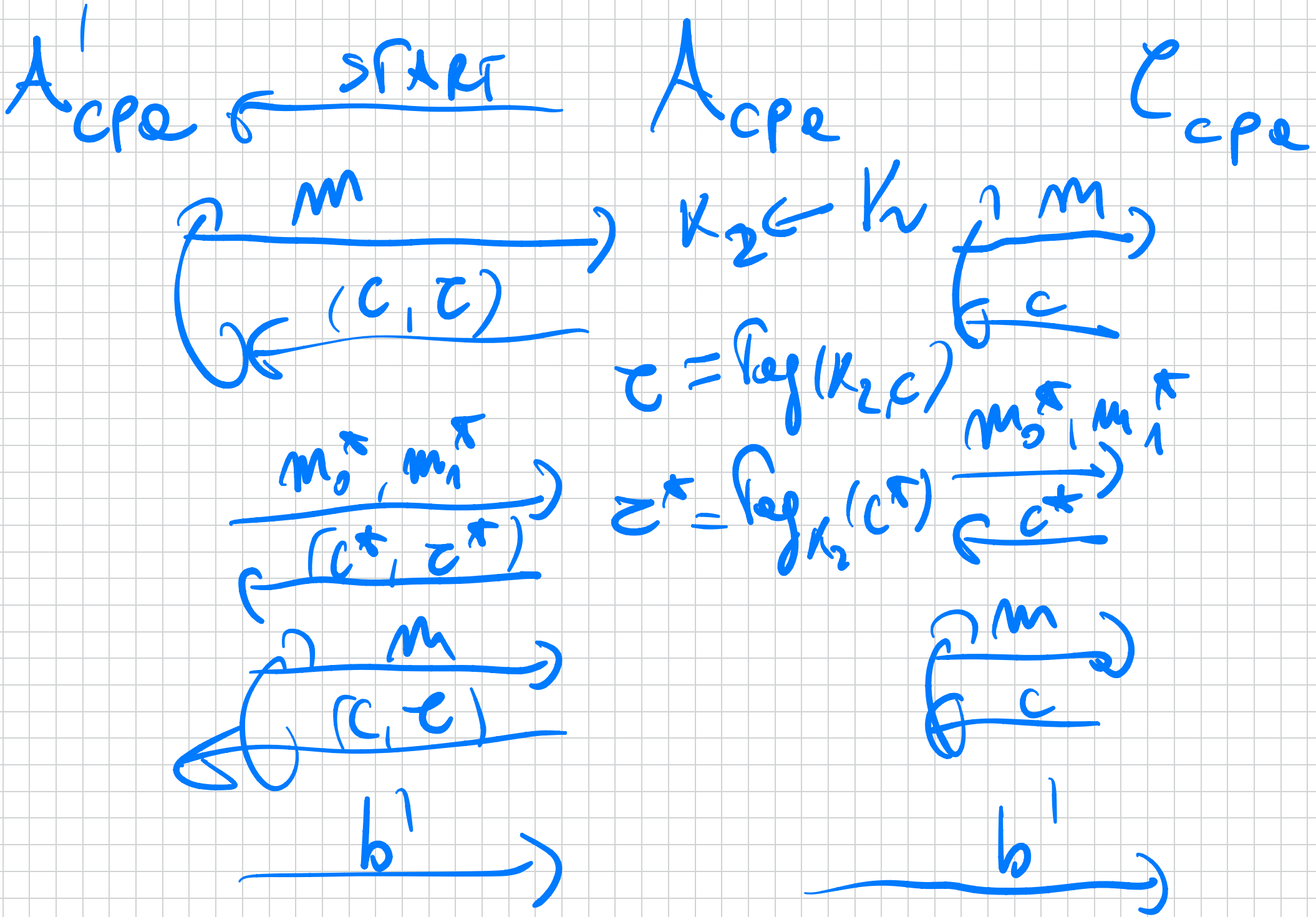
$\Pi' = (Enc', Dec' / MAC')$

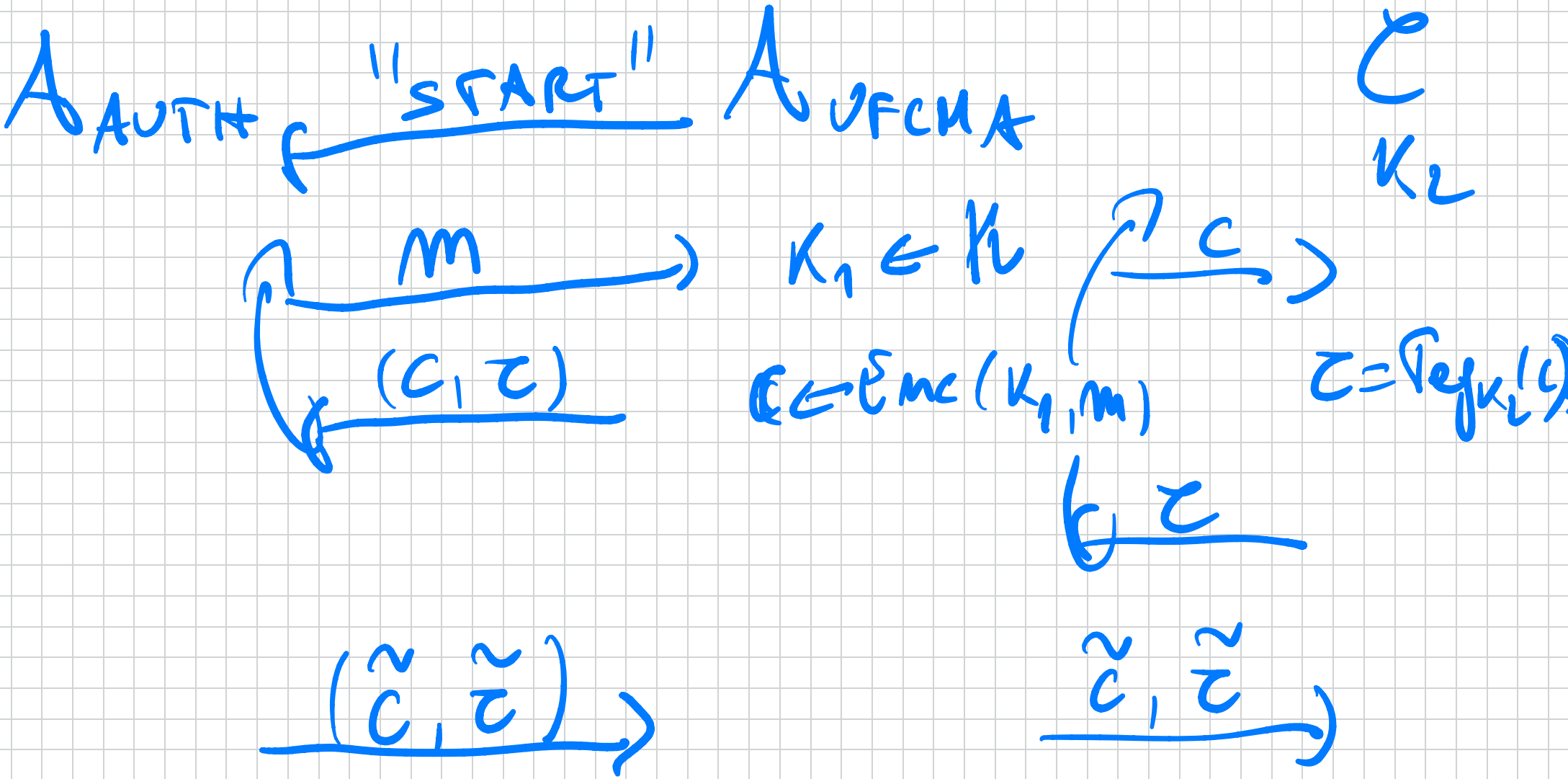


$c' = (c, \tau)$

THM The above is CPA + AUTH assuming $\Pi_1 = (Enc, Dec)$ is CPA and $\Pi_2 = Tag$ is UFCMA with unique tags.

Proof. We need to show both CPA and AUTH. Basically 2 reductions one to CPA and one to UFCMA.





Reduction wins IFF:

- $\tilde{\tau} = Tag(K_2, \tilde{c})$
- $\tilde{c} \neq c$ but we are

only proceed that

$$(\tilde{c}, \tilde{\tau}) \neq \{(c, \tau)\}$$

It's fine as long as tags are unique. ☑

(Subtle remark: Some schemes that is called STRONG UF-CMA: In UF-CMA A is allowed to

forge on $m^* \in \{m\}$ but

with fresh $c^* \notin \{c\}$.)