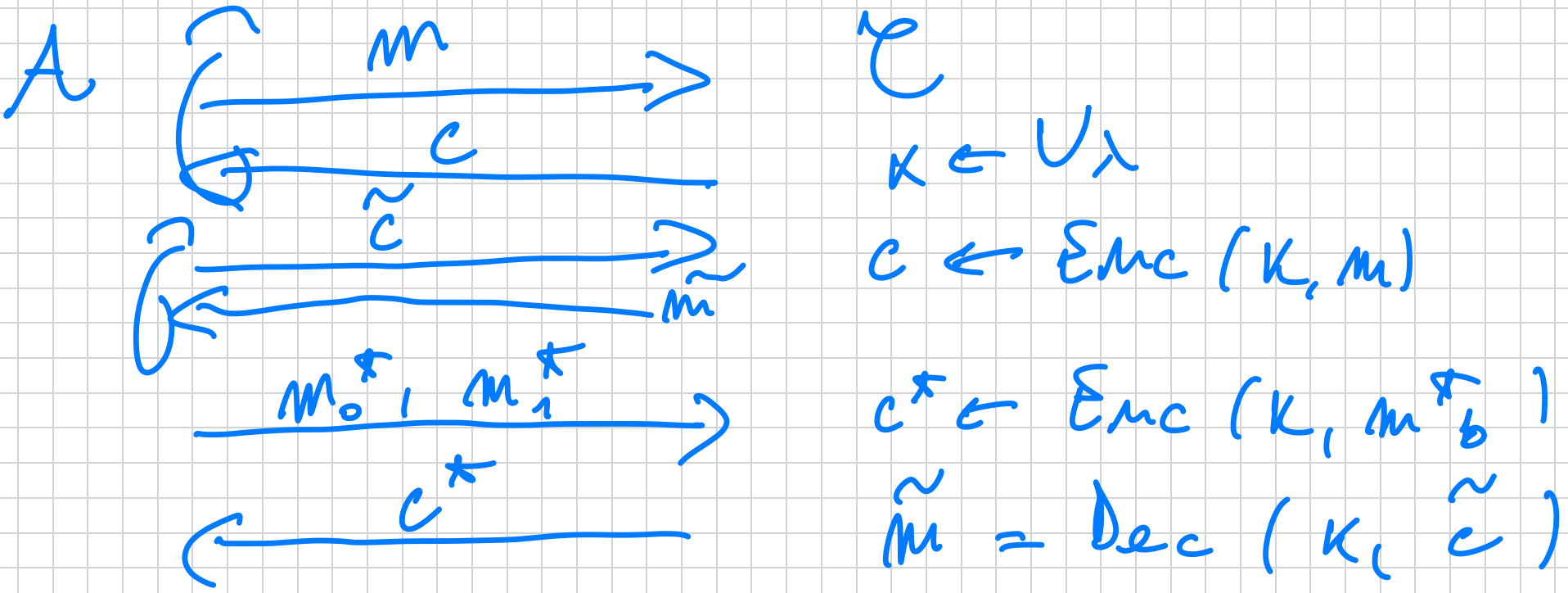
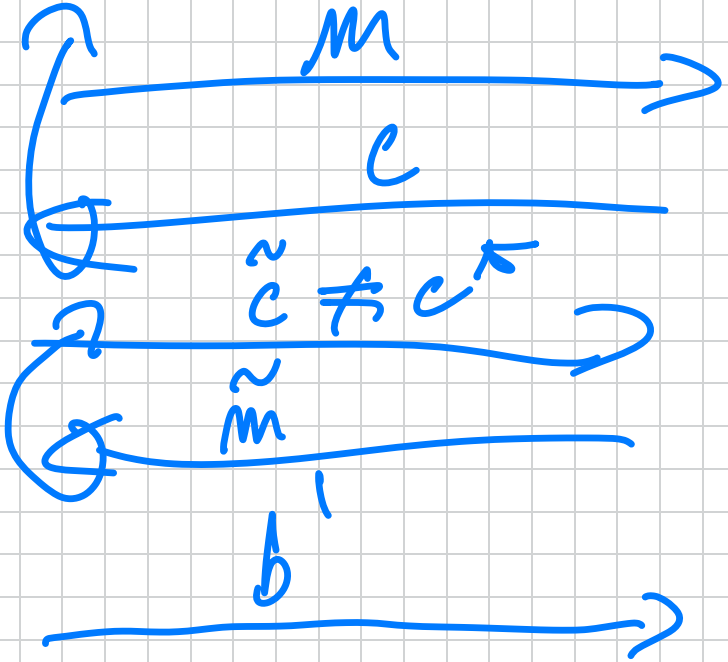
CCA SECURITY

Q: How to get both secrecy and also authenticity?

CCA: Chosen-ciphertext attacks.

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





Def (CCA security) $\Pi = (Enc, Dec)$

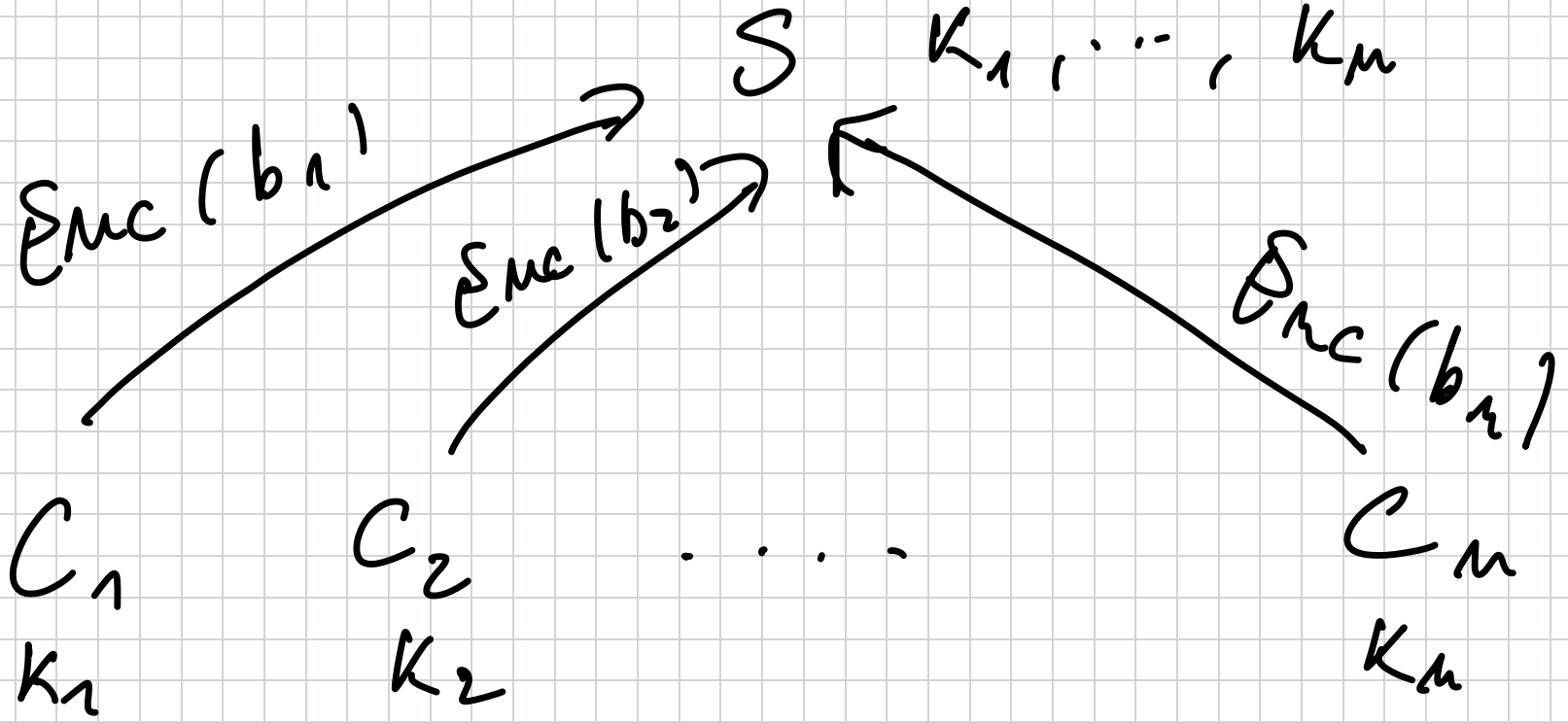
vs CCA-secure if

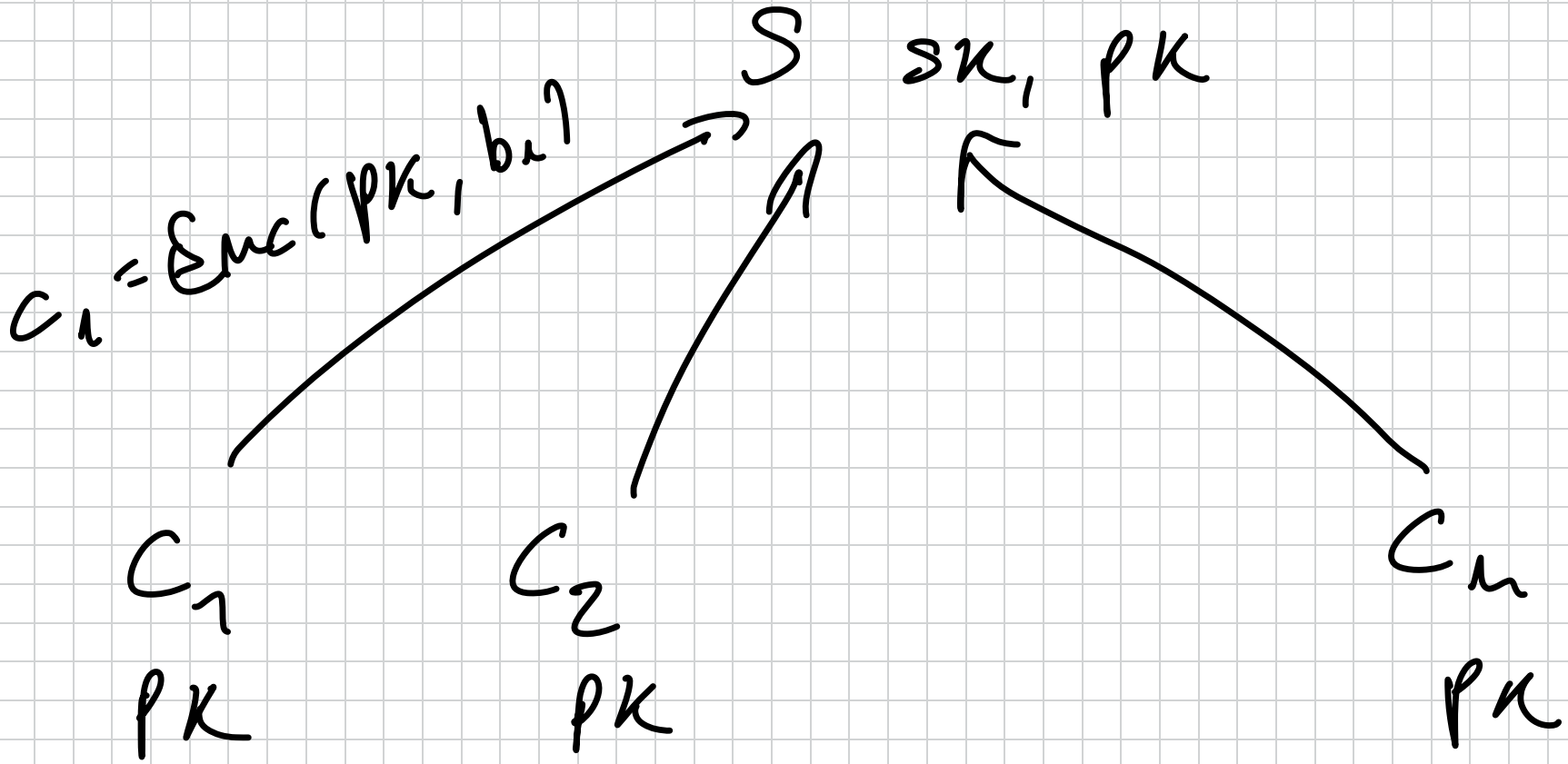
$$Game^{cca}_{\Pi,A}(\lambda, 0) \approx_c Game^{cca}_{\Pi,A}(\lambda, 1).$$

Malleability: Ability to take some c^*

containing unknown m^*, and HARD IT WAS $\tilde{c} \neq c^*$ s.t. you don't know the corresponding $\tilde{m}$, but you know $\tilde{m}$ is RELATED to m^* (e.g. $\tilde{m}[1] = m^*[1]$).

Think of encrypted ACCESS:





OBS. CCA $\Rightarrow$ Non-Malleability !

What about the ECB we studied? They are not (none of them, CBC, OFB, CFB, CTR).

For instance: $c = (r, F_k(r) \oplus m)$

Not CCA secure. ($r \leftarrow U_n$ is the randomness)

What happens if we do:

$$c = (r, s) \longmapsto F_k(r) \oplus (m \oplus 10^{n-1})$$

$$\tilde{c} = (r, s \oplus 10^{n-1})$$

↳ FLIPPING FIRST BIT OF s

Make it an attack!

t

$\mathcal{C}$ $\quad K \leftarrow U_\lambda$

$r^* \leftarrow U_n$

$s^* = f_K(r^*) \oplus m_b^*$

$m_0^* = 0^n, \; m_1^* = 1^n$

$c^* = (r^*, s^*)$

$\tilde{c} = (r^*, s^* \oplus (1 \| 0^{n-1}))$

$\tilde{m}$

b'

If $\tilde{m} = 10^{n-1}$ output $b' = 0$

$\tilde{m} = 01^{n-1}$ output $b' = 1$

$$Pr[b' = 1 : b = 0] = 0$$

$$Pr[b' = 1 : b = 1] = 1$$

Q: How do we get CCA security?

Natural idea: Combine CPA security with UF-CMA MAC.

Implementation: Make sure ctx contains a Tag of Smt. Then:

- CTX with valid Tag is VALID
- CTX with invalid Tag is INVALID
  (Dec outputs "⊥")

Attempts:

1) $C' = (C_1, \tau)$; $(K_1, K_2) = K$

$C \in Enc(K_1, m)$; $\tau = Tag(K_2, m)$
(CPA) (UFCMA)

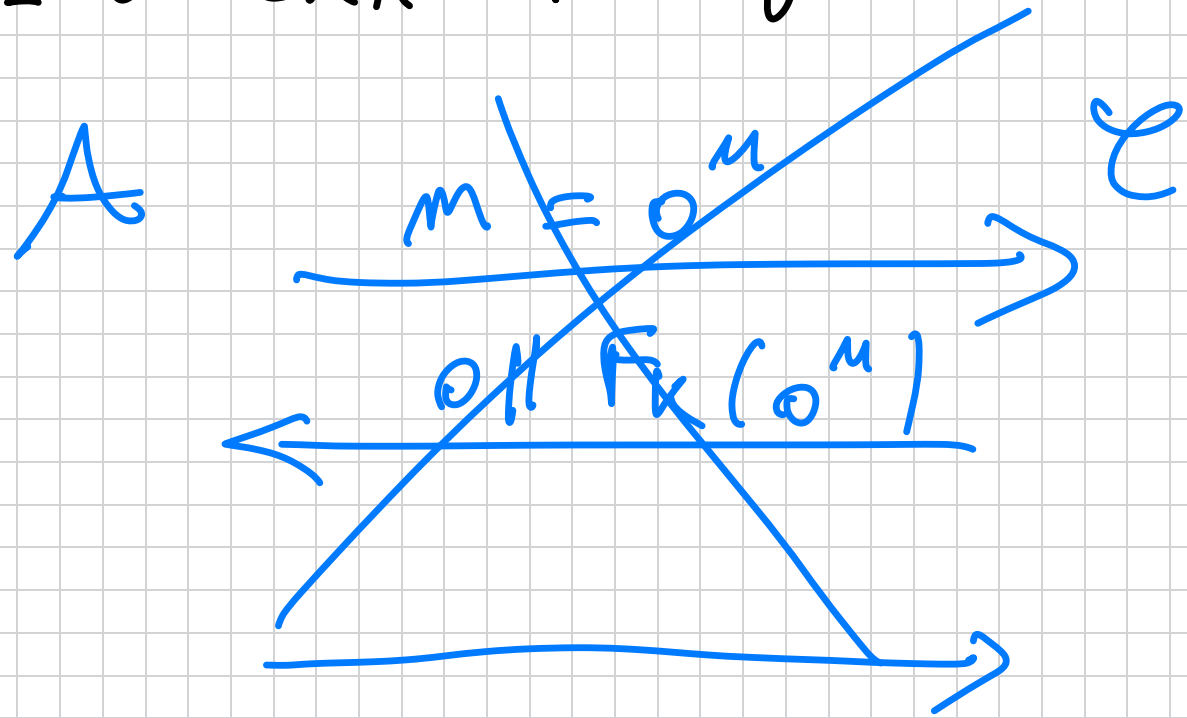
CCA? Not in general. In fact, not even CPA! Let Tag be UFCMA MAC.

Consider $\widetilde{Tag}(k_2, m) = b \| \tau$

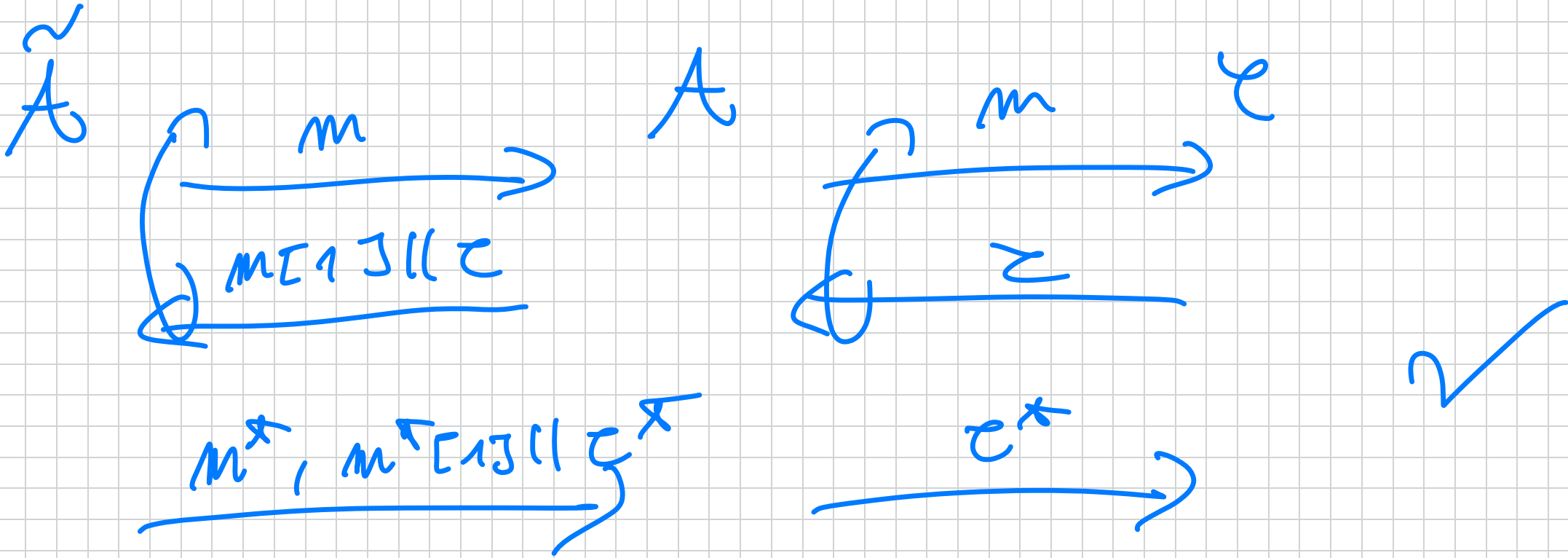
$\tau = \widetilde{Tag}(k_1, m)$

b = first bit of m

$\widetilde{Tag}$ = UF-CMA ? By reduction.



Attack does not work!



2) The problem was that τ can reveal something about m. Let's encrypt the tag!

$$c' \leftarrow Enc(k_1, m||\tau)$$

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

Output c' only.

This is used in TLS.

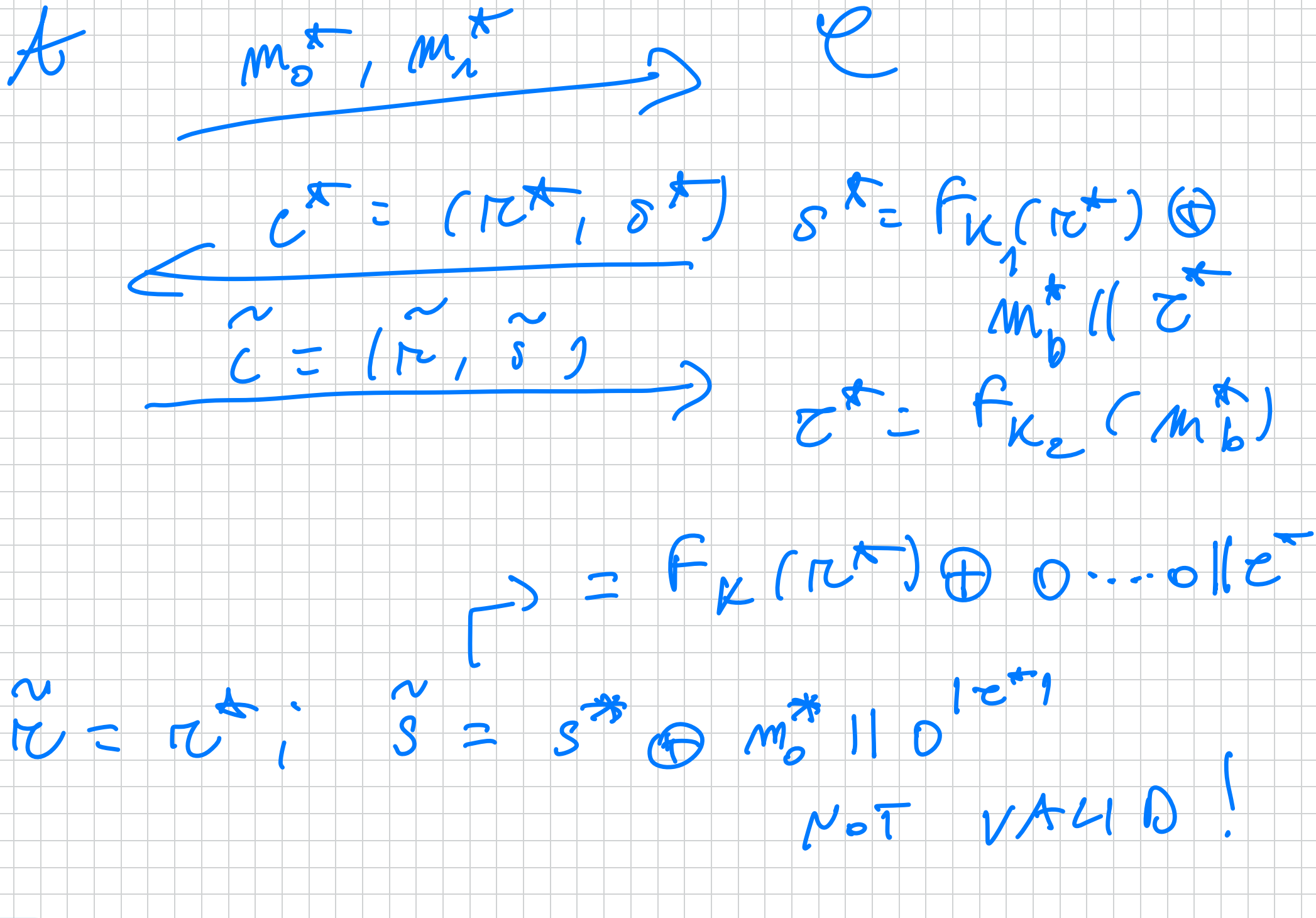
CCA ? No ! Not in general.

Enc = CPA ; Tag = uf-CMA.

$$c = (r, s) \quad ; \quad s = F_{k_1}(r) \oplus (m \| \tau)$$

$$\tau = F_{k_2}(m)$$

$$c = b \| \tau'$$



$\widetilde{Enc}(k_1, m)$: $c \leftarrow Enc(k_1, m)$

(Enc ~~ANY~~ CPA SKE.)

$c = 0\,1\,1\,1\,0\,0\,0\,1$

00 01 or 10

11 NS INVALID

$\tilde{c} = 00(01 \rightarrow 10) \cdots \neq c^*$

$$\tilde{Enc}(k_1, m) = b \| Enc(k_1, m)$$

$$b \leftarrow \{0,1\}$$

$$Enc \equiv CPA$$

$\tilde{Dec}(k_1, b\|c)$: Discard b

Decrypt c.

$$\tilde{Enc} \equiv CPA\ !$$

3) $c' = (c, \tau)$

$c \leftarrow Enc(k_1, m)$

$\tau = Tag(k_2, c)$ $\Big\}$ $\underline{\underline{Enc'}}$

T+M. If $\Pi_1 = (Enc, Dec)$ is CPA secure and $\Pi_2 = Tag$ is UF-CMA, then above $\Pi' = (Enc', Dec')$ is CCA-secure.

General Technique: CCA security follows from 2 essential properties:

- CPA security
- AUTHENTICITY → Not possible to create valid ctx without key

Π_{auth}, t (λ)

A ⟷ C

A → C: m

C → A: $c \leftarrow Enc(k, m)$

A → C: $\tilde{c}$

C: $k \leftarrow \{0,1\}^\lambda$

Output 1 iff $Dec(k, \tilde{c}) \neq \perp$

$\tilde{c} \notin \{c\}$

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