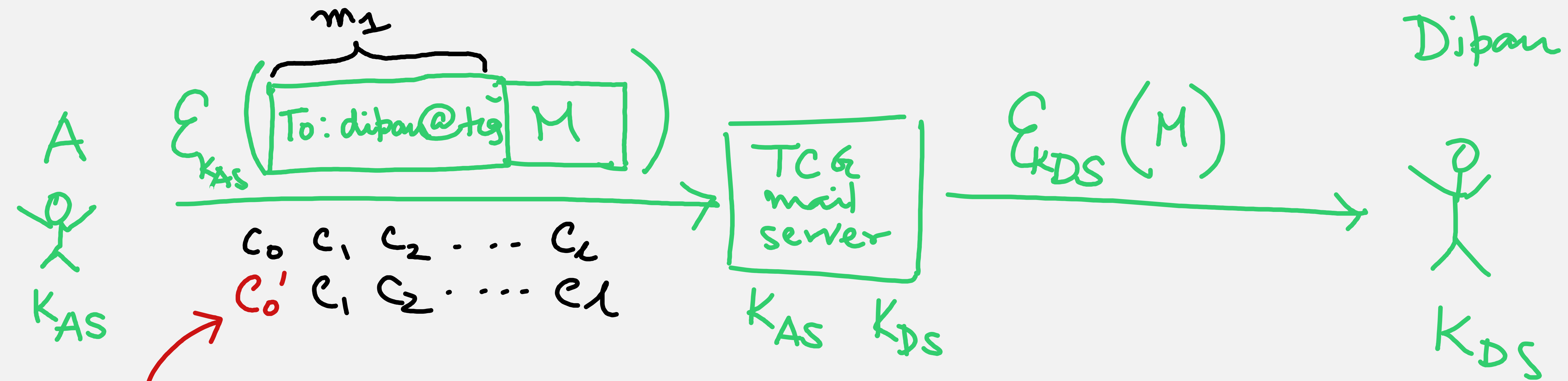


Authenticated Encryption

(Privacy + Authenticity)



(Target)

IND-CPA may not be sufficient

Pritam

$$m_1 = c_0 \oplus \text{To: dipan@tcg}$$

$$m_1' = c_0' \oplus \text{To: pritam@tcg}$$

$$c_0' = c_0 \oplus m_1 \oplus m_1'$$

$$m_1 = \text{To: Dipan@tcg.org}$$

$$M = m_2 \dots m_L$$

$$m_1 = \text{To: Pritam@tcg.org}$$

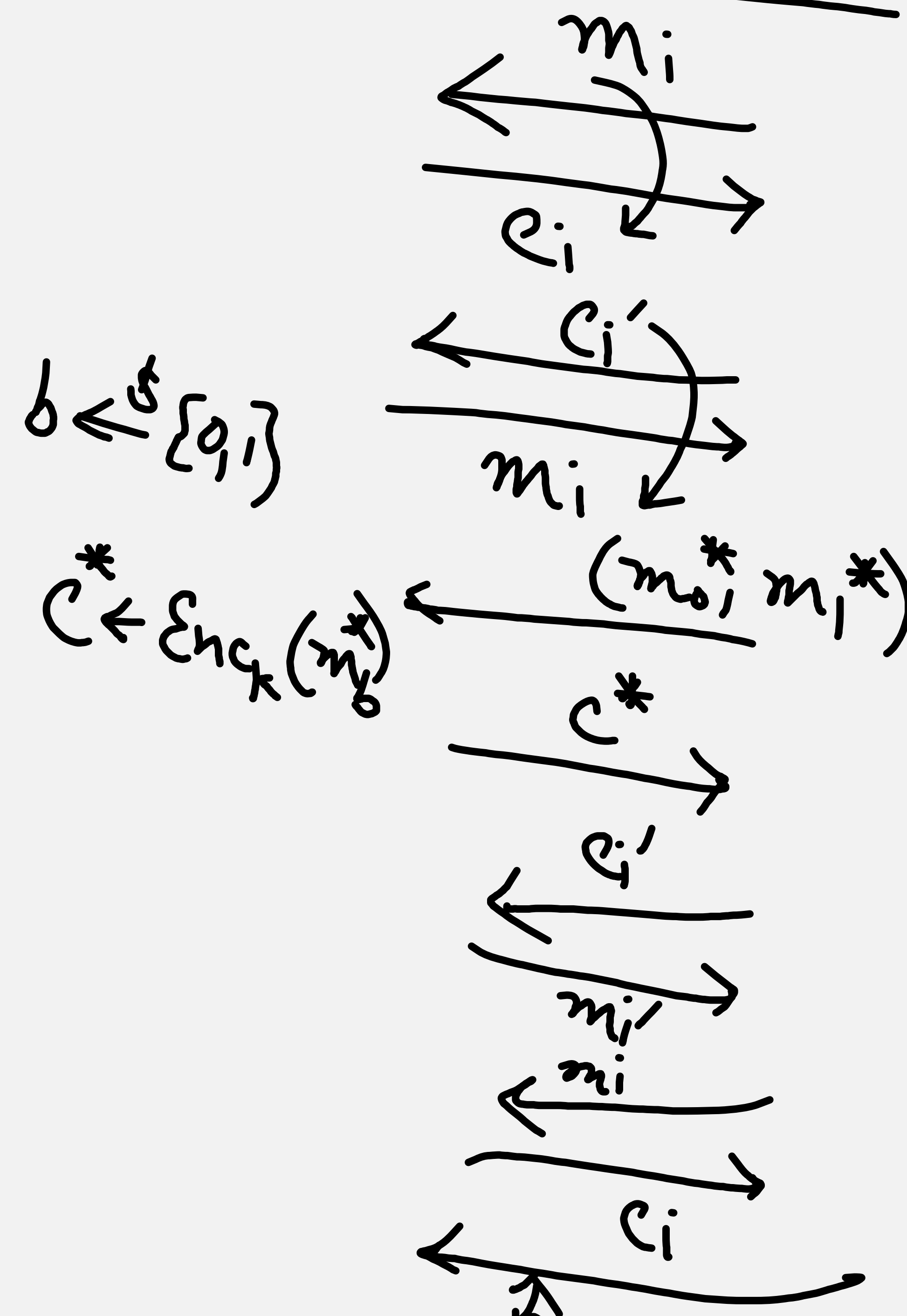
$$M = m_2 \dots m_L$$

$$c_0, c_1, \dots, c_L$$

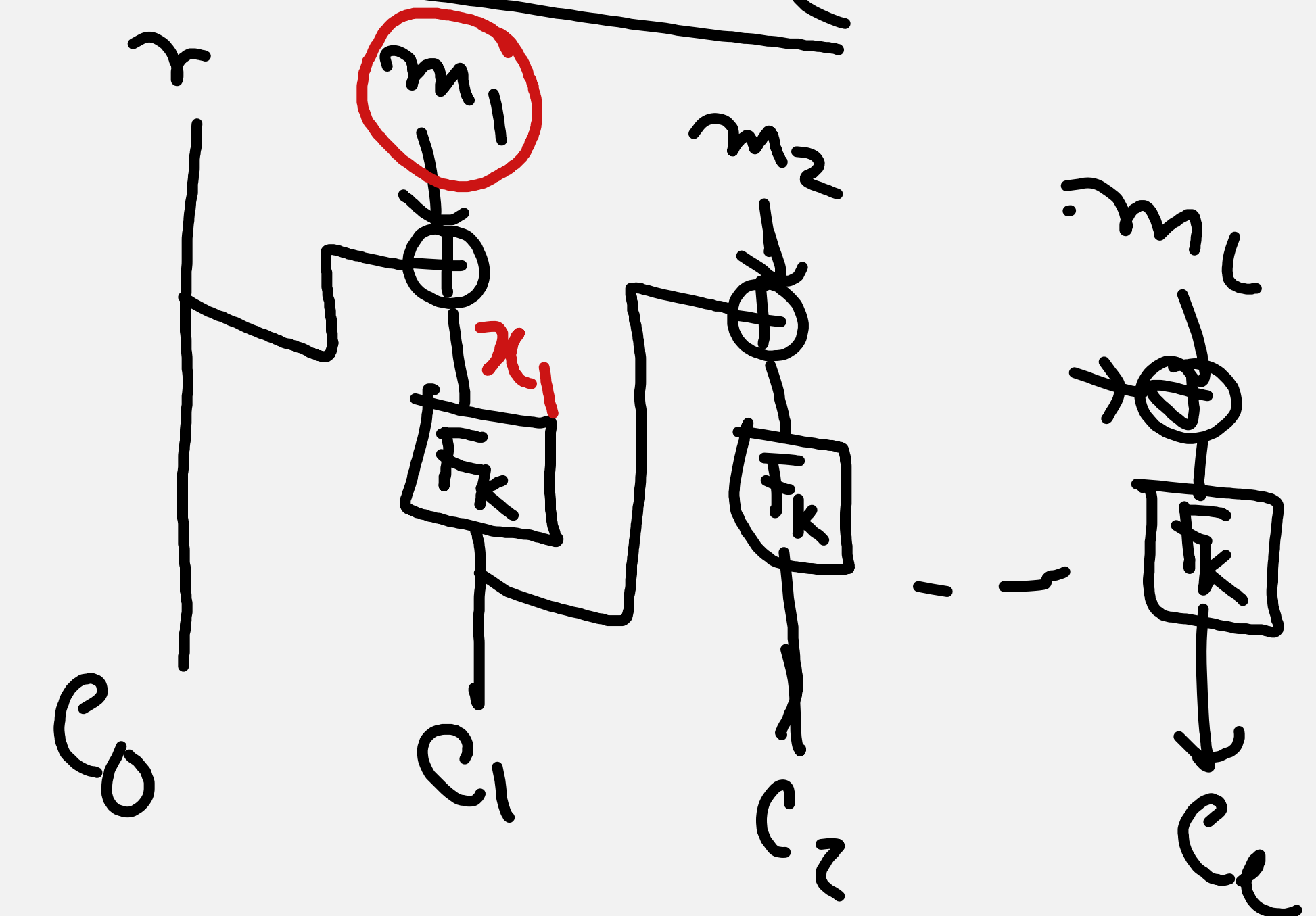
Can you modify this

CCA Notion

C_L A



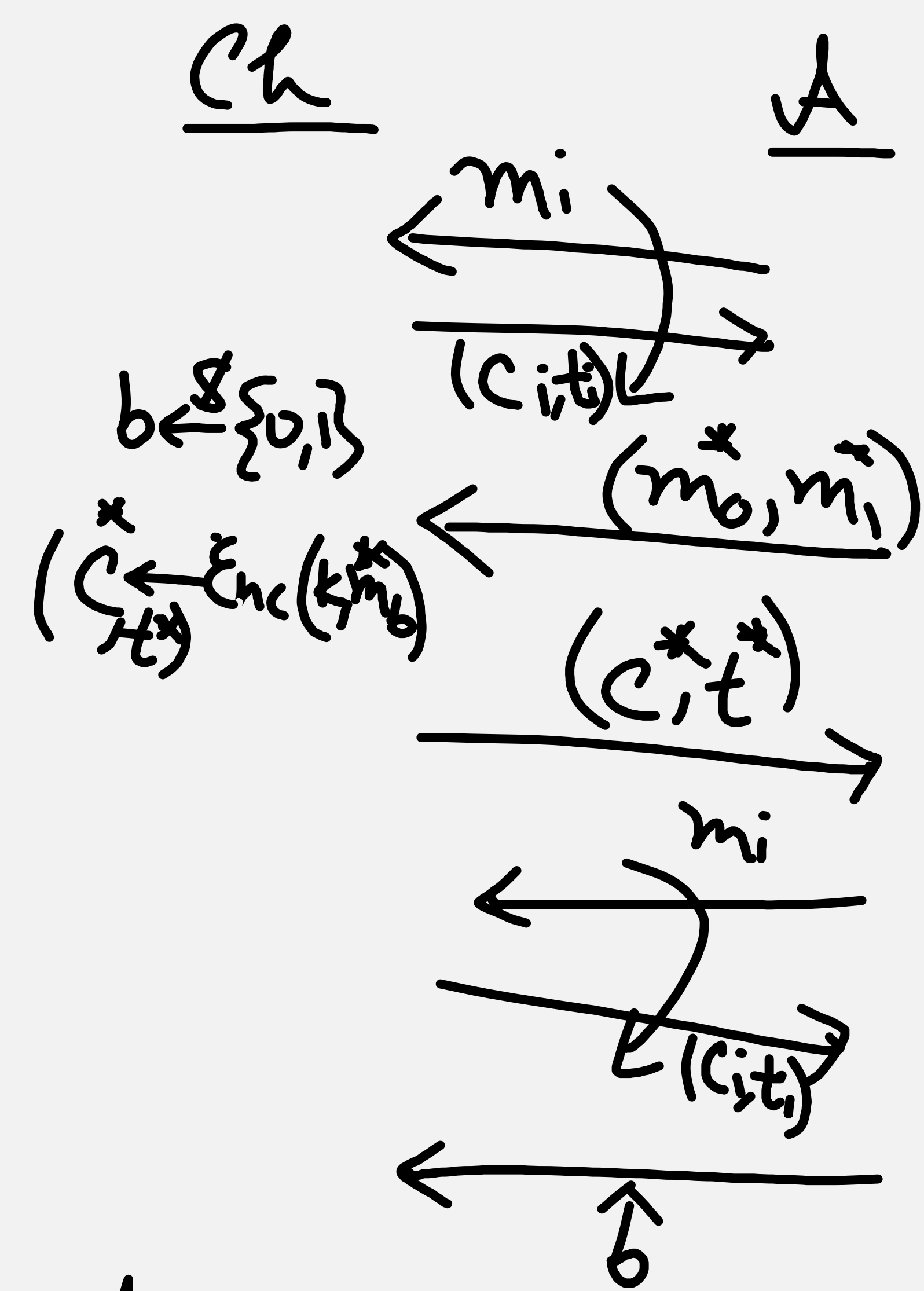
randomized-CBC



Security Notion for Authenticated Encryption

$$AE = (KG, Enc, VDec) \quad \text{Verified decryption}$$

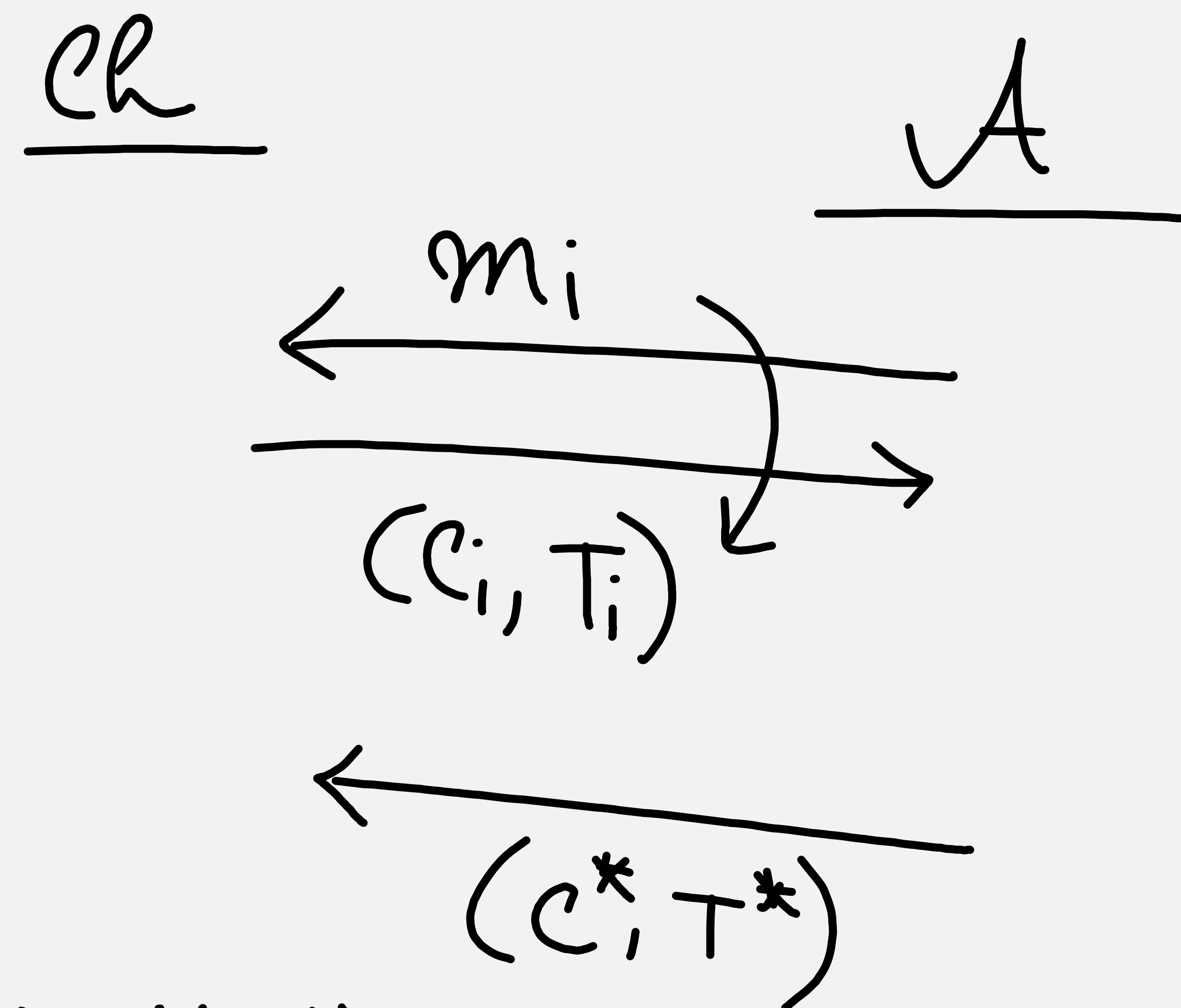
IND-CPA



AE is IND-CPA secure if for all $\mathcal{A}$

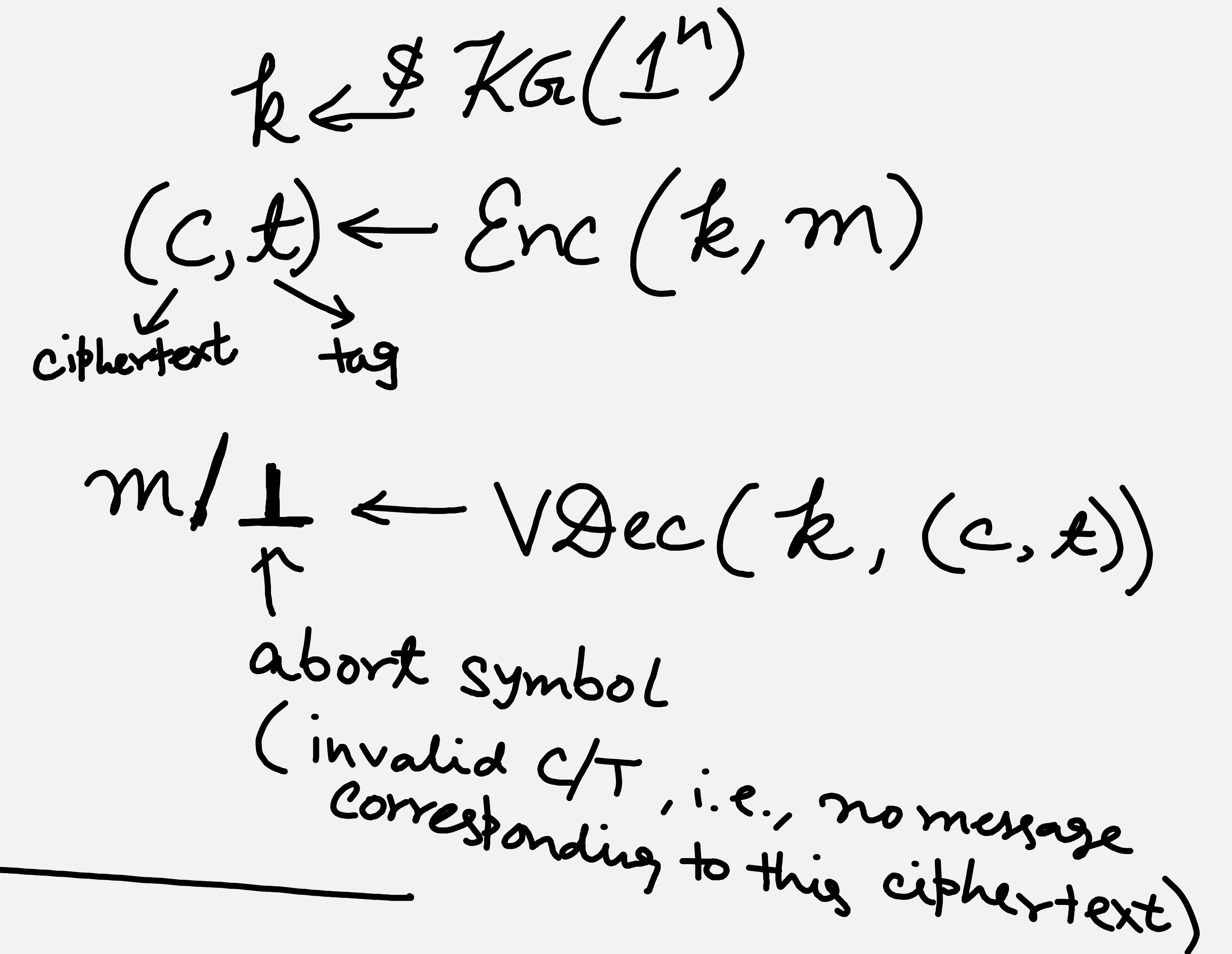
$$\Pr[b = \hat{b}] \leq \frac{1}{2} + \text{negl}(n).$$

INT-CTXT (Integrity of Ciphertext)



$\mathcal{A}$ wins if

- (c^*, t^*) should be valid
- (c^*, t^*) is fresh (i.e., $(c^*, t^*) \neq (c_i, t_i)$).



AE is INT-CTXT secure if $\forall \mathcal{A}$, $\Pr[\mathcal{A} \text{ wins}] \leq \text{negl}(n)$.

A construction $AE = (KG, Enc, VDec)$ is AE-secure if AE is both

- IND-CPA Secure
- INT-CTXT Secure

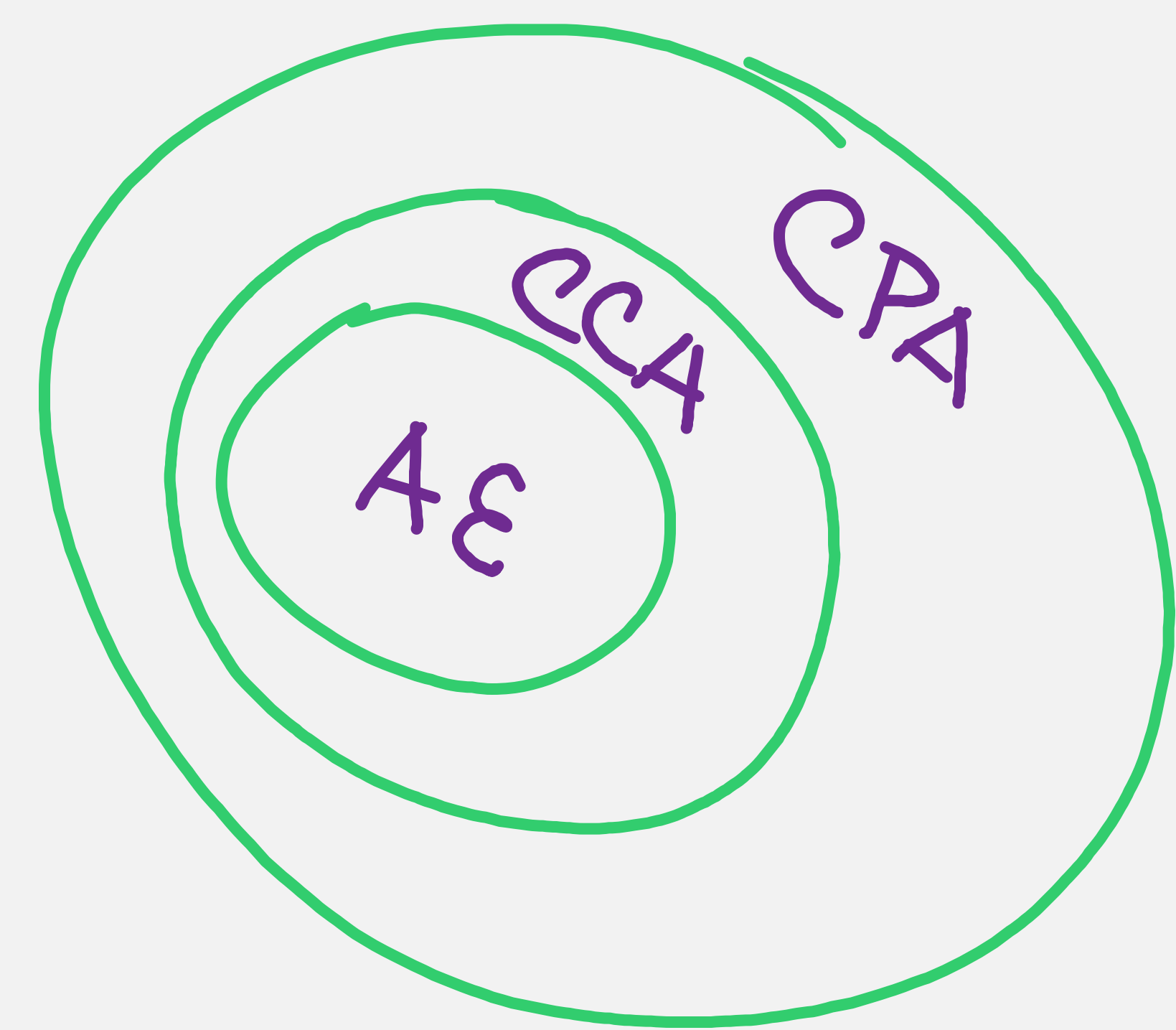
Lemma: If $\Pi = (KG, Enc, VDec)$ is AE-Secure, then Π is CCA-Secure.

$$\text{CPA Security} + \text{INT-CTXT Security} \implies \text{CCA Security}$$

Π is CPA Secure. Π won't be CCA Secure if there is some valid, fresh (ciphertext, tag) query.

↓
 Π is not INT-CTXT Secure

H/W: Show that CCA-Security $\not\Rightarrow$ AE Security.

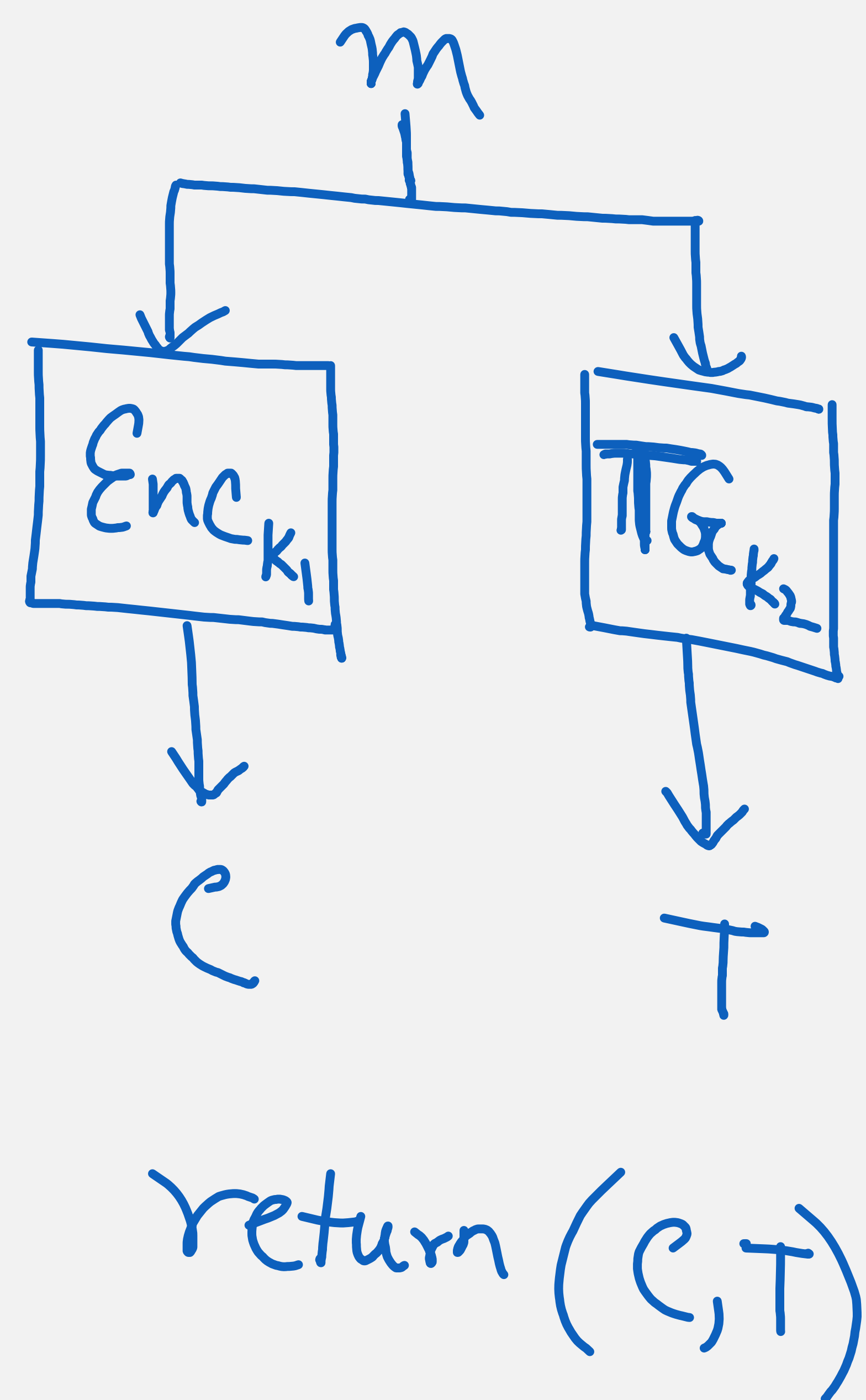


Generic Compositions

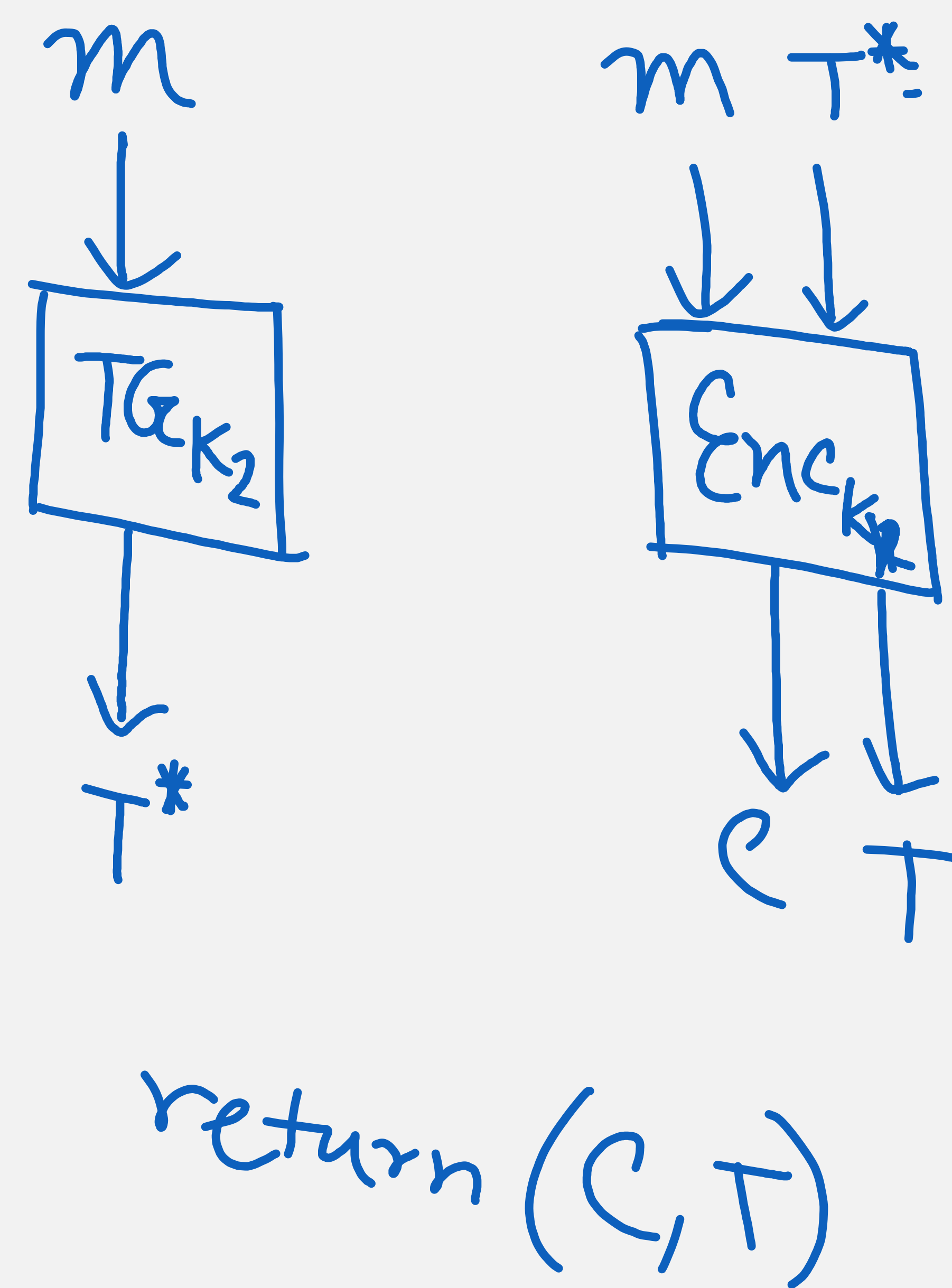
$\Pi_1 = (KG, Enc, Dec) \rightarrow \text{IND-CPA secure Encryption}$

$\Pi_2 = (KG', TG, Vrfy) \rightarrow \text{EUF-CMA secure MAC}$

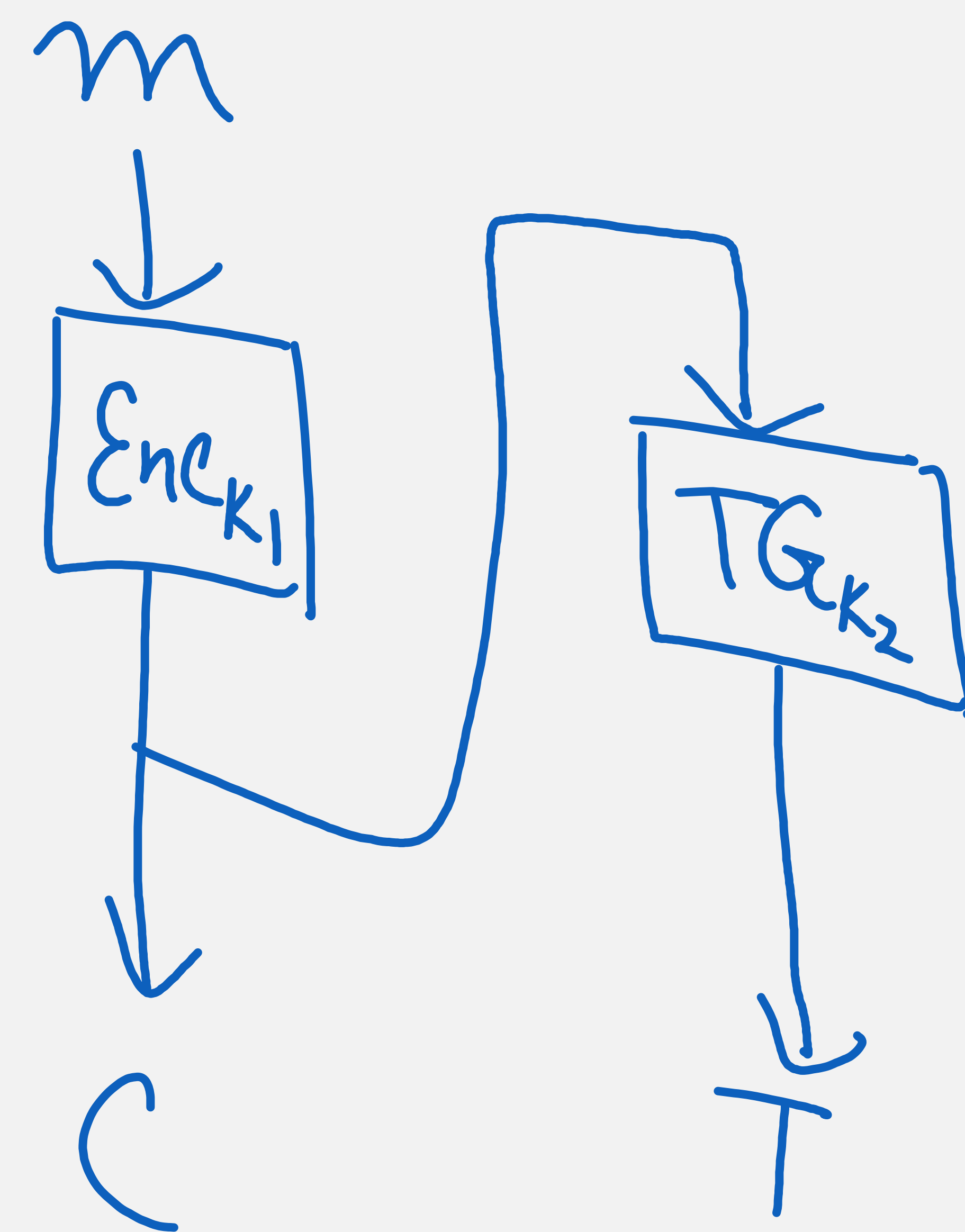
Encrypt-and-MAC



MAC-then-Encrypt



Encrypt-then-MAC



Verified Decryption Algorithms

Enc & MAC

$VDec((k_1, k_2), c, T)$
 $m := Dec(k_1, c)$
 if $(Vrfy(k_2, m, T) = 1)$
 o/w return m
 return $\perp$

MAC then Encrypt

$VDec((k_1, k_2), c, T)$
 $(m, T^*) := Dec(k_1, c, T)$
if $(Vrfy(k_2, m, T^*) = 1)$
 return m
o/w
 return $\perp$

Encrypt then MAC

$VDec((k_1, k_2), c, T)$
if $(Vrfy(k_2, c, T) = 1)$
 $m := Dec(k_1, c)$
 return m
else
 return $\perp$

* No need for decryption
if verification is not
successful.

Security of Generic Compositions

Enc-and-MAC is not generically Secure

$\pi_2 = (KG, TG, Vrfy)$ - EUF-CMA Secure

$\pi_2' = (KG', TG', Vrfy')$

$\Downarrow$

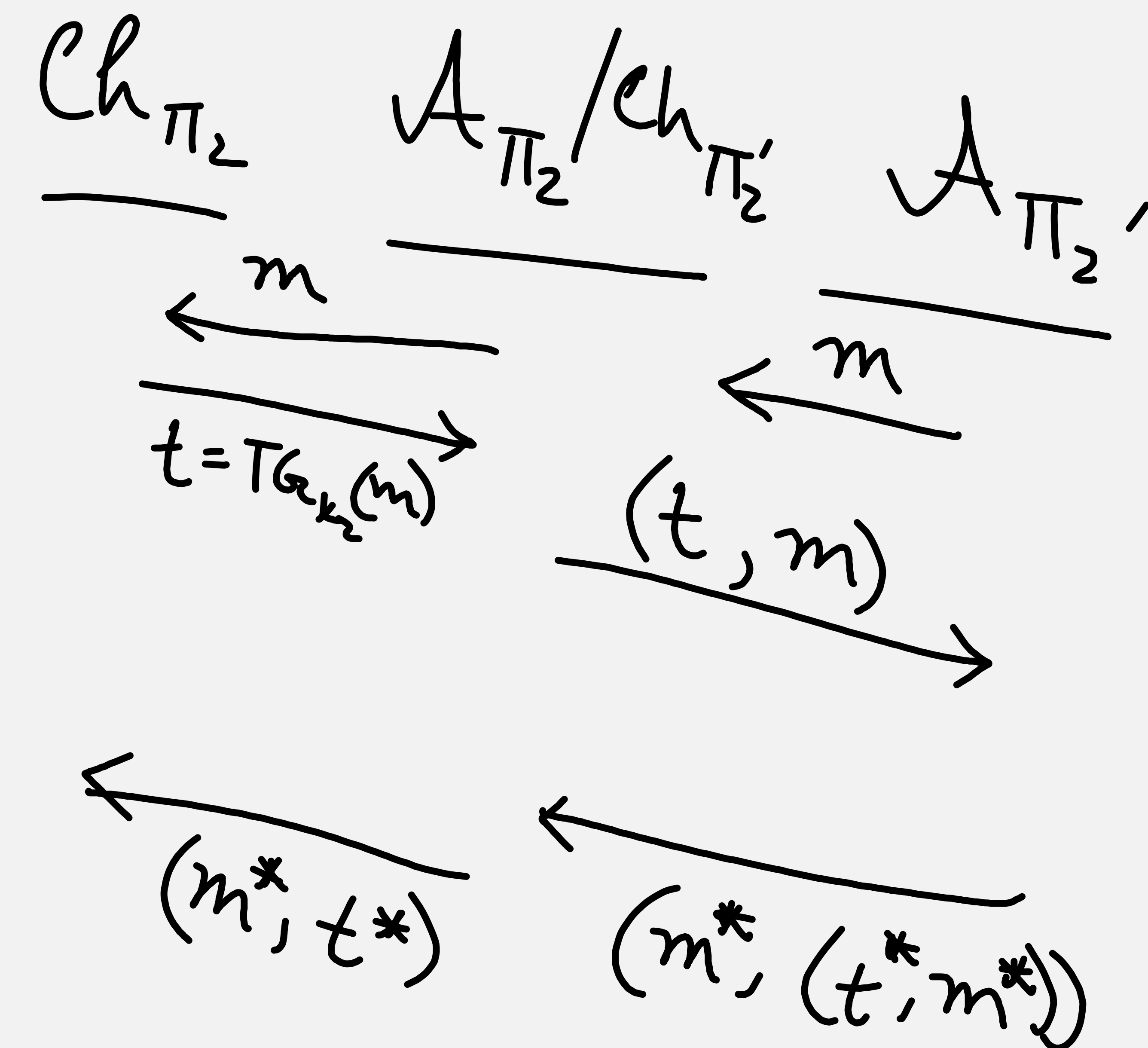
$\left\{ \begin{array}{l} KG \equiv KG' \\ TG'(m) := (TG(m), m) \\ Vrfy'(k, m, (t, m)) := Vrfy(k, m, t) \end{array} \right.$

then

π_2' is also EUF-CMA Secure

$\left\{ \begin{array}{l} \text{If we use } \pi_2' \text{ as EUF-CMA} \\ \text{Secure MAC then Enc \& MAC} \\ \text{is not secure as the complete} \\ \text{message is revealed} \end{array} \right. \Rightarrow \text{IND-CPA attack}$

$\nexists \exists A_{\pi_2'}$ that breaks EUF-CMA of π_2'
 then $\exists A_{\pi_2}$ that breaks EUF-CMA of π_2 .



- Mac-then-Encrypt is also not generically Secure

- Encrypt-then-MAC is generically Secure

