Authenticated Encryption

K_{AM} → A, M common key

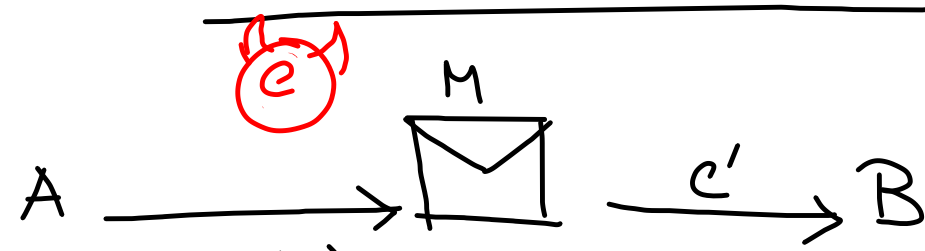
K_{BM} → B, M common key

Motivation:

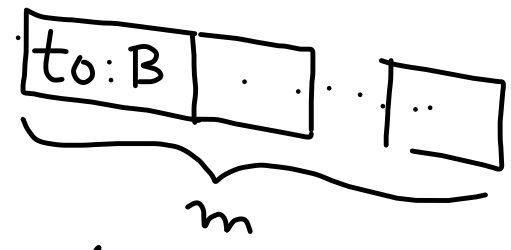
- Medical Test
  - Privacy of the report
  - Authenticity of the report
- Results
  - Result should be only known to the candidate
  - The student should be sure that the marks have been uploaded by respective faculty

Privacy + Authenticity

Requirement of CCA:

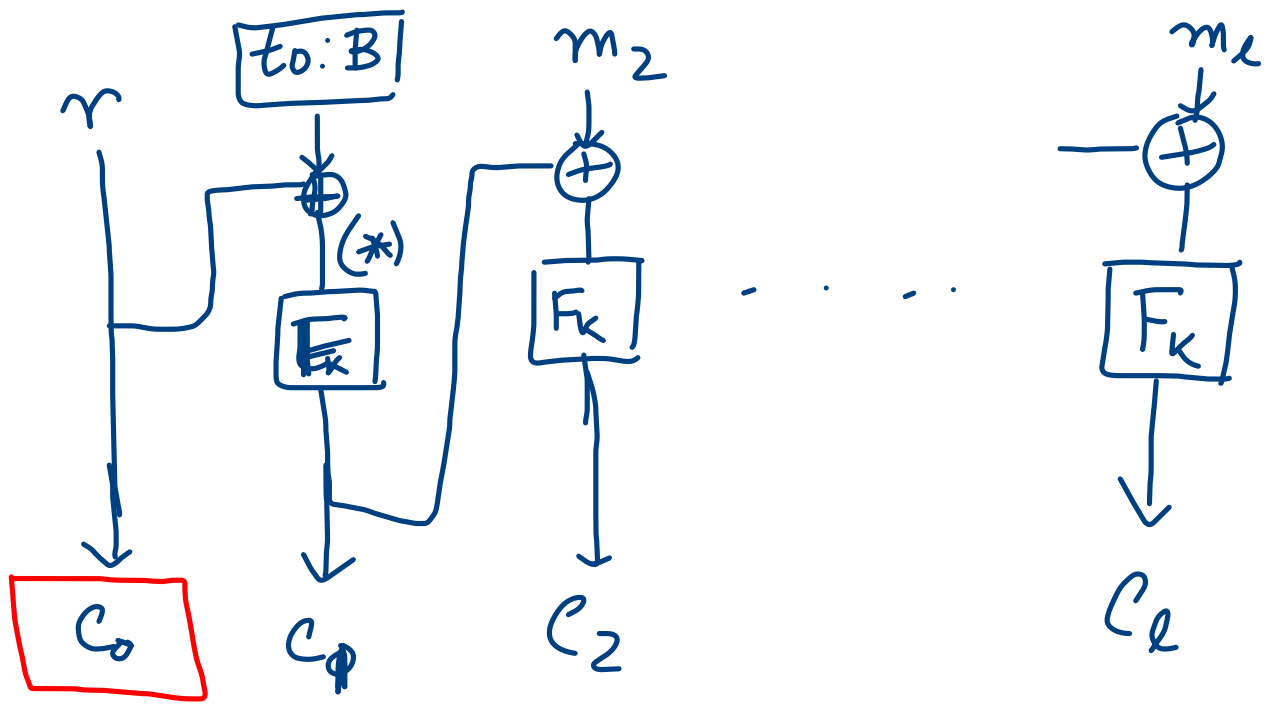


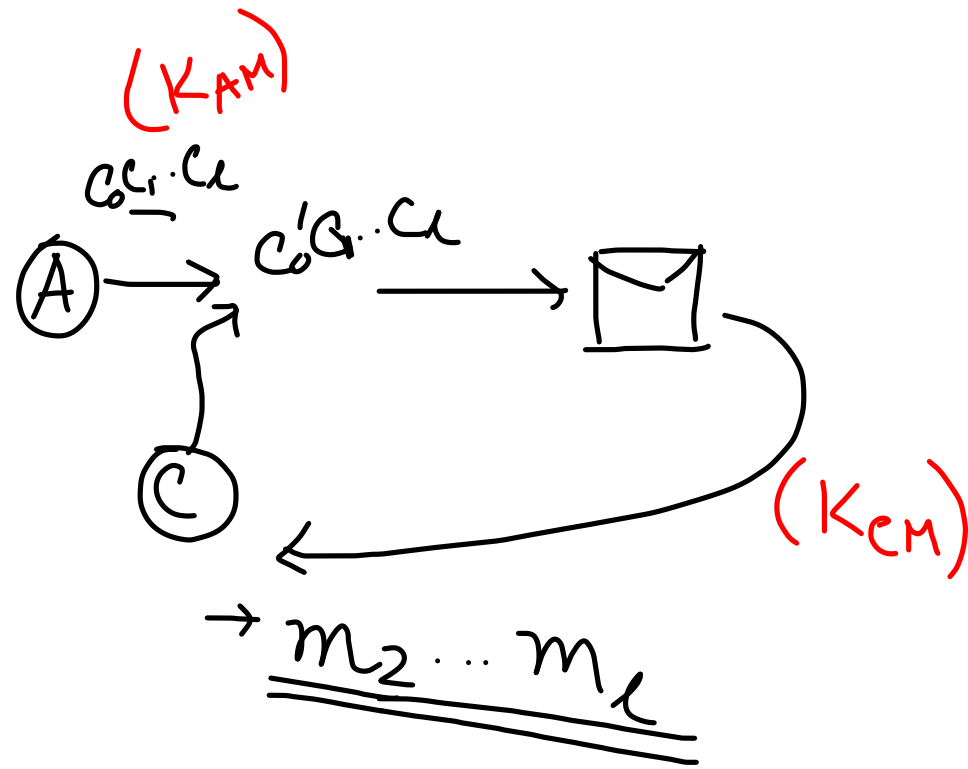
Message format:

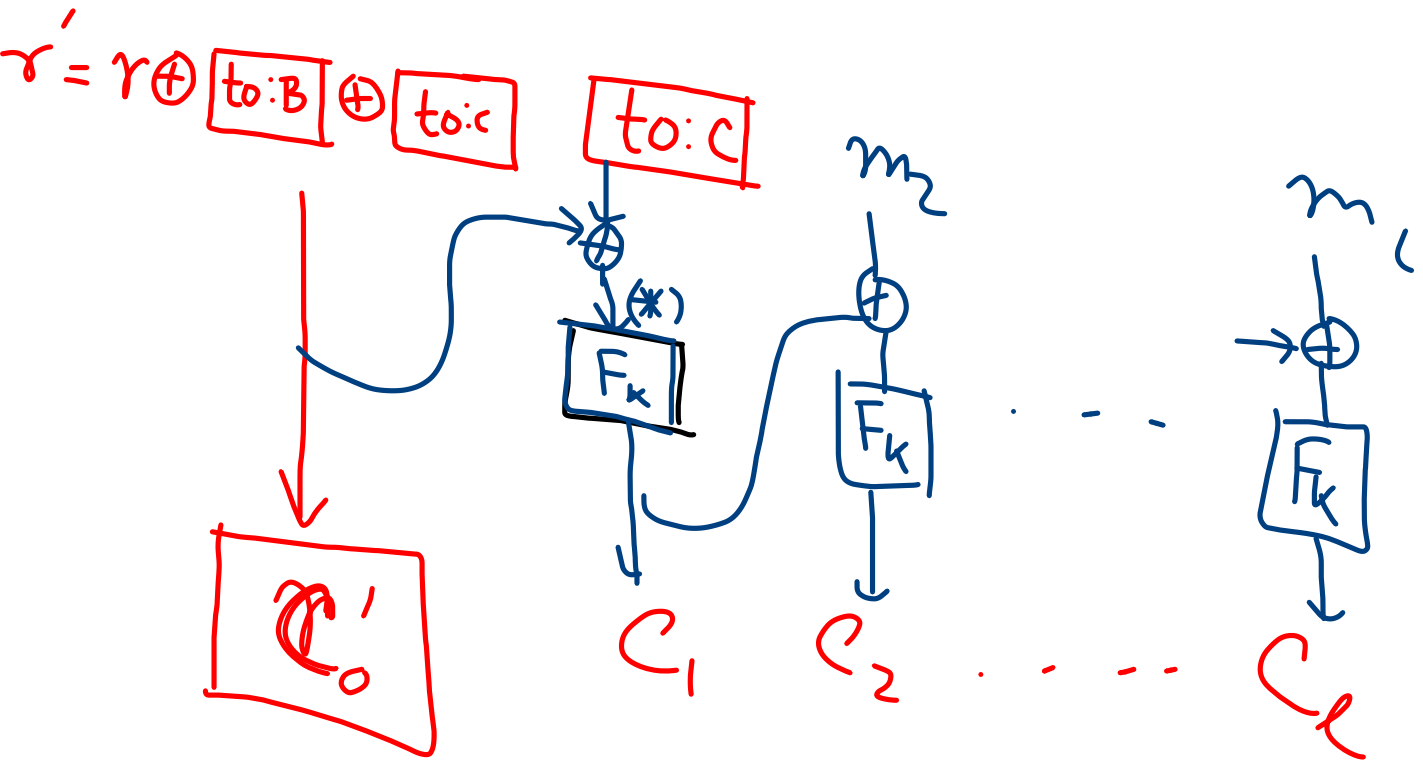


Say, I use randomized CBC (CPA-Secure) Encryption.

↳ NOT Secure


to:B
m_2
m_ℓ
r
(*)
F_k
F_k
F_k
C_0
C_1
C_2
C_ℓ


(K_{AM})
$C_0 C_1 \cdots C_\ell$
$C_0' C_1 \cdots C_\ell$
A
C
(K_{CM})
$\rightarrow m_2 \cdots m_\ell$


$r' = r \oplus$ to:B $\oplus$ to:c
to:C
m_2
m_ℓ
(*)
F_k
F_k
F_k
C_0'
C_1
C_2
C_ℓ

Authenticated Encryption

- Key Gen : $k \xleftarrow{\$} \mathcal{K}$
- Authenticated Encryption : $(c, t) \leftarrow AE_k(m)$
- Verified Decryption : $m / \perp \leftarrow VD_k(c, t)$

Correctness :

$$\left.\begin{array}{l} \forall k, m \\ VD_k(AE_k(m)) = m \end{array}\right\}$$

AE Security

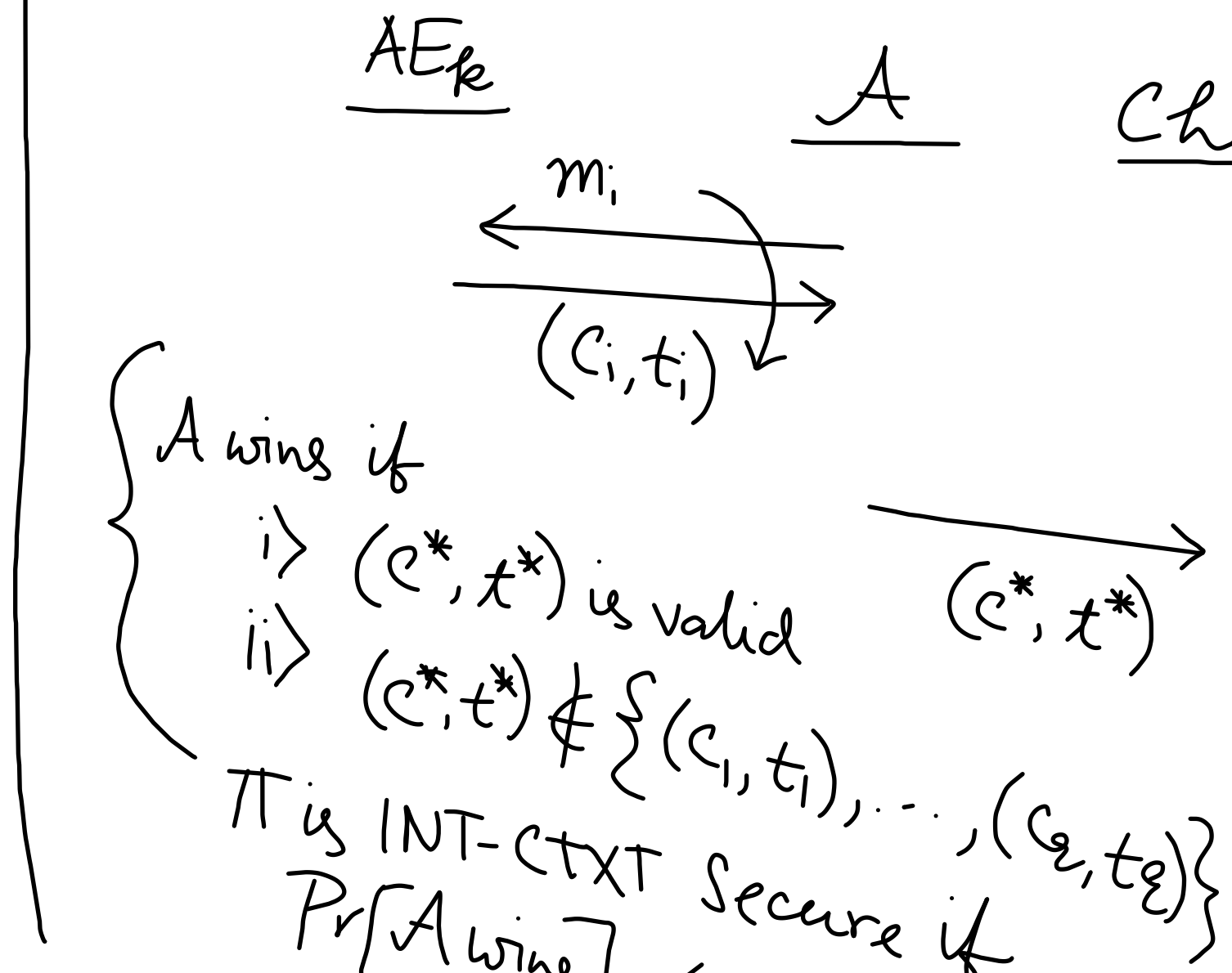
1) Privacy (IND-CPA)
2) Integrity (INT-CTXT)

IND-CPA + INT-CTXT

⇓

IND-CCA

INT-CTXT (Integrity under Ciphertext)



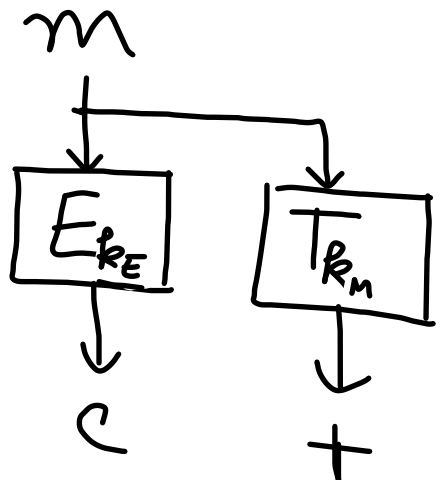
A wins if
i) (c^*, t^*) is valid
ii) $(c^*, t^*) \notin \{(c_1, t_1), \ldots, (c_q, t_q)\}$

Π is INT-CTXT secure if
$Pr[A \text{ wins}] \leq negl(n)$

Generic Constructions

1) Encrypt & MAC (E&M)

$AE_{(k_E, k_M)}(m) \Rightarrow$



$\pi \rightarrow (KG_E, E, D)$ — enc

$\tilde{\pi} \rightarrow (KG_M, T, V)$ — mac

$VD_{(k_E, k_M)}(c, t) \Rightarrow$

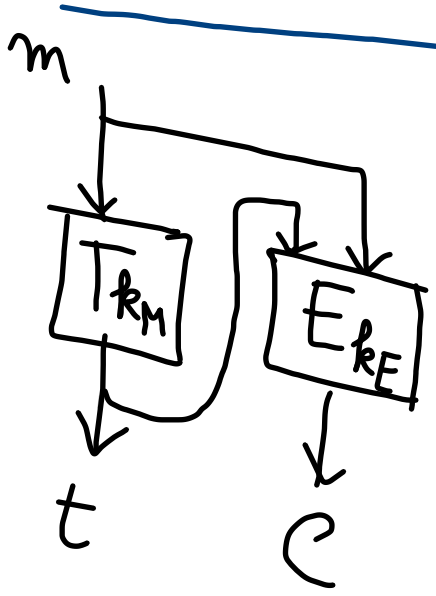
$m := D_{k_E}(c)$

$b = V_{k_M}(m, t)$

if $(b == 1)$ return m

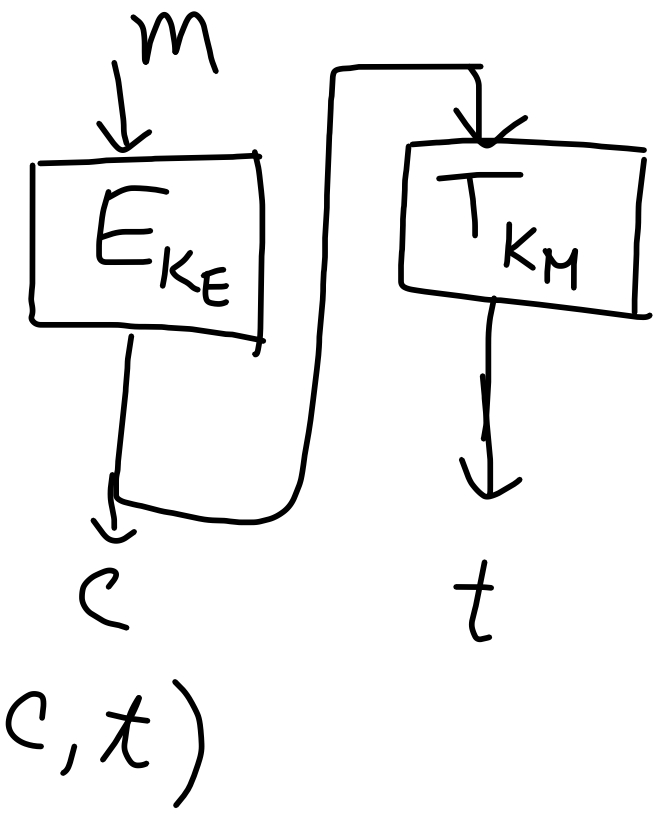
else return $\perp$

2) MAC then Encrypt (MtE)



return c

3) Encrypt then MAC (EtM)



If verified then only execute decryption

return (c, t)

Security of Generic Constructions

1) E & M is not generically secure

2) M t E is not generically secure

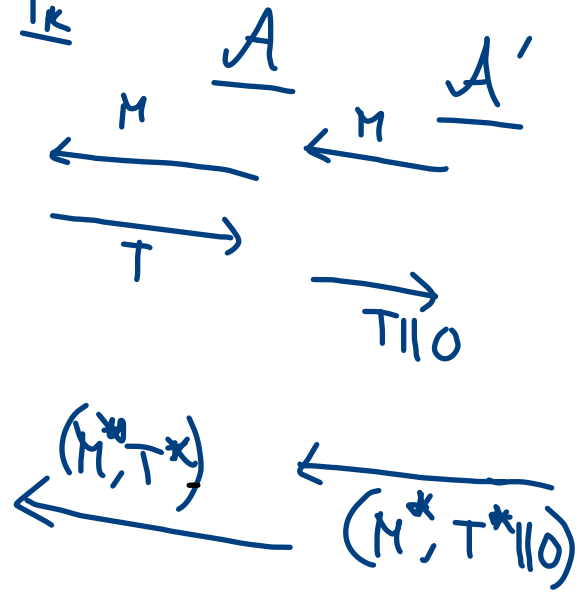
3) E t M is generically Secure:

If Π is IND-CPA & Π is EUF-CMA then E t M gives Secure AE.

$\Pi = (KG, TG, Vrfy)$

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

Thm: If Π is EUF-CMA Secure then Π' is EUF-CMA.



MAC	Vrfy
$T := F_k(M)$ $\|\|M$	

MAC'

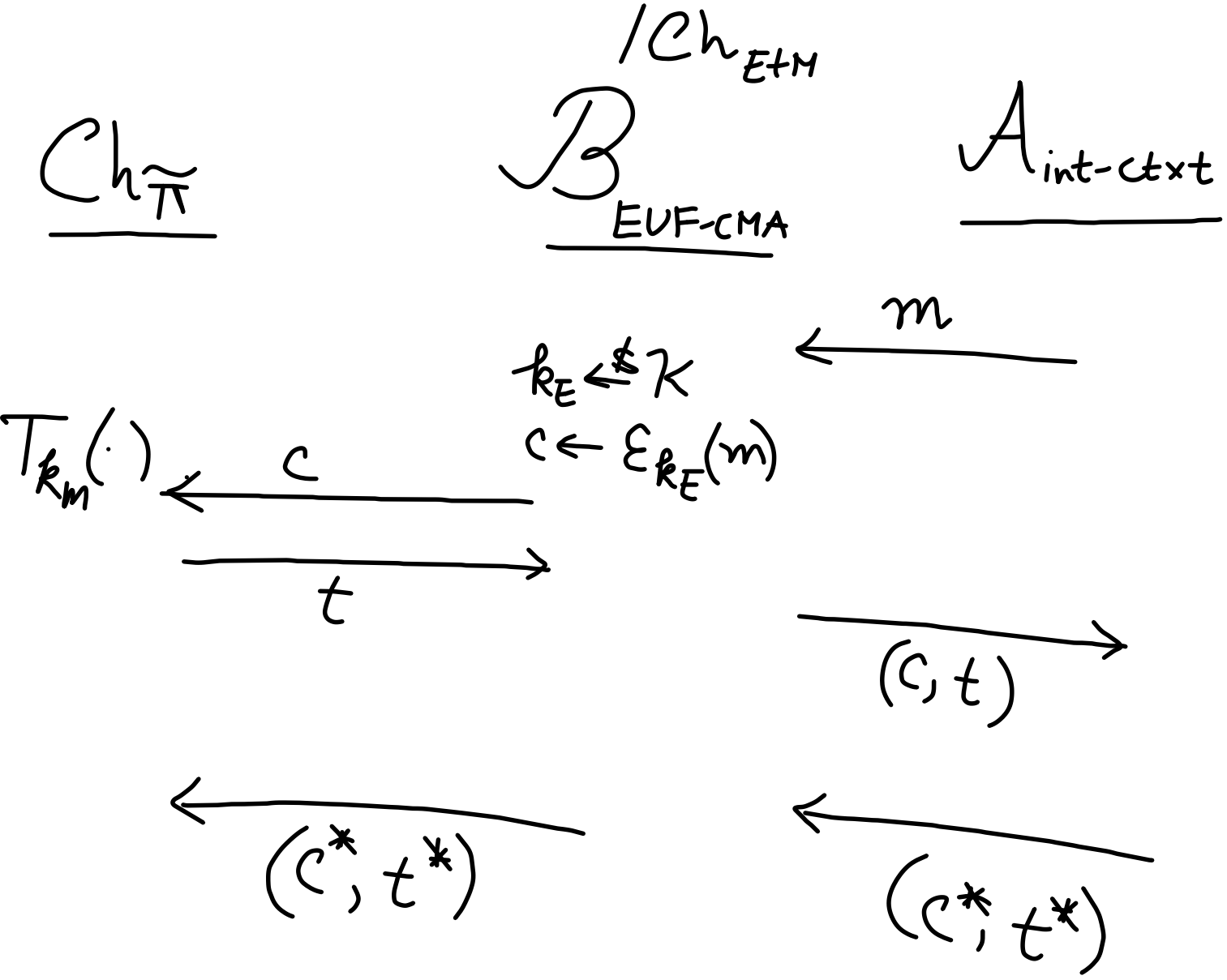
$T' = F_k(M) \| M$

Vrfy'

$T'' \leftarrow chop(T')$

$Vrfy(M, T'')$ | Removes last-bit

IND-CPA + EUF-CMA $\Rightarrow$ INT-CTXT

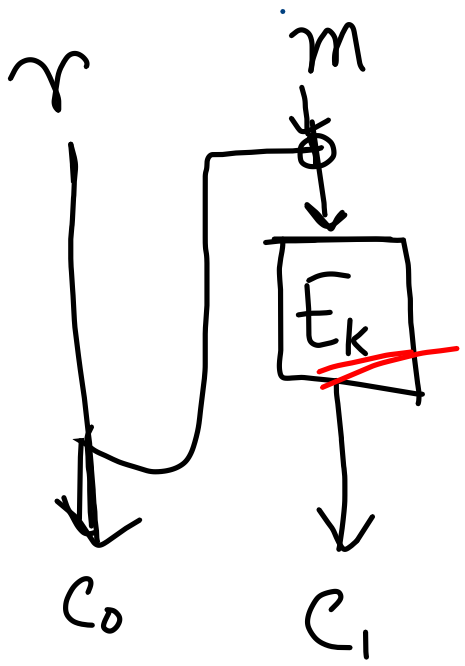


$$\Pr[\mathcal{A}_{int\text{-}ctxt} \text{ wins}]$$

$$= \Pr[\mathcal{B}_{EUF\text{-}CMA}]$$

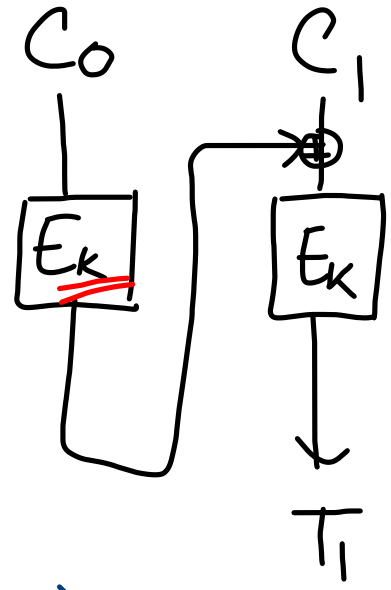
Interesting Problems

(1) Interesting Problems



Fixed-length CBC encryption

(IND-CPA)



fixed length MAC

(EUF-CMA Secure)

$E_k(C_0 \oplus \overbrace{m}^{=0^n}) = C_1$

$E_k(E_k(C_0) \oplus C_1) = T_1$

$E_k(C_1 \oplus C_1) = T_1$

$\Rightarrow E_k(0) = T_1$

$E_k(C_0) = C_1$

$(0,0) \rightarrow (0, T_1)$

$\downarrow$

T_1

$(0, T_1, T_1)$

$\Downarrow$

INT-CTXT Attack

Encryption and MAC key should be independent

CPA-secure

② $(r, C_1) \leftarrow CBC_{k_E}(m)$

$T_1 \leftarrow MAC_{k_E}(C_1)$

EUF-CMA secure

return (r, C_1, T_1)

AE

- Prove this is insecure.
- Why?