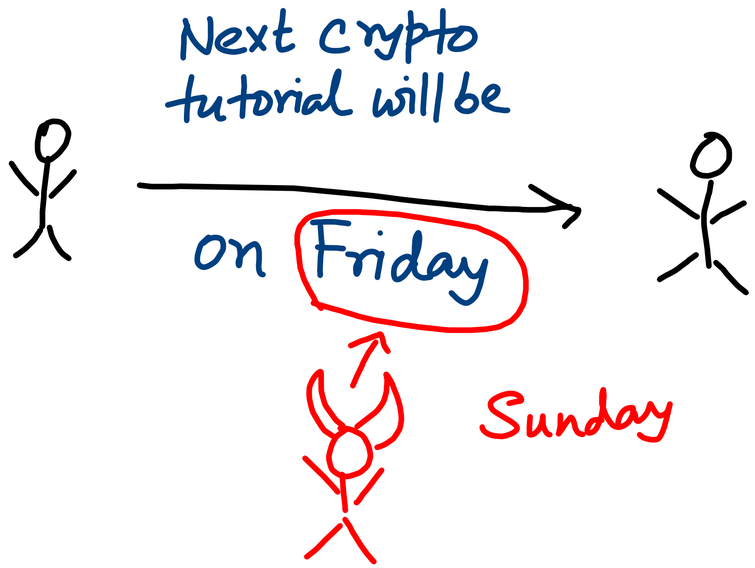
Message Authentication Code (MAC)

M=



- No privacy is required
- Integrity / Authenticity is required.

$MAC = (KG, TG, Vrfy)$

$k \leftarrow KG(1^n)$

$t \leftarrow TG(k, m)$

$T/\perp \leftarrow Vrfy(k, (m, t))$

$T = 1$

$\perp = 0$

TG → Tag Generation

→ Verify algo

$\perp$ → abort or unsuccessful

T → top or successful

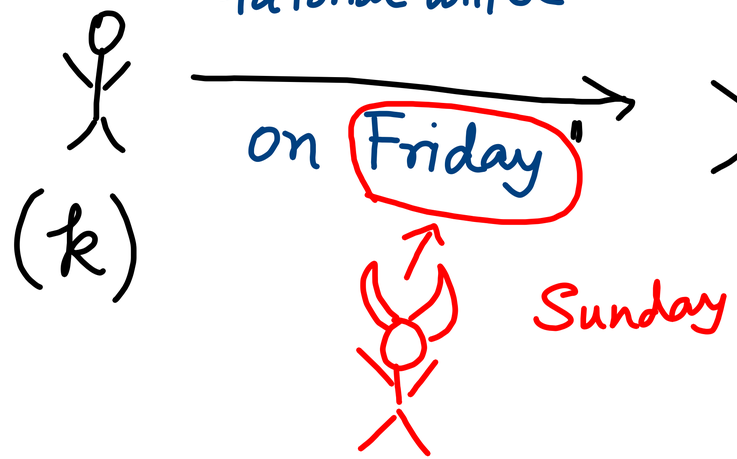
```
Vrfy(k, (m,t))
{
        t' ← TG(k,m)
        if (t == t')
        else   return T/1
}                return ⊥/0
```

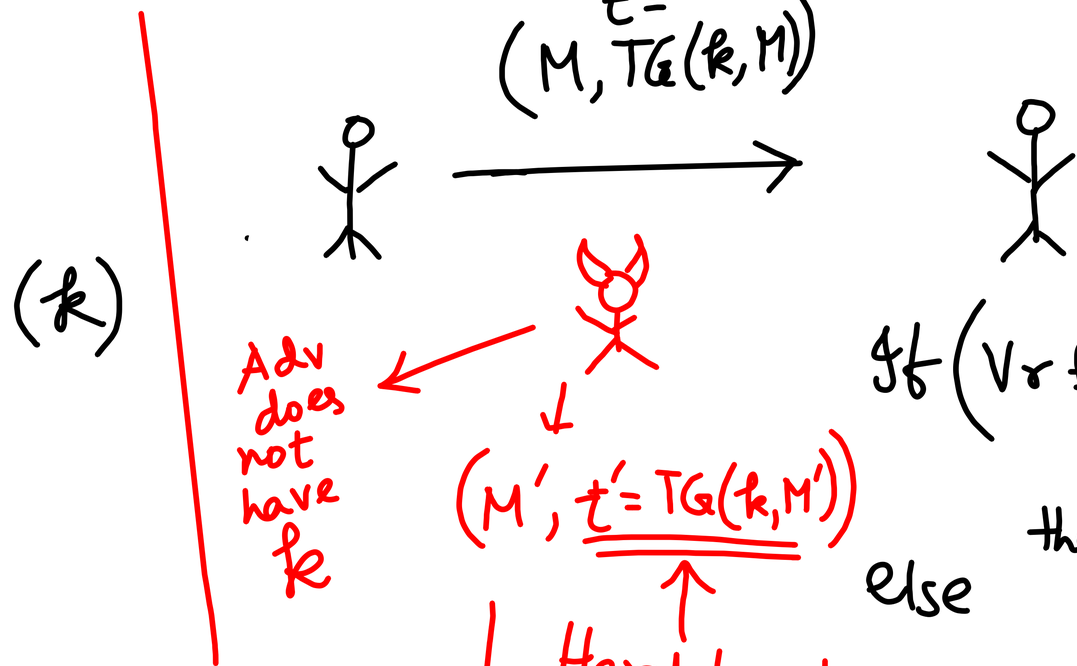
Message Authentication Code

(MAC)

MAC = (KG, TG, Vrfy)

M = "Next crypto tutorial will be on Friday"





If (Vrfy (k, (m, t)) == T/1) then read M

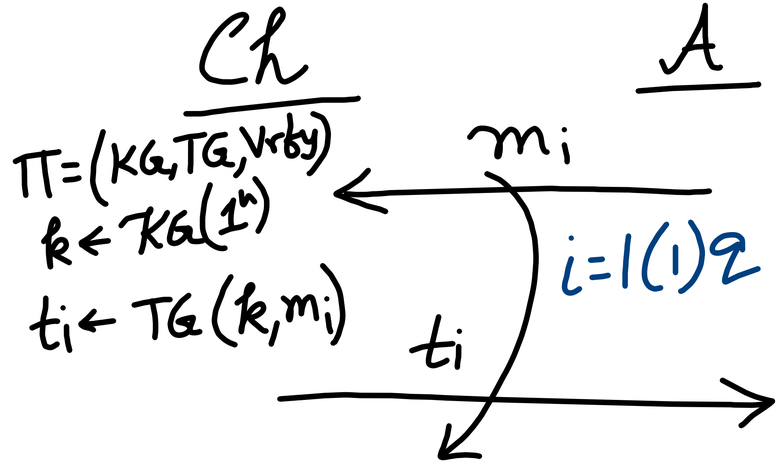
else

There are some modification

MAC - Security

EUF → existential unforgeability
CMA → Chosen message attack

Existential Unforgeability



A forges if

(fresh) → (i) $m^* \notin \{m_1, \ldots, m_Q\}$

(valid) → (ii) $Vrfy(k, (m^*, t^*)) = T/1$

$MAC_\pi(A) = 1$ if A forges

$\pi \rightarrow$ EUF-CMA Secure

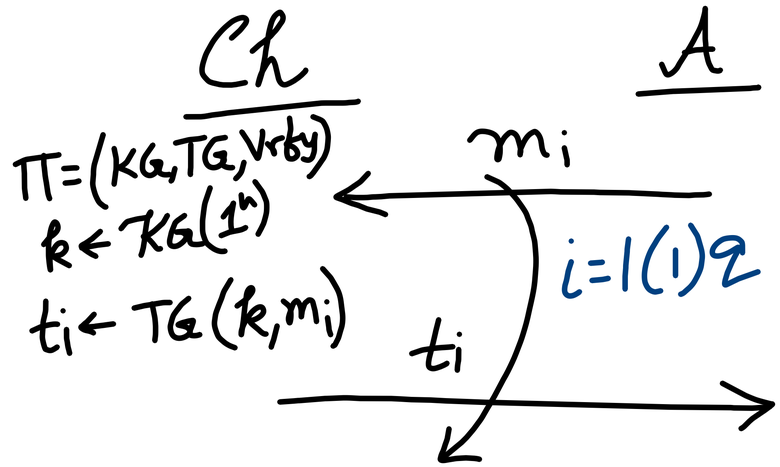
if $Pr[MAC_\pi(A) = 1] \leq negl(n)$

$\forall$ PPT A.

MAC- Security

SUF → Strong unforgeability
CMA → Chosen message attack

Strong Unforgeability



A forges if

(fresh) → (i) $(m^*, t^*) \notin \{(m_1, t_1), \ldots, (m_Q, t_Q)\}$

(valid) → (ii) $Vrfy(k, (m^*, t^*)) = T/1$

$MAC_\pi(A) = 1$ if A forges

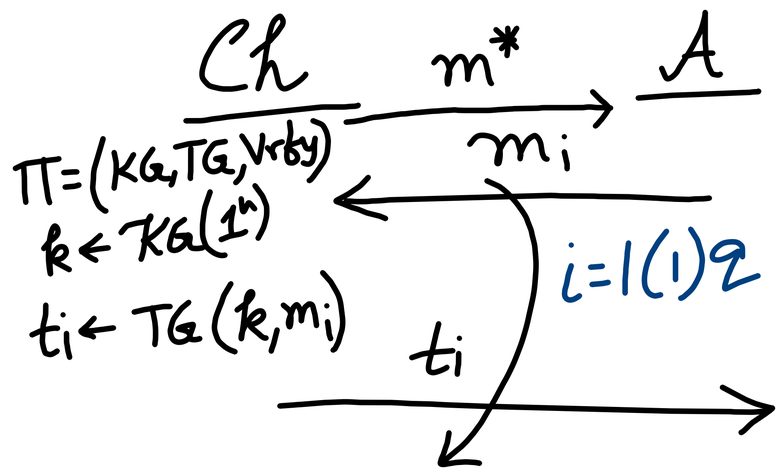
$\pi \rightarrow$ SUF-CMA Secure if $Pr[MAC_\pi(A) = 1] \leq negl(n)$

$\forall$ PPT A.

MAC - Security

UUF → Universal unforgeability
CMA → Chosen message attack

Universal Unforgeability



A forges if

(fresh) → (i) $m^* \notin \{m_1, \ldots, m_Q\}$

(valid) → (ii) $Vrfy(k, (m^*, t^*)) = T/1$

$MAC_\Pi(A) = 1$ if A forges

$\Pi \rightarrow$ UUF-CMA Secure

if $Pr[MAC_\Pi(A) = 1] \leq negl(n)$

$\forall$ PPT A.

MACs for Fixed-length Message

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

$m \in \{0,1\}^n$

$F \to PRF$

$KG \to \quad k \xleftarrow{\$} \{0,1\}^k$

$TG \to \quad t \leftarrow F_k(m)$

$Vrfy \to \quad Vrfy(k, (m', t'))$

$t'' \leftarrow F_k(m')$

if $(t' == t'')$ then 1

else 0

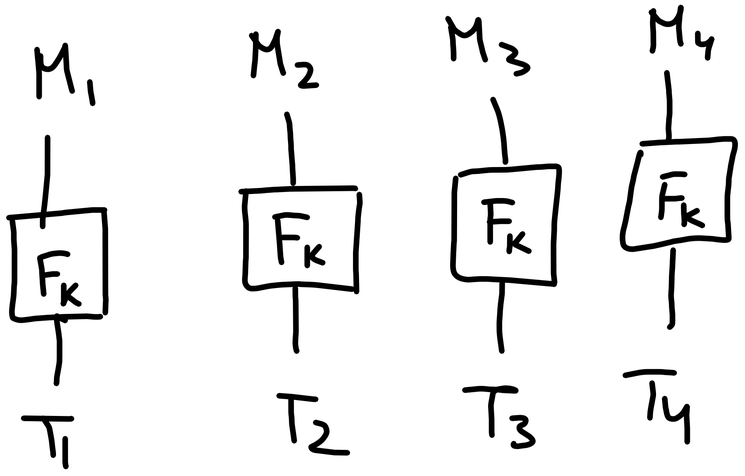
Thm

If F is PRF then

Π is EUF-CMA Secure

Try Reduction

MACs for Variable length Messages



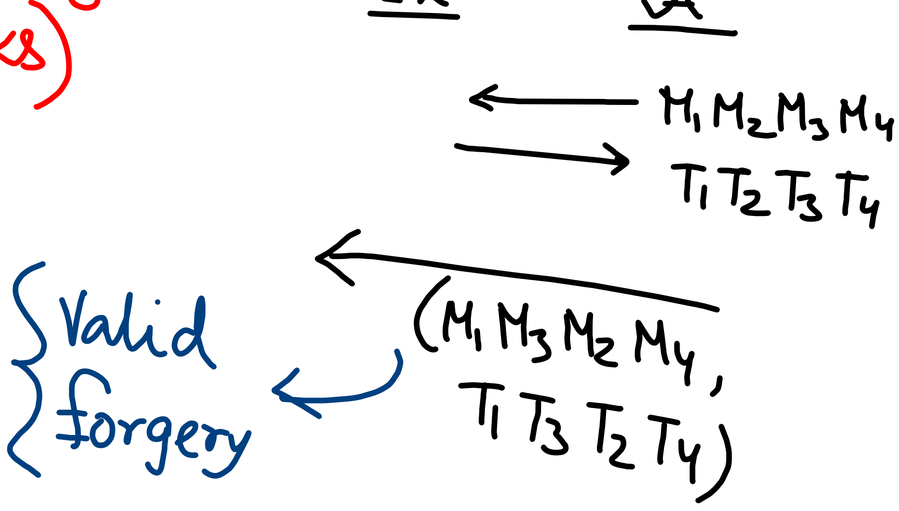
$TG(k, M_1 \| M_2 \| M_3 \| M_4)$

$= (T_1 \| T_2 \| T_3 \| T_4)$

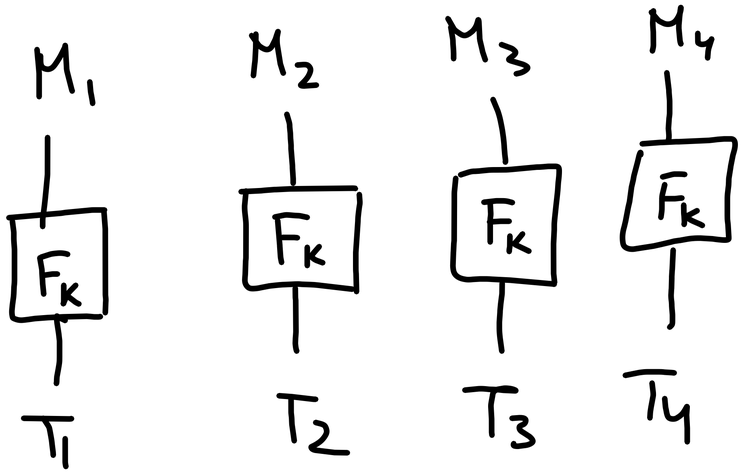
Is it EUF-CMA Secure?

No

(Re-arrange the blocks)



MACs for Variable length Messages



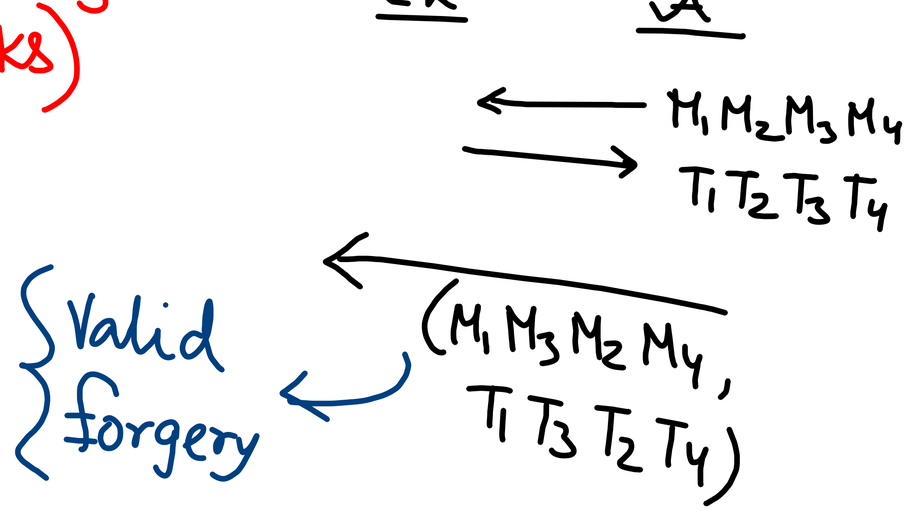
$TG(k, M_1 || M_2 || M_3 || M_4)$

$= (T_1 || T_2 || T_3 || T_4)$

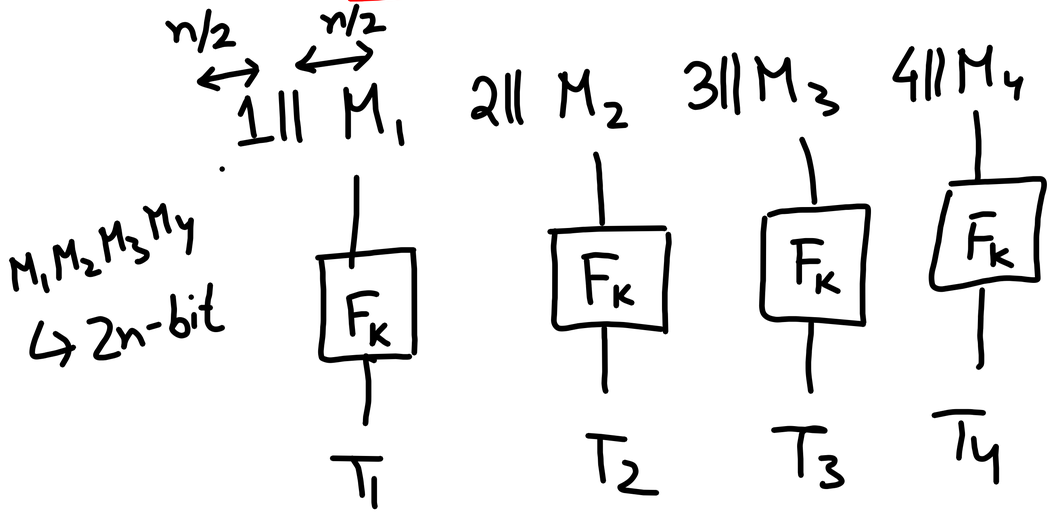
Is it EUF-CMA Secure?

No

(Re-arrange the blocks)



MACs for Variable length Messages

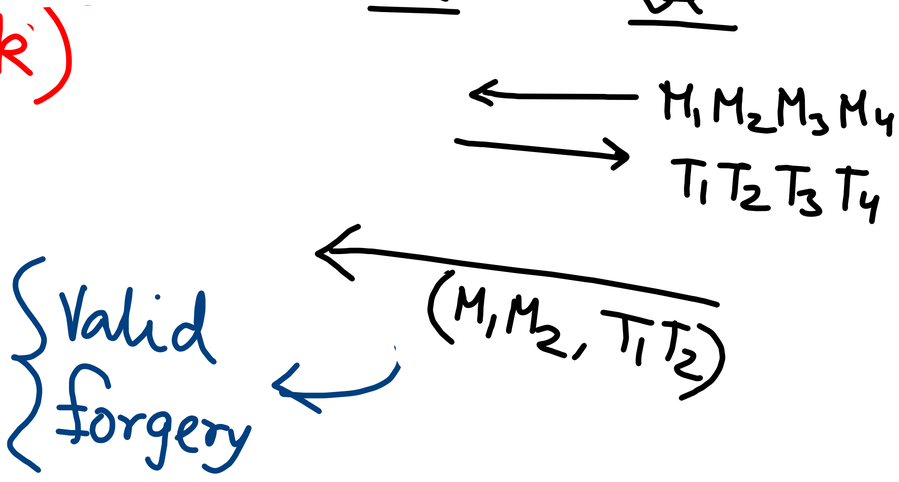


$$TG(k, M_1 \| M_2 \| M_3 \| M_4)$$
$$= (T_1 \| T_2 \| T_3 \| T_4)$$

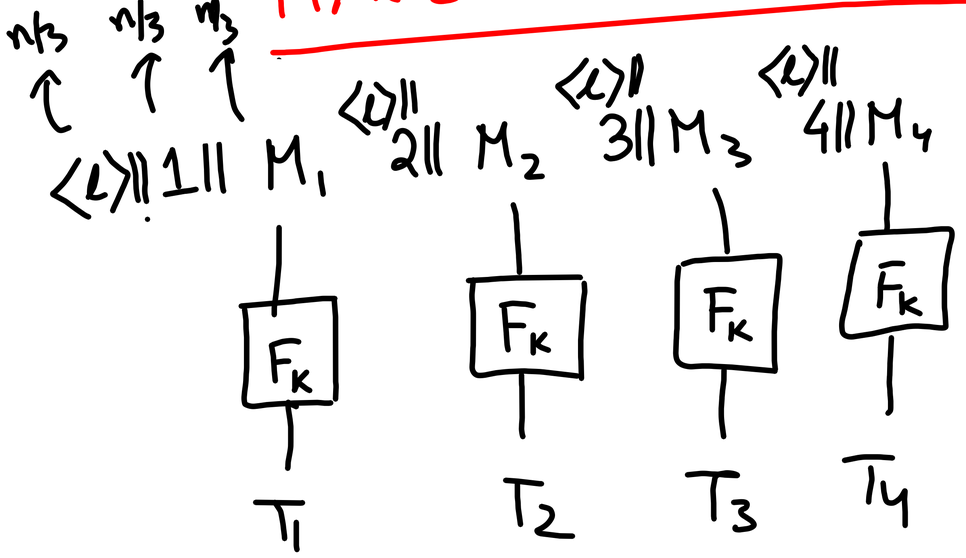
Is it EUF-CMA Secure?

No

(Truncation Attack)



MACs for Variable length Messages



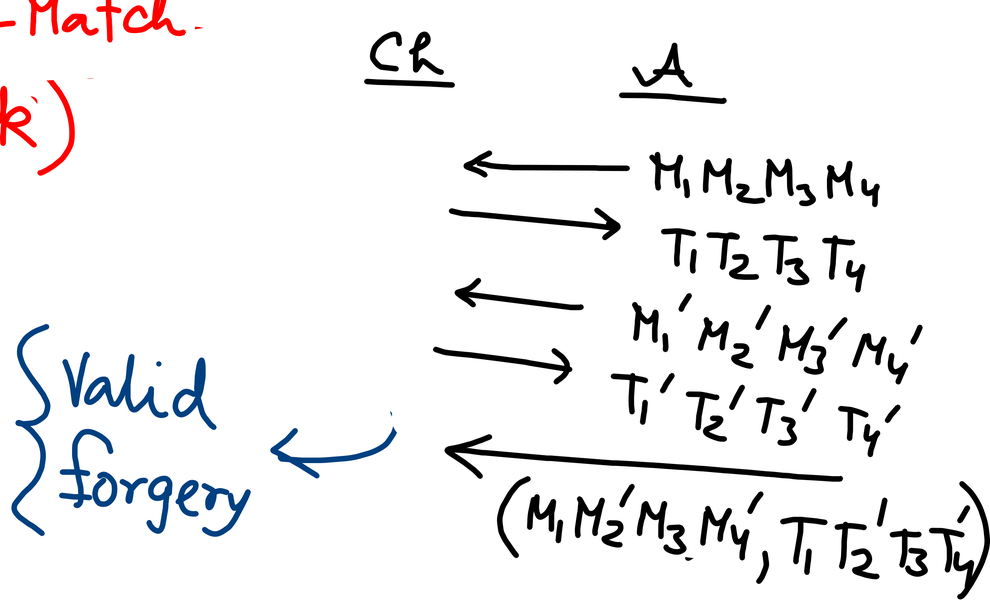
$TG(k, M_1 \| M_2 \| M_3 \| M_4)$

$= (T_1 \| T_2 \| T_3 \| T_4)$

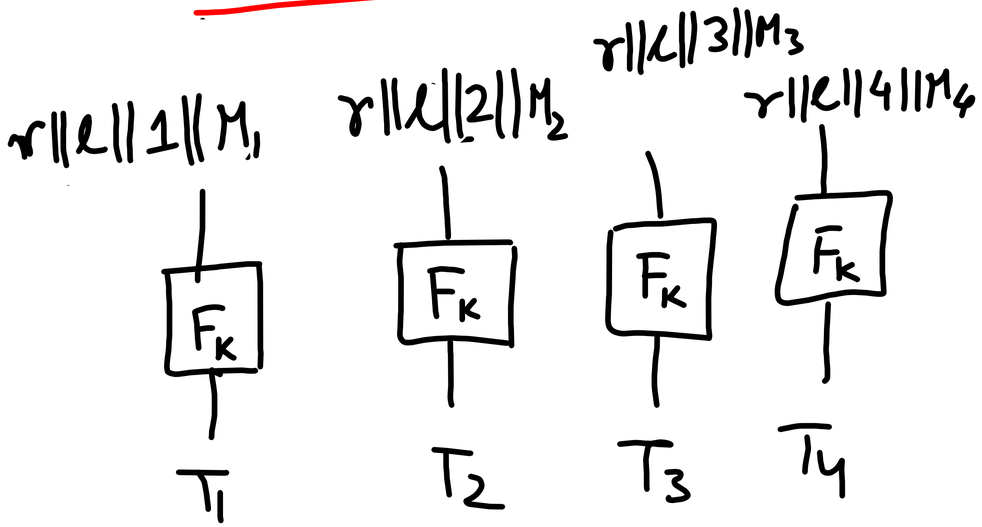
Is it EUF-CMA Secure?

No

(Mix-&-Match Attack)



MACs for Variable length Messages



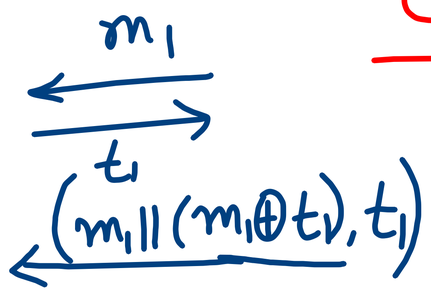
$TG(k, M_1 || M_2 || M_3 || M_4)$

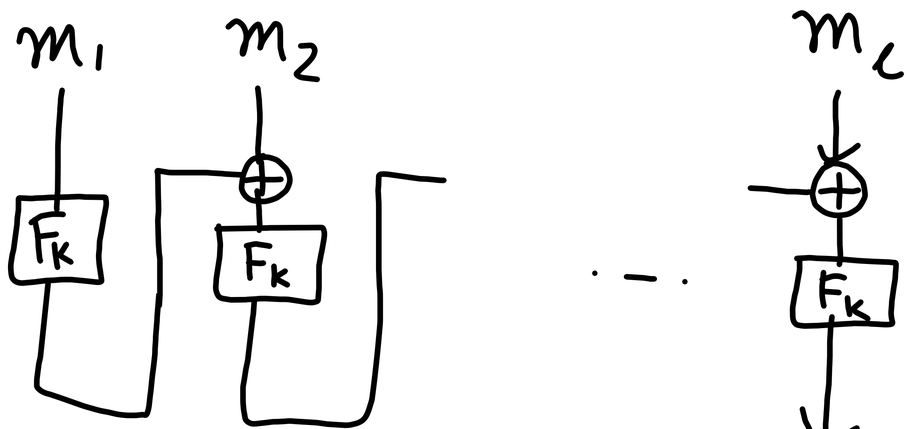
$= (r || T_1 || T_2 || T_3 || T_4)$

Is it EUF-CMA Secure?

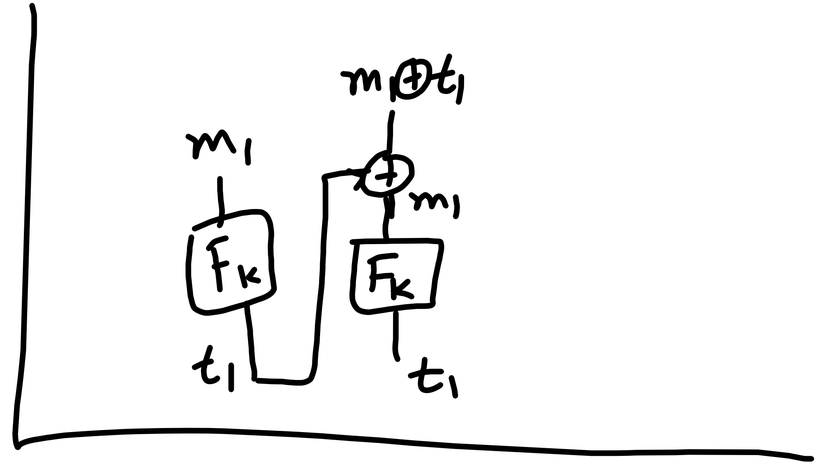
Yes $\Rightarrow$ $\dfrac{q^2}{2^{n/4}}$

CBC- MAC (Fix length)





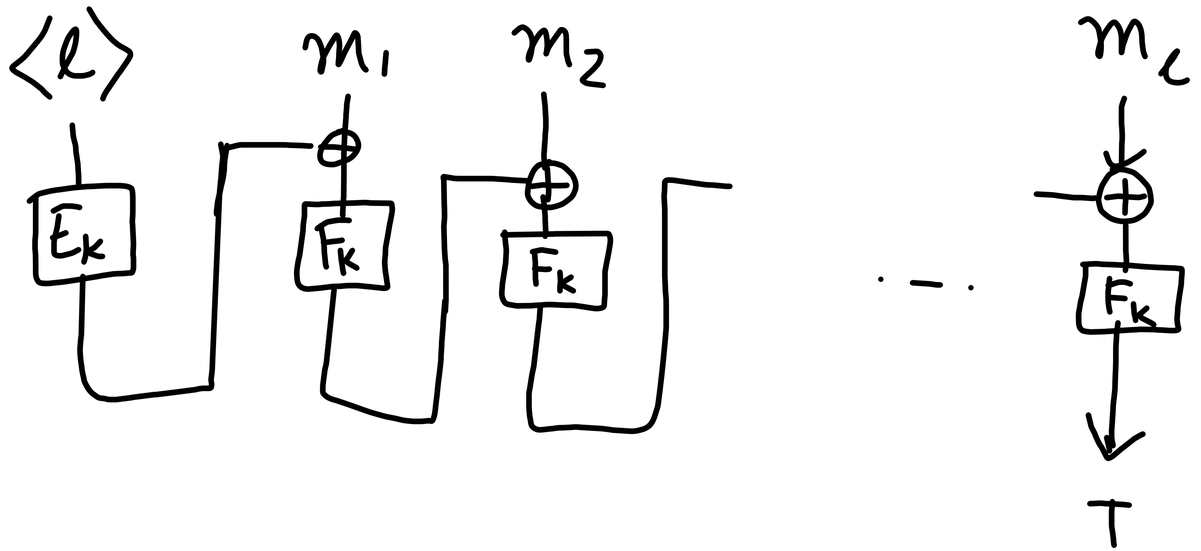
If ℓ is not fixed → Attack



$\ell \rightarrow$ fixed

Secure

CBC-MAC (Variable length)



ℓ → fixed

⇐ Secure

Recap (Last class)

Counter Mode

$$\Pr[\text{BAD}] \leq \sum_{i=1}^{q(n)} \frac{l_i \cdot l}{2^n} \Rightarrow \leq \sum_{i=1}^{q(n)} \frac{l_i + l}{2^n} = \frac{2\, q(n)\, l_{max}}{2^n}$$

↳ $\Pr\left[\text{PrivK}^{\text{ind-cpa}}_{\text{CTR}}(A) = 1\right] \leq \frac{q(n) \cdot l_{max}^2}{2^n} + \frac{1}{2}$

$$\Downarrow$$

$$\frac{2 \cdot q(n) \cdot l_{max}}{2^n} + \frac{1}{2}$$