
Lecture 4 – Message authentication, UF-CMA, CBC-MAC, CMAC

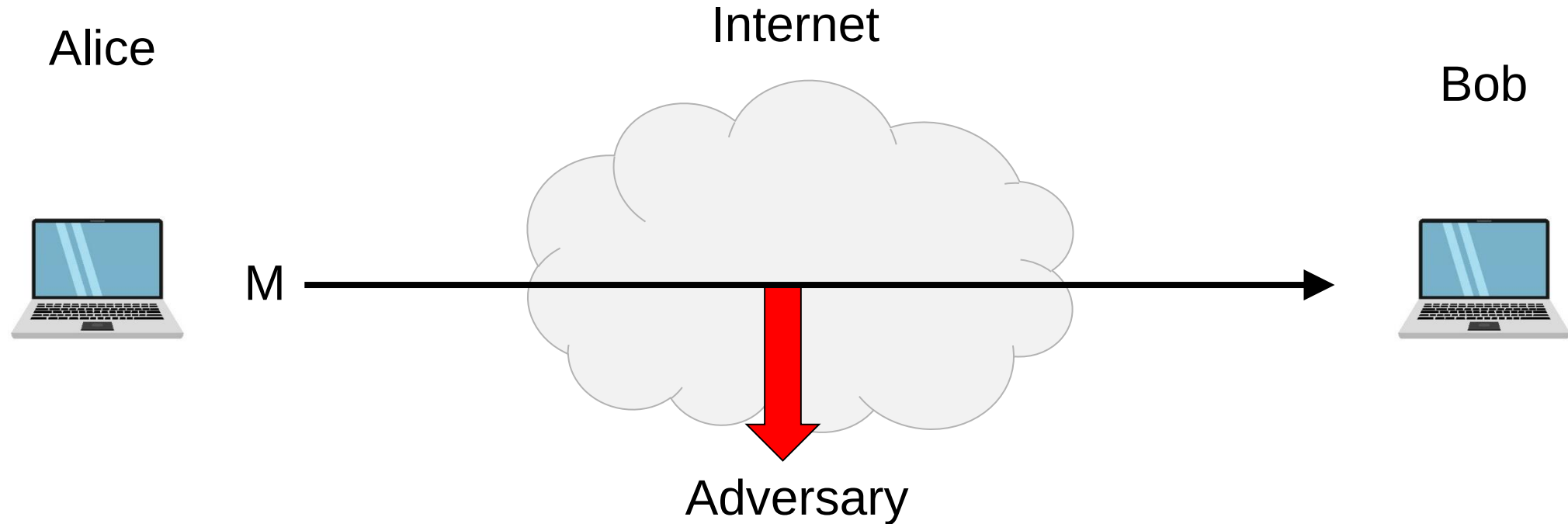
TEK4500

18.09.2024

Håkon Jacobsen

hakon.jacobsen@its.uio.no

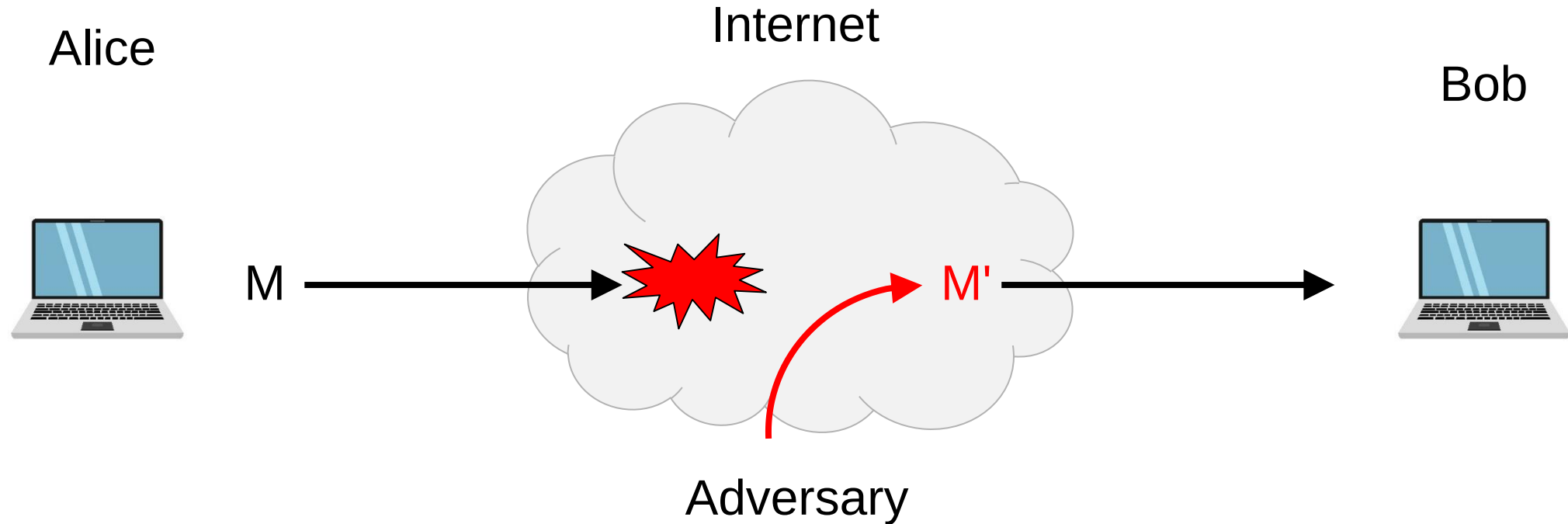
What is cryptography?



Security goals:

- **Data privacy:** adversary should not be able to read message M
- **Data integrity:** adversary should not be able to modify message M
- **Data authenticity:** message M really originated from Alice

What is cryptography?



Security goals:

- **Data privacy:** adversary should not be able to read message M
- **Data integrity:** adversary should not be able to modify message M
- **Data authenticity:** message M really originated from Alice

Basic goals of cryptography

	Message privacy	Message integrity / authentication
Symmetric keys	Symmetric encryption	Message authentication codes (MAC)
Asymmetric keys	Asymmetric encryption (a.k.a. public-key encryption)	Digital signatures

Motivation

- Goal: *integrity*, not privacy
- Examples:
 - Protecting OS system files against tampering
 - Browser cookies stored by web servers
 - Control signals in network management

Encryption $\neq$ integrity

CTR. Enc($K, \cdot$)



0110100 1110 100101100110



"Send Bob \$10"

1001010 1010 000000001010

1111110 0100 **0110**01101100

CTR. Dec($K, \cdot$)



1111110 0100 **0110**01101100



0110100 1110 100101100110

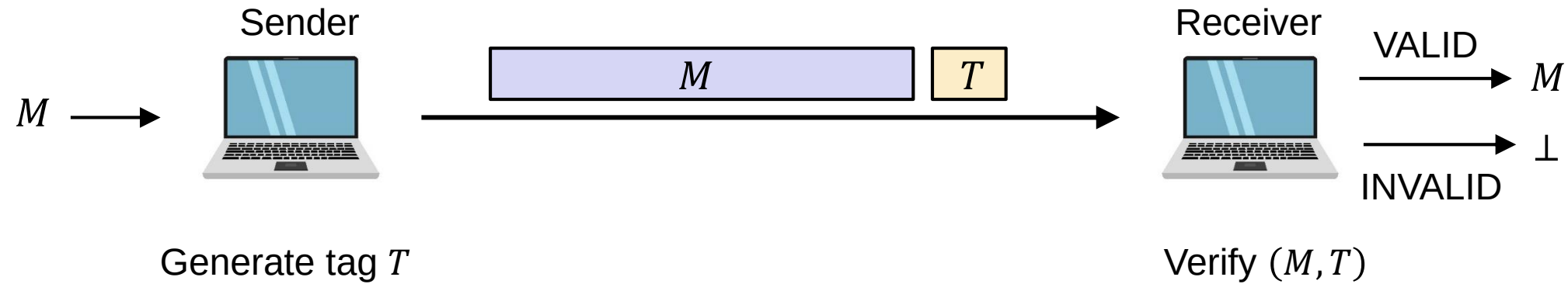
=

1001010 1010 **1111**00001010

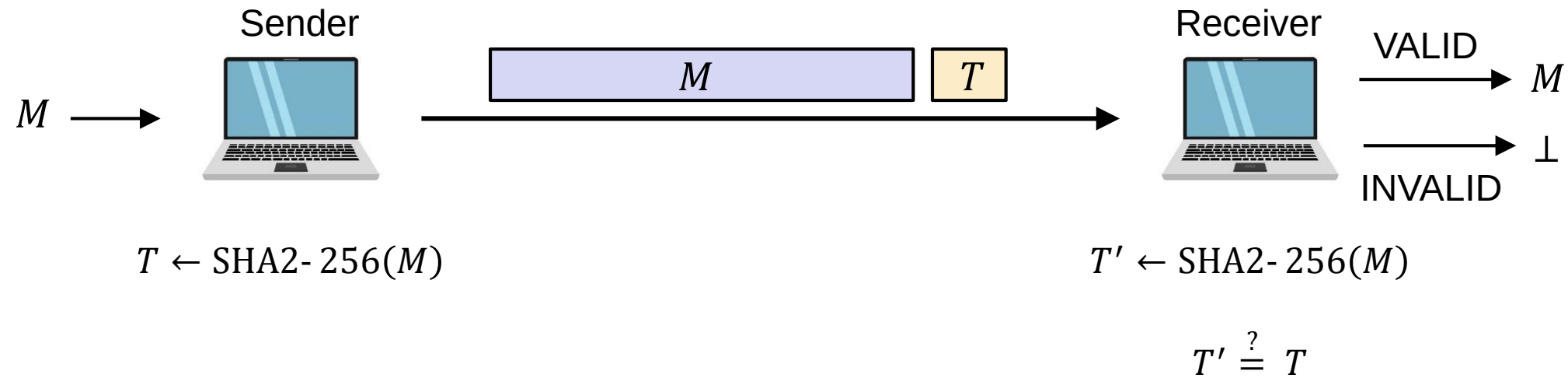
"Send Bob **\$3850**"



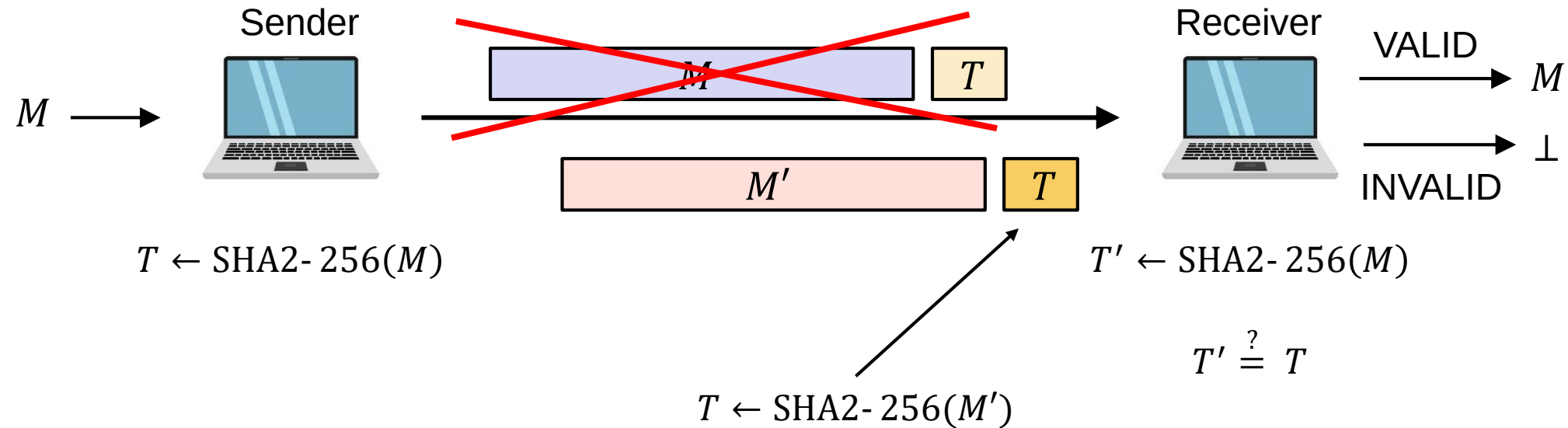
Message authentication – idea



Message authentication – idea



Message authentication – idea



Message authentication schemes – syntax

A **message authentication scheme** is a triple $\Sigma = (\text{KeyGen}, \text{Tag}, \text{Vrfy})$ of algorithms:

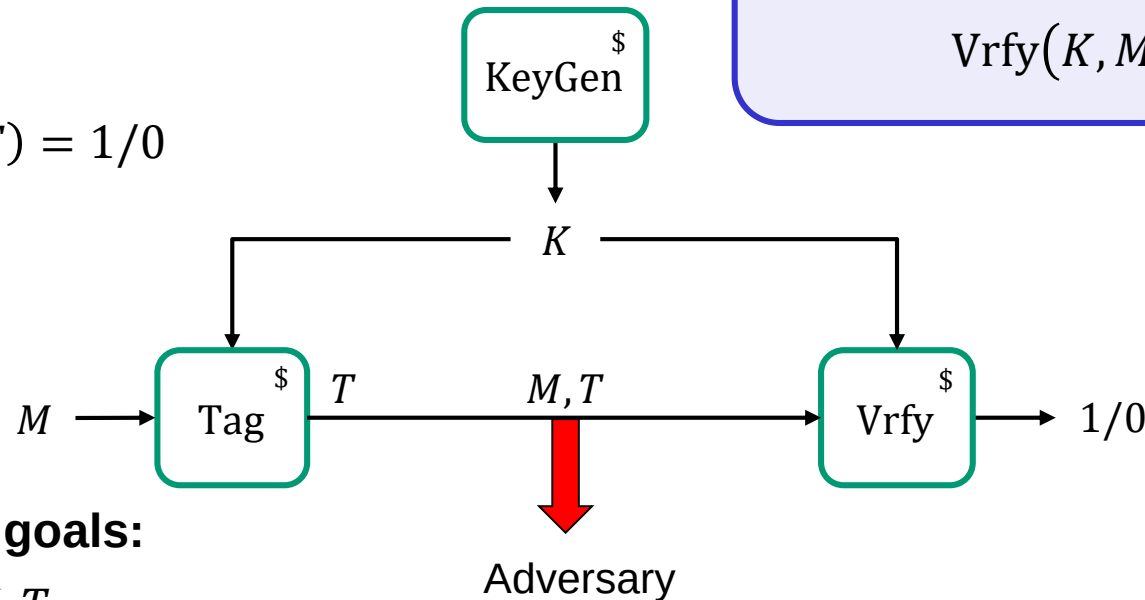
$$\text{Tag} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{T}$$

$$\text{Tag}(K, M) = \text{Tag}_K(M) = T$$

$$\text{Vrfy} : \mathcal{K} \times \mathcal{M} \times \mathcal{T} \rightarrow \{0,1\}$$

$$\text{Vrfy}(K, M, T) = \text{Vrfy}_K(M, T) = 1/0$$

Correctness: $\forall K \xleftarrow{\$} \text{KeyGen}$ and $\forall M \in \mathcal{M}$:

$$\text{Vrfy}(K, M, \text{Tag}(K, M)) = 1$$


Possible integrity security goals:

- Hard to recover K from M, T
- Hard to **forge** T for a specific message M
- Hard to forge T for *any* M
- Hard to forge T for any chosen M after seeing valid tags on (chosen) $M_1, M_2, \dots$ first

UF-CMA – Unforgability against chosen-message attacks

Exp_Σ^{uf-cma}(A)

1. $K \xleftarrow{\$} \Sigma.\text{KeyGen}$
2. $\mathcal{S} \leftarrow []$
3. $\text{forge} \leftarrow 0$
4. $A^{\text{TAG}(\cdot), \text{VF}(\cdot, \cdot)}$
5. **return** forge

TAG(M)

1. $T \leftarrow \Sigma.\text{Tag}(K, M)$
2. $\mathcal{S}.\text{add}(M)$
3. **return** T

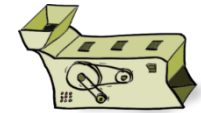
VF(M, T)

1. $d \leftarrow \Sigma.\text{Vrfy}(K, M, T)$
2. **if** $d = 1$ **and** $M \notin \mathcal{S}$ **then:**
3. $\text{forge} \leftarrow 1$
4. **return** d



Challenger

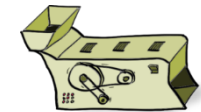
Tag(K, ·)



$M_1, M_2, \dots$

$T_1, T_2, \dots$

Vrfy(K, ·, ·)



$(M'_1, T'_1), (M'_2, T'_2), \dots$

$1/0, 1/0, \dots$

Adversary wins if:

- one (M'_i, T'_i) is *valid*, i.e., $\text{Vrfy}(K, M'_i, T'_i) = 1$
- and M'_i is *fresh*, i.e., $M'_i \notin \{M_1, M_2, \dots\}$

Definition: The **UF-CMA advantage** of an adversary A is

$$\text{Adv}_{\Sigma}^{\text{uf-cma}}(A) = \Pr[\text{Exp}_{\Sigma}^{\text{uf-cma}}(A) \Rightarrow 1]$$

Properties of UF-CMA definition

- UF-CMA security implies:
 - Hard to recover K
 - Hard forge a *specific* message chosen by the adversary
 - Tag lengths must be *long enough*!
 - Suppose $|T| = 10$; then

$$\mathbf{Adv}_{\Sigma}^{\text{uf-cma}}(\text{"Guess } T\text{"}) = \frac{1}{2^{10}} \approx \frac{1}{1000}$$

- Does *not* give protection against **replay attacks**
 - Message counters
 - Nonces
 - Timestamps

$\mathbf{Exp}_{\Sigma}^{\text{uf-cma}}(A)$	
1.	$K \xleftarrow{\$} \Sigma.\text{KeyGen}$
2.	$\mathcal{S} \leftarrow []$
3.	$\text{forge} \leftarrow 0$
4.	$A^{\text{TAG}(\cdot), \text{VF}(\cdot, \cdot)}$
5.	return forge
$\text{TAG}(M)$	
1.	$T \leftarrow \Sigma.\text{Tag}(K, M)$
2.	$\mathcal{S}.\text{add}(M)$
3.	return T
$\text{VF}(M, T)$	
1.	$d \leftarrow \Sigma.\text{Vrfy}(K, M, T)$
2.	if $d = 1$ and $M \notin \mathcal{S}$ then:
3.	$\text{forge} \leftarrow 1$
4.	return d

$$\mathbf{Adv}_{\Sigma}^{\text{uf-cma}}(A) = \Pr[\mathbf{Exp}_{\Sigma}^{\text{uf-cma}}(A) \Rightarrow 1]$$

Message authentication codes (MACs)

deterministic function



$$\text{Tag}_K(M) = T$$

$$\text{Vrfy}_K(M, T) = \begin{cases} 1, & \text{if } \text{Tag}_K(M) = T \\ 0, & \text{otherwise} \end{cases}$$

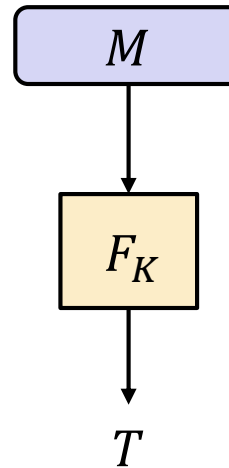


"recompute and check"

- MAC = special class of message authentication *schemes*
...but actually most common in practice
- MAC $\Rightarrow$ unique tags

PRFs are good MACs

$$F : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^\tau$$



$\Sigma_F.\text{Tag}(K, M)$

1. **return** $F_K(M)$

$\Sigma_F.\text{Vrfy}(K, M, T)$

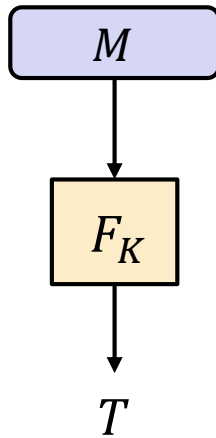
1. **return** $F_K(M) \stackrel{?}{=} T$

Theorem: If F is a secure PRF then Σ_F is UF-CMA secure for *fixed-length* messages

PRFs are good MACs – proof sketch

Theorem: For any UF-CMA adversary A , asking v V_F queries, there is a PRF-adversary B such that

$$\mathbf{Adv}_{\Sigma_F}^{\text{uf-cma}}(A) \leq \mathbf{Adv}_F^{\text{prf}}(B) + \frac{v}{2^\tau}$$

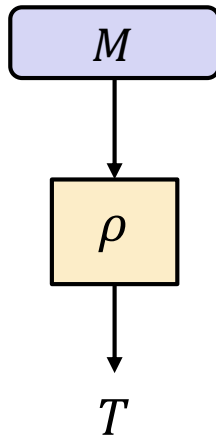


$$\Pr[F_K(M) = T] = ?$$

PRFs are good MACs – proof sketch

Theorem: For any UF-CMA adversary A , asking v V_F queries, there is a PRF-adversary B such that

$$\mathbf{Adv}_{\Sigma_F}^{\text{uf-cma}}(A) \leq \mathbf{Adv}_F^{\text{prf}}(B) + \frac{v}{2^\tau}$$

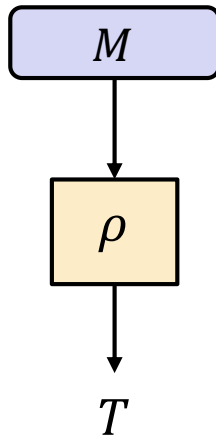


$$\rho \stackrel{\$}{\leftarrow} \text{Func}[n, \tau]$$

PRFs are good MACs – proof sketch

Theorem: For any UF-CMA adversary A , asking v V_F queries, there is a PRF-adversary B such that

$$\mathbf{Adv}_{\Sigma_F}^{\text{uf-cma}}(A) \leq \mathbf{Adv}_F^{\text{prf}}(B) + \frac{v}{2^\tau}$$



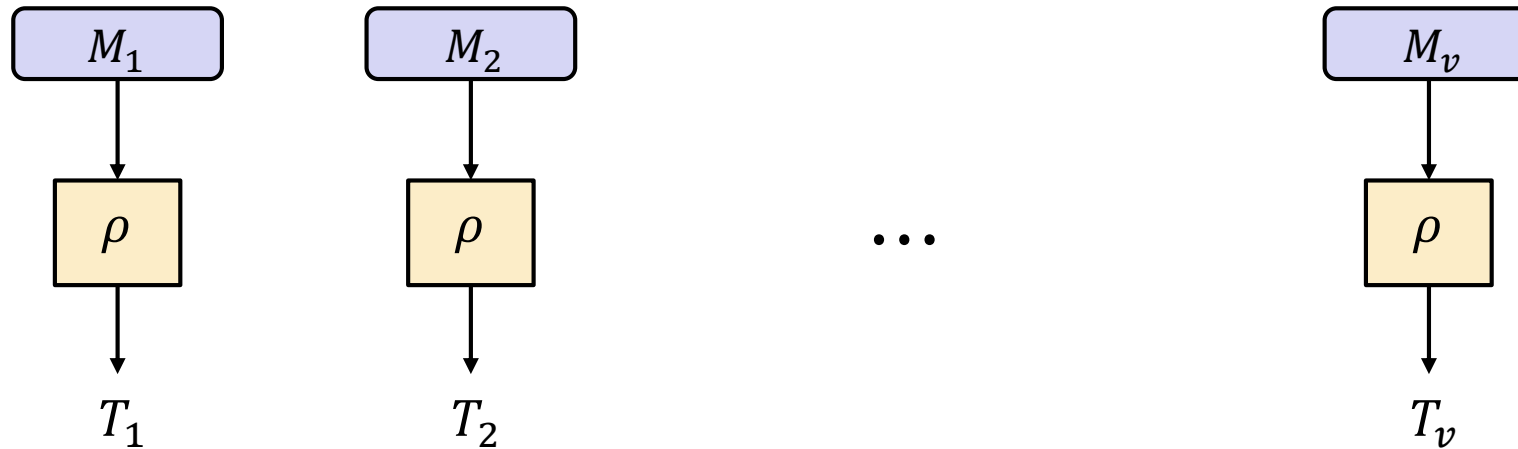
$$\rho \stackrel{\$}{\leftarrow} \text{Func}[n, \tau]$$

$$\Pr[\rho(M) = T] = \frac{1}{2^\tau}$$

PRFs are good MACs – proof sketch

Theorem: For any UF-CMA adversary A , asking v V_F queries, there is a PRF-adversary B such that

$$\mathbf{Adv}_{\Sigma_F}^{\text{uf-cma}}(A) \leq \mathbf{Adv}_F^{\text{prf}}(B) + \frac{v}{2^\tau}$$

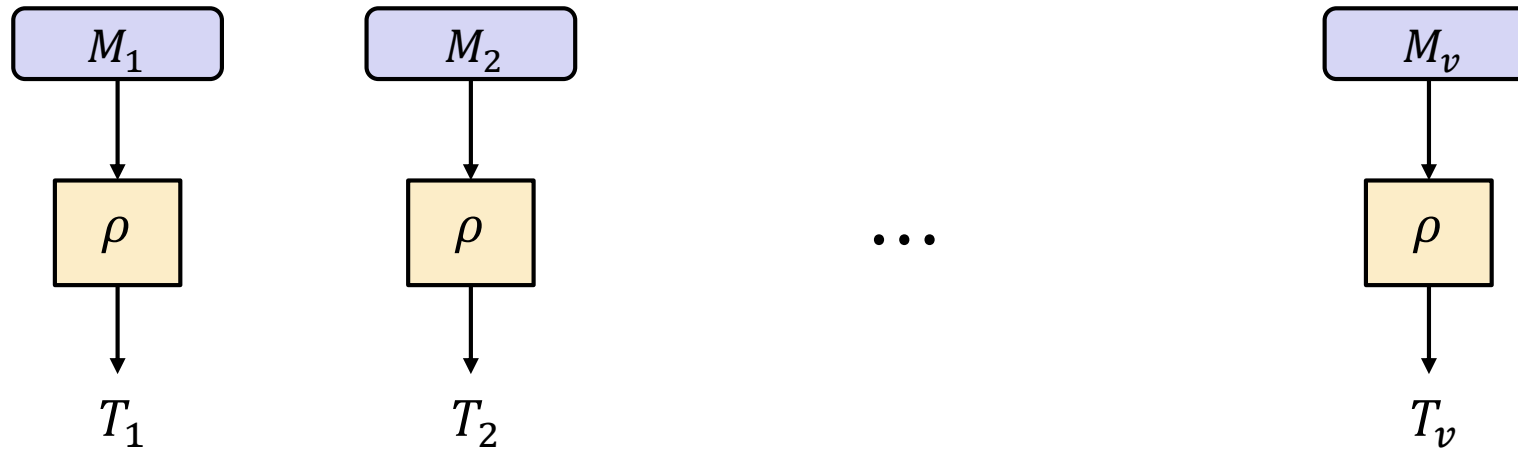


$$\Pr[\rho(M_1) = T_1 \vee \dots \vee \rho(M_v) = T_v] \leq \sum_{i=1}^v \Pr[\rho(M_i) = T_i] = \frac{v}{2^\tau}$$

PRFs are good MACs – proof sketch

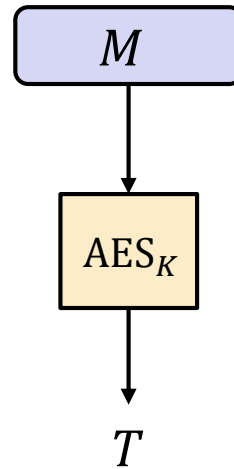
Theorem: For any UF-CMA adversary A , asking v V_F queries, there is a PRF-adversary B such that

$$\mathbf{Adv}_{\Sigma_F}^{\text{uf-cma}}(A) \leq \mathbf{Adv}_F^{\text{prf}}(B) + \frac{v}{2^\tau}$$

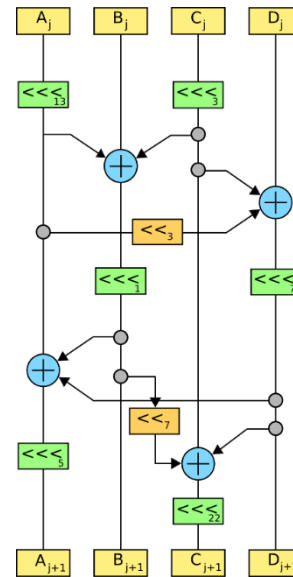


$$\Pr[\rho(M_1) = T_1 \vee \dots \vee \rho(M_v) = T_v] \leq \sum_{i=1}^v \Pr[\rho(M_i) = T_i] = \frac{v}{2^\tau}$$

PRFs are good MACs

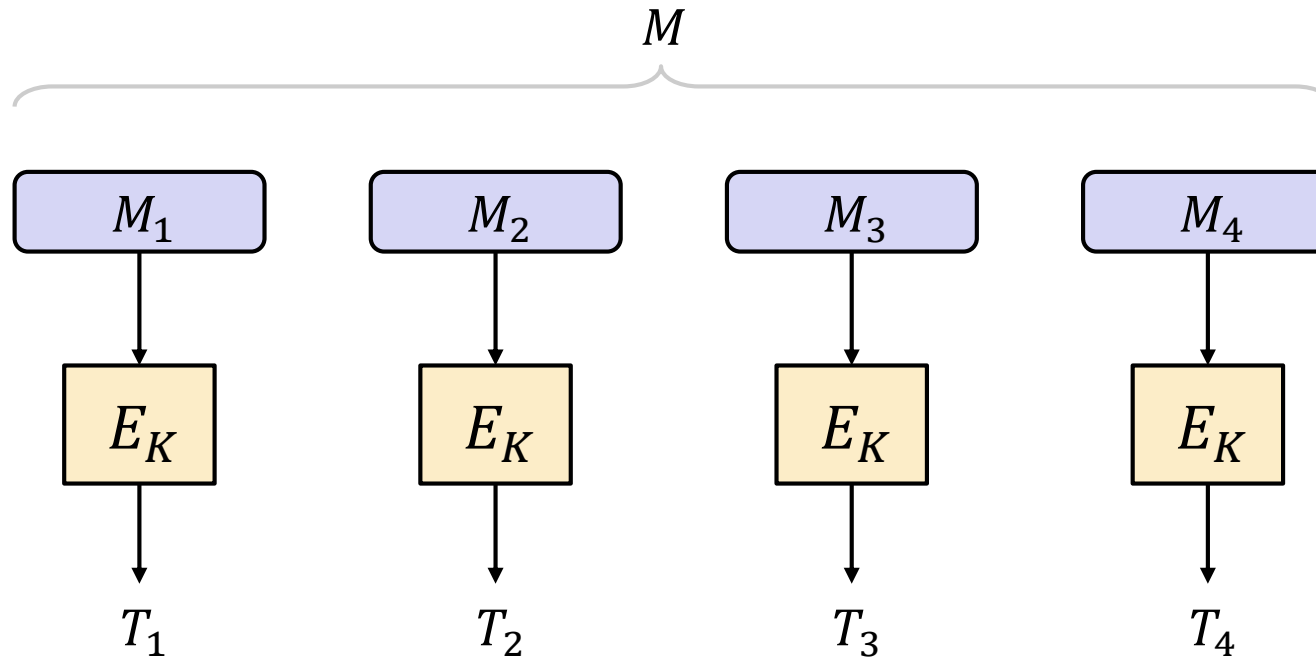


Conclusion: AES-256 : $\{0,1\}^{256} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ is a good MAC



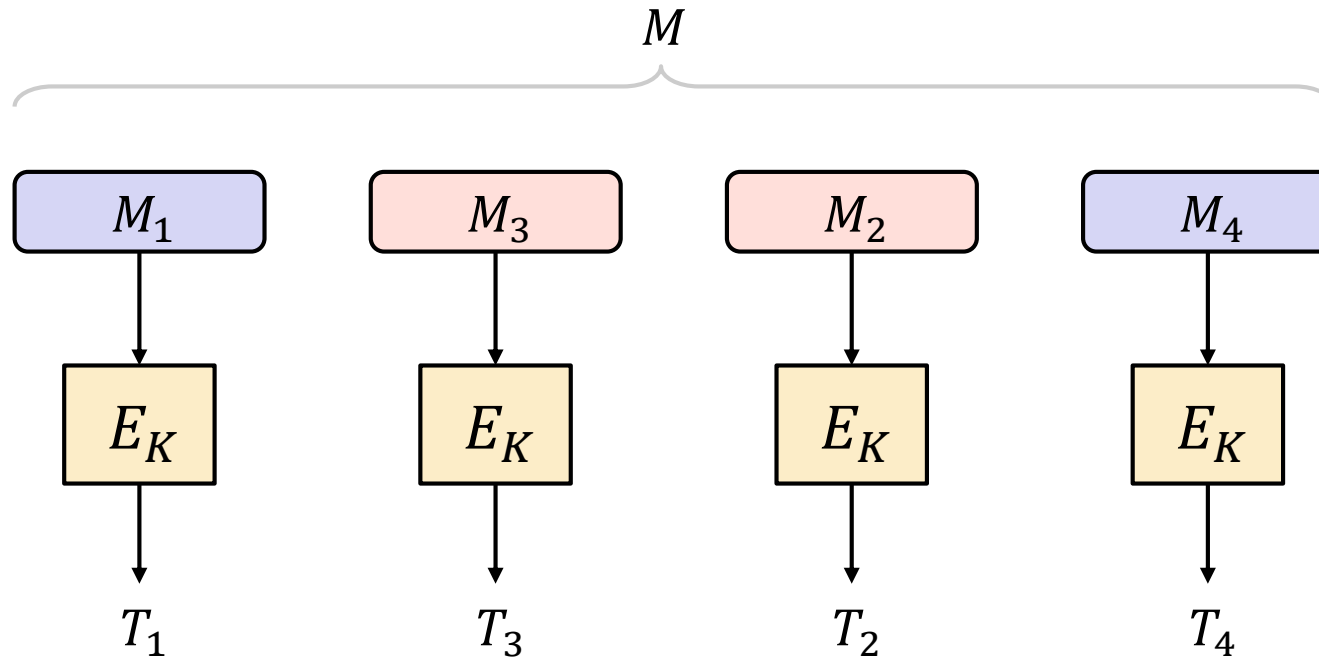
MACs for long messages

MACs from block ciphers – Attempt 1



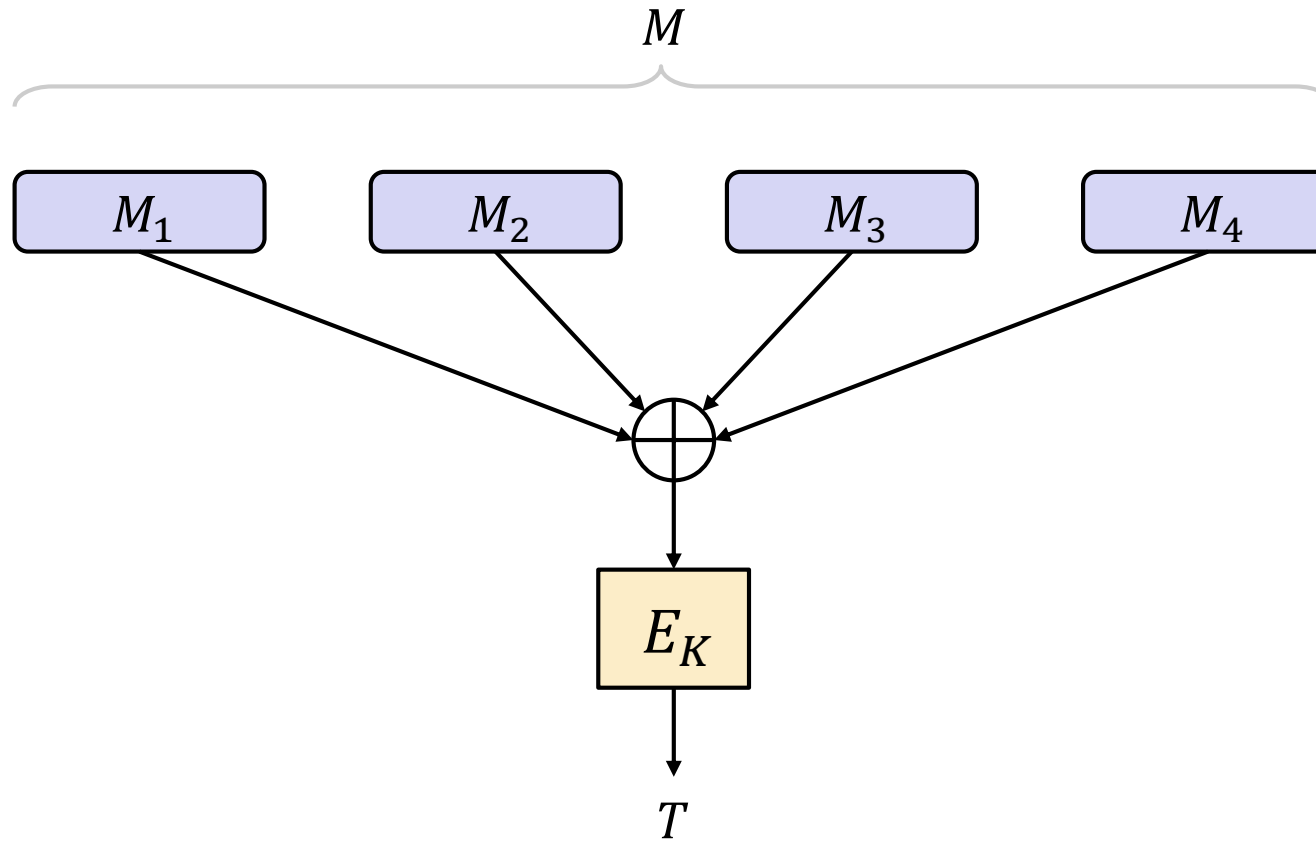
$$T = T_1 || T_2 || T_3 || T_4$$

Attempt 1 – an attack

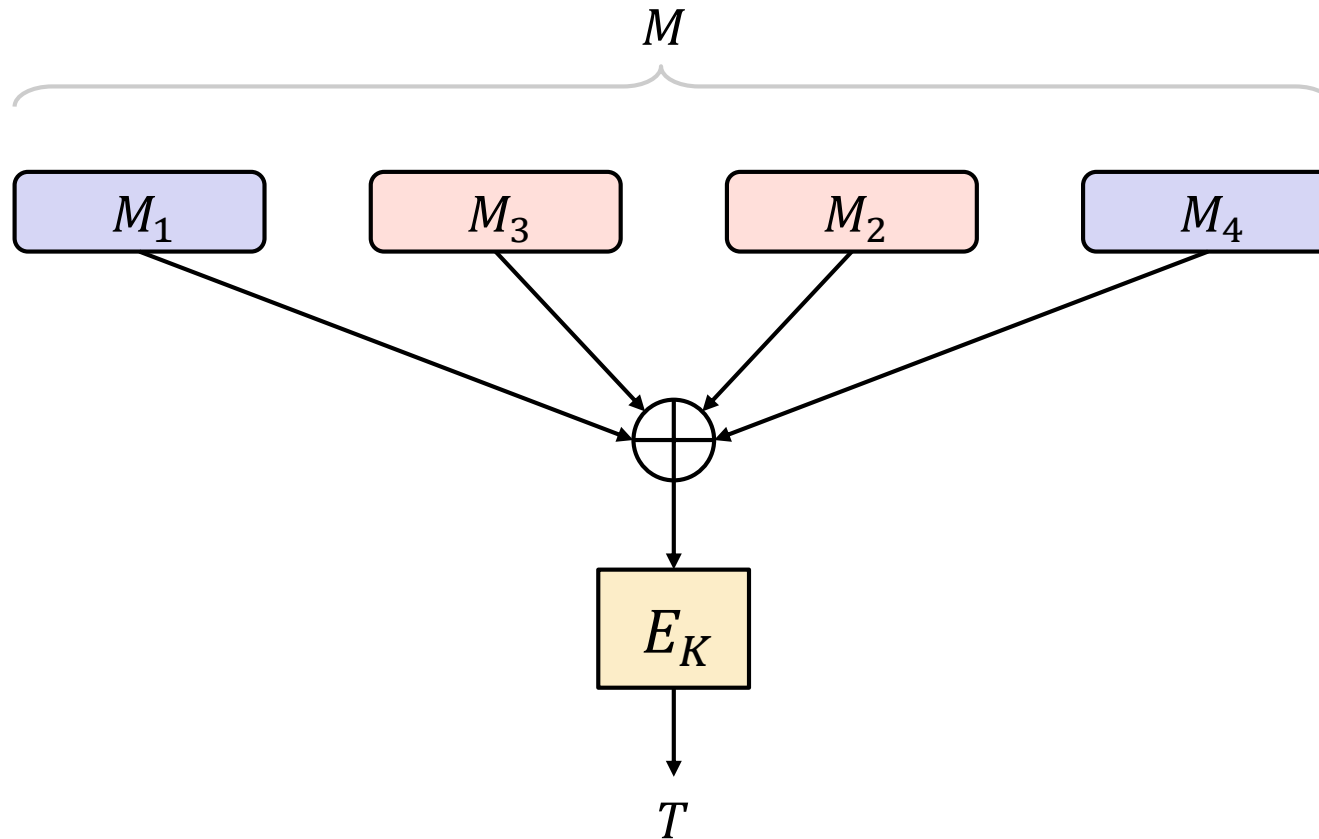


$$T = T_1 || T_3 || T_2 || T_4$$

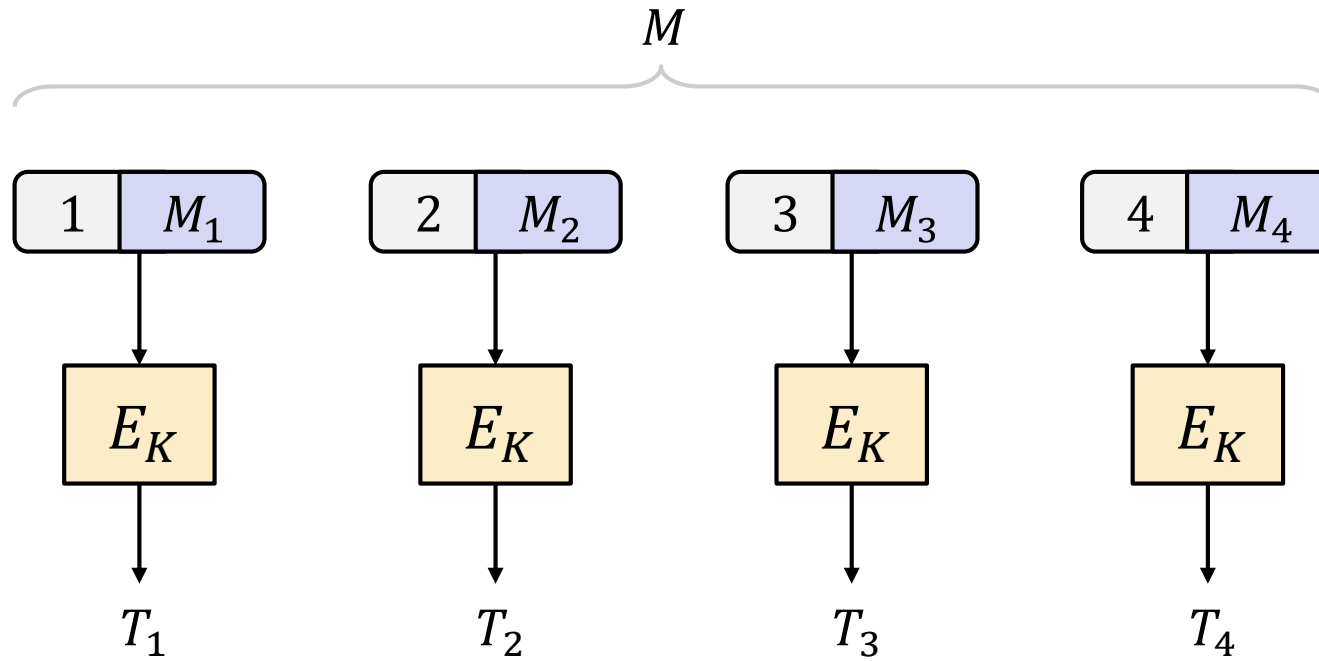
Attempt 2



Attempt 2 – an attack

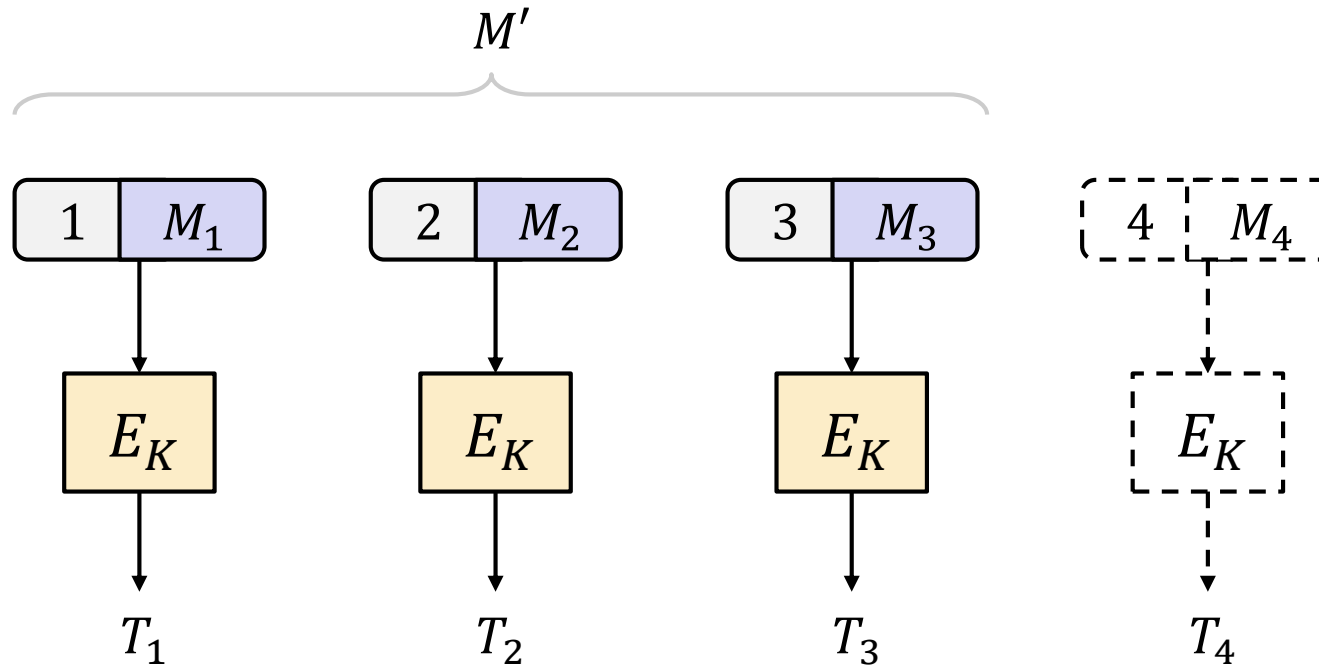


Attempt 3



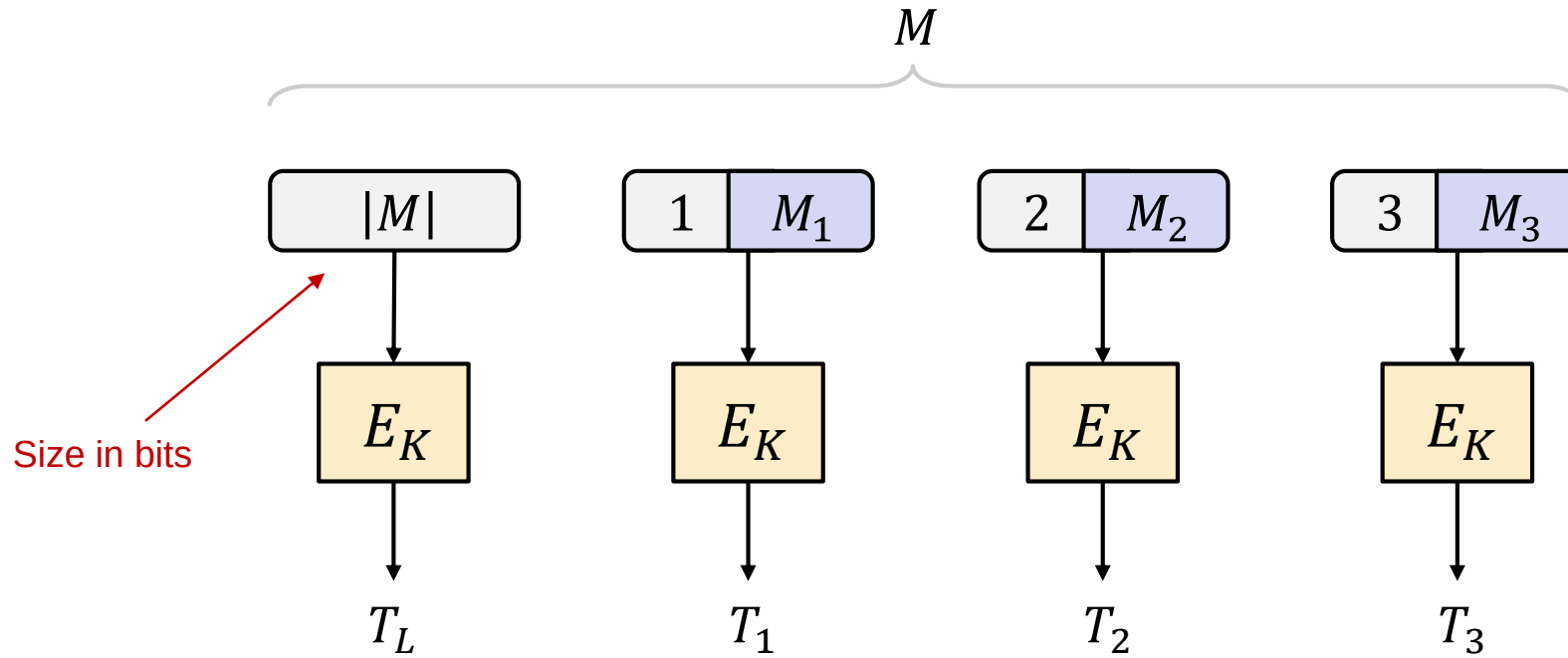
$$T = T_1 || T_2 || T_3 || T_4$$

Attempt 3 – an attack



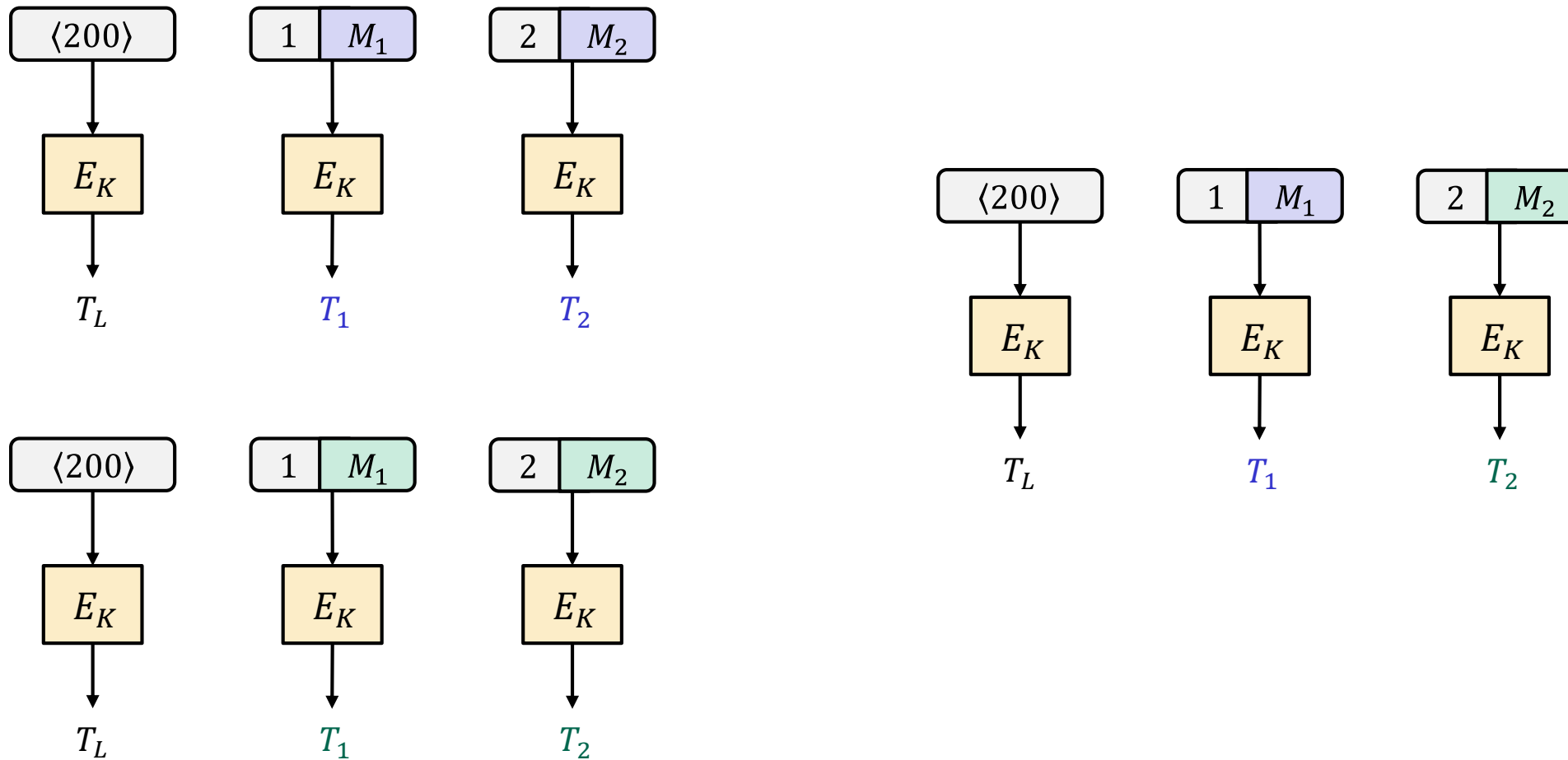
$$T = T_1 || T_2 || T_3 \text{ } \cancel{\text{ } T_4}$$

Attempt 4

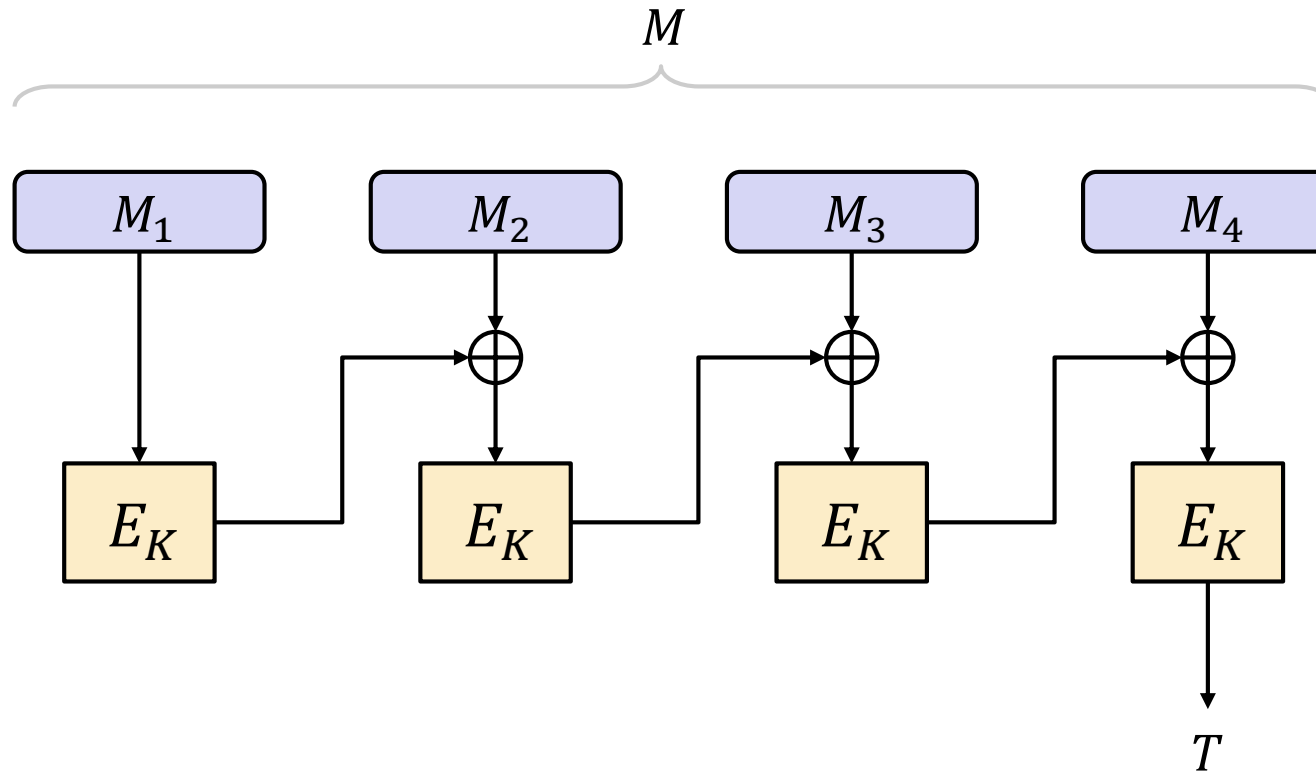


$$T = T_L || T_1 || T_2 || T_3$$

Attempt 4 – an attack



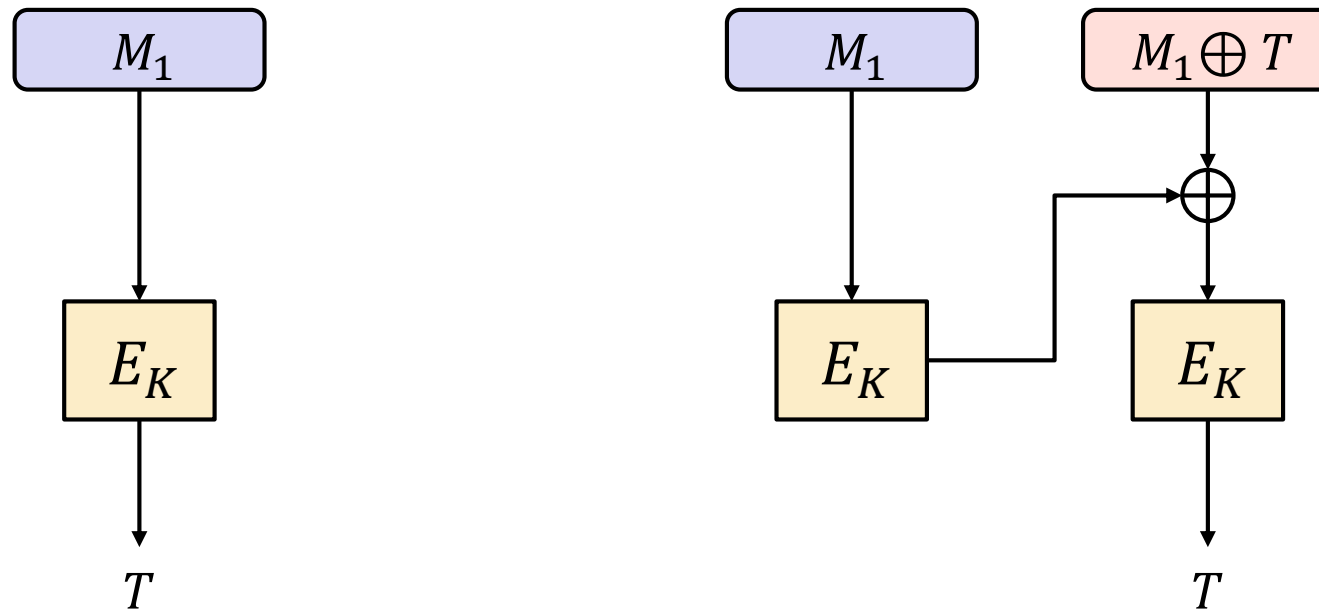
CBC-MAC



Theorem: secure if all messages have the *same* length

Warning: not secure if messages have *different* lengths!

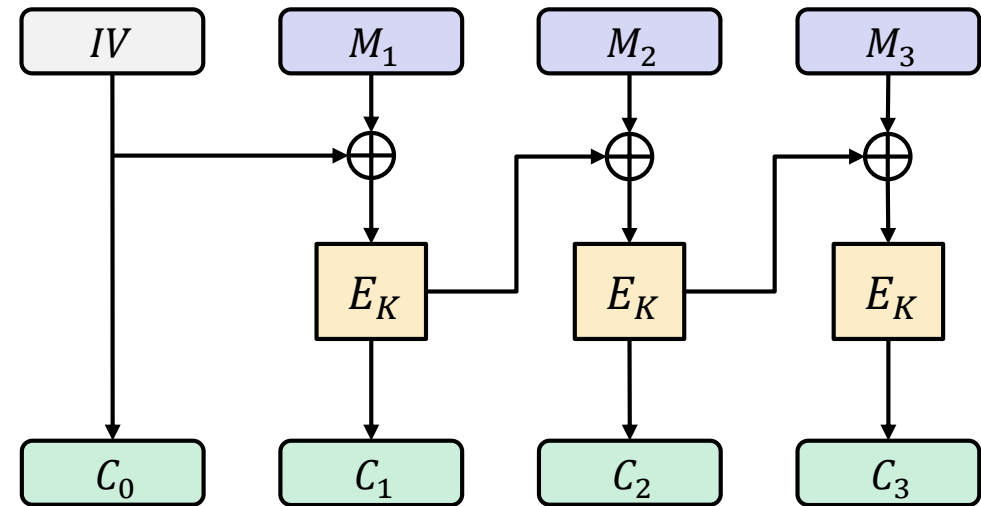
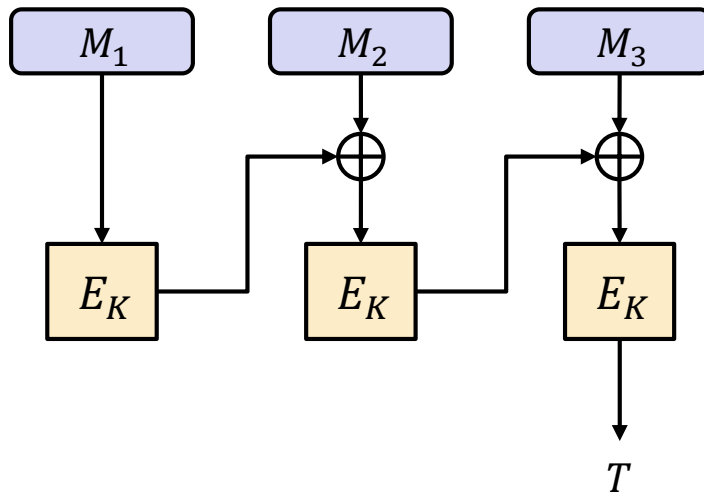
CBC-MAC



$$\mathbf{Adv}_{\text{CBC-MAC}}^{\text{uf-cma}}(A) = 1$$

Warning: not secure if messages have *different* lengths!

CBC-MAC vs. CBC\$-ENC

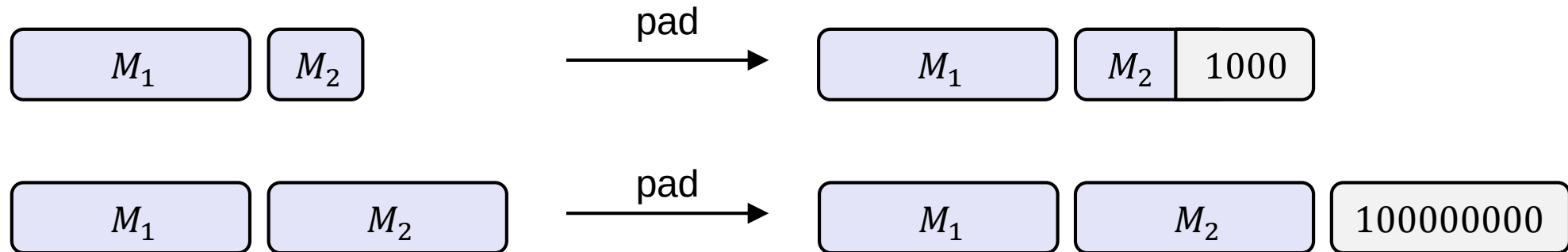


Warning 1: CBC-MAC is insecure *with* an IV!

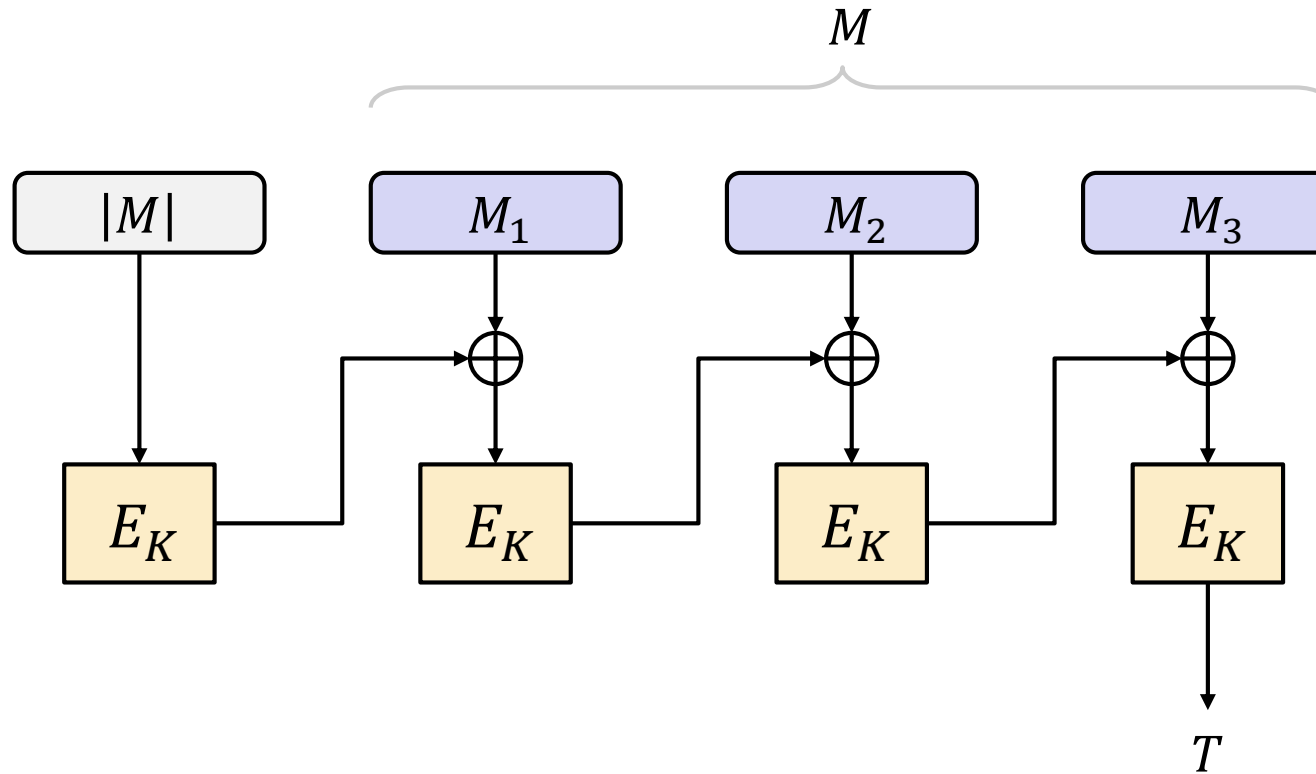
Warning 2: CBC\$-ENC is insecure *without* an IV!

Allowing variable-length messages

- Want to support different-length messages
 - Could use different keys for each length $\Rightarrow$ not practical
- Want to support message not a multiple of the block length
 - **Padding** needed



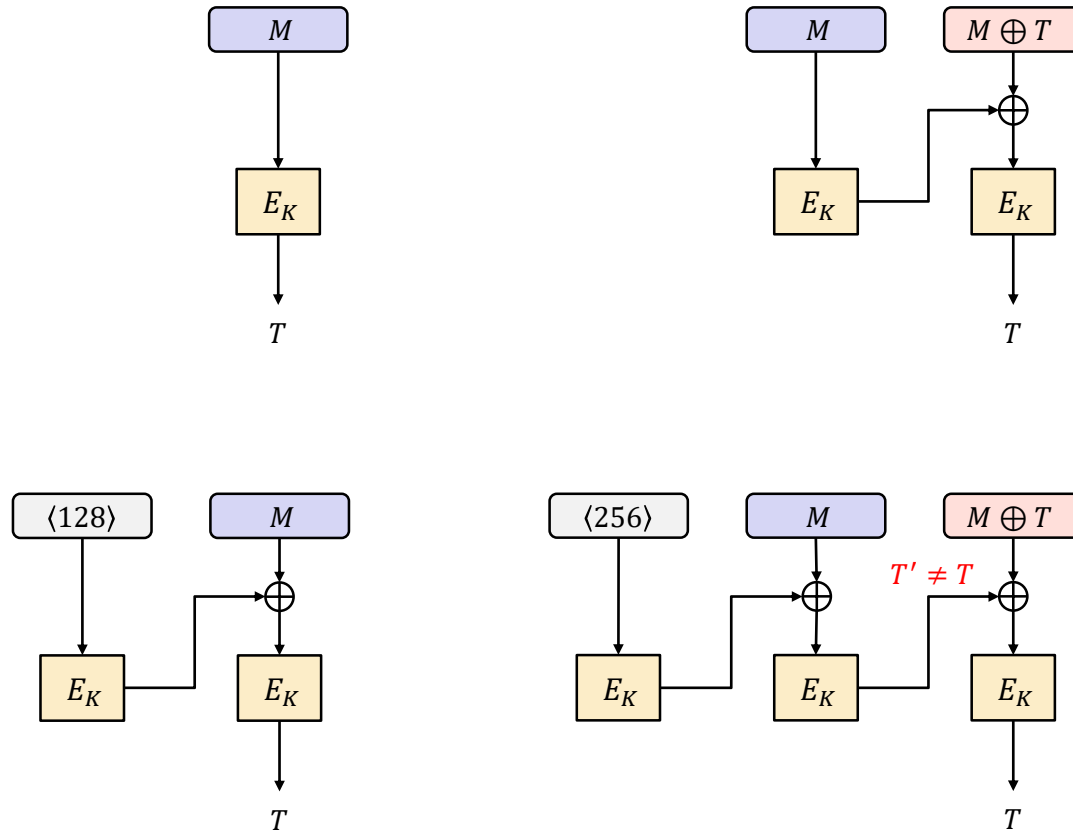
Length-prepend CBC-MAC



Theorem: Length-prepend CBC-MAC is UF-CMA secure if E is a secure PRP

Question: What if you instead add the length to the end?

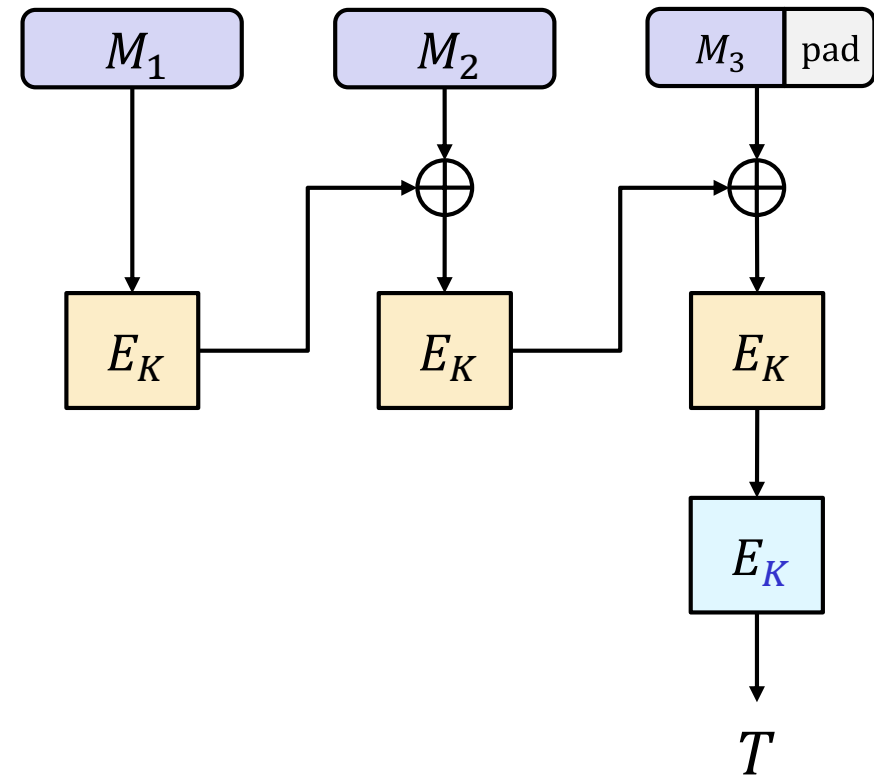
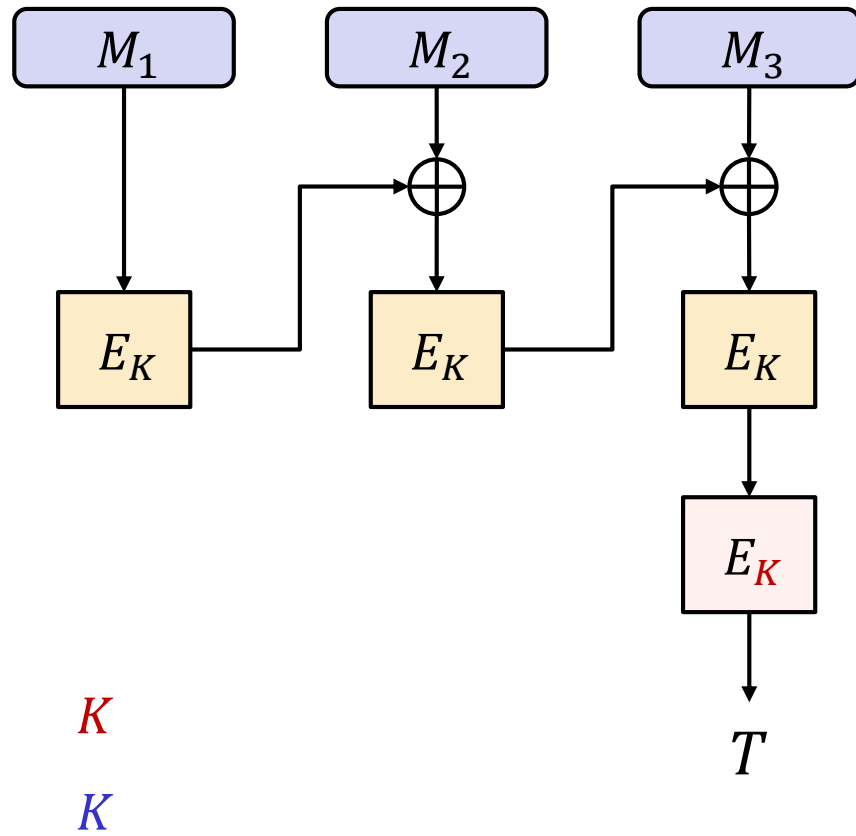
Length-prepend CBC-MAC



Forgery!

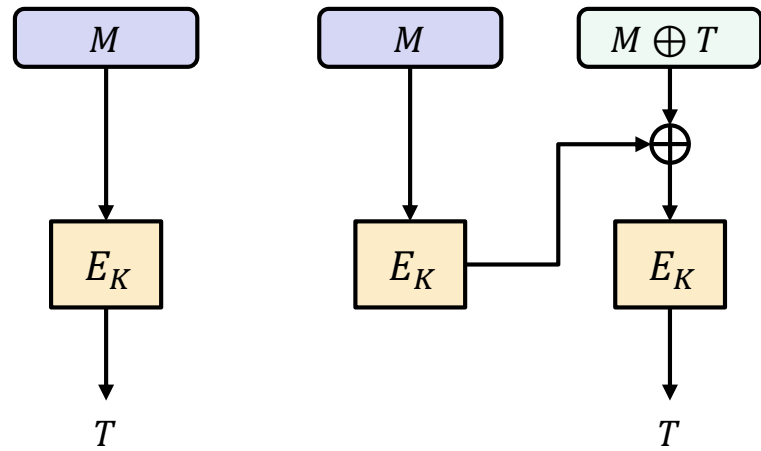
Not a forgery

ECBC-MAC



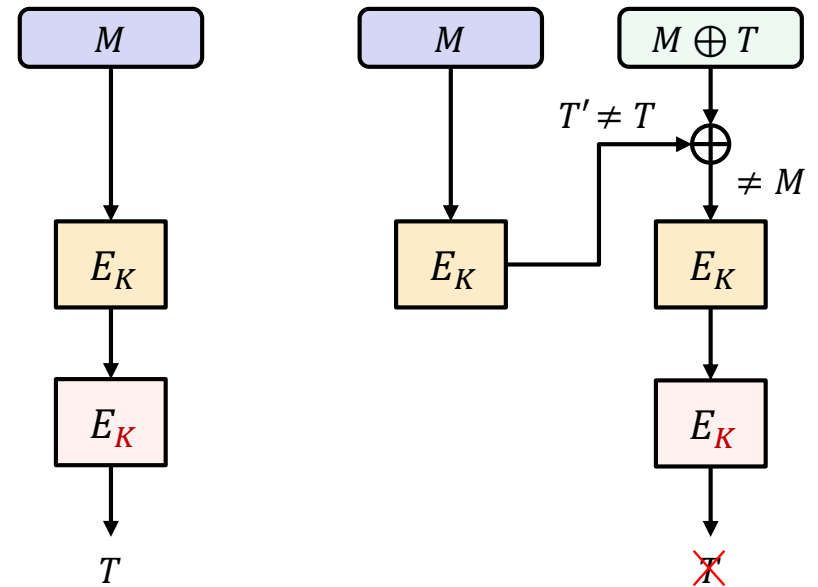
CBC-MAC vs ECBC-MAC

CBC-MAC



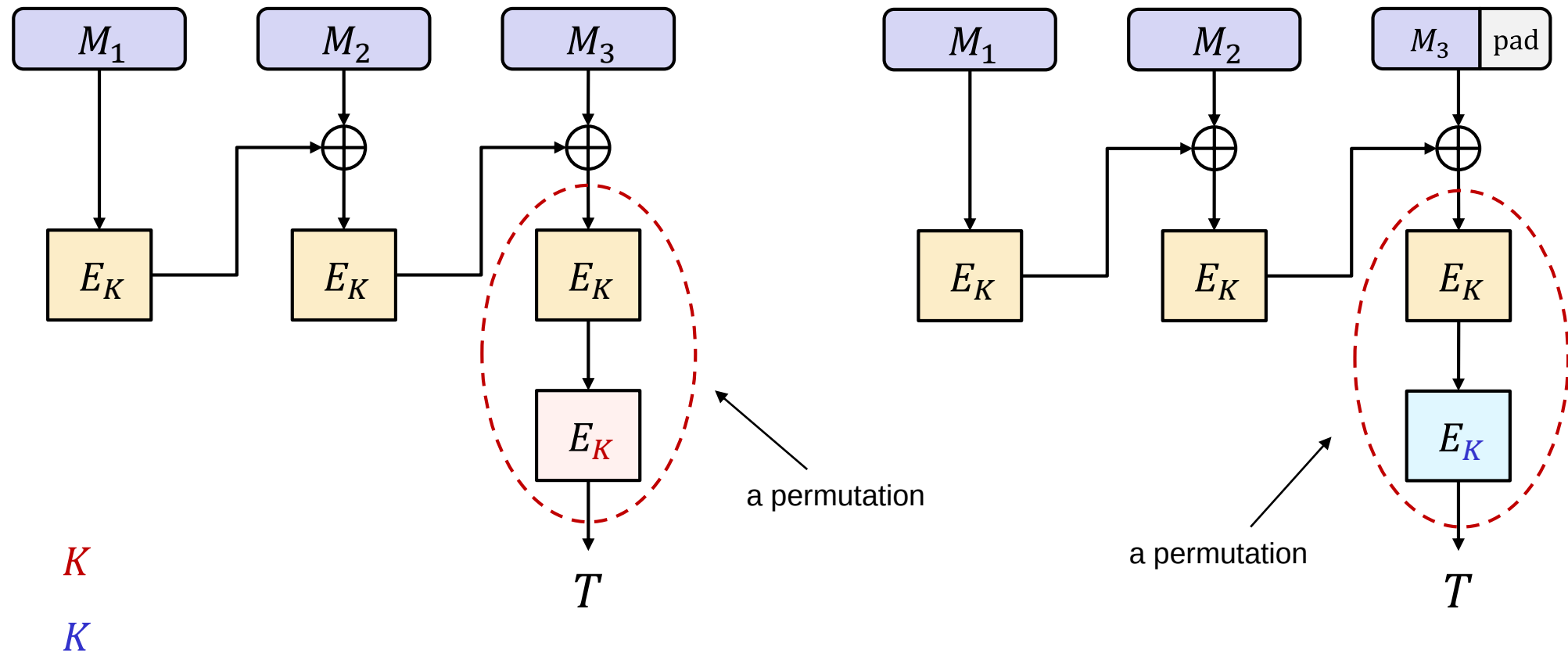
Forgery!

ECBC-MAC

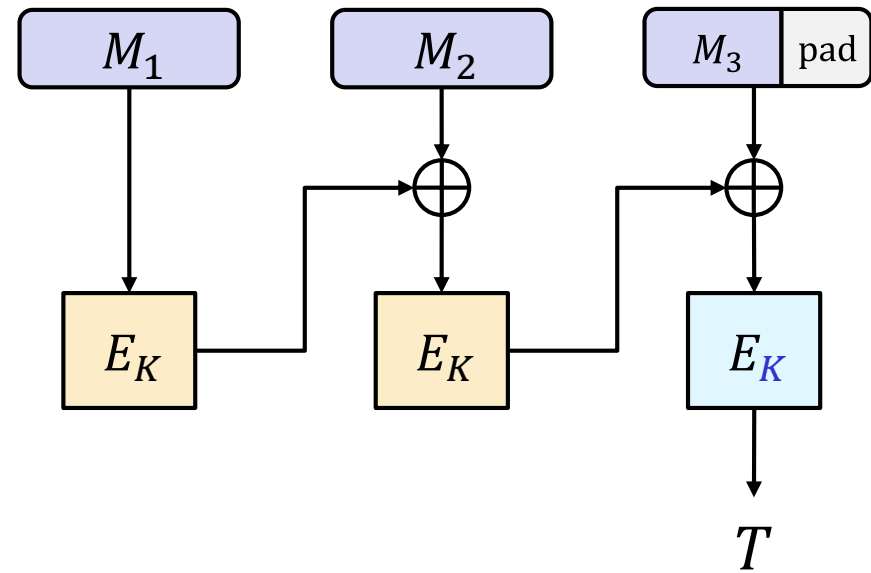
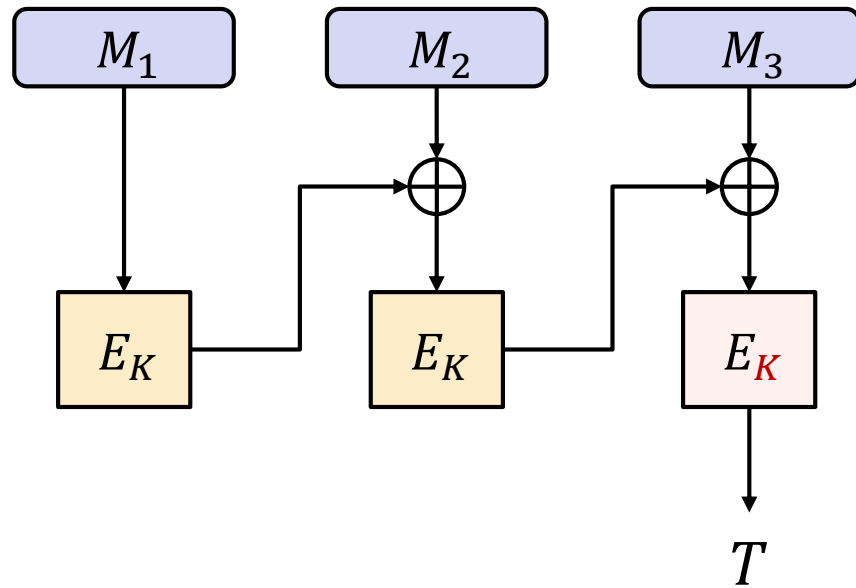


Not a forgery

ECBC-MAC



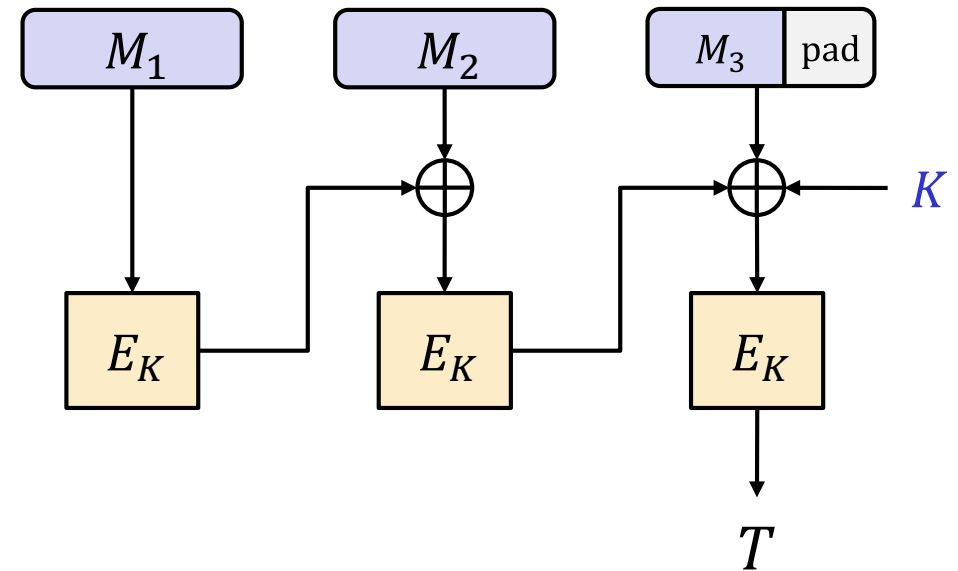
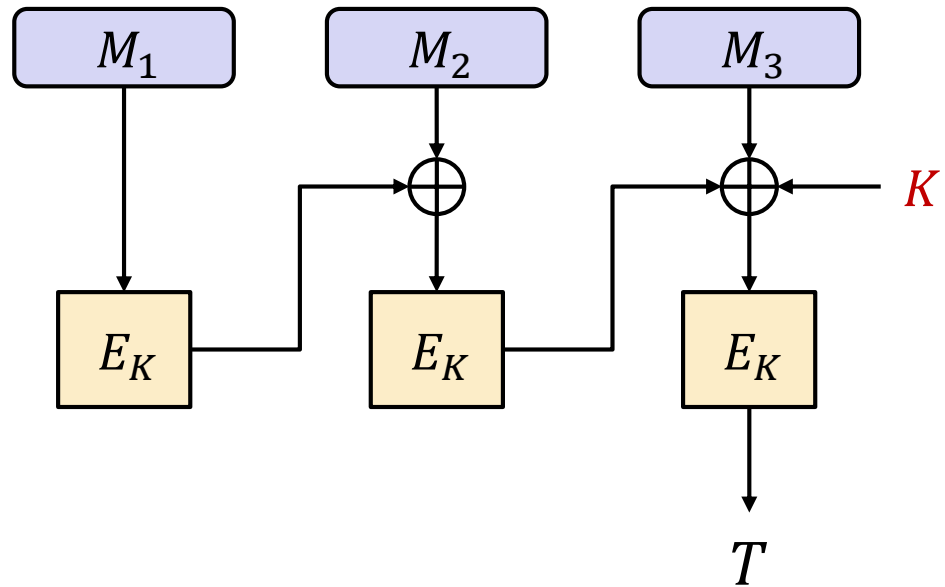
FCBC-MAC



K

K

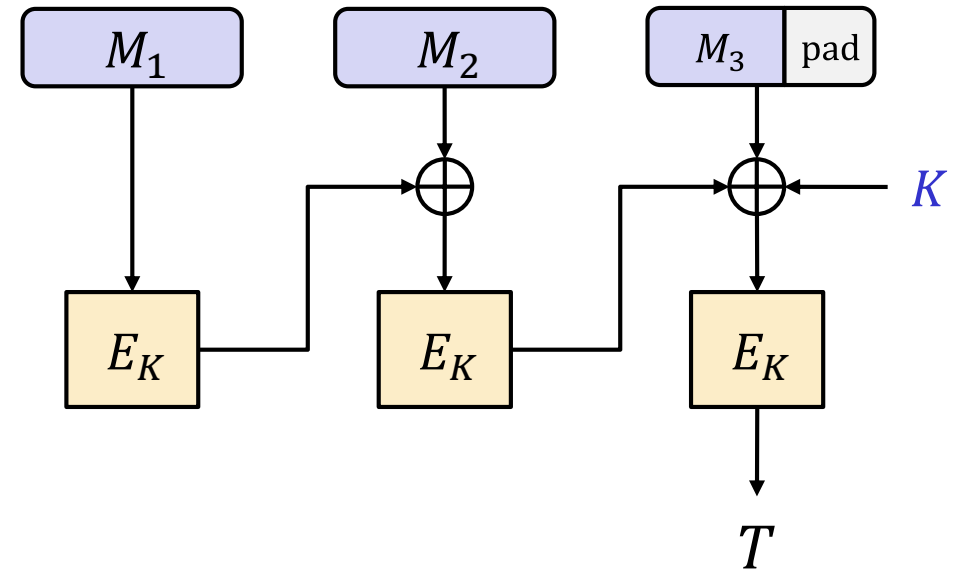
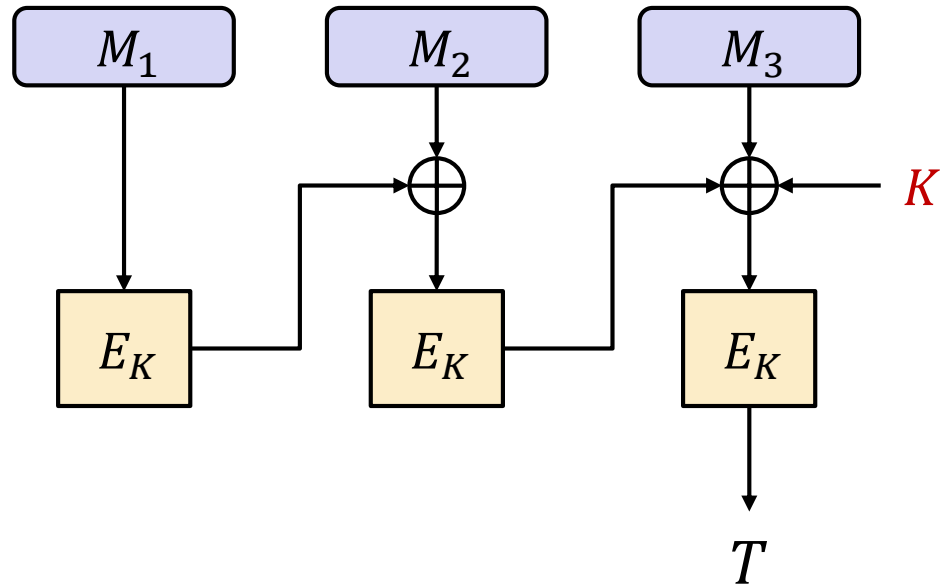
XCBC-MAC



K

K

CMAC a.k.a One-key MAC



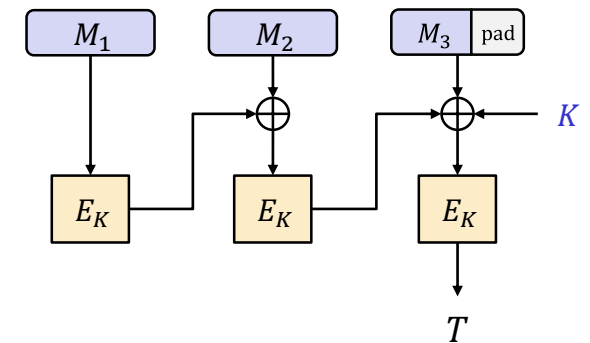
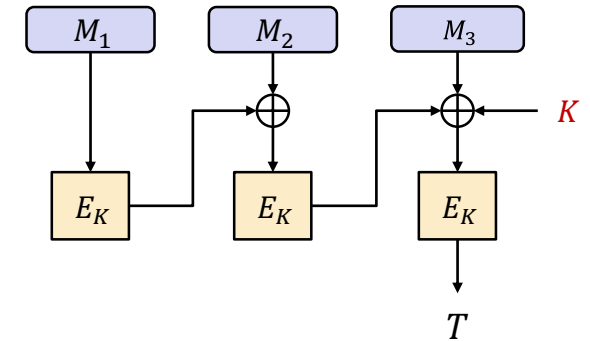
$$K = 2 * E_K(0^n)$$

$$K = 4 * E_K(0^n)$$

Theorem: secure for messages of *all* lengths

CMAC

- **Theorem:** UF-CMA secure if E is a secure PRP
- 1 E -call per message block + 1 E -call to derive K_2, K_3
- Fully sequential
 - Cannot utilize parallel AES cores
- Only one key
- Standardized by NIST
 - Widely used



$$K = 2 * F_K(0^n)$$

$$K = 4 * F_K(0^n)$$

CMAC security

Theorem: For any UF-CMA adversary making q TAG-queries (each having ℓ blocks), and v VF-queries, there is a PRP-adversary B such that

$$\mathbf{Adv}_{\text{CMAC}}^{\text{uf-cma}}(A) \leq \mathbf{Adv}_E^{\text{prp}}(B) + \frac{5 \cdot \ell \cdot q^2}{2^n} + \frac{v}{2^n}$$

- **Example:**

- $E = \text{AES}$ ($n = 128$)
- Number of Tag-queries: $q = 2^{40} \approx 1$ trillion queries
- Max blocks per message: $\ell = 2^{10} \approx 16$ kB
- Number of Vrfy-queries: $v = 2^{20}$
- $\mathbf{Adv}_E^{\text{prp}}(B) \approx 0$

$$\mathbf{Adv}_{\text{AES-CMAC}}^{\text{uf-cma}}(A) \leq \frac{5 \cdot 2^{10} \cdot (2^{40})^2}{2^{128}} + \frac{2^{20}}{2^{128}} \approx \frac{2^{3+10+80}}{2^{128}} = \frac{1}{2^{35}}$$

CMAC security

Theorem: For any UF-CMA adversary making q TAG-queries (each having ℓ blocks), and v VF-queries, there is a PRP-adversary B such that

$$\mathbf{Adv}_{\text{CMAC}}^{\text{uf-cma}}(A) \leq \mathbf{Adv}_E^{\text{prp}}(B) + \frac{5 \cdot \ell \cdot q^2}{2^n} + \frac{v}{2^n}$$

- **Example:**

- $E = \text{DES}$ ($n = 64$)
- Number of Tag-queries: $q = 2^{40} \approx 1$ trillion queries
- Max blocks per message: $\ell = 2^{10} \approx 16$ kB
- Number of Vrfy-queries: $v = 2^{20}$
- $\mathbf{Adv}_E^{\text{prp}}(B) \approx 0$



$$\mathbf{Adv}_{\text{DES-CMAC}}^{\text{uf-cma}}(A) \leq \frac{5 \cdot 2^{10} \cdot (2^{40})^2}{2^{64}} + \frac{2^{20}}{2^{64}} \approx \frac{2^{3+10+80}}{2^{64}} = 2^{29}$$

CMAC security

Theorem: For any UF-CMA adversary making q TAG-queries (each having ℓ blocks), and v VF-queries, there is a PRP-adversary B such that

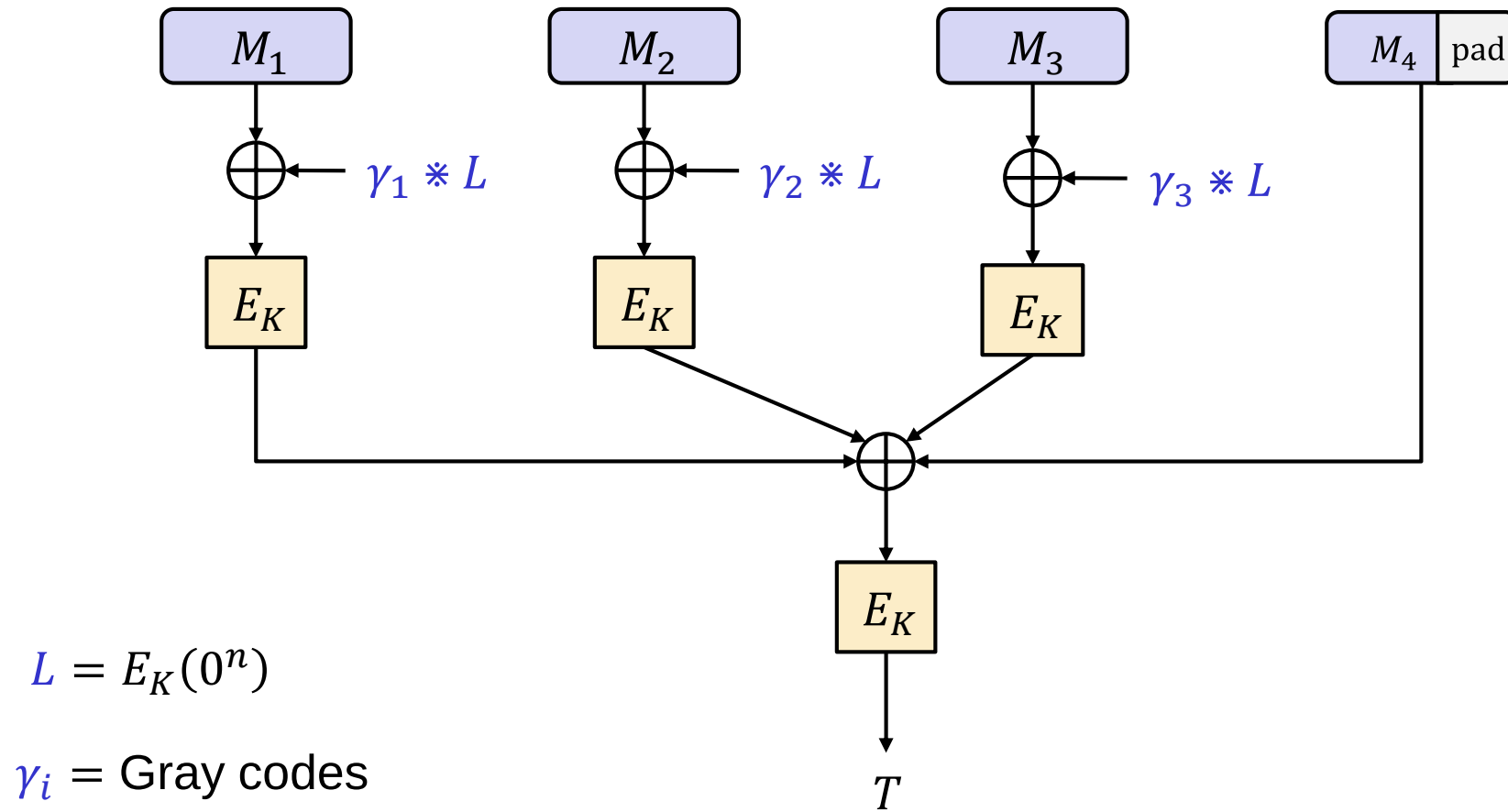
$$\mathbf{Adv}_{\text{CMAC}}^{\text{uf-cma}}(A) \leq \mathbf{Adv}_E^{\text{prp}}(B) + \frac{5 \cdot \ell \cdot q^2}{2^n} + \frac{v}{2^n}$$

- **Example:**

- $E = \text{DES}$ ($n = 64$)
- Number of Tag-queries: $q = 2^{16} \approx 65\,000$ queries
- Max blocks per message: $\ell = 2^{10} \approx 16$ kB
- Number of Vrfy-queries: $v = 2^{20}$
- $\mathbf{Adv}_E^{\text{prp}}(B) \approx 0$

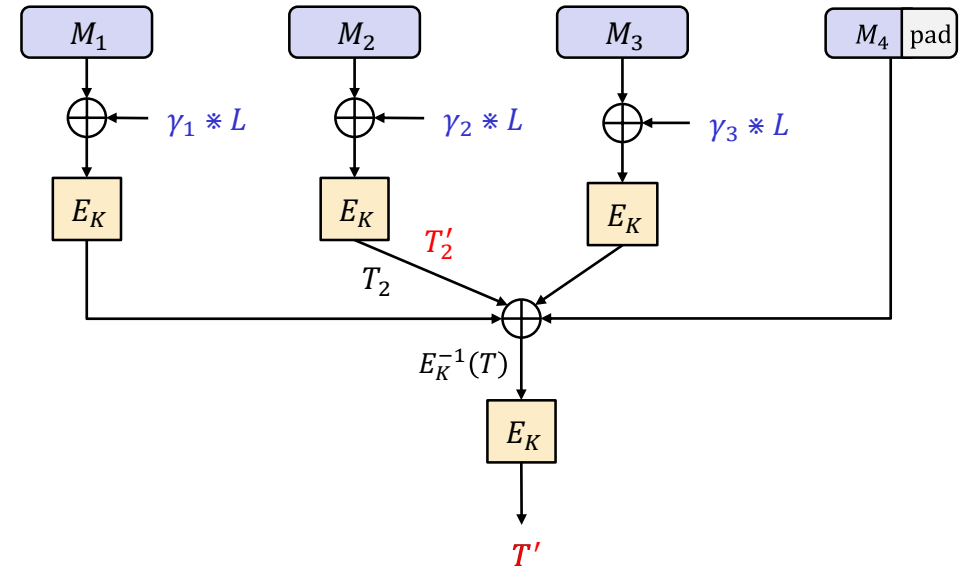
$$\mathbf{Adv}_{\text{DES-CMAC}}^{\text{uf-cma}}(A) \leq \frac{1}{2^{19}}$$

PMAC



PMAC properties

- **Theorem:** UF-CMA secure if E is a secure PRP
- One key
- Fully parallelizable
- Incremental
- ...not used in practice



$$\text{PMAC}_K(M_1 || M_2 || \dots || M_{1000}) = T$$

$$\text{PMAC}_K(M_1 || \mathbf{M'_2} || \dots || M_{1000}) = E_K(E_K^{-1}(T) \oplus T_2 \oplus \mathbf{T'_2}) = \mathbf{T'}$$

$$T_2 = E_K(M_2 \oplus \gamma_2 * L)$$

$$\mathbf{T'_2} = E_K(\mathbf{M'_2} \oplus \gamma_2 * L)$$

Summary

- UF-CMA the right security notion for message integrity
 - Does not cover replay attacks
- PRFs are good MACs
 - But only for short (fixed) input length
- CBC-MAC good MAC for messages of a ***single fixed*** length
- CMAC upgrades CBC-MAC to variable-length messages