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

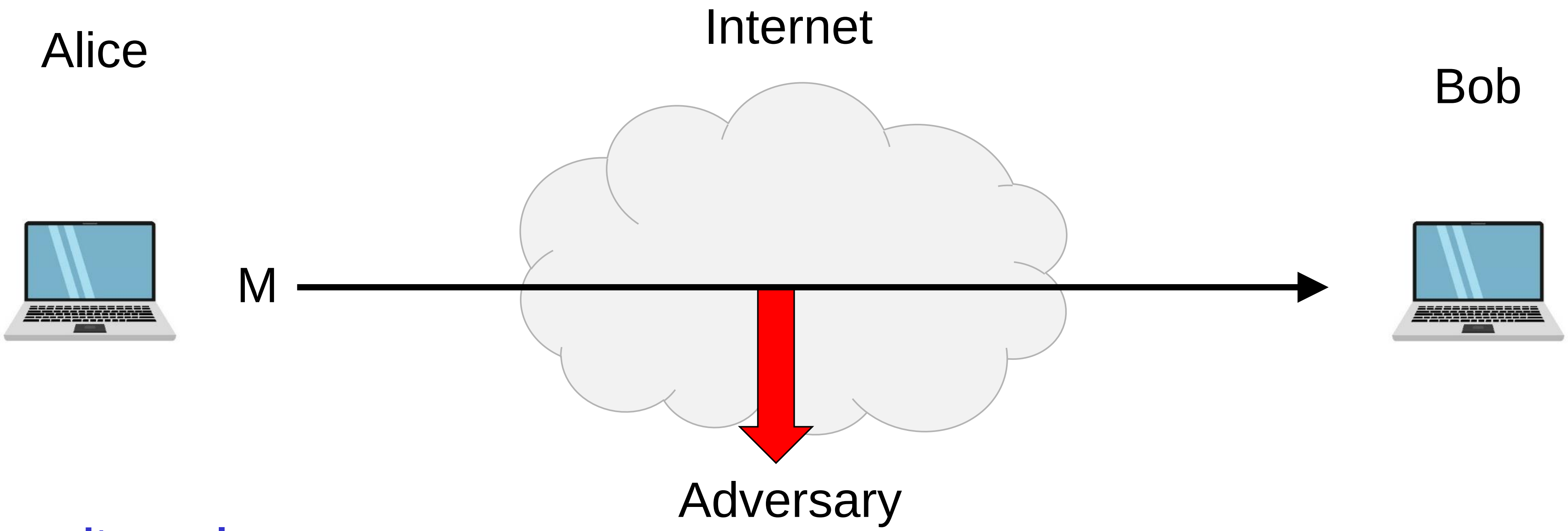
TEK4500

15.09.2021

Håkon Jacobsen

hakon.jacobsen@its.uio.no

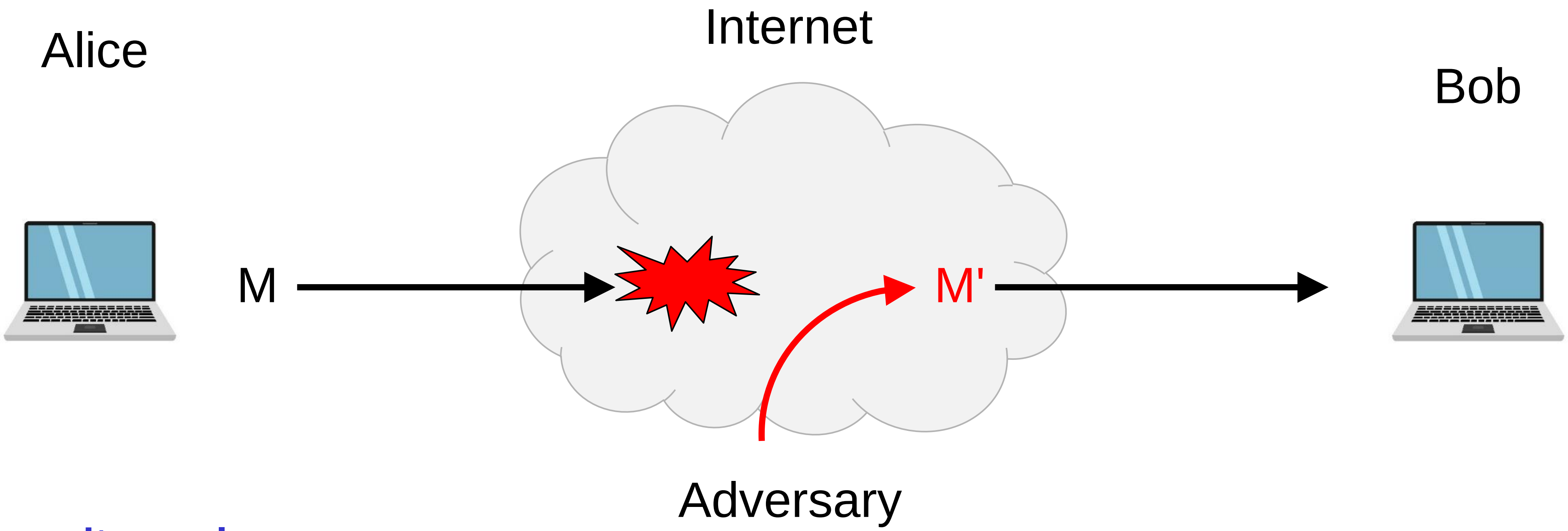
What is cryptography?



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*, but not privacy

- Examples:
  - Protecting OS system files against tampering
  - Browser cookies stored by web servers
  - Control signals in network management

Encryption ≠ integrity

CTR. Enc(K,·)

0110100 1110 100101100110

⊕

"Send Bob $10"

1001010 1010 000000001010

→

1111110 0100 011001101100

CTR. Dec(K,·)

1111110 0100 011001101100

⊕

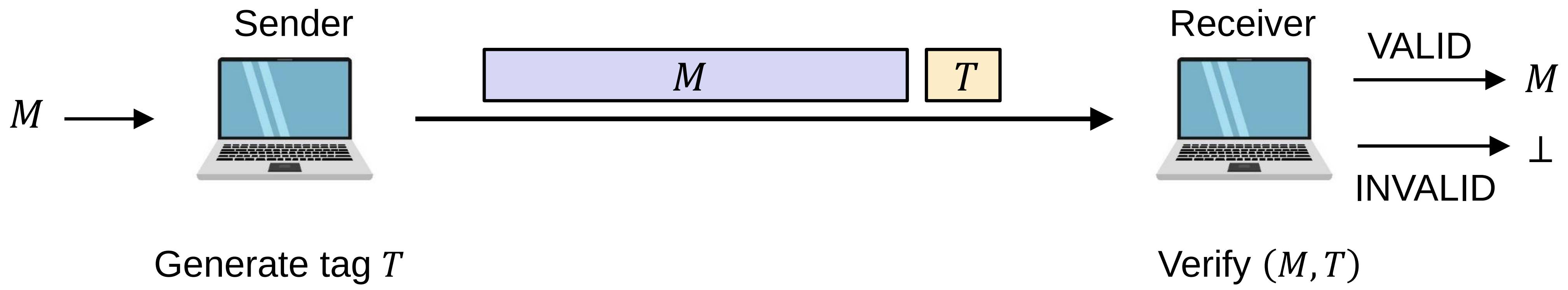
0110100 1110 100101100110

=

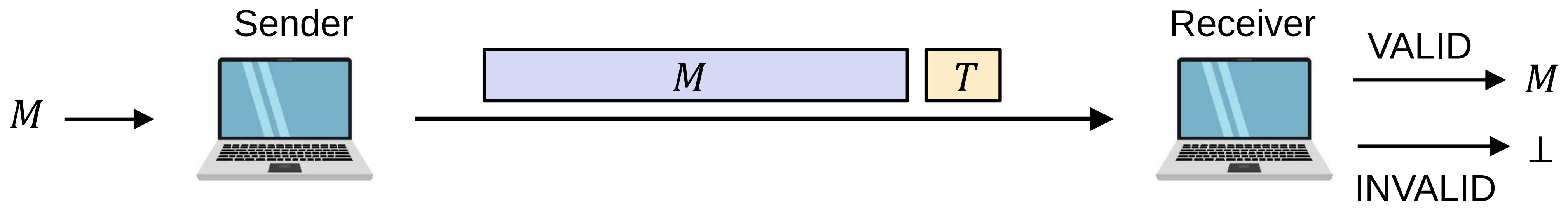
1001010 1010 111100001010

"Send Bob **$3850**"

Message authentication – idea



Message authentication – idea

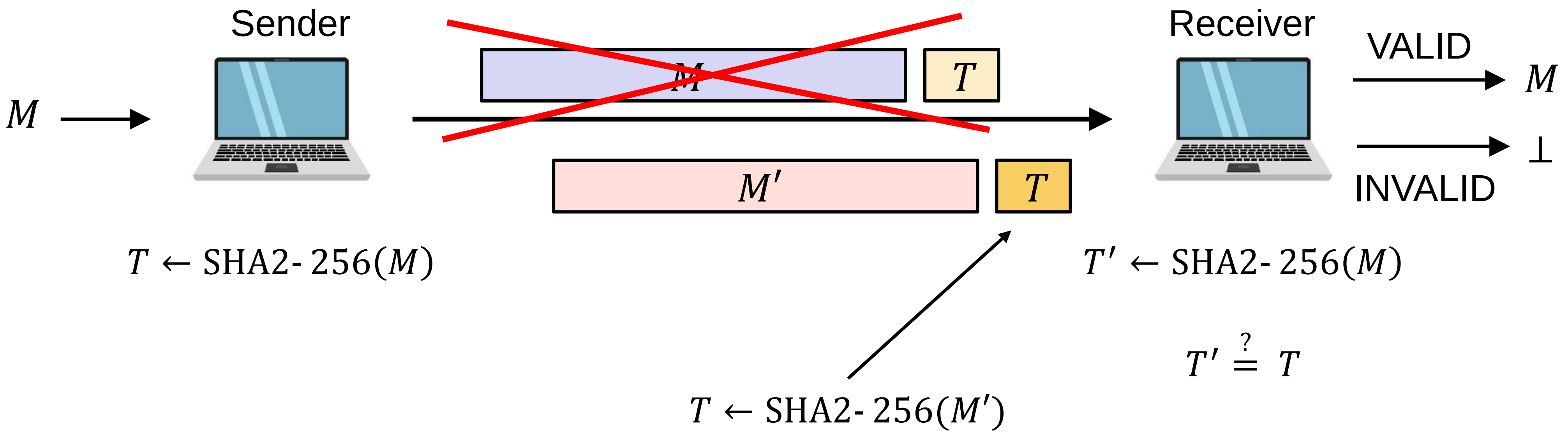


$T \leftarrow \text{SHA2-256}(M)$

$T' \leftarrow \text{SHA2-256}(M)$

$T' \stackrel{?}{=} T$

Message authentication – idea



Message authentication schemes – syntax

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

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

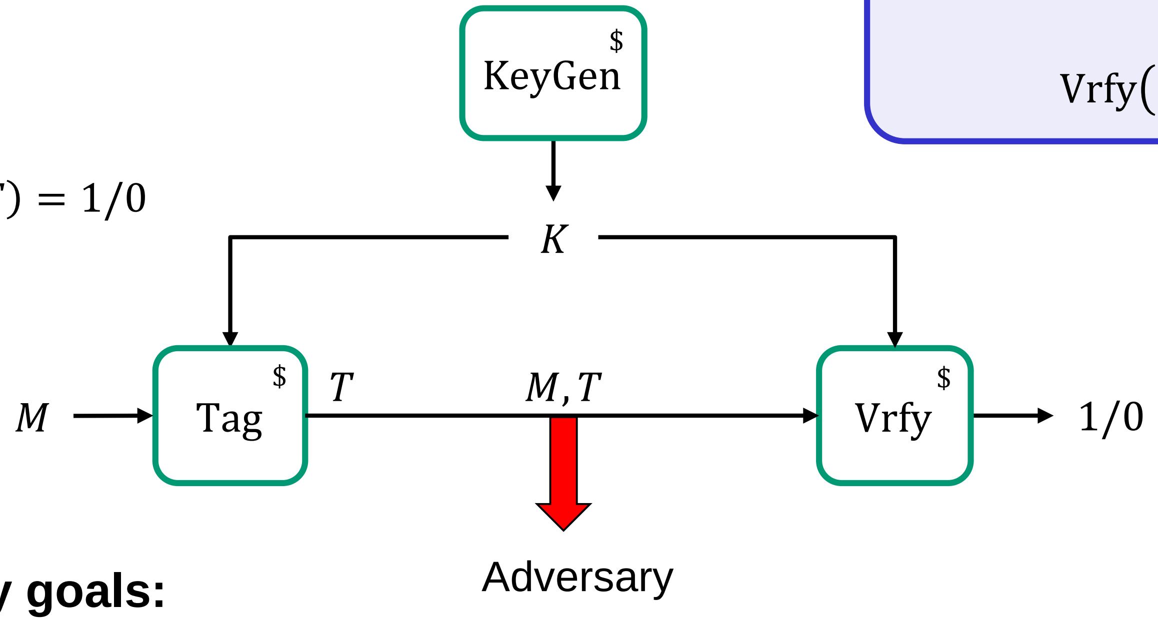
$\mathrm{Tag}(K, M) = \mathrm{Tag}_K(M) = T$

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

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

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

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



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) $M_1, M_2, \ldots$ first

UF-CMA – Unforgability against chosen-message attacks

$\mathbf{Exp}_{\Sigma}^{\text{uf-cma}}(A)$

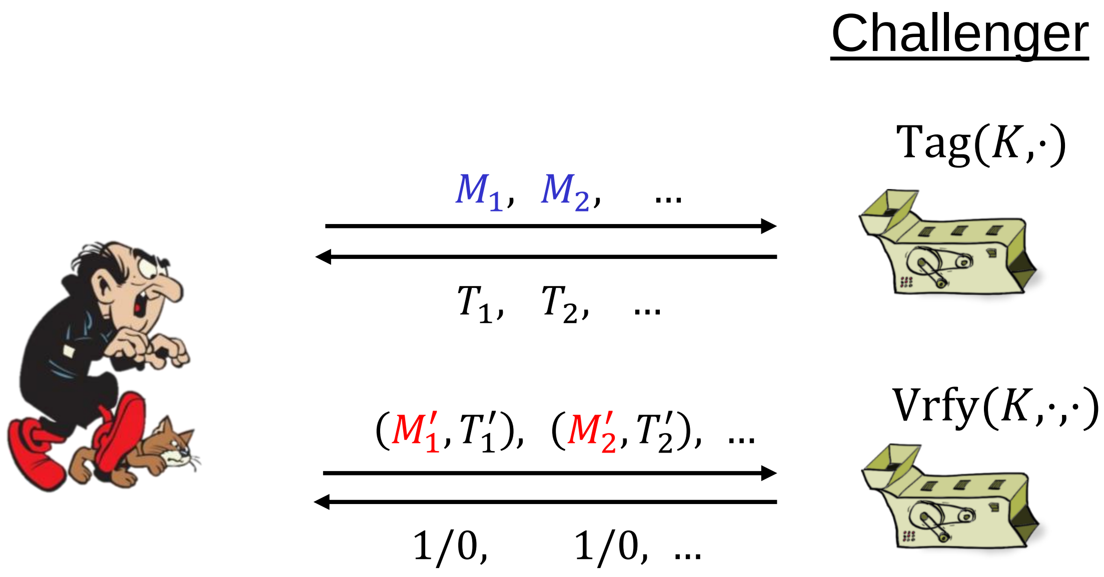
$K \xleftarrow{\$} \Sigma.\text{KeyGen}$
$\mathcal{S} \leftarrow [\,]$
$\text{forge} \leftarrow 0$
$A^{\text{Tag}(\cdot),\,\text{VF}(\cdot,\cdot)}$
return forge

$\text{Tag}(M)$

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

$\text{VF}(M, T)$

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



Adversary *wins* if:

- one (M_i', T_i') is *valid*, i.e., $\text{Vrfy}(K, M_i', T_i') = 1$
- *and* $M_i' \notin \{M_1, M_2, \dots,\}$

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

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

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. $\quad$ $\text{forge} \leftarrow 1$
4. **return** d

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

Message authentication *codes* (MACs)

deterministic *function*

$$\Sigma.\mathrm{Tag}(K, M) = T$$

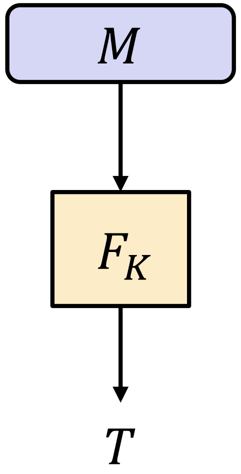
$$\Sigma.\mathrm{Vrfy}(K, M, T) \stackrel{\text{def}}{=} \begin{cases} 1, & \text{if } T = \Sigma.\mathrm{Tag}(K, M) \\ 0, & \text{otherwise} \end{cases}$$

simply recompute tag

- MAC = special class of message authentication schemes
  …actually most common in practice
- MAC $\Longrightarrow$ unique tags $\Longrightarrow$ forgeries must be on new *messages*

PRFs are good MACs

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



Alg $\Sigma_{\text{PRF}}.\text{Tag}\big(K, M \in \{0,1\}^k\big)$

---

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

Alg $\Sigma_{\text{PRF}}.\text{Vrfy}(K, M, T)$

---

1. $T' \leftarrow F_K(M)$
2. **return** $T' \stackrel{?}{=} T$

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

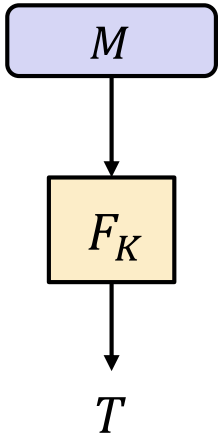
Detailed: for *any* UF-CMA adversary A against Σ_{PRF}, asking v Vrfy queries, there is an adversary B against F such that

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

PRFs are good MACs – proof sketch

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

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

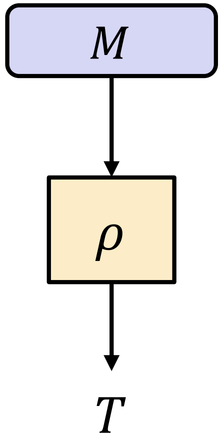


$$\Pr[F_K(M) = T] = \ ?$$

PRFs are good MACs – proof sketch

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

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

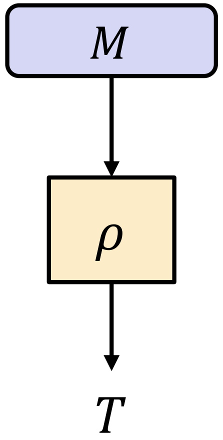


$$\rho \xleftarrow{\$} \text{Func}[n, \tau]$$

PRFs are good MACs – proof sketch

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

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



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

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

PRFs are good MACs – proof sketch

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

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

$$\rho \xleftarrow{\$} \text{Func}[n,\tau] \qquad \Pr[\rho(M_1) = T_1 \lor \cdots \lor \rho(M_v) = T_v] \leq \sum_{i=1}^{v} \Pr[\rho(M_i) = T_i] = \frac{v}{2^\tau}$$

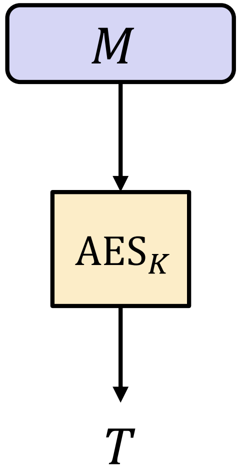
PRFs are good MACs – proof sketch

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

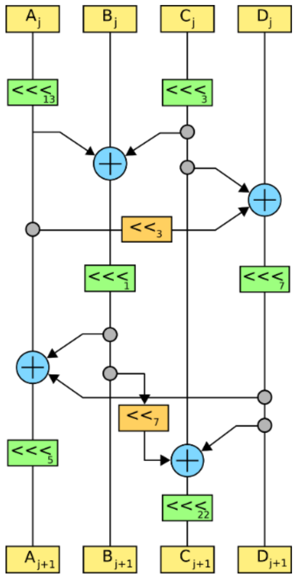
$$\mathbf{Adv}^{\text{uf-cma}}_{\Sigma_{\text{PRF}}}(A) \leq \mathbf{Adv}^{\text{prf}}_{F}(B) + \frac{v}{2^\tau}$$

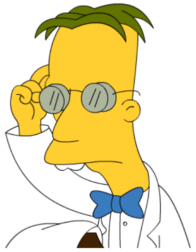
$$\rho \overset{\$}{\leftarrow} \text{Func}[n, \tau] \qquad \Pr[\rho(M_1) = T_1 \vee \cdots \vee \rho(M_v) = T_v] \leq \sum_{i=1}^{v} \Pr[\rho(M_i) = T_i] = \frac{v}{2^\tau}$$

PRFs are good MACs



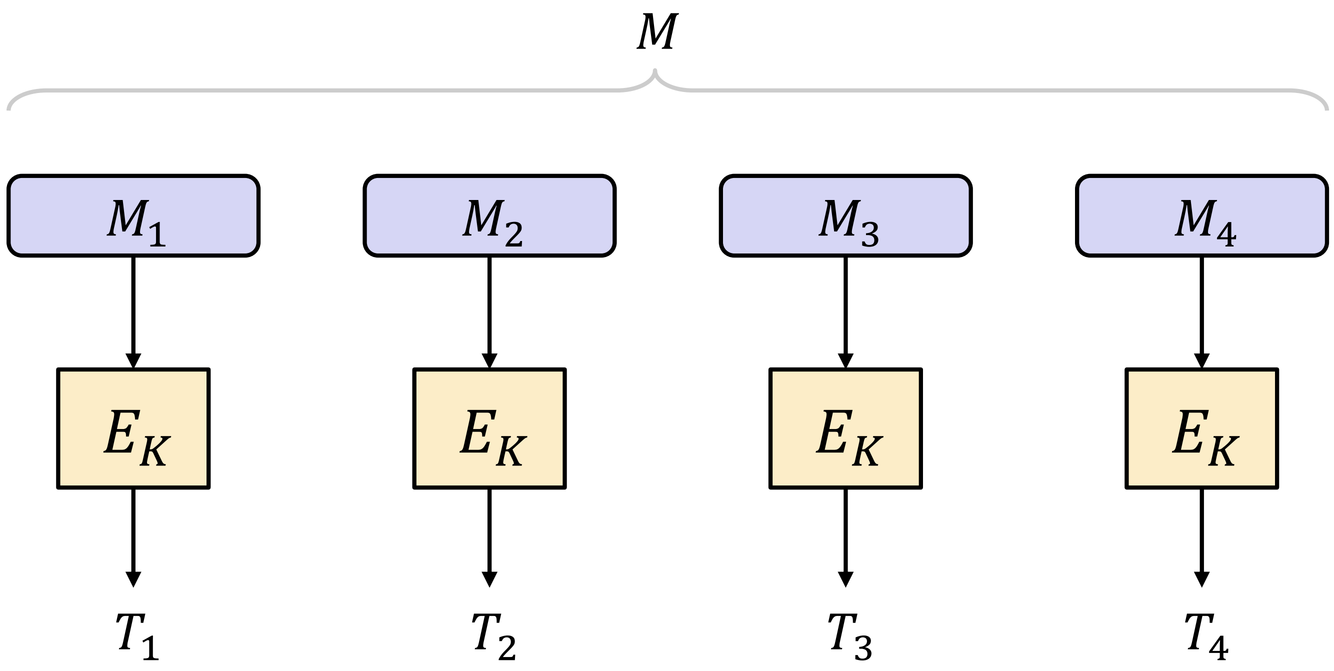
Conclusion: $\mathrm{AES}-256 : \{0,1\}^{256} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ is a good MAC





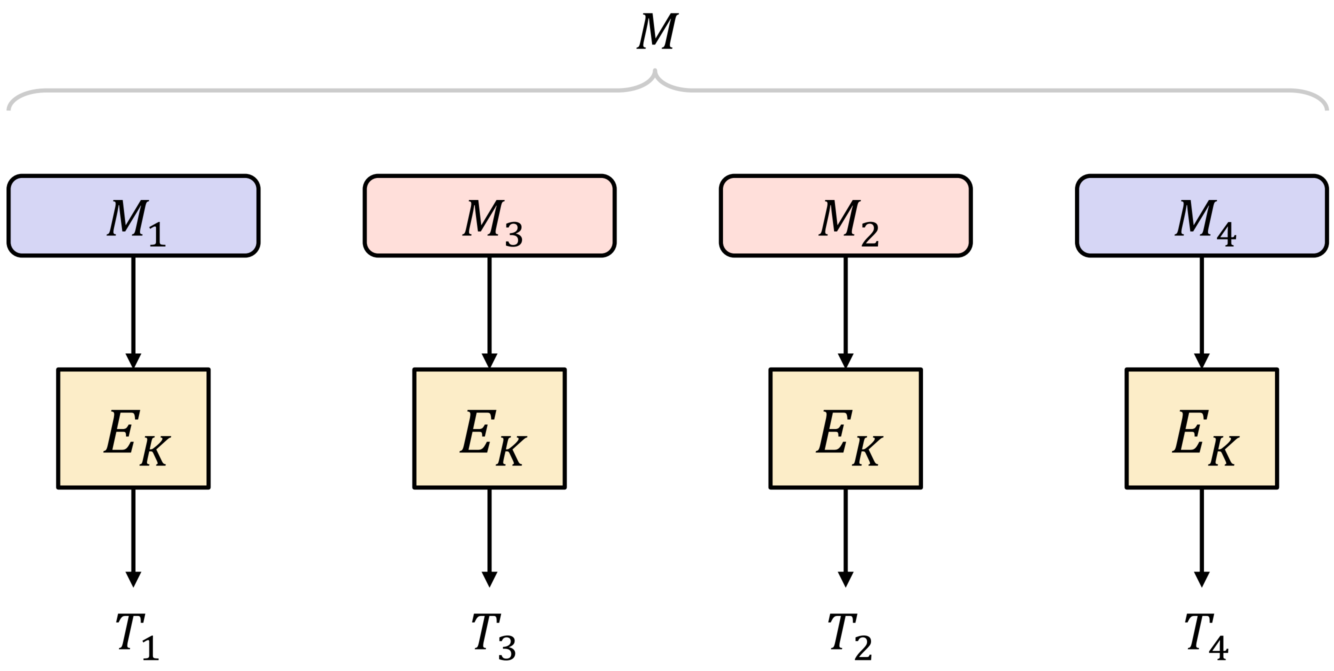
MACs for long messages

MACs from block ciphers – Attempt 1



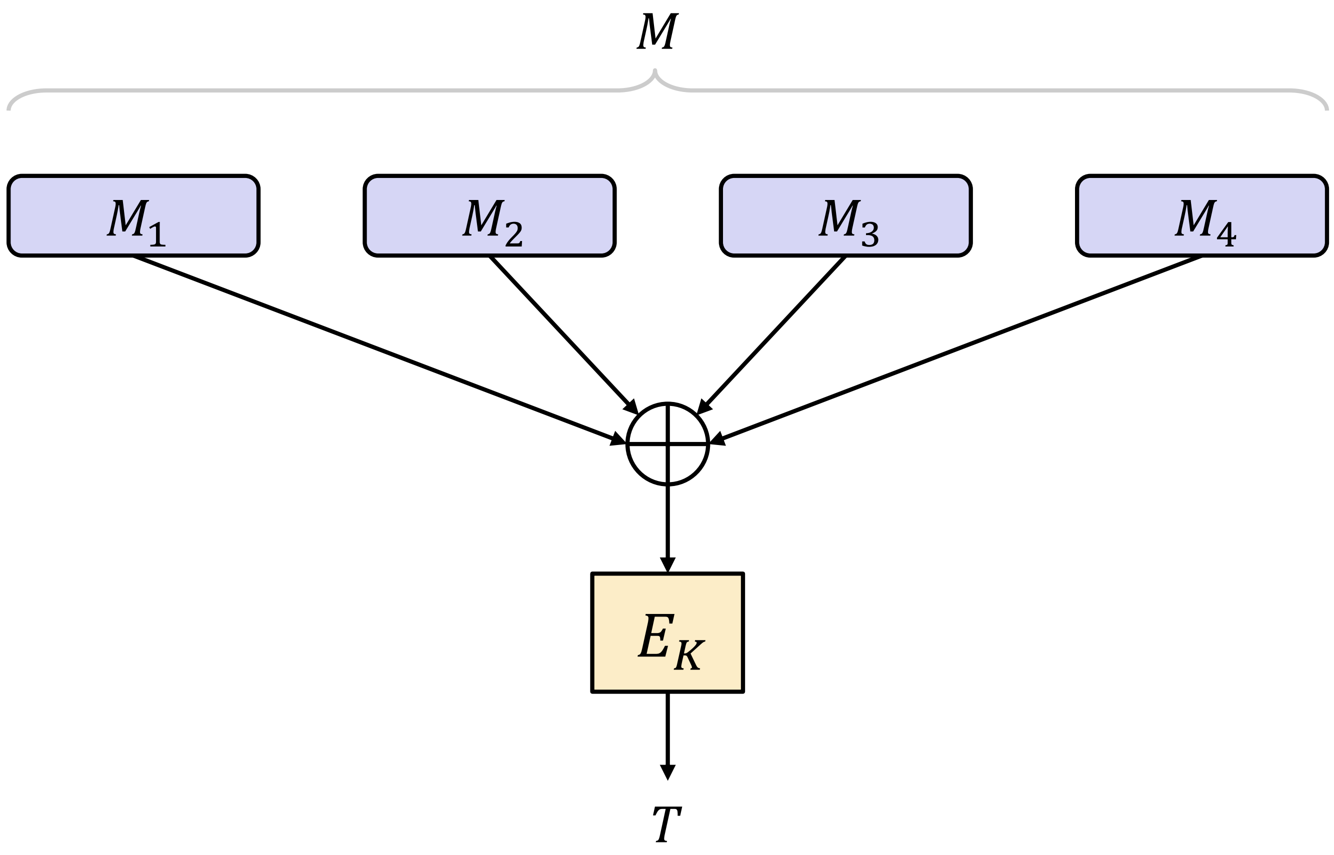
$$T = T_1||T_2||T_3||T_4$$

Attempt 1 – an attack

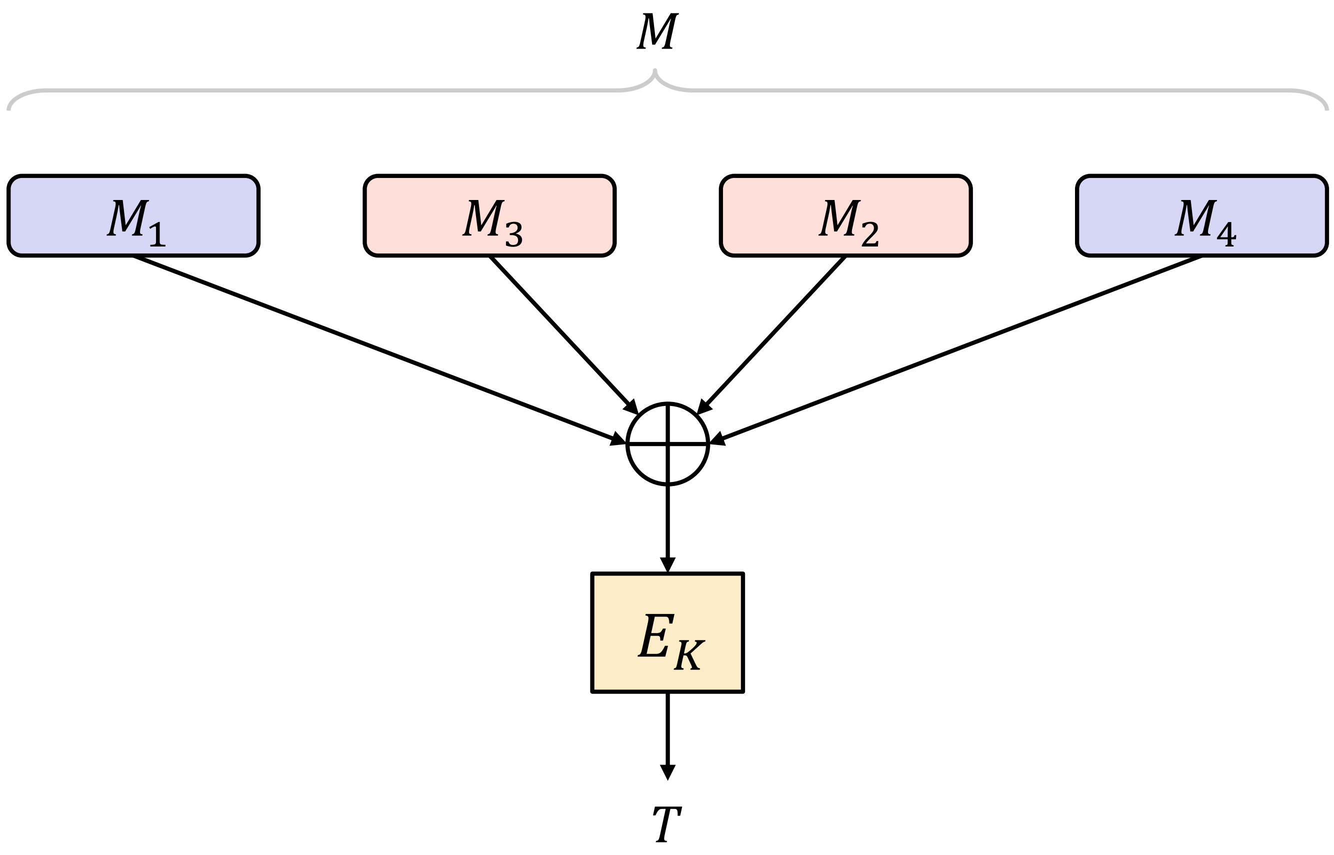


$$T = T_1||T_3||T_2||T_4$$

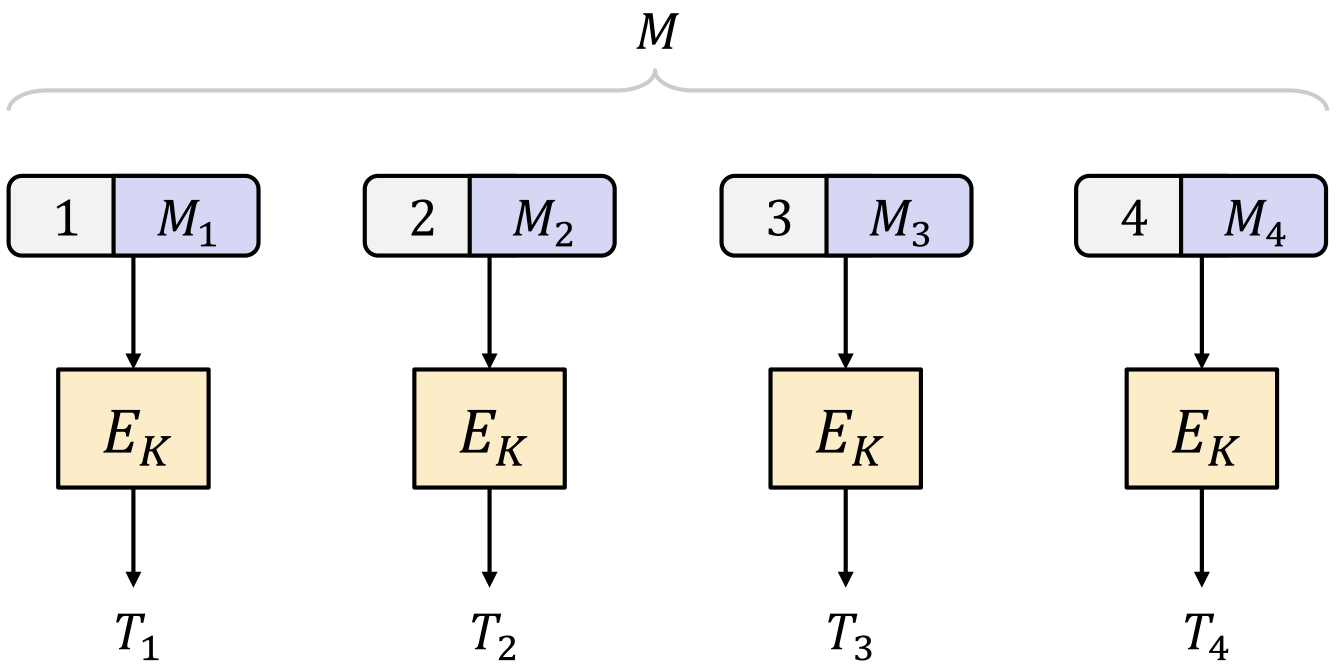
Attempt 2



Attempt 2 – an attack

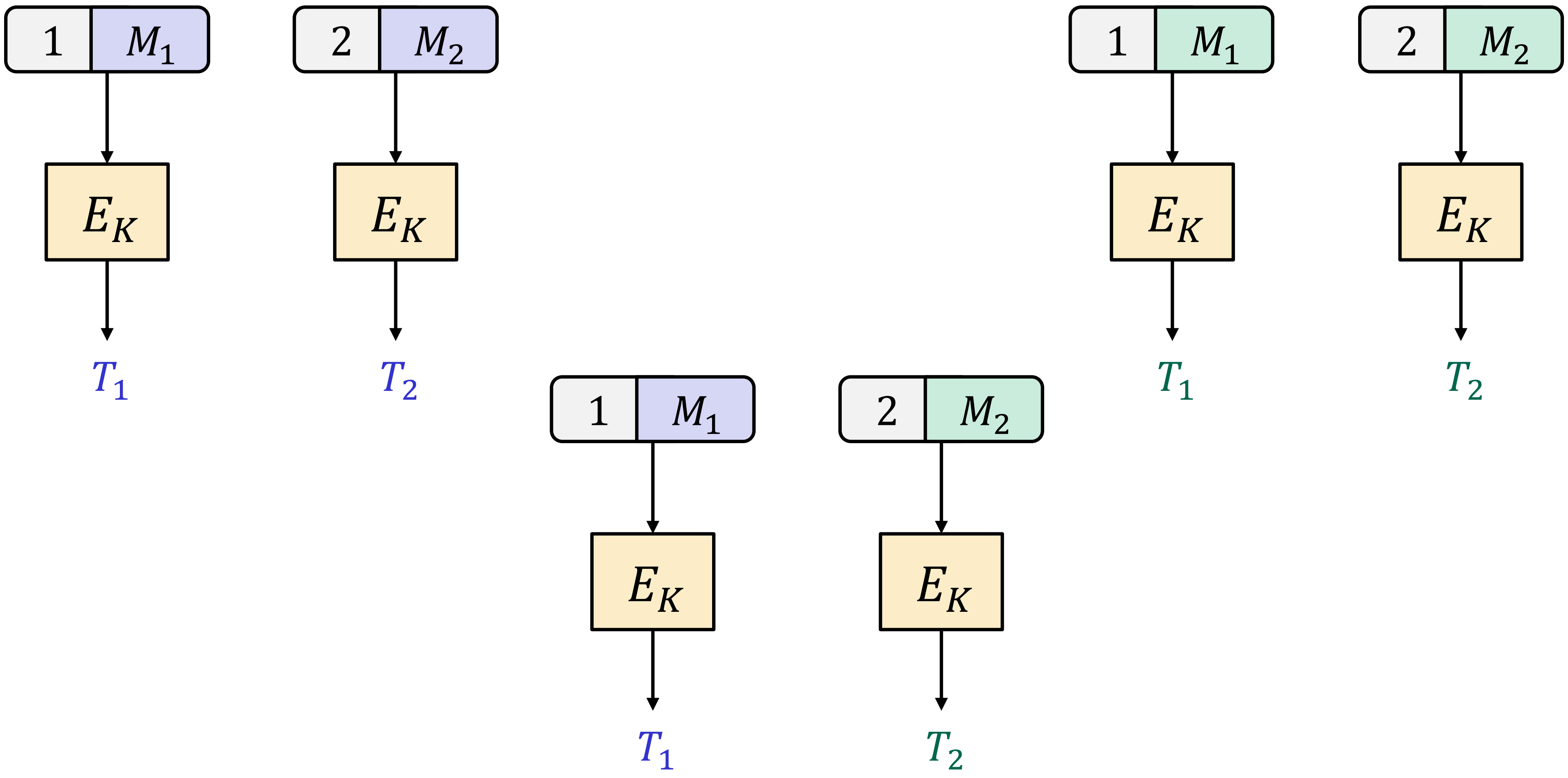


Attempt 3

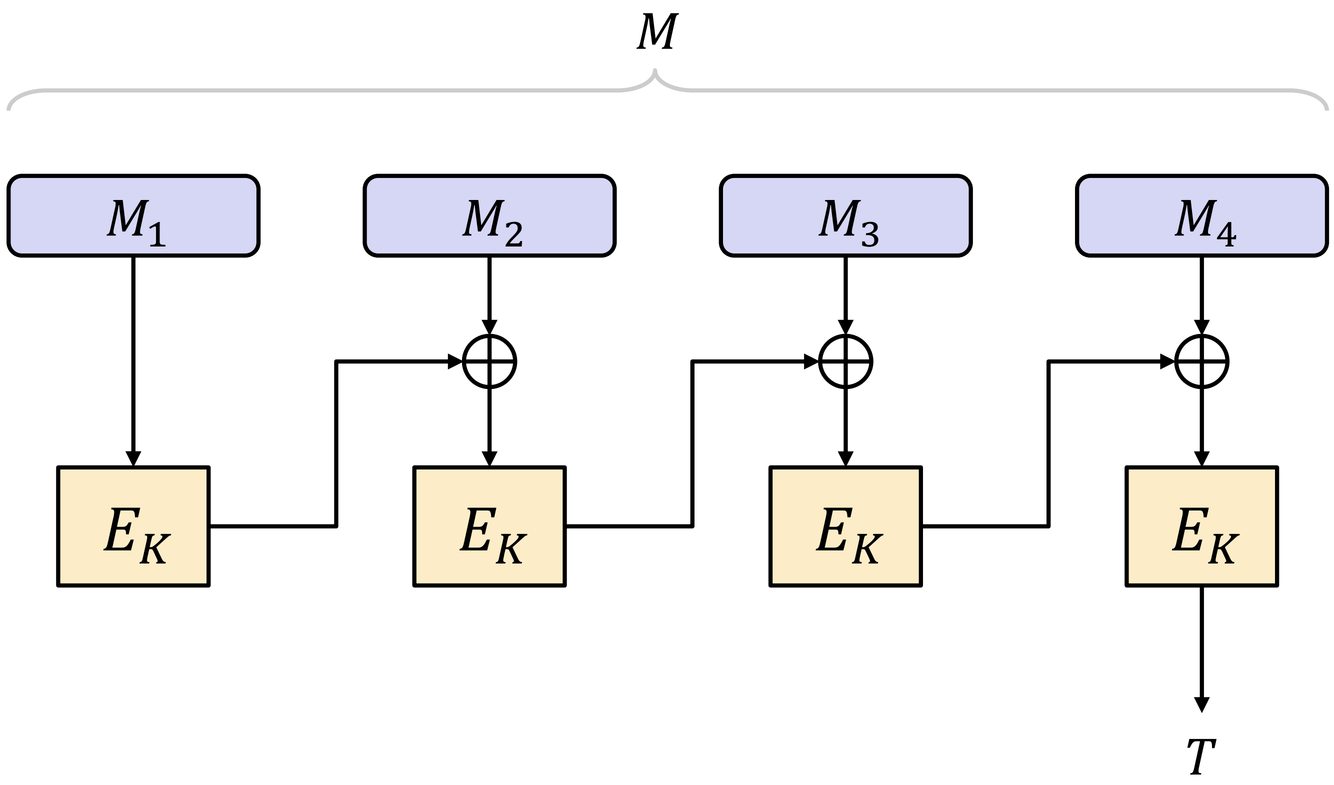


$$T = T_1 || T_2 || T_3 || T_4$$

Attempt 3 – an attack



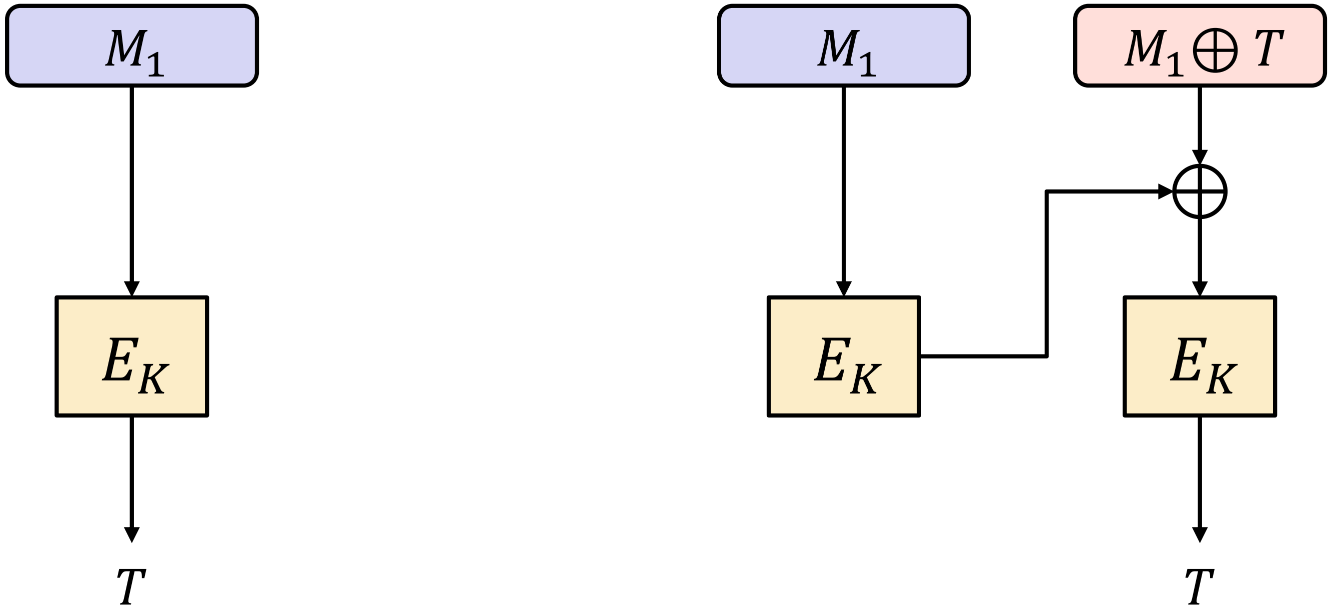
CBC-MAC



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

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

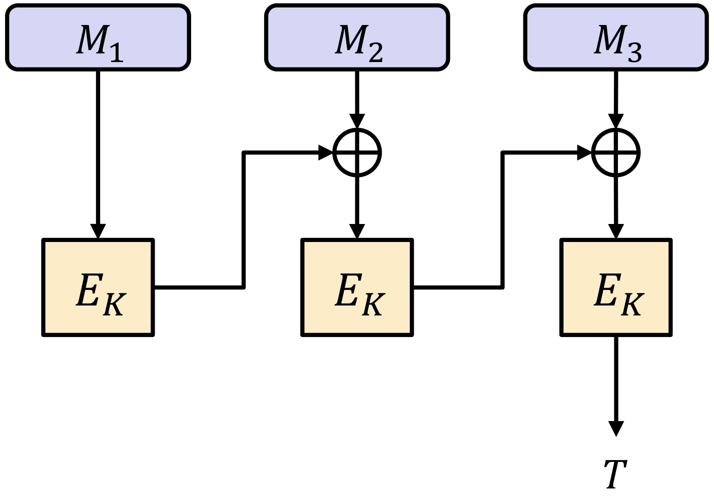
CBC-MAC

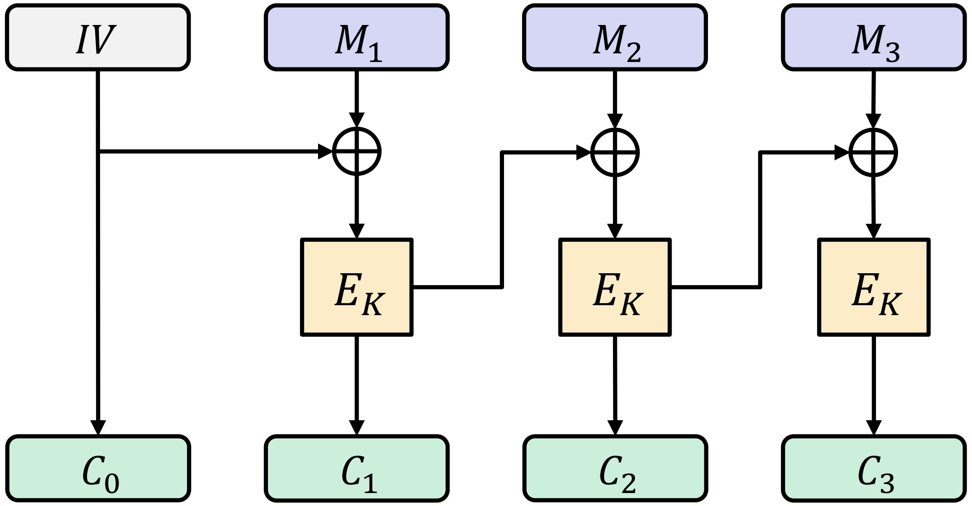


$$\mathbf{Adv}^{\text{uf-cma}}_{\text{CBC-MAC}}(A) = 1$$

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

CBC-MAC vs. CBC$-ENC





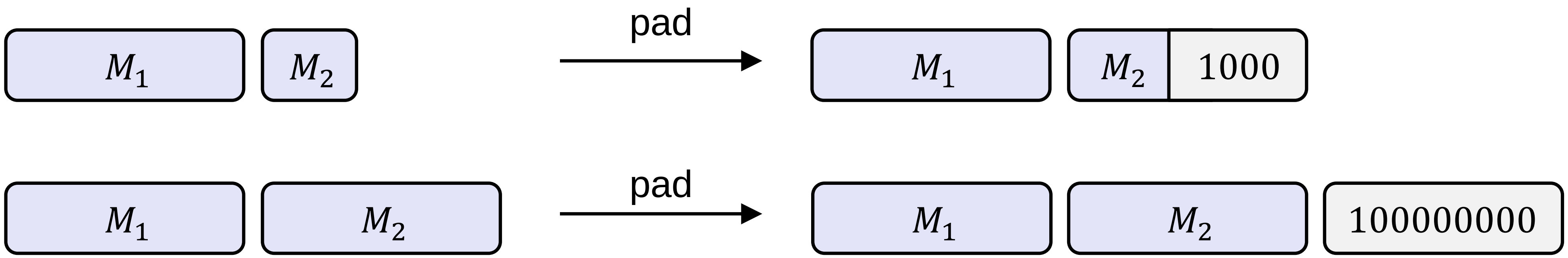
Warning 1: CBC-MAC is insecure *with* an IV!

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

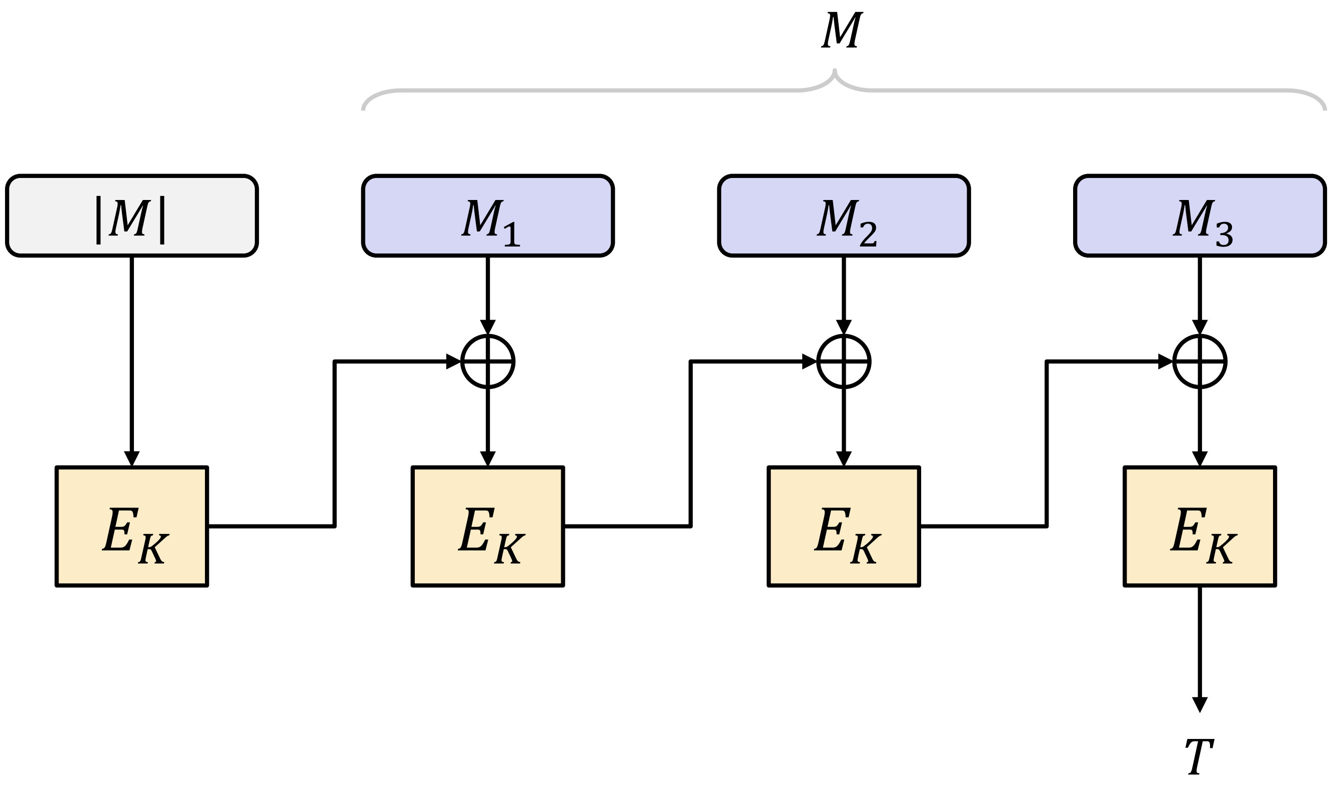
Allowing variable-length messages

- Want to support different-length messages
  - Could use different keys for each length ⟹ not practical

- Want to support message not a multiple of the block length
  - **Padding** needed



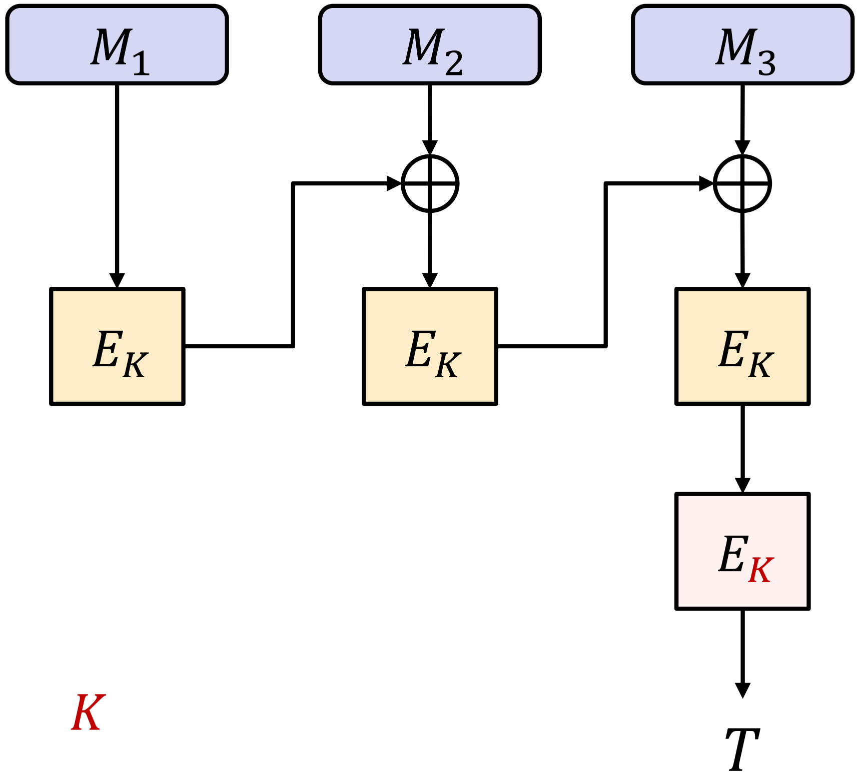
Length-prepended CBC-MAC

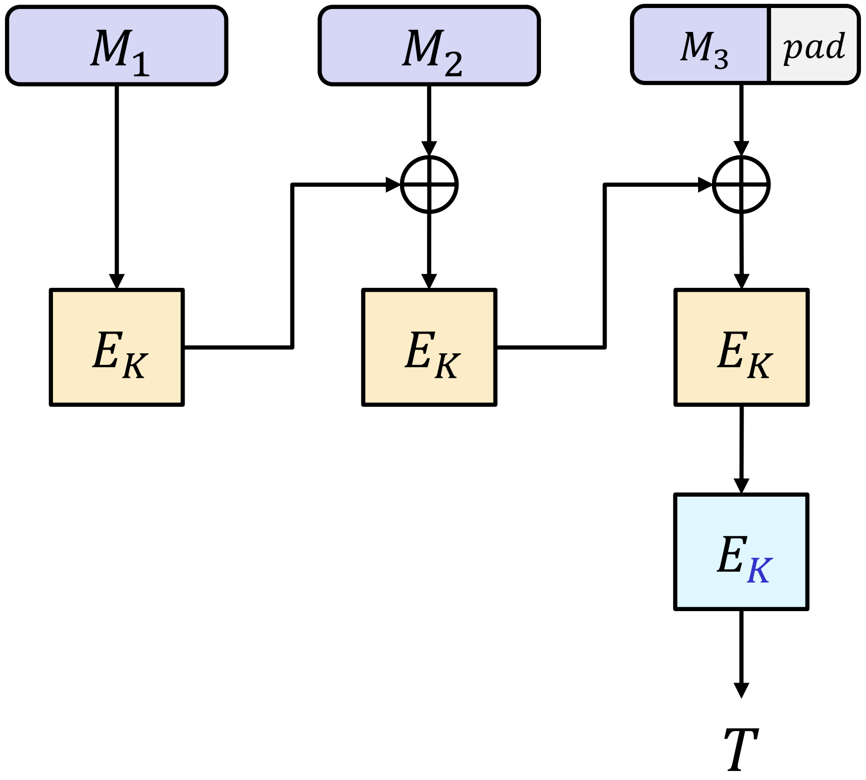


Theorem: Length-prepended CBC-MAC is UF-CMA secure if E is a secure PRP

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

ECBC-MAC



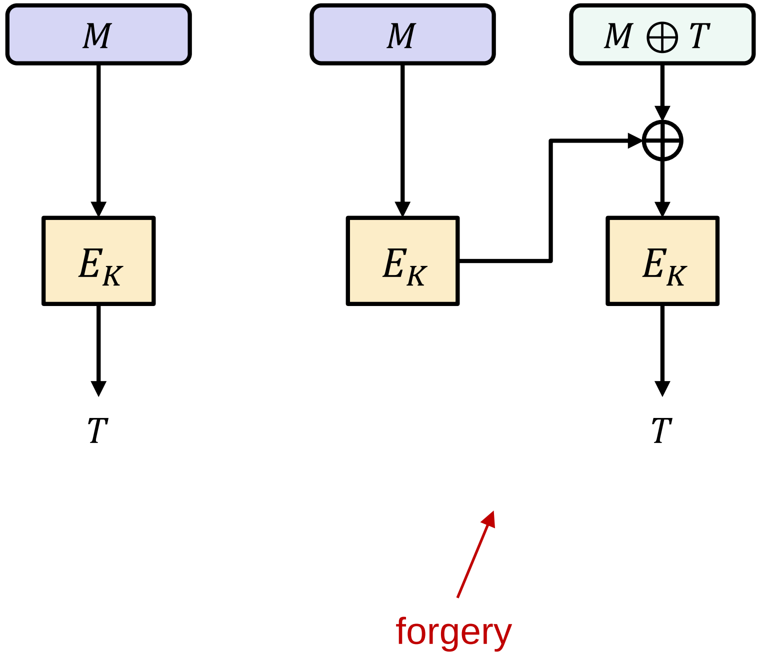


K

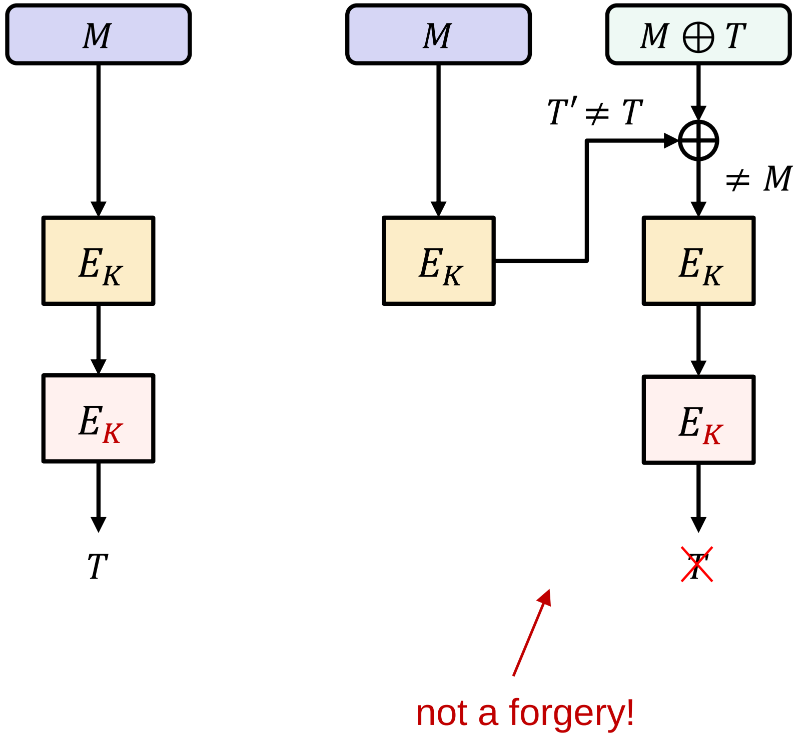
K

CBC-MAC vs ECBC-MAC

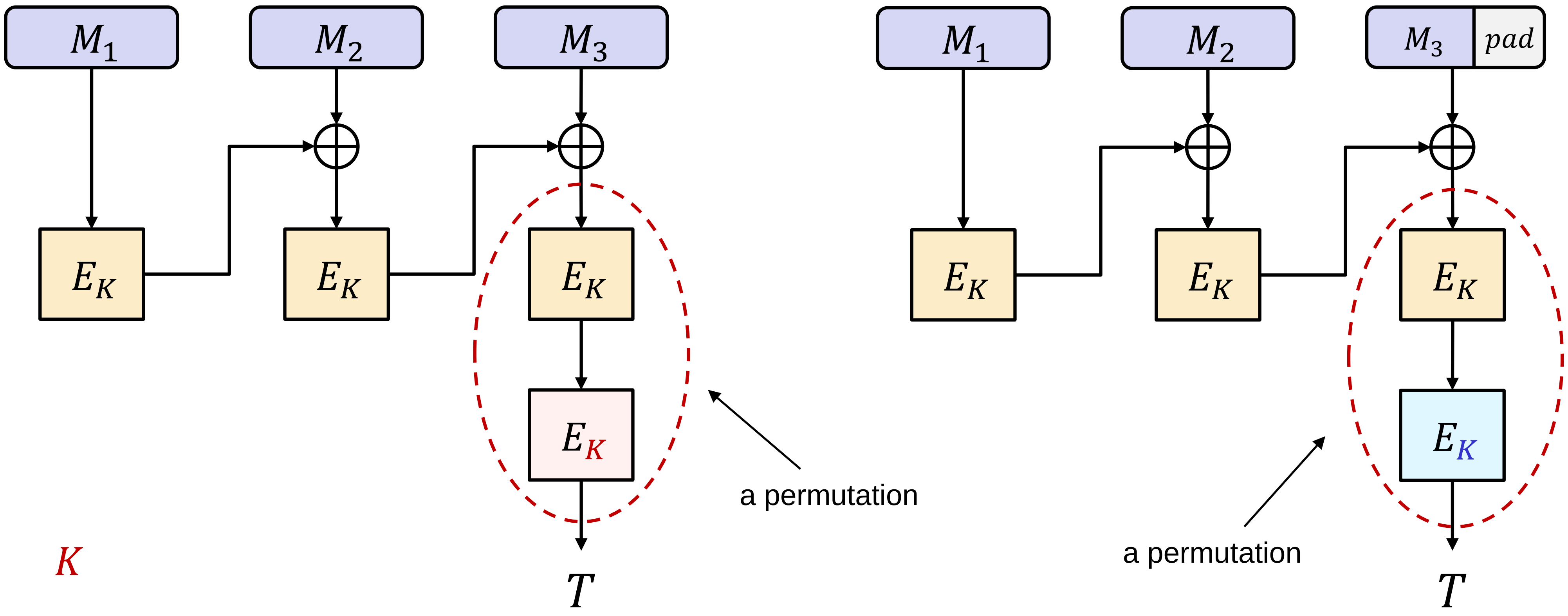
CBC-MAC



ECBC-MAC



ECBC-MAC

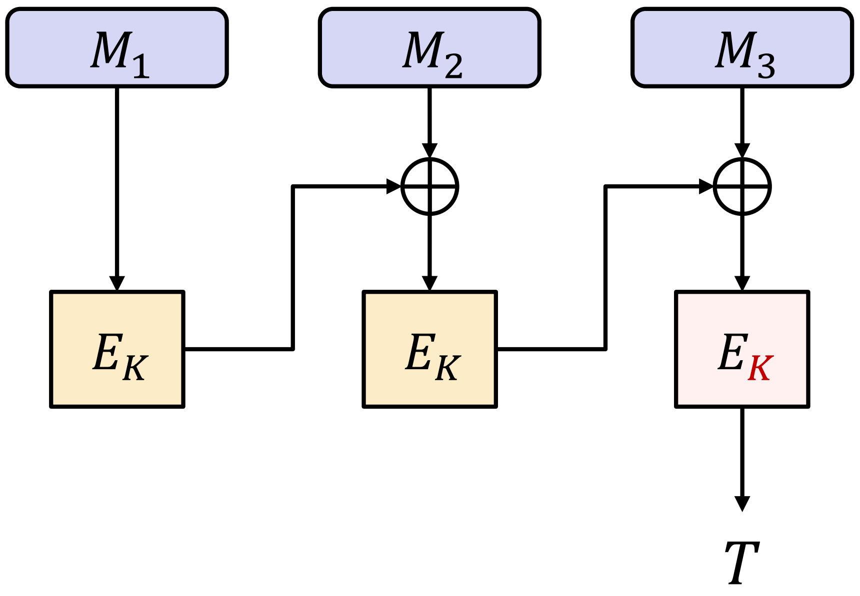


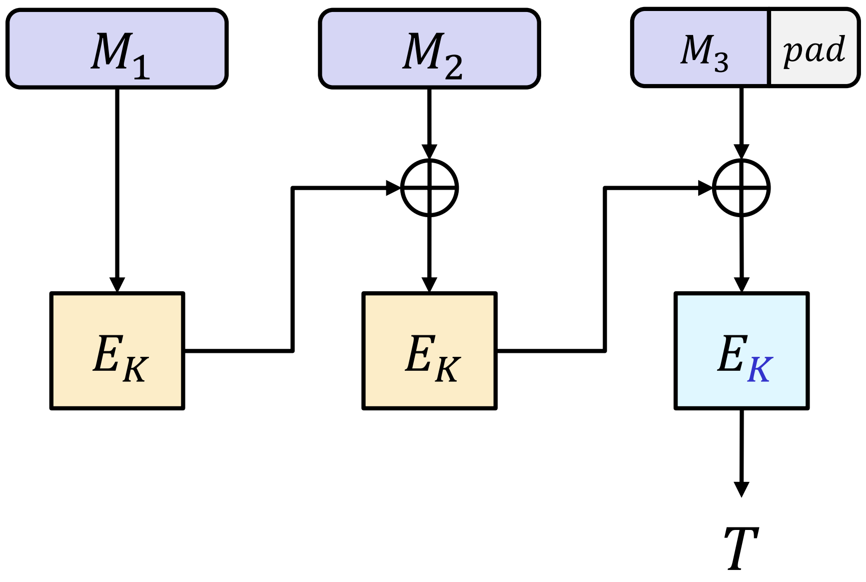
M_1
M_2
M_3
E_K
E_K
E_K
E_K
a permutation
T
M_1
M_2
M_3
pad
E_K
E_K
E_K
E_K
a permutation
T

K

K

FCBC-MAC

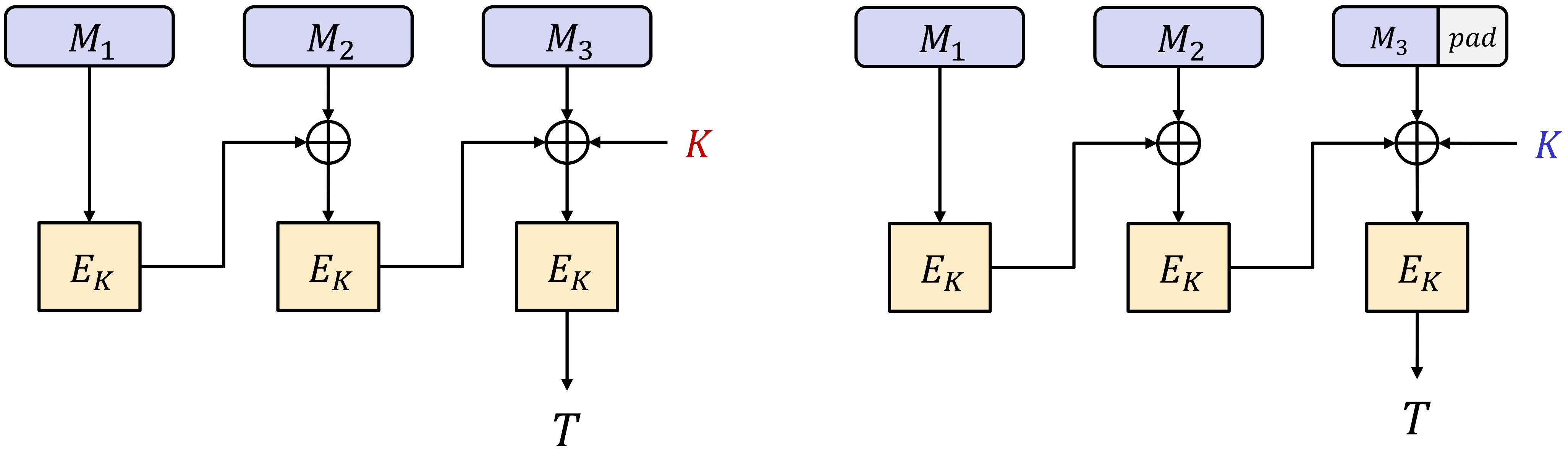




K

K

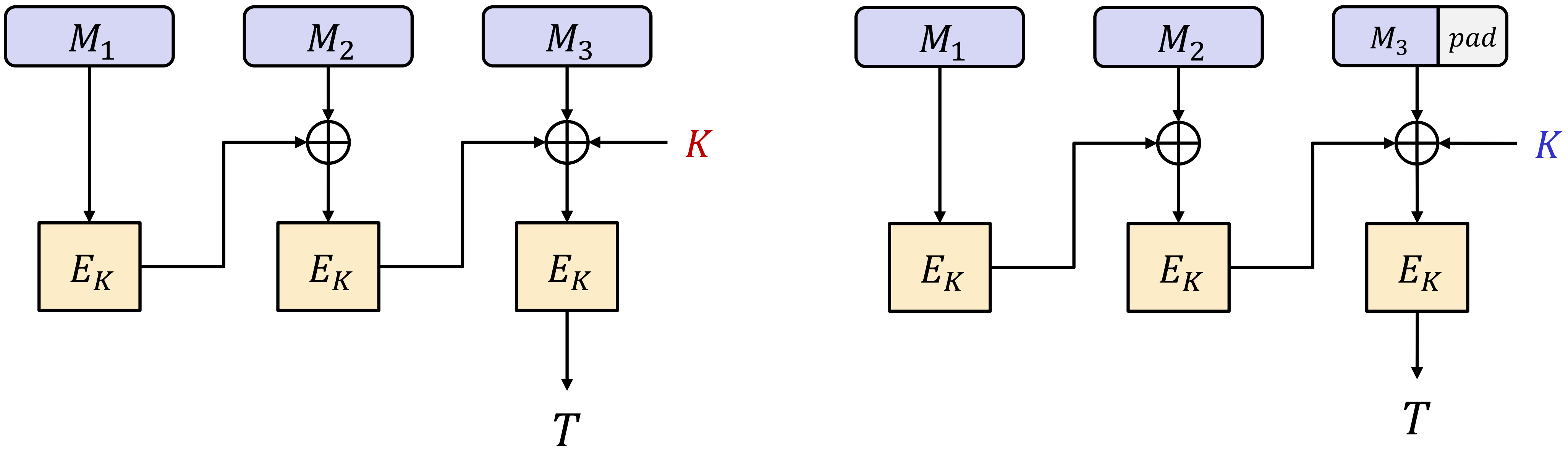
XCBC-MAC



K

K

CMAC a.k.a One-key MAC (CMAC)



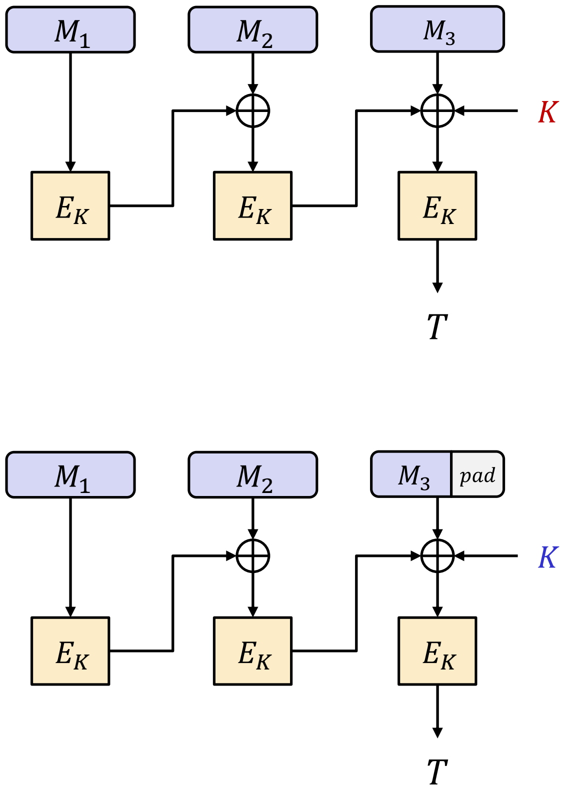
$K = 2 * E_K(0^n)$

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

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
  - Wide used



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

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

CMAC security

Theorem: If $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is a secure PRP then CMAC is UF-CMA secure.

Detailed: For *any* UF-CMA adversary making q Tag-queries, each having blocks, and v Vrfy-queries, there is a PRP-adversary B such that

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

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

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

CMAC security

Theorem: If $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is a secure PRP then CMAC is UF-CMA secure.

Detailed: For *any* UF-CMA adversary making q Tag-queries, each having blocks, and v Vrfy-queries, there is a PRP-adversary B such that

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

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

Prob. > 1!

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

CMAC security

Theorem: If $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is a secure PRP then CMAC is UF-CMA secure.

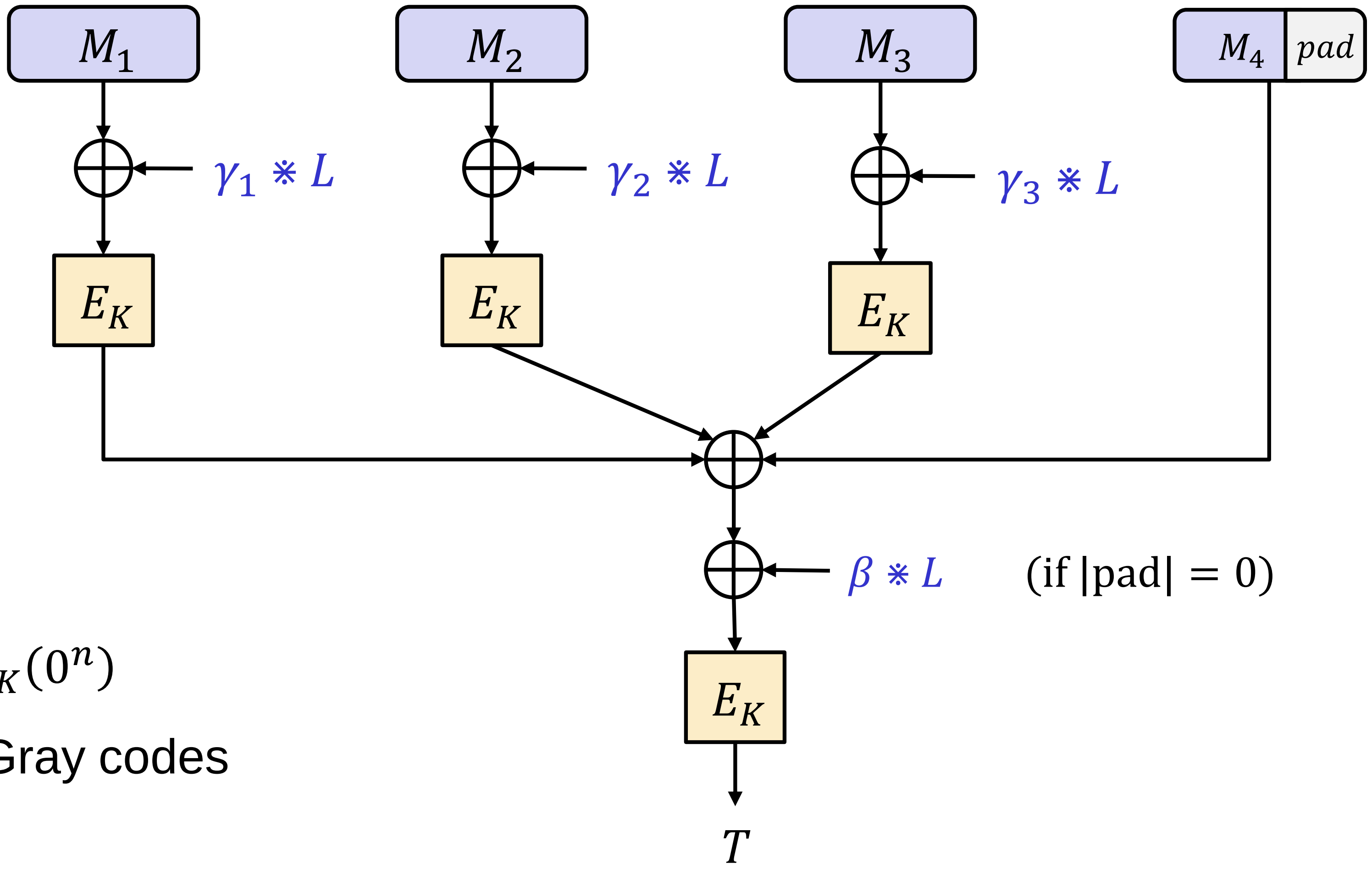
Detailed: For *any* UF-CMA adversary making q Tag-queries, each having blocks, and v Vrfy-queries, there is a PRP-adversary B such that

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

- **Example:**
  - $E = \mathrm{DES} \quad (n = 64)$
  - Number of Tag-queries: $q = 2^{16} \approx 65\,000$ queries
  - Max blocks per message: $\ell = 2^{10} \approx 1\ \mathrm{kB}$
  - Number of Vrfy-queries: $v = 2^{40}$
  - $\mathbf{Adv}_{E}^{\mathrm{prp}}(B) \approx 0$

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

PMAC

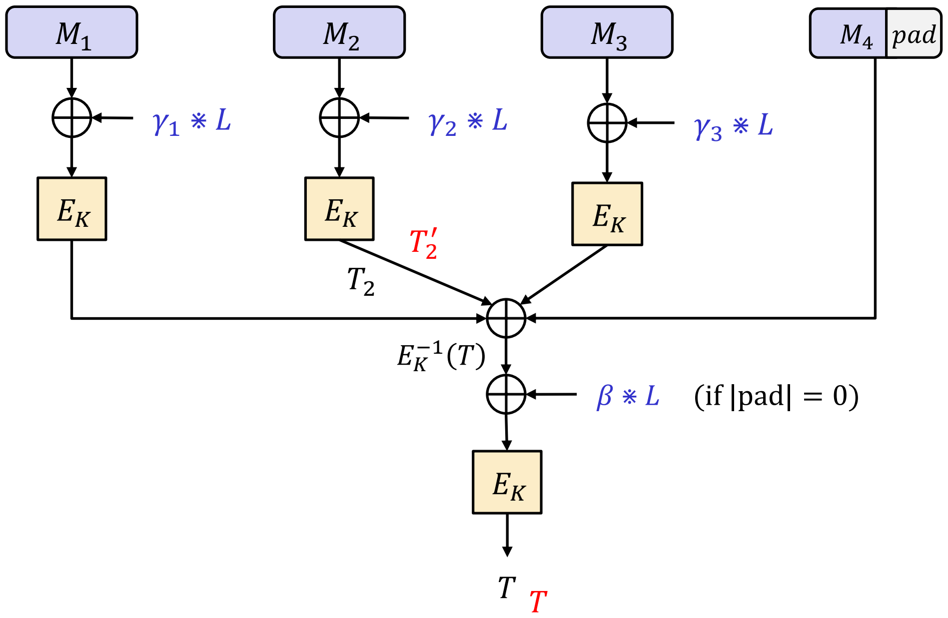


$L = F_K(0^n)$

γ_i = Gray codes

PMAC properties

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



$$\mathrm{PMAC}(K, M_1||M_2||\ldots||M_{1000}) = T$$

$$\mathrm{PMAC}(K, M_1||M'_2||\ldots||M_{1000}) = E_K(E_K^{-1}(T) \oplus T_2 \oplus T'_2) = T$$

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

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

Summary

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