CIS 4360: Computer Security Fundamentals

Message Authentication Code

Viet Tung Hoang

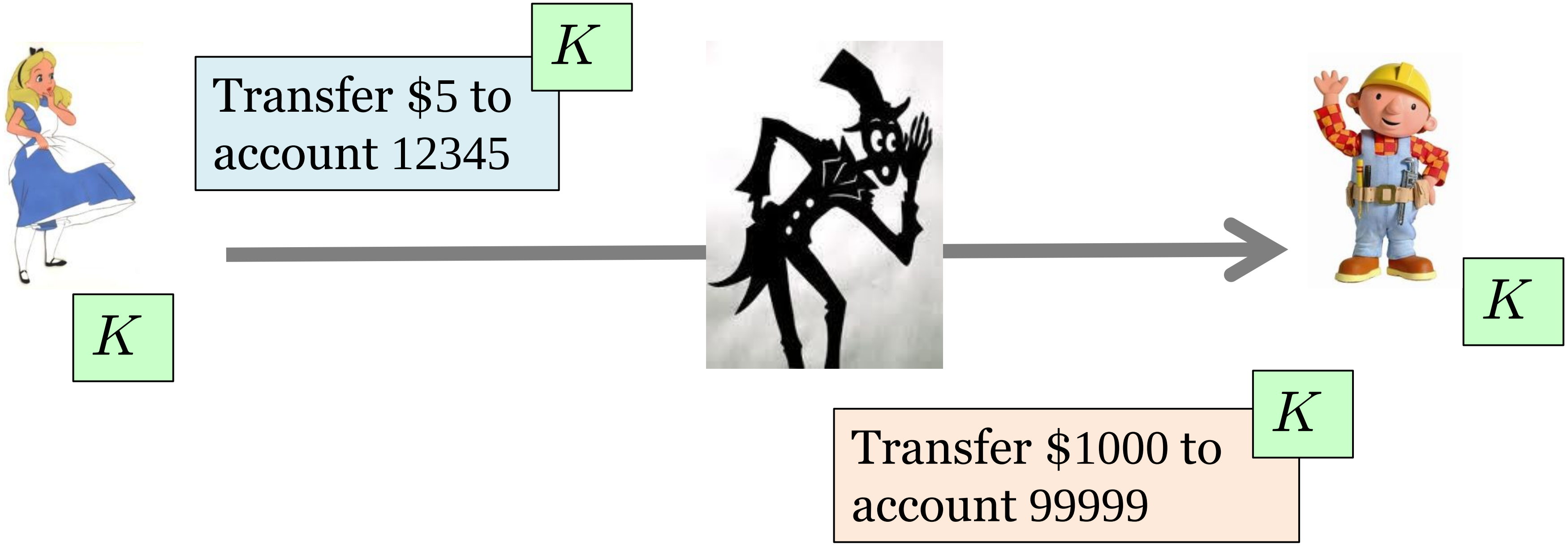
The slides are loosely based on those of
Prof. Mihir Bellare, UC San Diego.

Agenda

1. MAC and Authenticity

2. MAC Constructions

The Need for Authenticity



K

Transfer $5 to account 12345

K

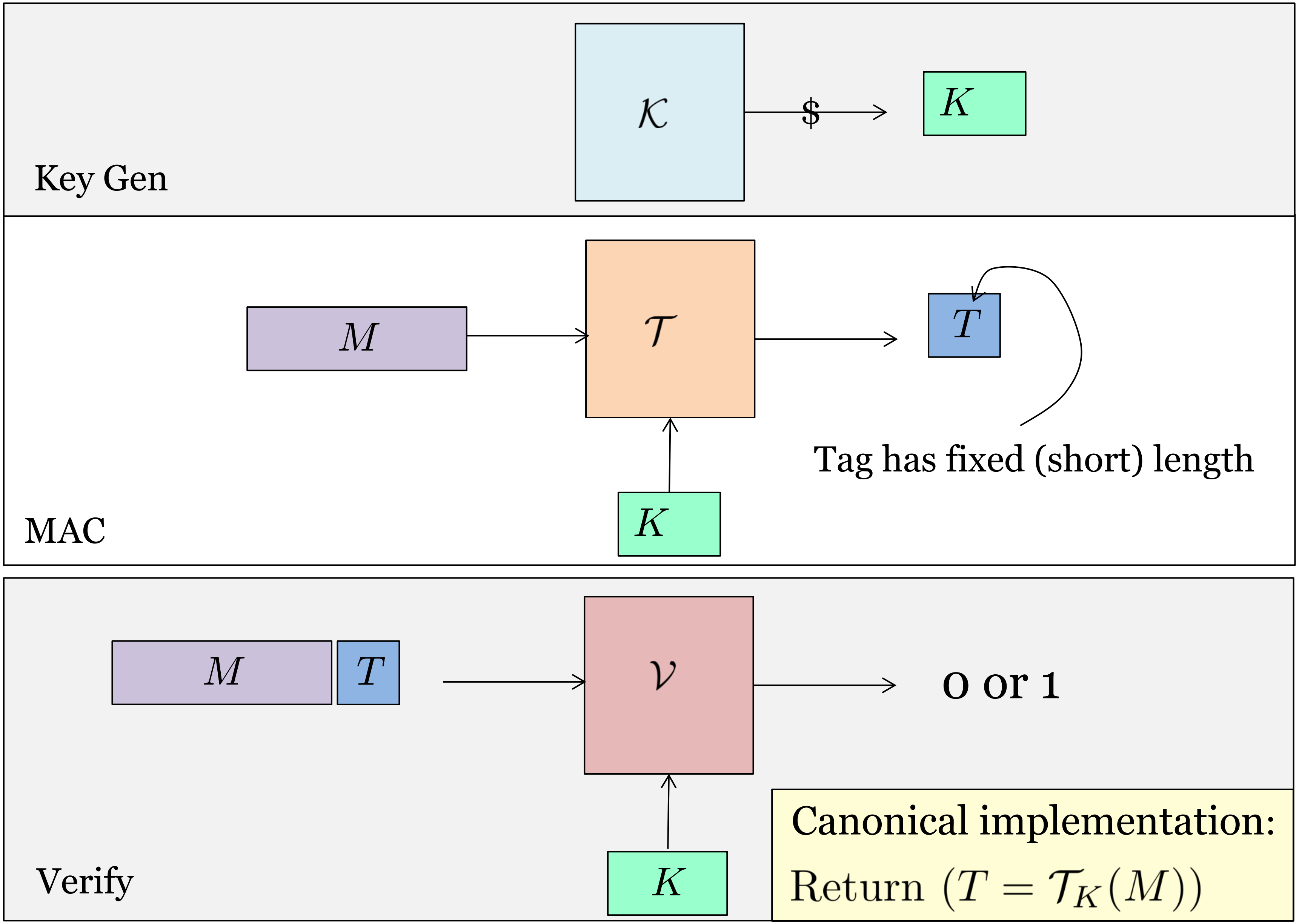
K

K

Transfer $1000 to account 99999

Classical encryptions (CTR, CBC) don’t provide authenticity

MAC Syntax



Key Gen

$\mathcal{K} \xrightarrow{\$} K$

MAC

$M \rightarrow \mathcal{T} \rightarrow T$, with K going into $\mathcal{T}$

Tag has fixed (short) length

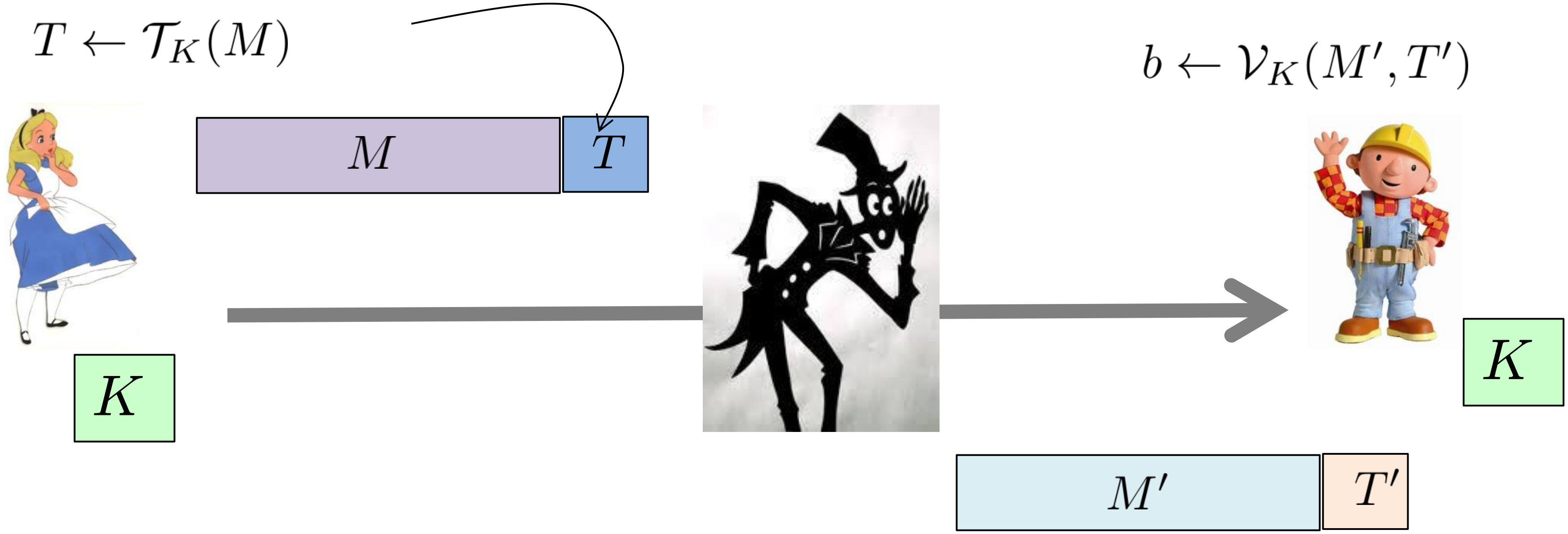
Verify

$M \; T \rightarrow \mathcal{V} \rightarrow$ 0 or 1, with K going into $\mathcal{V}$

Canonical implementation:

Return $(T = \mathcal{T}_K(M))$

MAC Usage



$T \leftarrow \mathcal{T}_K(M)$

M T

K

$b \leftarrow \mathcal{V}_K(M', T')$

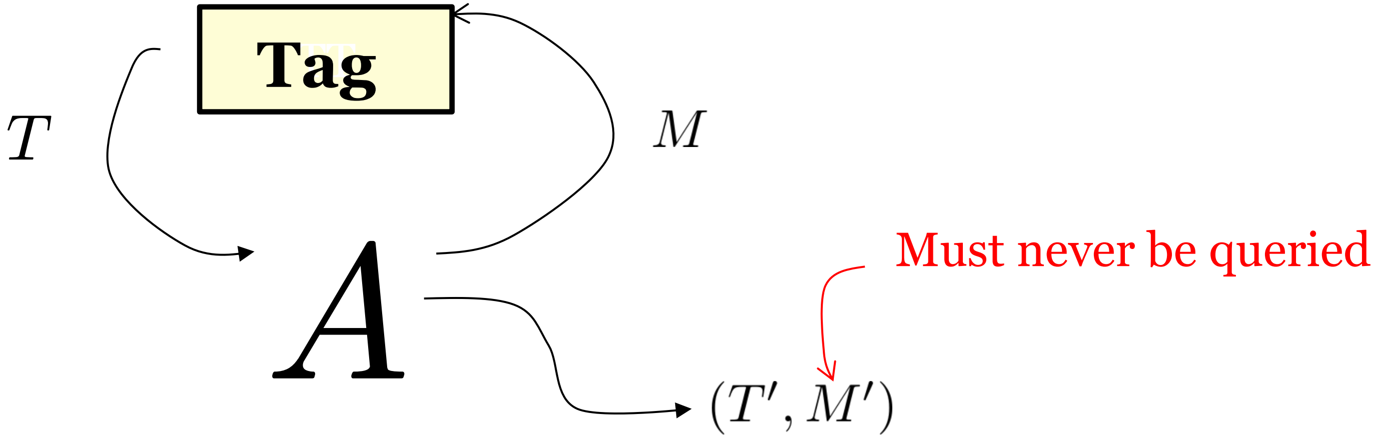
K

M' T'

Formalizing Security

MAC$_{\mathcal{T}}$

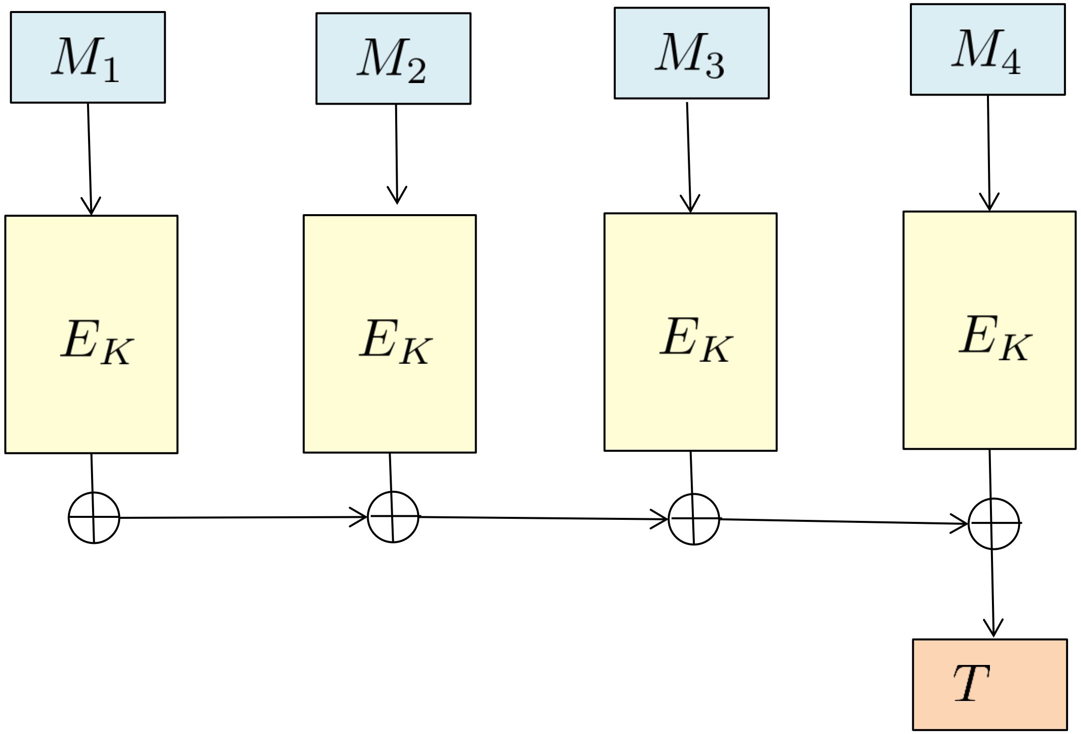
```
procedure Initialize()
    $K \xleftarrow{\$} \mathcal{K}$

procedure Tag($M$)
    Return $\mathcal{T}_K(M)$

procedure Finalize($T', M'$)
    Return $(T' = \mathcal{T}_K(M'))$
```



Must never be queried

$$\mathbf{Adv}^{\mathrm{mac}}_{\mathcal{T}}(A) = \Pr[\mathrm{MAC}^{A}_{\mathcal{T}} \Rightarrow 1]$$

Exercise: Breaking MAC Security With No Query

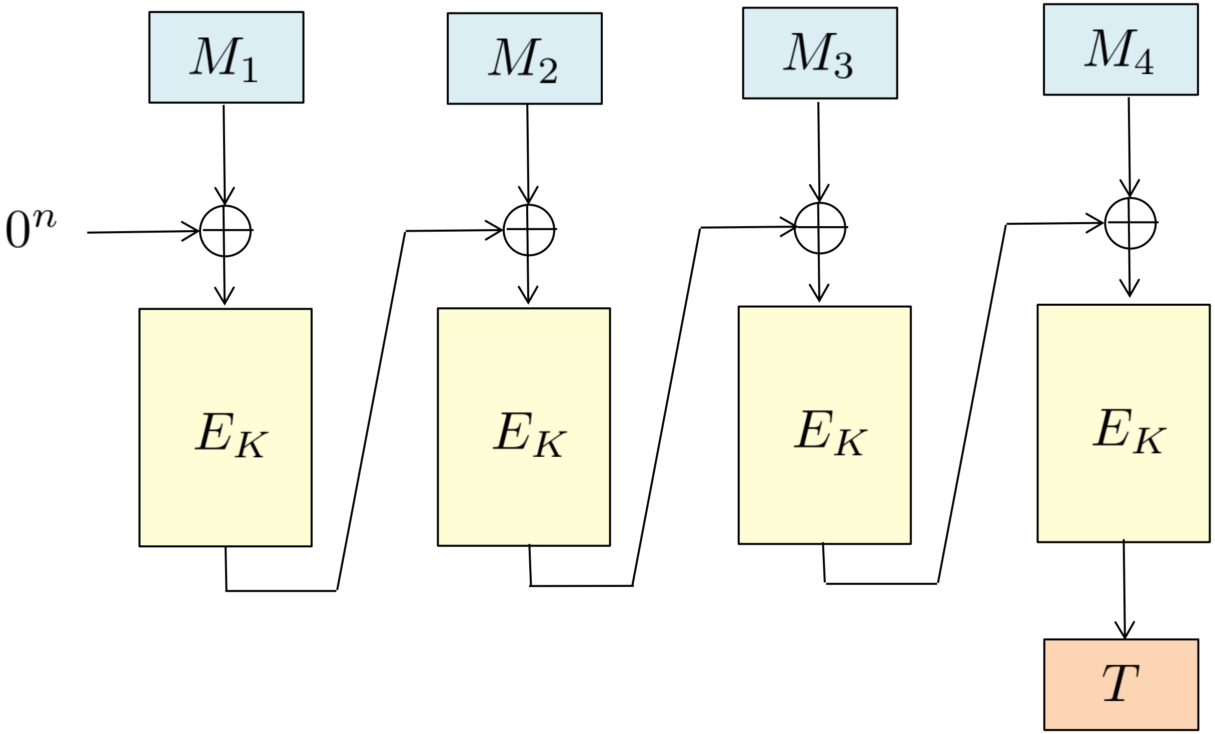


Agenda

1. MAC and Authenticity

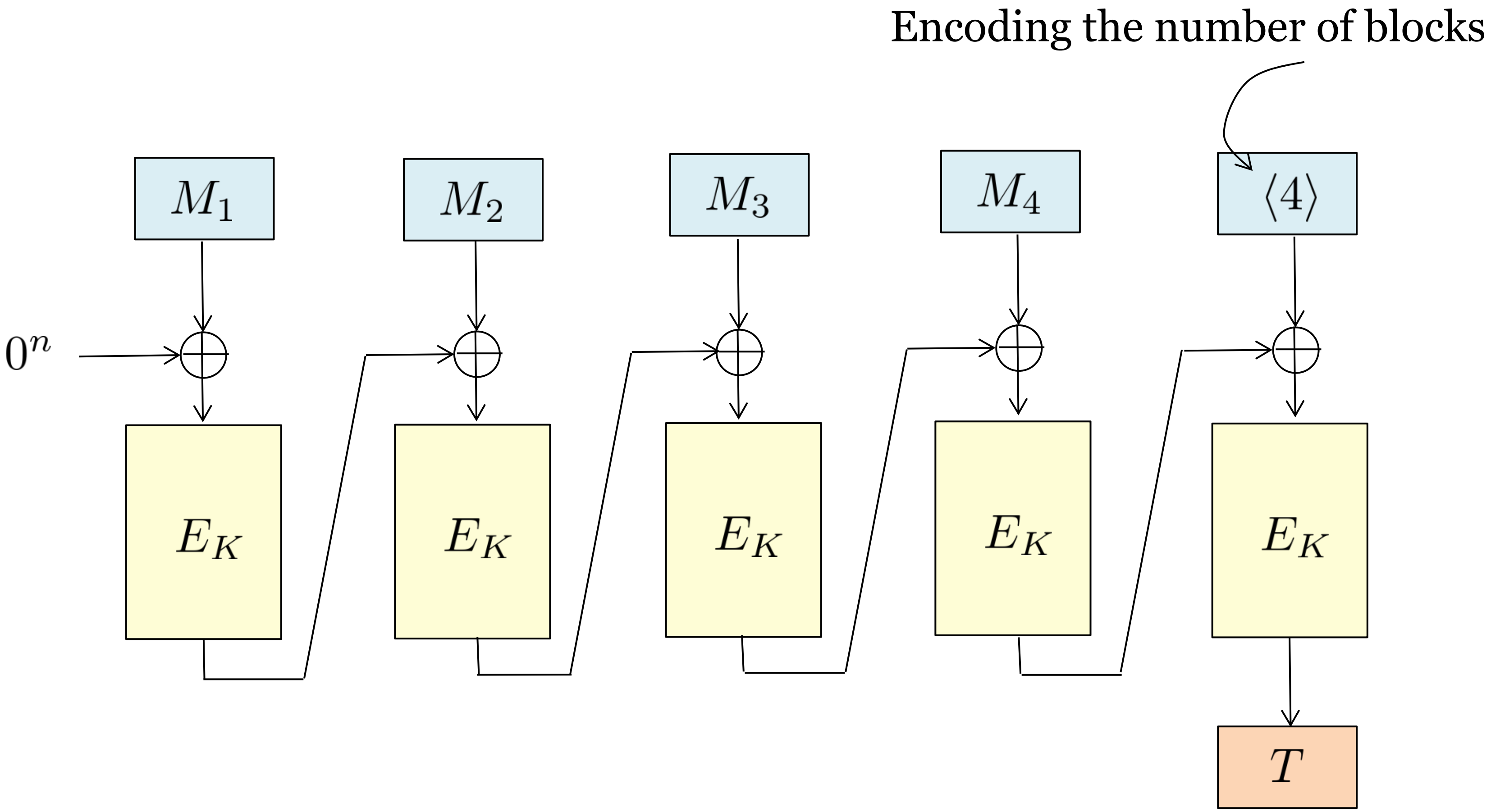
2. **MAC Constructions**

An Insecure Construction: Plain CBC-MAC



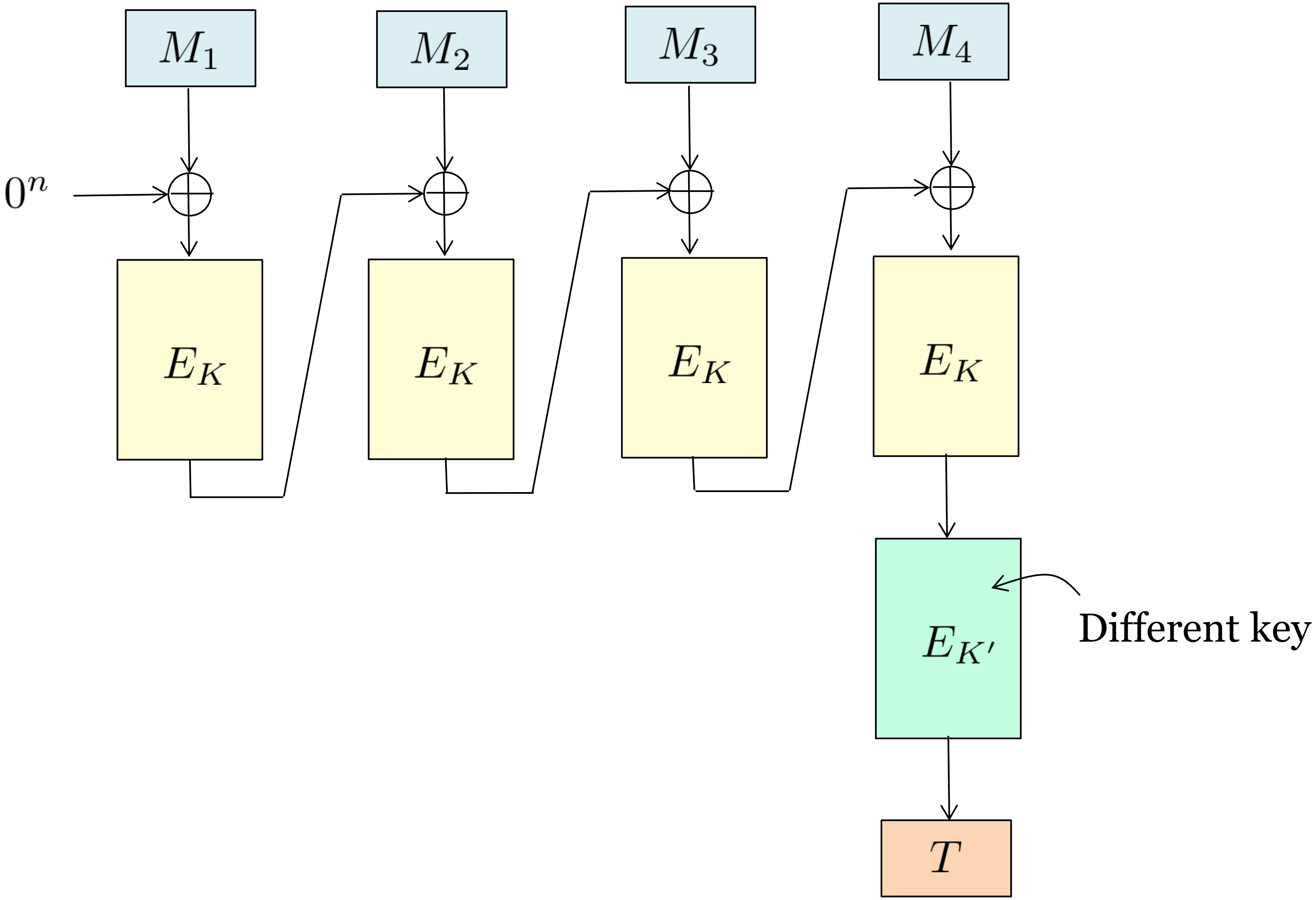
Question: Break CBC-MAC with a single Tag query

An Incorrect Fix of CBC-MAC



Exercise: Break this version using 3 Tag queries

A Good Construction: Encrypted CBC-MAC



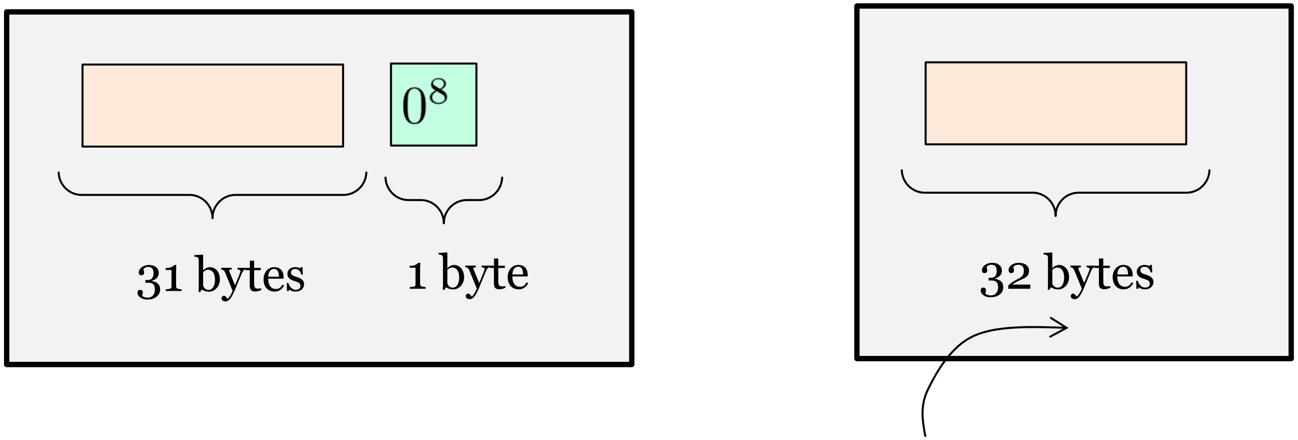
Different key

Dealing with Fragmentary Data

Solution: Padding with 10^*

Question: Can we instead use padding with 0^*?

Example: Suppose that the block length is 16 bytes.



No padding → save bandwidth

Answer: No, can break this with a single Tag query