

CIS 5371, FALL 2025

MESSAGE AUTHENTICATION CODE

VIET TUNG HOANG

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

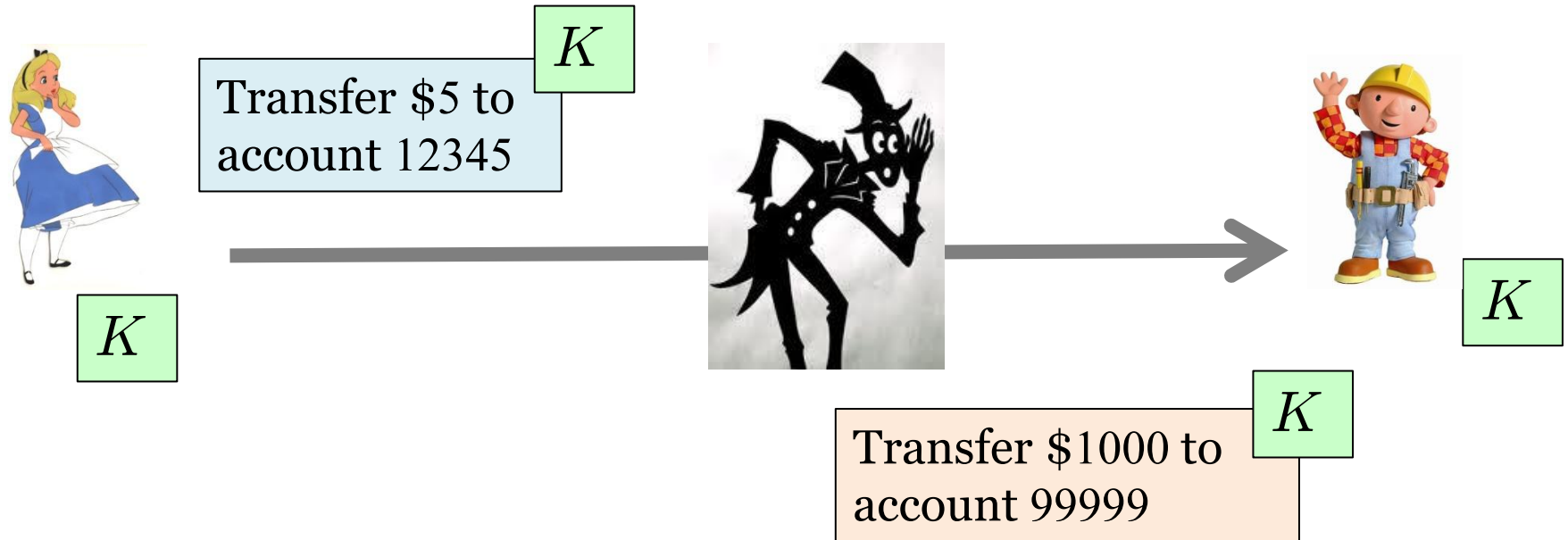
Agenda

1. MAC and Authenticity

2. MAC Constructions

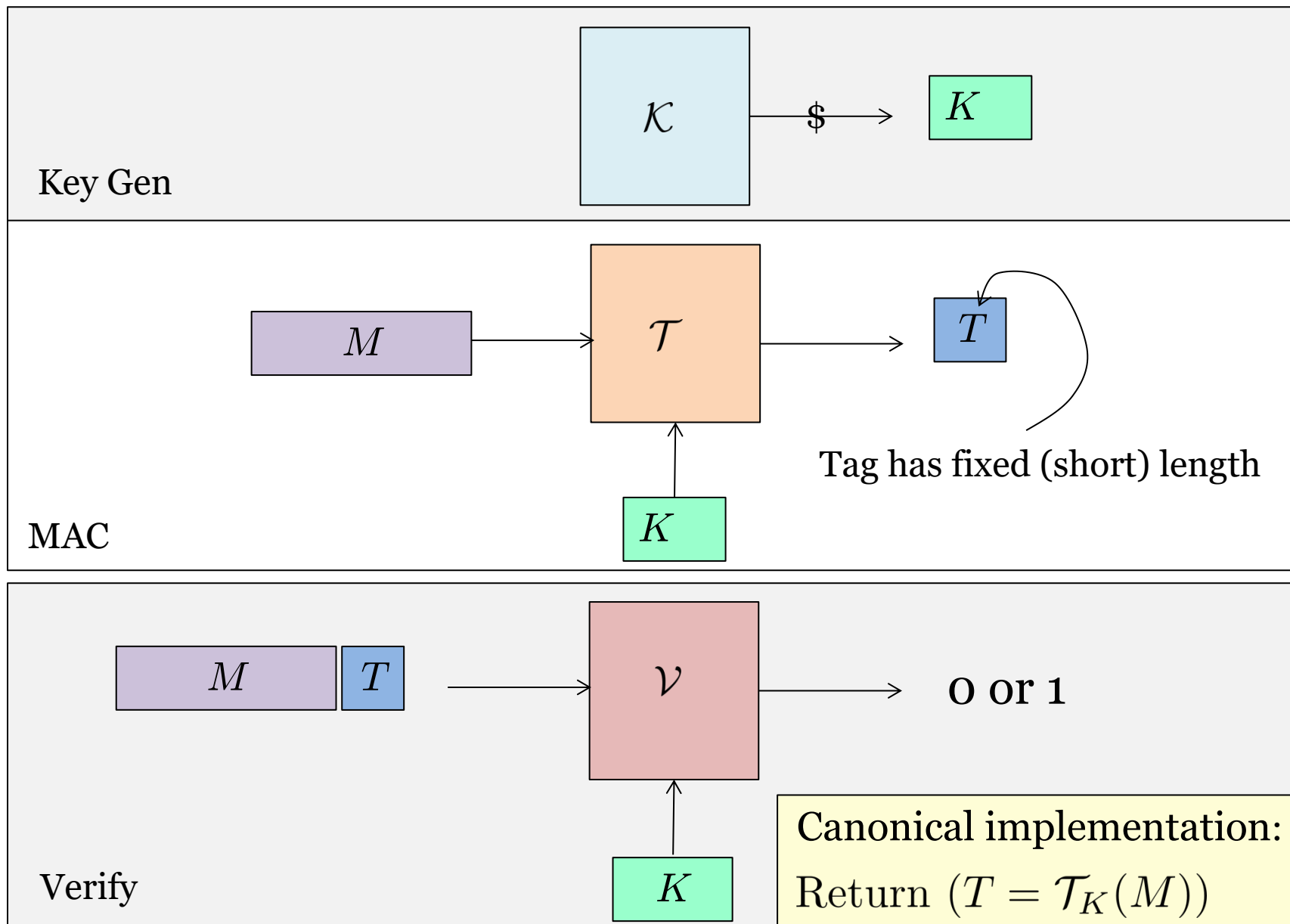
3. How to Construct Good MAC

The Need for Authenticity

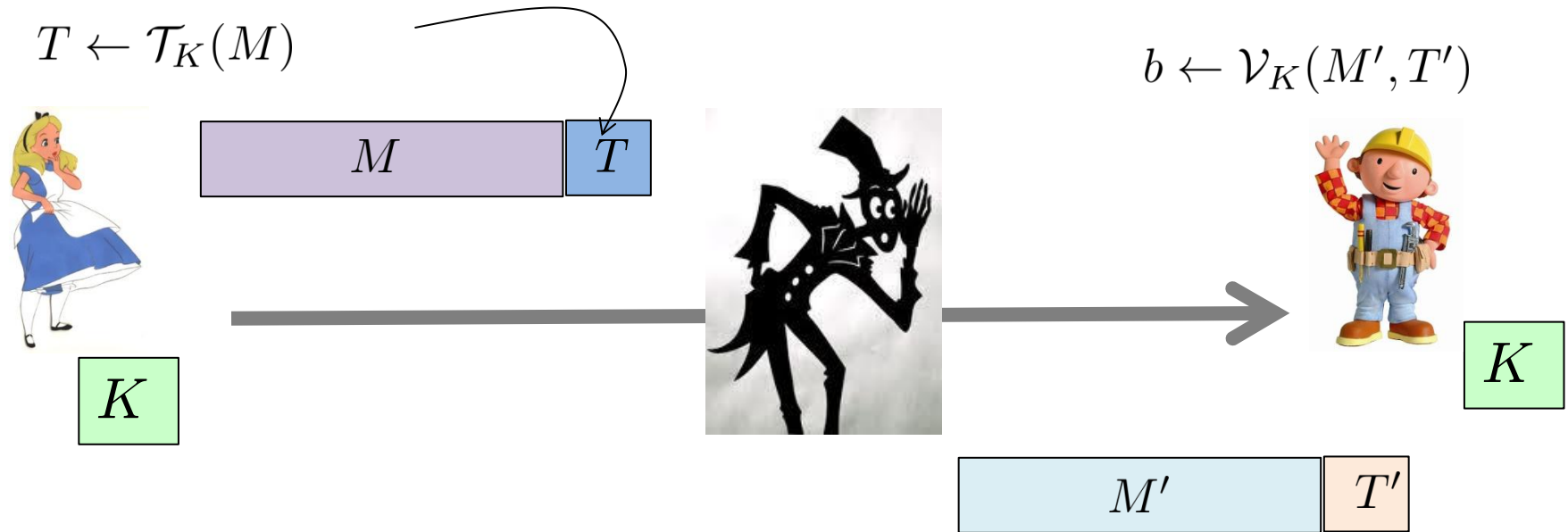


Classical encryptions (CTR, CBC) don't provide authenticity

MAC Syntax



MAC Usage



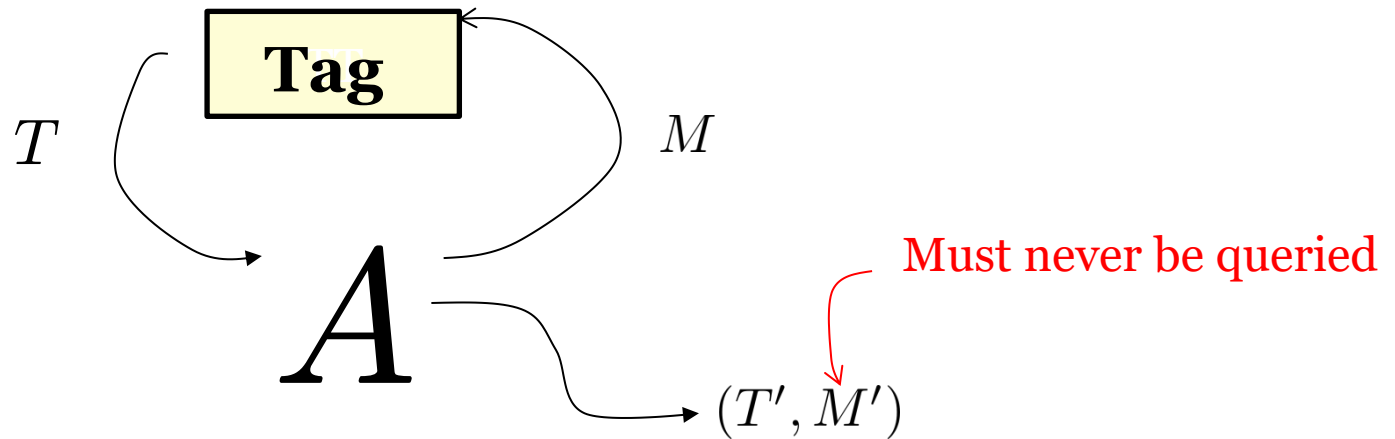
Formalizing Security

MAC _{\mathcal{T}}

procedure **Initialize**()
 $K \leftarrow \$ \mathcal{K}$

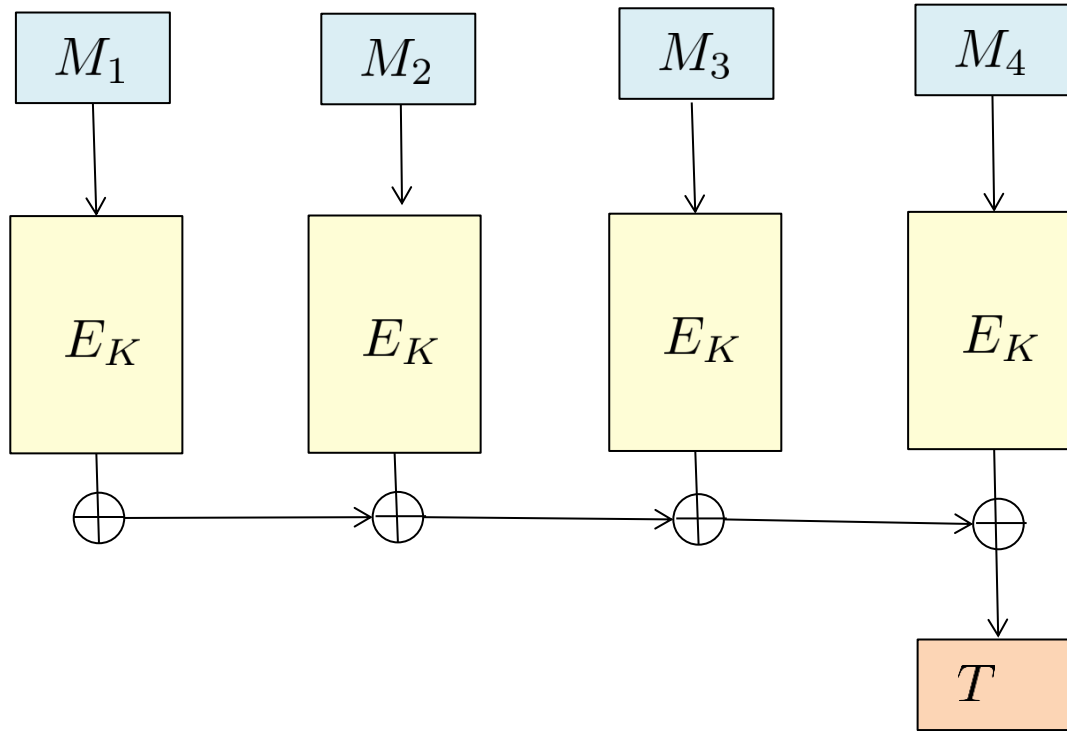
procedure **Tag**(M)
Return $\mathcal{T}_K(M)$

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

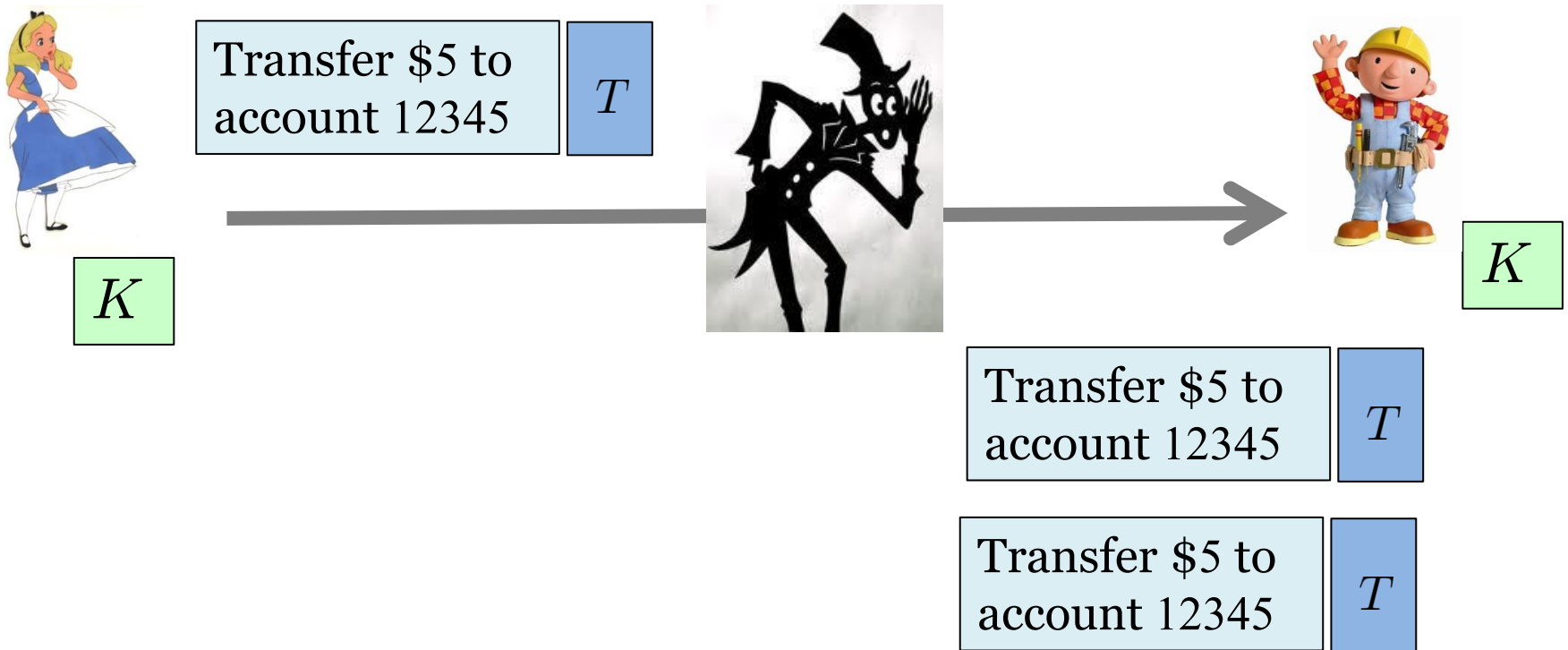


$$\mathbf{Adv}_{\mathcal{T}}^{\text{mac}}(A) = \Pr[\text{MAC}_{\mathcal{T}}^A \Rightarrow 1]$$

Practice: Breaking MAC Security With No Query



Replay Attack

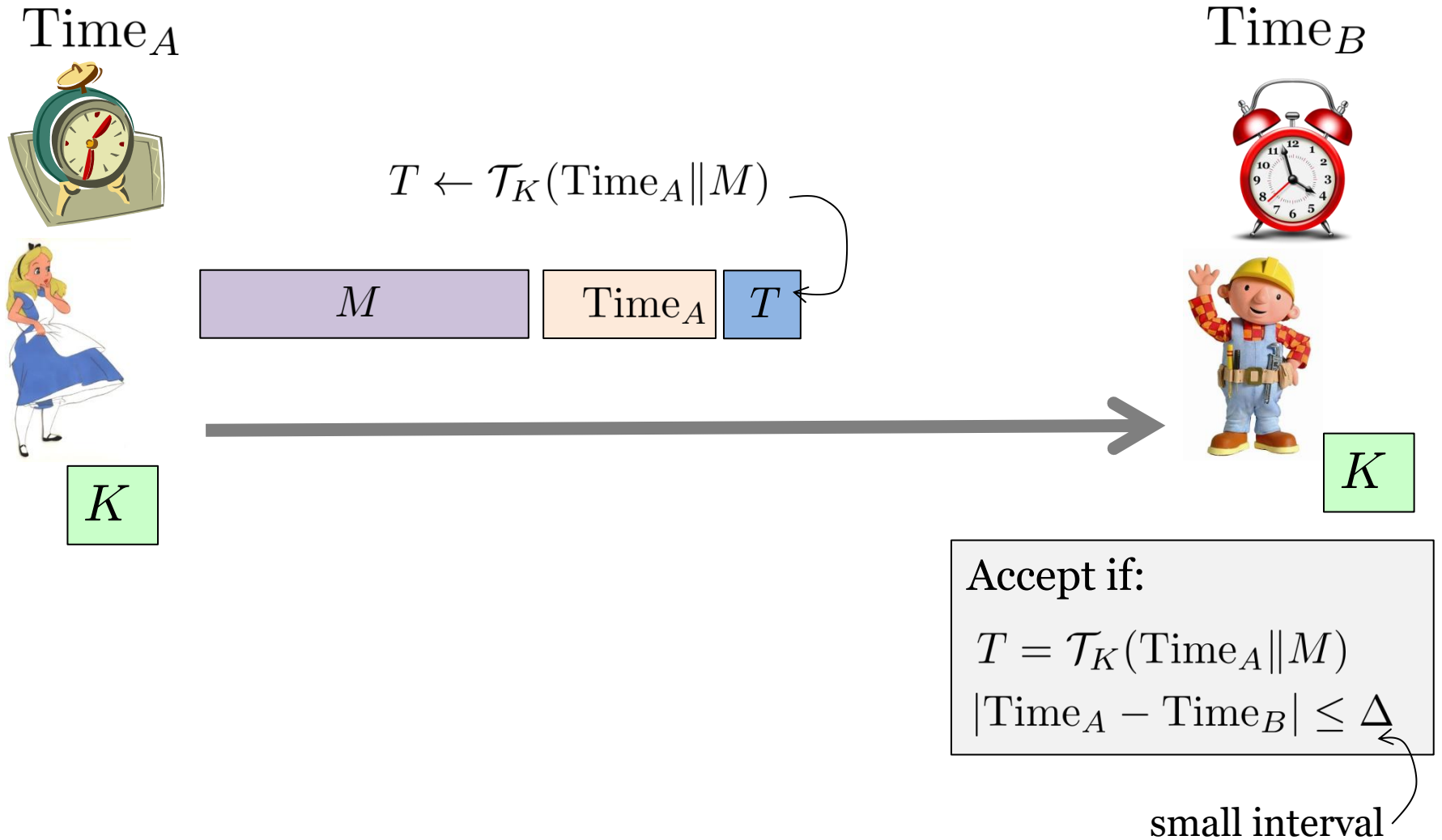


Bob transfers \$10 instead of \$5 !!

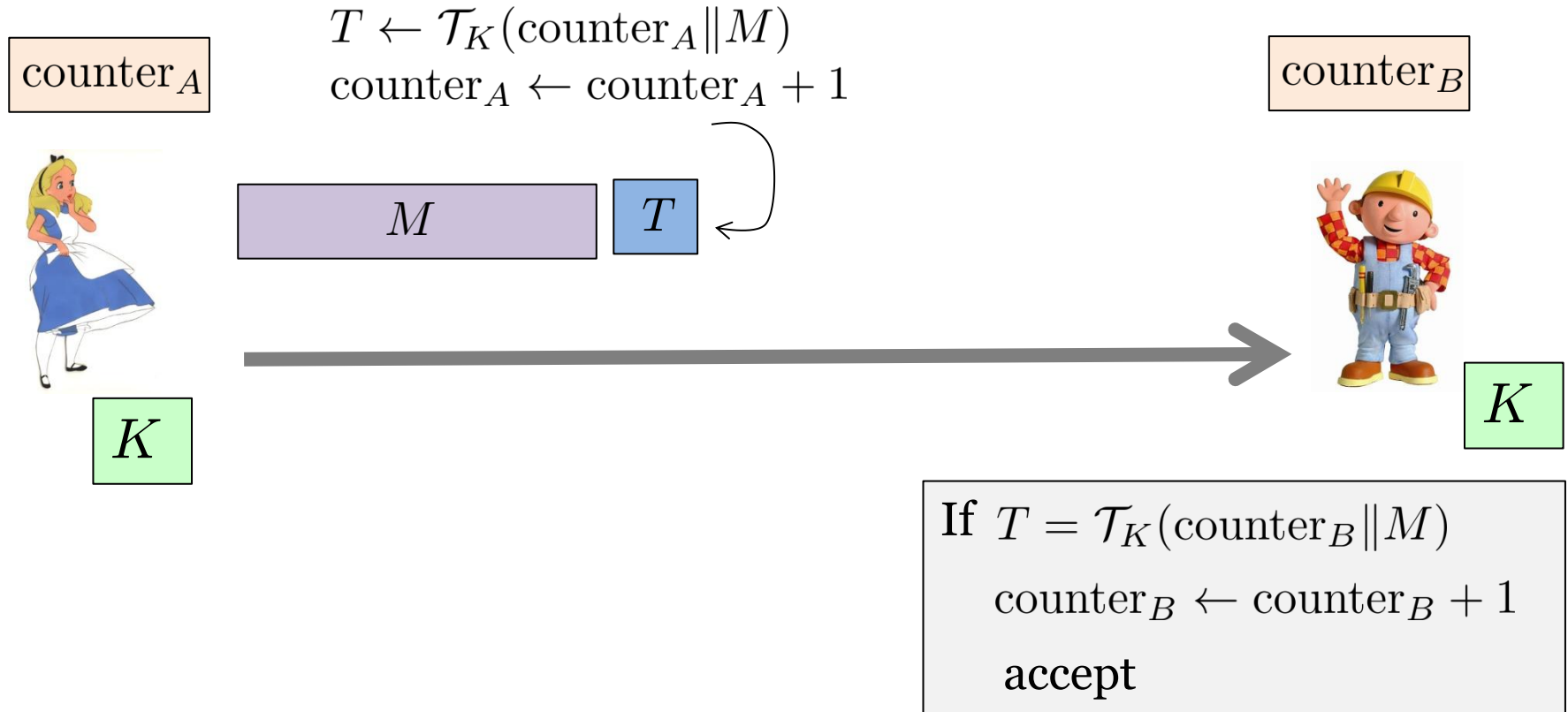
MAC wasn't defined to handle replay attack.

Replay is best addressed as an add-on to standard msg authentication

Prevent Replay Attack Using Timestamp



Prevent Replay Attack Using Counter



Counters need to be synchronized

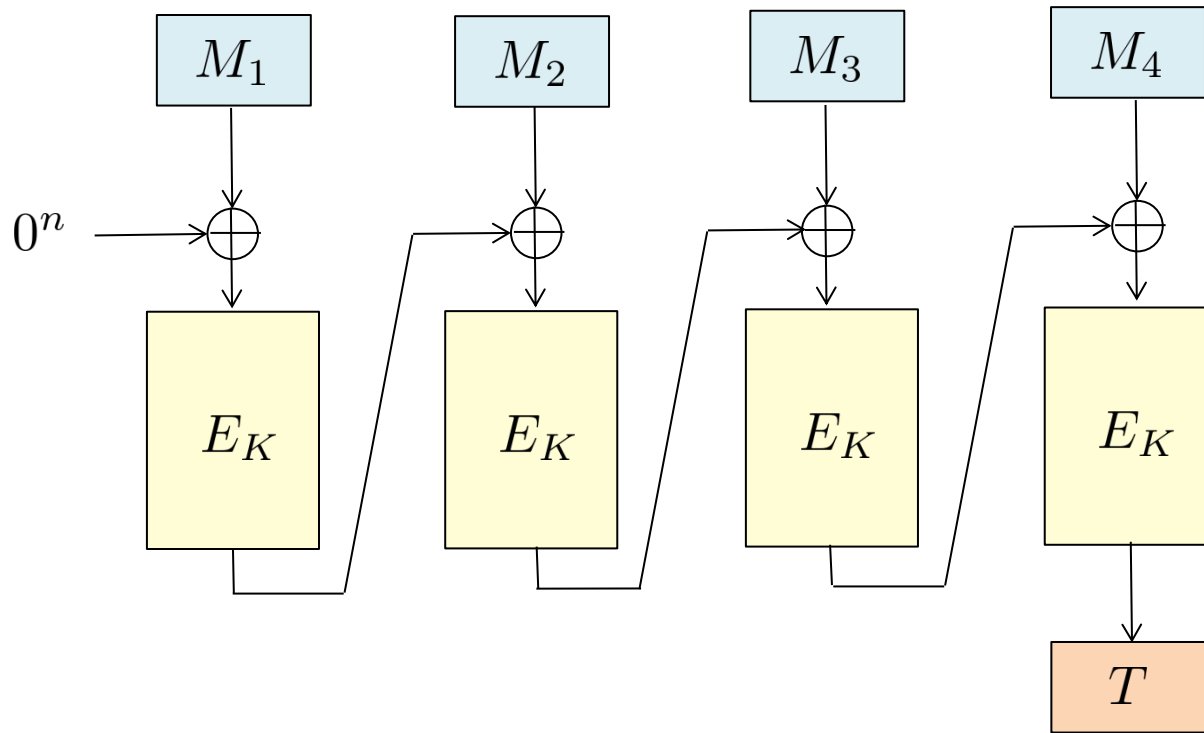
Agenda

1. MAC and Authenticity

2. MAC Constructions

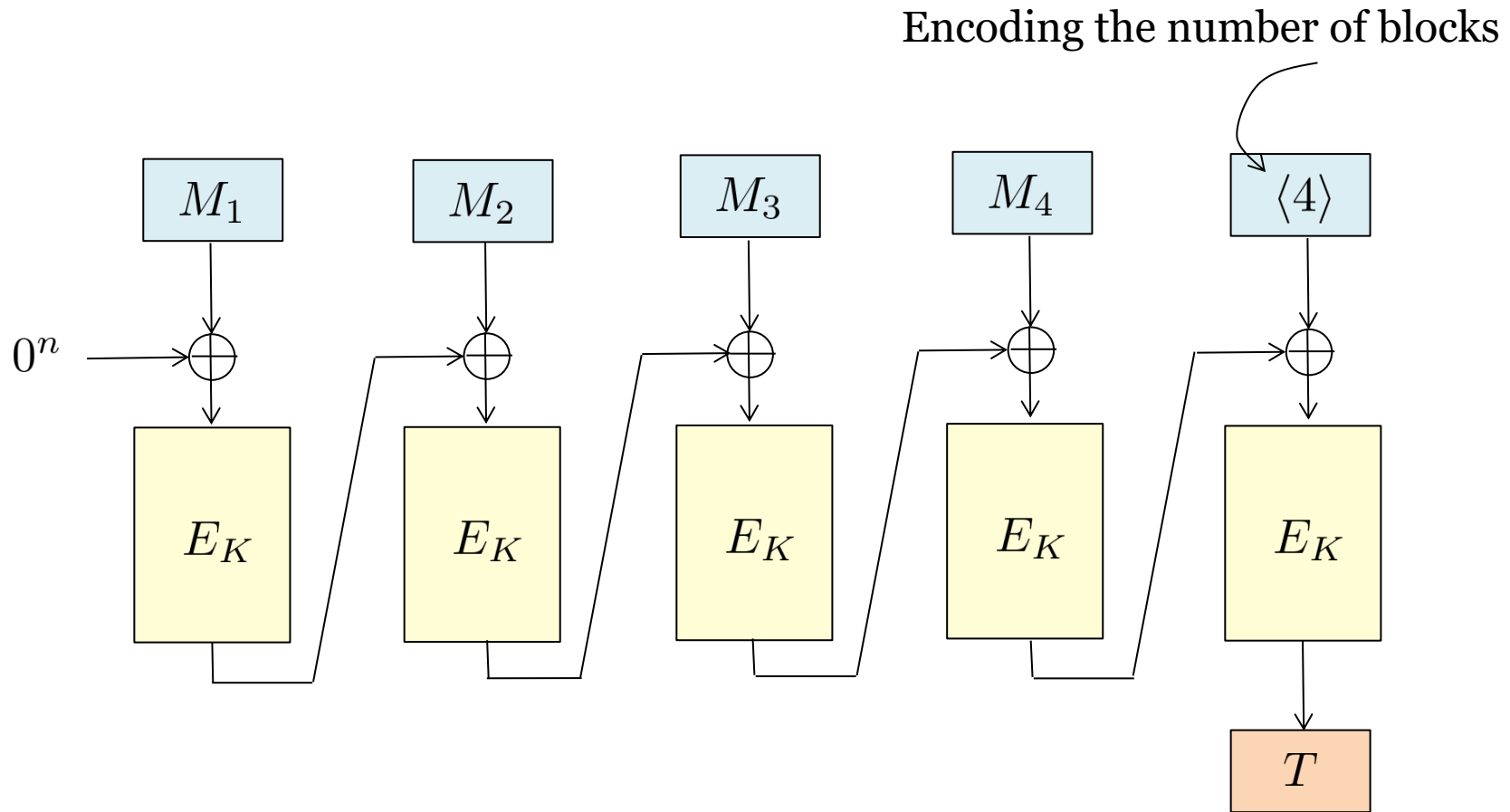
3. How to Construct Good MAC

An Insecure Construction: Plain CBC-MAC



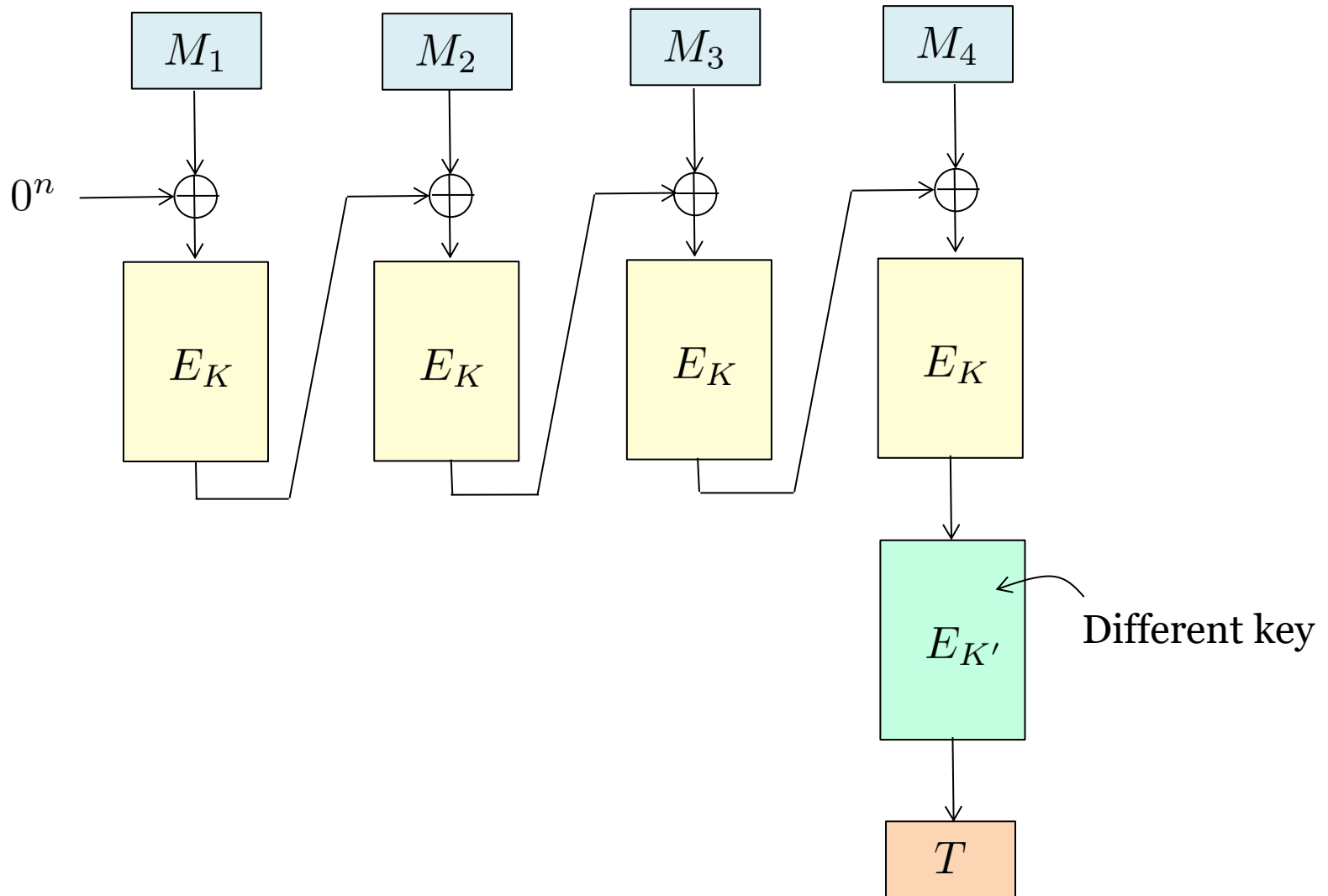
Question: Break CBC-MAC with a single Tag query

An Incorrect Fix of CBC-MAC



Practice: Break this version using 3 Tag queries

A Good Construction: Encrypted CBC-MAC

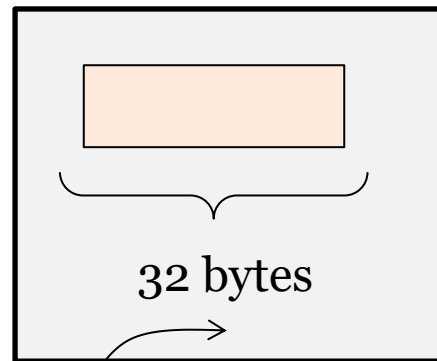
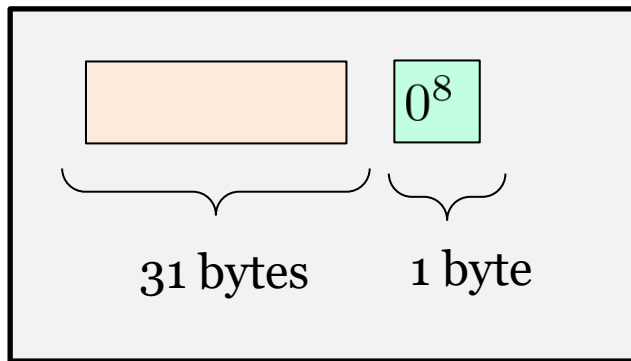


Dealing with Fragmentary Data

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

Agenda

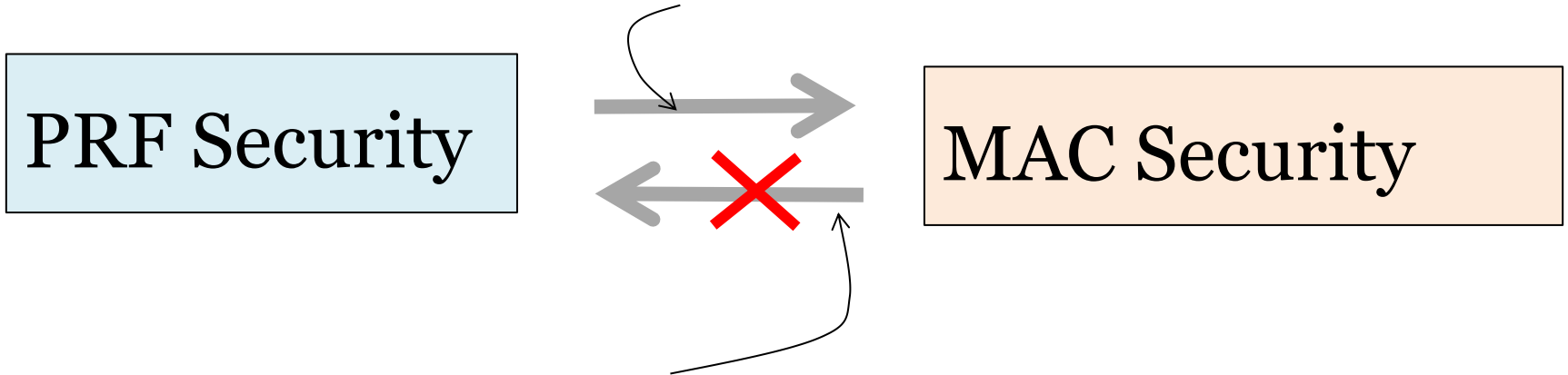
1. MAC and Authenticity

2. MAC Constructions

3. How to Construct Good MAC

PRF Is a Good MAC

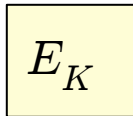
Intuition: - A good MAC means the output should be unpredictable
- Random strings are unpredictable



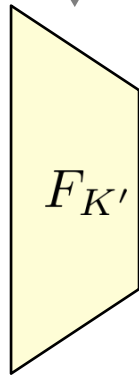
Question: Given a good MAC F , construct F' that is still a good MAC but has a trivial PRF attack.

PRF Extension

Blockcipher: Good PRF with **small** domain $\{0, 1\}^n$

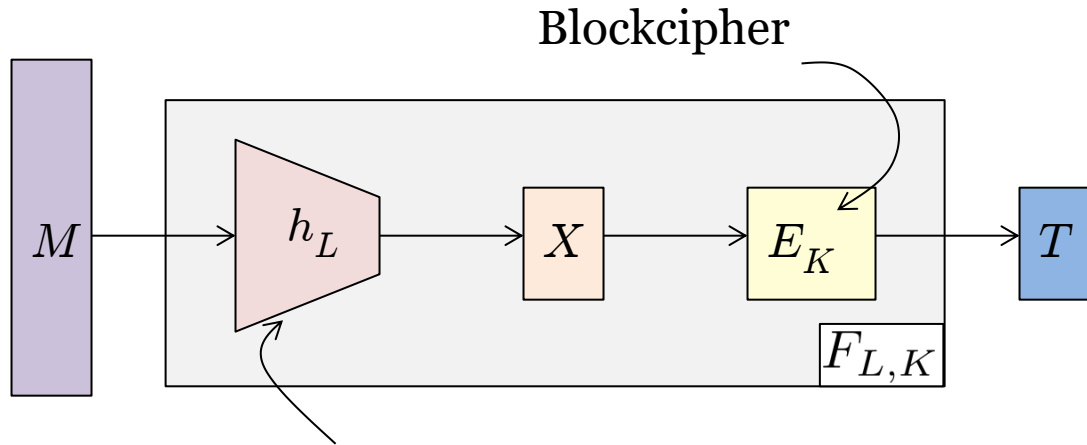


How to extend the domain of a PRF?



Want: Good PRF with **large** domain $\{0, 1\}^*$

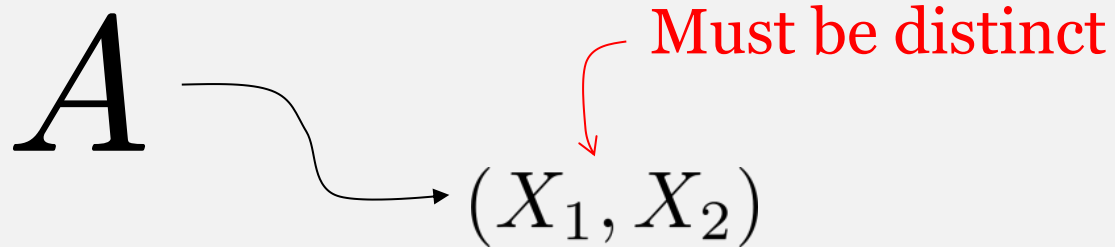
Extending Domain: Carter-Wegman Paradigm



Condensing msg using a (keyed) hash

What's the needed property for the hash?

Computationally Almost Universal Hash



$$\mathbf{Adv}_h^{\text{cau}}(A) = \Pr_{L \leftarrow \$\mathcal{L}}[h_L(X_1) = h_L(X_2)]$$

Building A PRF Via Carter-Wegman

Encrypted CBCMAC

