OMAC (Short slides)

January 16, 2004

Kaoru Kurosawa (Ibaraki University)

OMAC: One-Key CBC MAC

Presented at Fast Software Encryption 2003

Tetsu Iwata and Kaoru Kurosawa

(Ibaraki University)

What is a MAC?

Alice wishes to send Bob a message in such a way that Bob can be **certain** (with very high probability) that Alice was the **true originator** of the message.

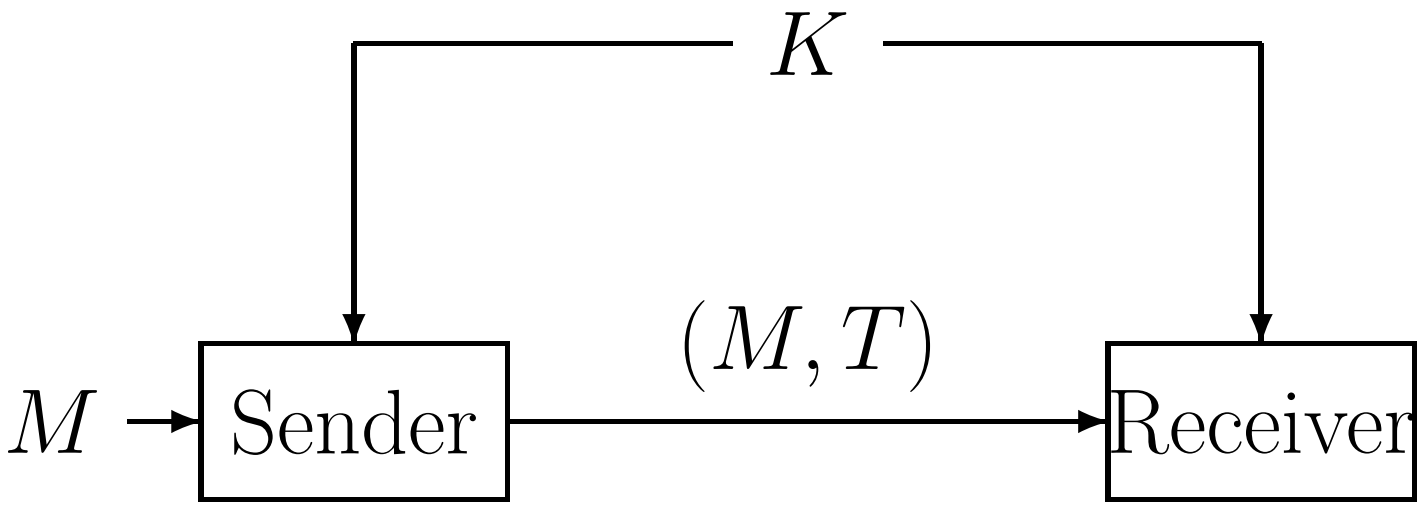
What is a MAC?

Alice wishes to send Bob a message in such a way that Bob can be **certain** (with very high probability) that Alice was the **true originator** of the message.

$$\Downarrow$$

MAC (Message Authentication Code)

What is a MAC?



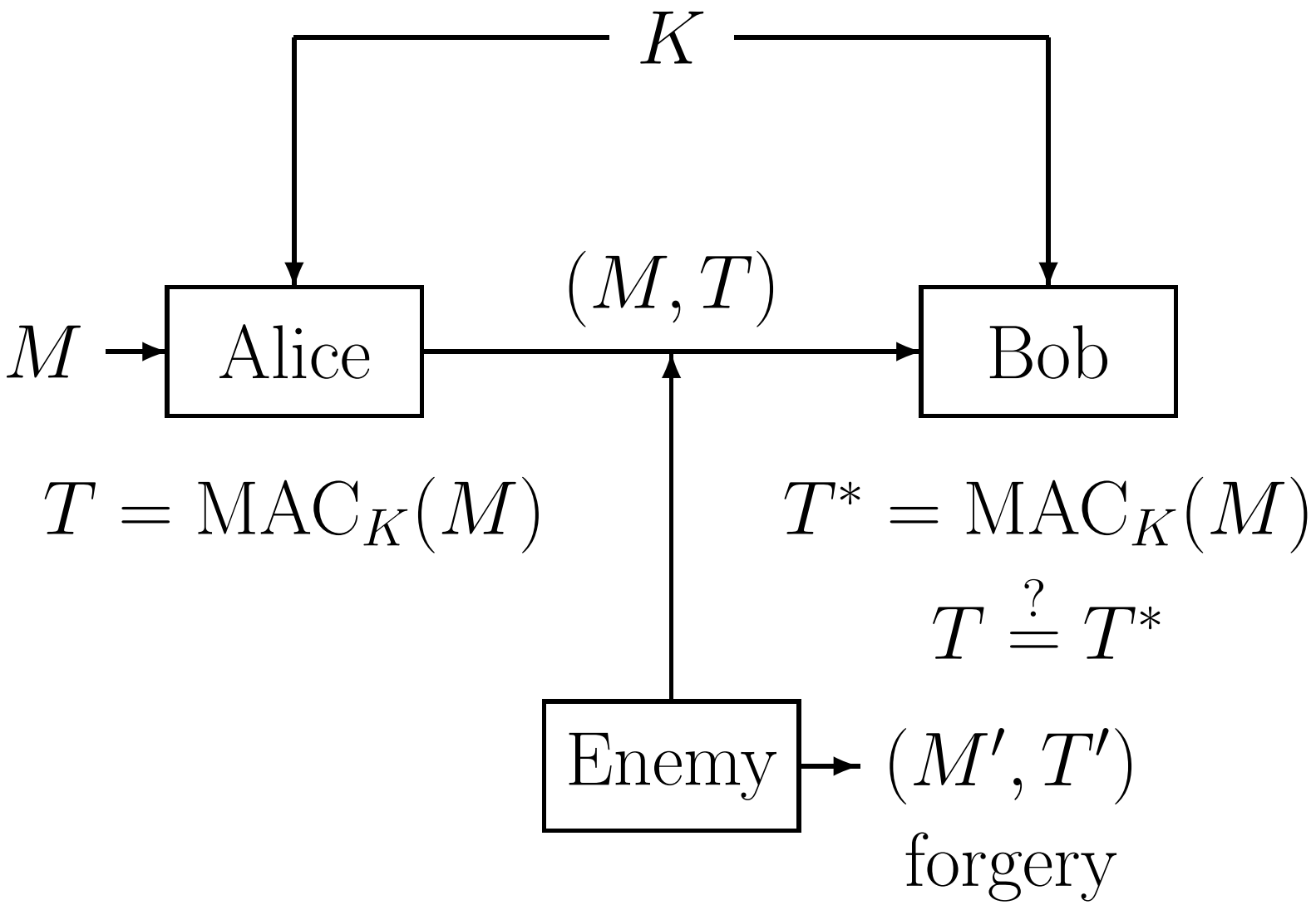
$T = \mathrm{MAC}_K(M)$ $\qquad$ $T^* = \mathrm{MAC}_K(M)$

$T \stackrel{?}{=} T^*$

K = secret key

M = message, T = Tag (or MAC).

Ssecurity against forgery



NIST and OMAC

NIST = US government

- NIST is in the process of specifying modes in a series of special publications.
- Special Publication 800-38B will specify MAC.
- NIST currently intends to specify our "OMAC".

Block cipher is used for MAC

E: encryption algorithm of a block cipher

$$E_K(n\text{-bit Plaintext}) = (n\text{-bit Ciphertext}),$$

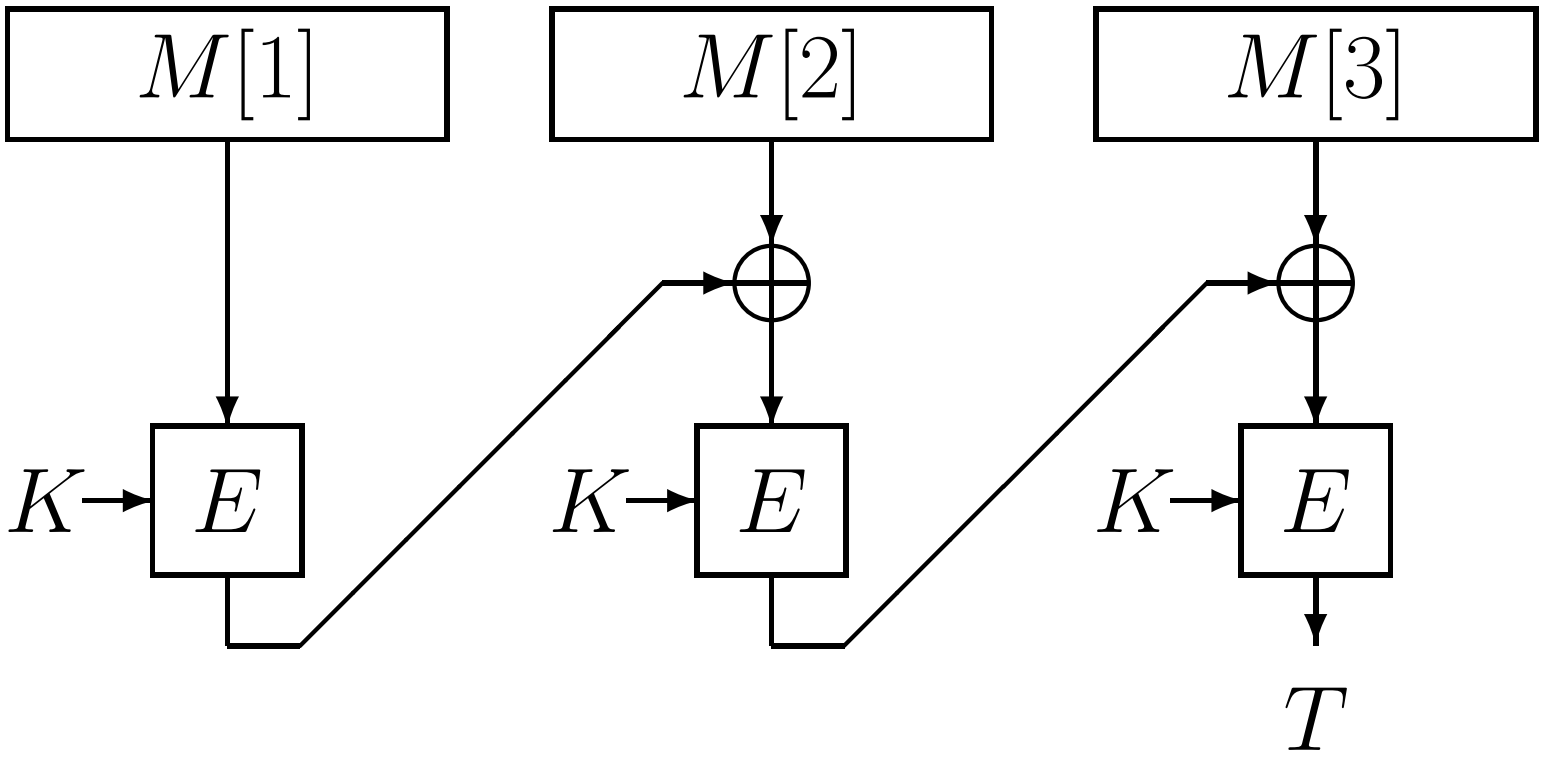
where K is a k-bit secret key.

AES: New standard of US.

$$n = 128,\ k = 128, 192 \text{ or } 256.$$

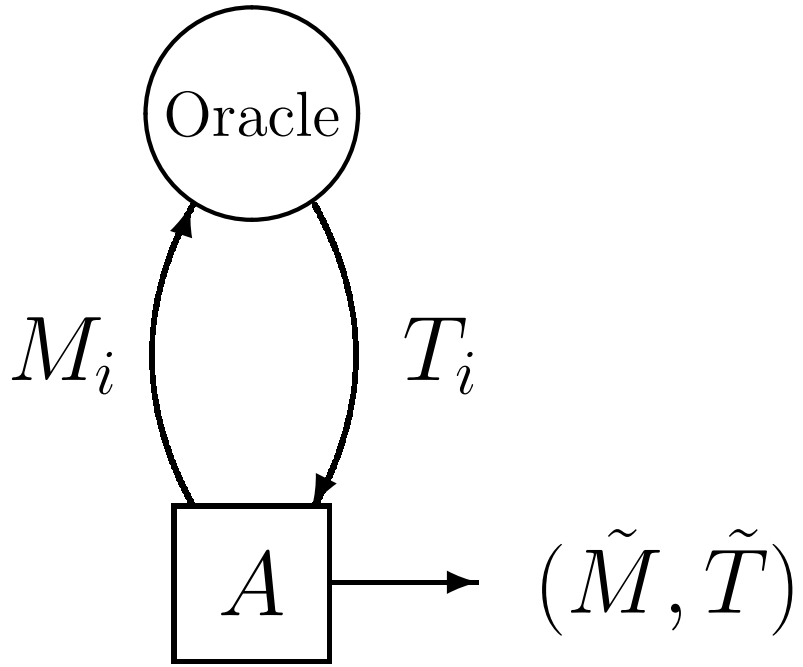
CBC-MAC is well known

If Message $= (M[1], M[2], M[3])$,

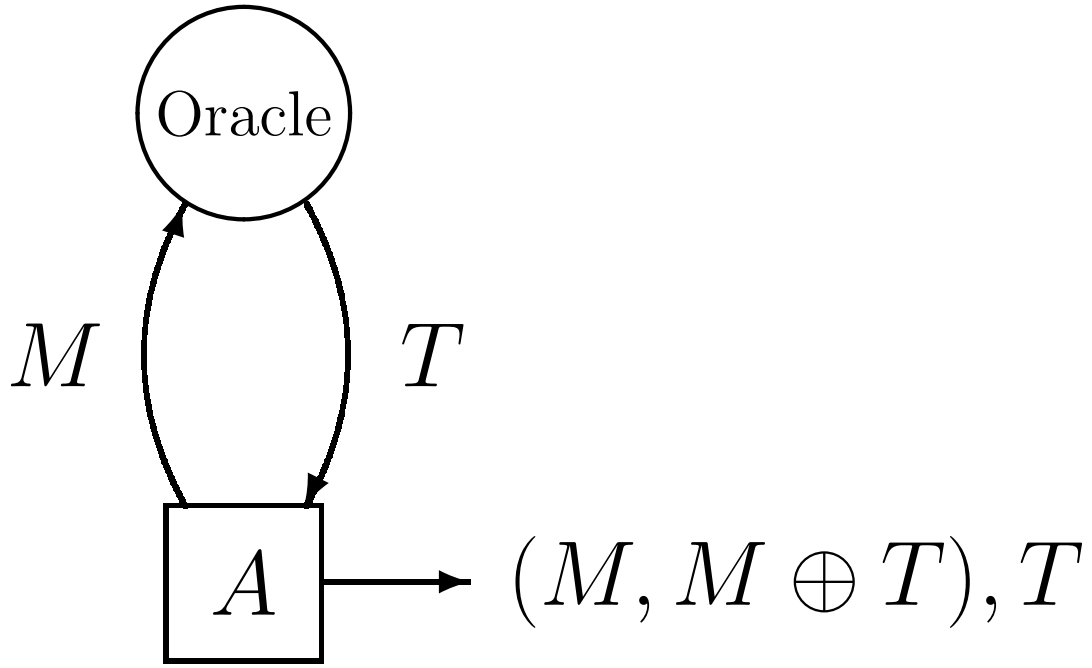


Chosen Message Attack

The most powerful forgery attack

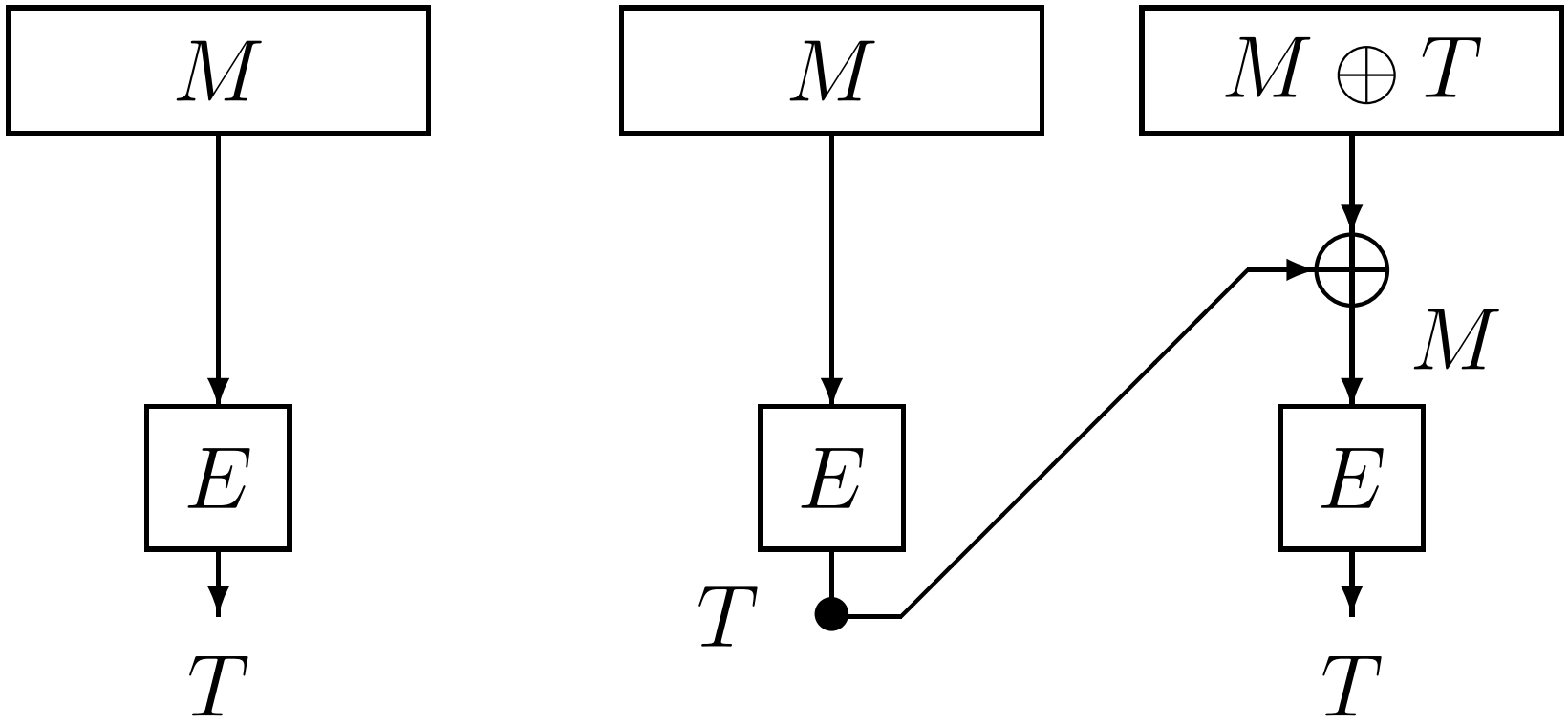


CBC-MAC is not secure



$[(M, M \oplus T), T]$ is a valid (message, tag) pair.

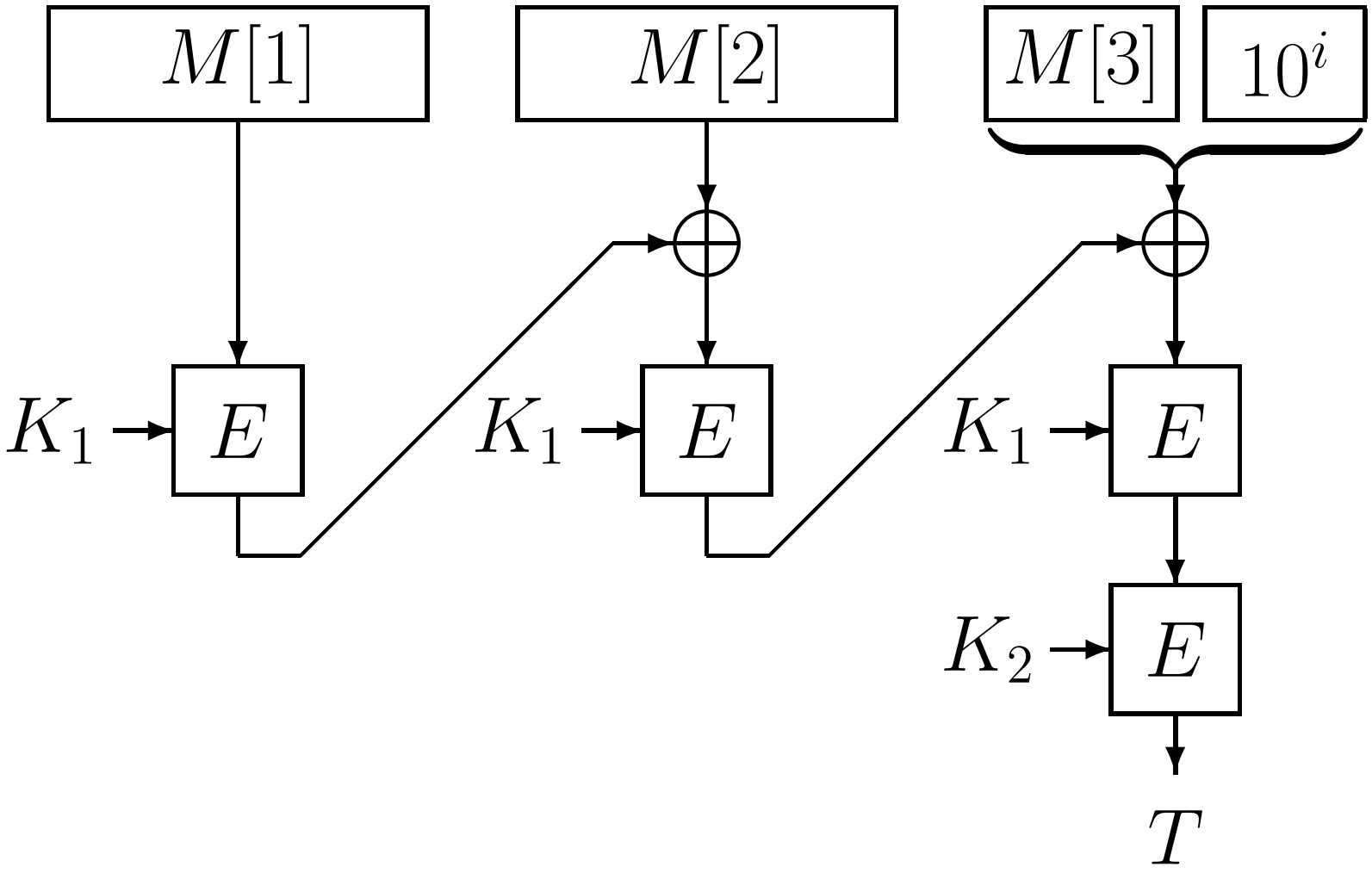
The reason



Therefore, the attack succeeds.

EMAC (Race Project)

$$T = E_{K_2}(CBC_{K_1}(M)).$$



Mathematical definitions

Psuedorandom Function

$$\mathsf{Random} = \{ \text{ all functions } f \}$$

$$F \subset \mathsf{Random}$$

Informally,

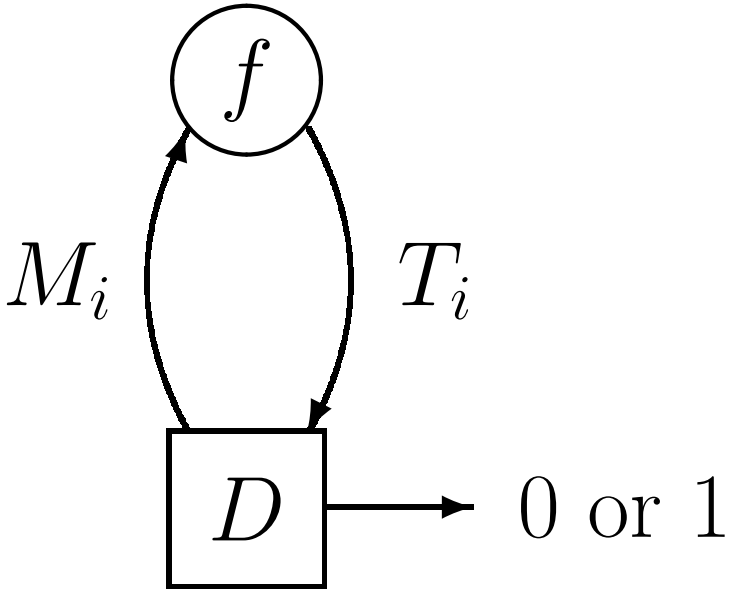
F is pseudorandom if

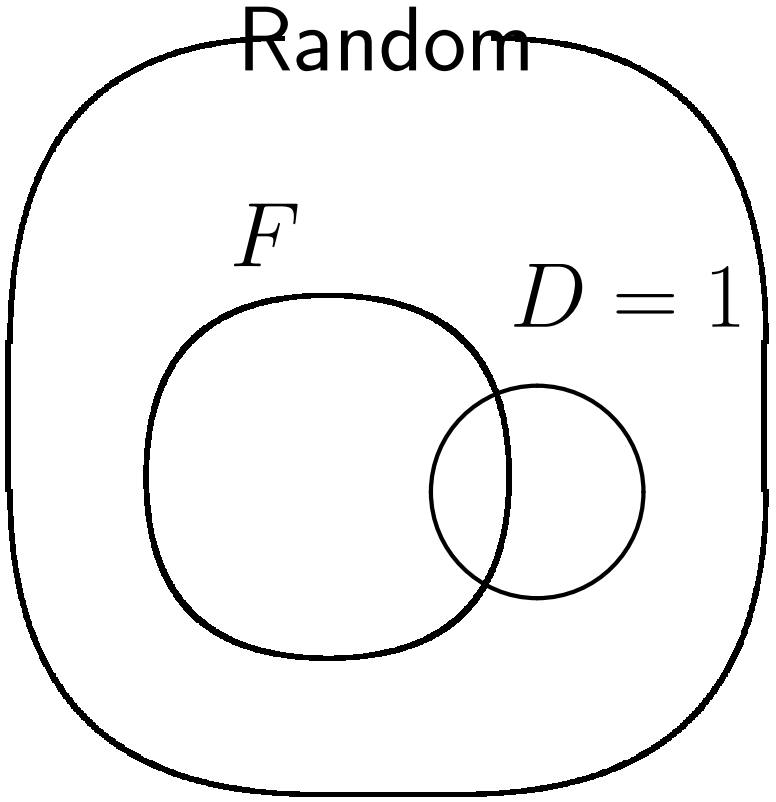
F and Random are indistinguishable.

Distinguisher D for (Random,F)

Game 0: $f \leftarrow$ Random

Game 1: $f \leftarrow F$





Probability of $D = 1$

1. $f \xleftarrow{R}$ Random:

$$p_0 = \Pr(D = 1) = \frac{|\{f \mid D = 1, f \in \mathsf{Random}\}|}{|\mathsf{Random}|}.$$

2. $f \xleftarrow{R} F$:

$$p_1 = \Pr(D = 1) = \frac{|\{f \mid D = 1, f \in F\}|}{|\mathsf{F}|}.$$

Formally

F is (q, ϵ)-random if

$$|p_0 - p_1| \leq \epsilon$$

for any D

which makes at most q queries to f.

Security of MAC

Similarly, we say that

MAC scheme is (q, ϵ)-secure if

$$\Pr(A \text{ can forge}) \leq \epsilon$$

for any A

which makes at most q queries to f.

Ideal MAC

$$f \xleftarrow{R} \mathsf{Random}, \quad T = f(M)$$

Suppose that A forges $(\tilde{M}, \tilde{T})$. Then

$$\Pr(A \text{ succeeds}) = \frac{1}{2^n}$$

for any q (queries).

Proposition 1

MAC scheme is (q, ϵ)-*secure* if

it is $(q+1, \epsilon')$-*random*, where

$$\epsilon = \epsilon' + \frac{1}{2^n}.$$

$$\Downarrow$$

We prove that MAC is *pseudorandom*.

Permutation

A block cipher is a permutation over $\{0,1\}^n$.

(Otherwise, we cannot decrypt uniquely.)

$$\mathsf{Perm} = \{ \text{ all permutations over } \{0,1\}^n \}$$

$$P \subset \mathsf{Perm}$$

P is pseudoramdomP if

P and Perm are indistinguishable.

Ideal world and Real world

- Ideal world:

  Block cipher: $f \longleftarrow \mathsf{Perm}$.

- Real world:

  Block cipher: $f \longleftarrow P \subset \mathsf{Perm}$.

Security of EMAC

(Proposition)

EMAC is secure if P is pseudorandomP.

However, if $|M| \neq$ a muptiple of n,

$M \longrightarrow M \circ 10^i$

so that $|M \circ 10^i|$ is a multiple of n.

$$T = EMAC(M \circ 10^i).$$

(Extra padding problem)

If $|M|$ is a multiple of n already,

then $M \longrightarrow M \circ 10^{n-1}$.

Drawback of EMAC

- Extra padding
- 2 key-schedulings

$$T = E_{K_2}(CBC_{K_1}(M))$$

In a block cipher,

K is expanded into many subkeys.

Improvements of EMAC

1. XCBC

   Black and Rogaway (Crypto 2000)

2. TMAC

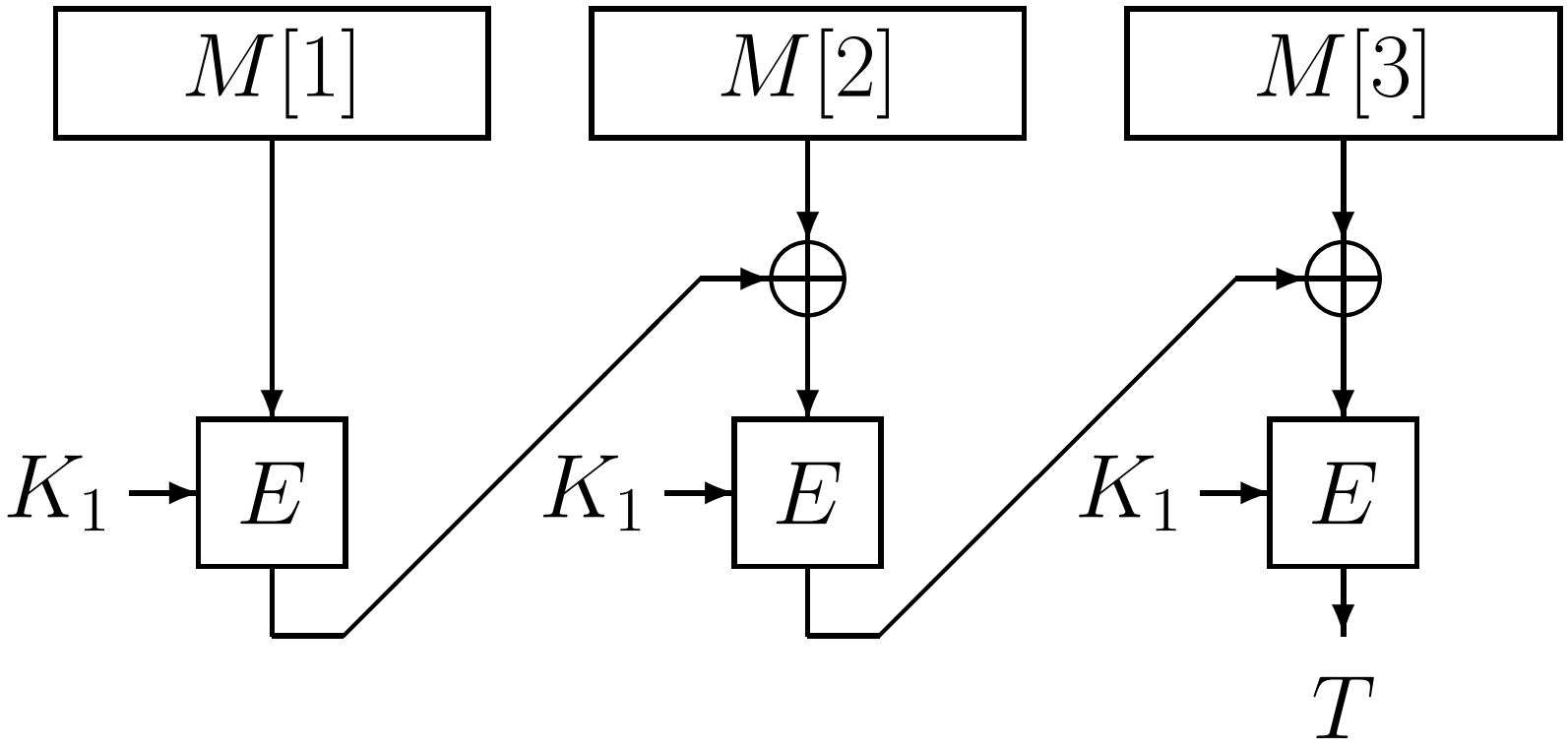
   Kurosawa and Iwata (CT-RSA 2003)

3. OMAC

   Iwata and Kurosawa (FSE 2003)

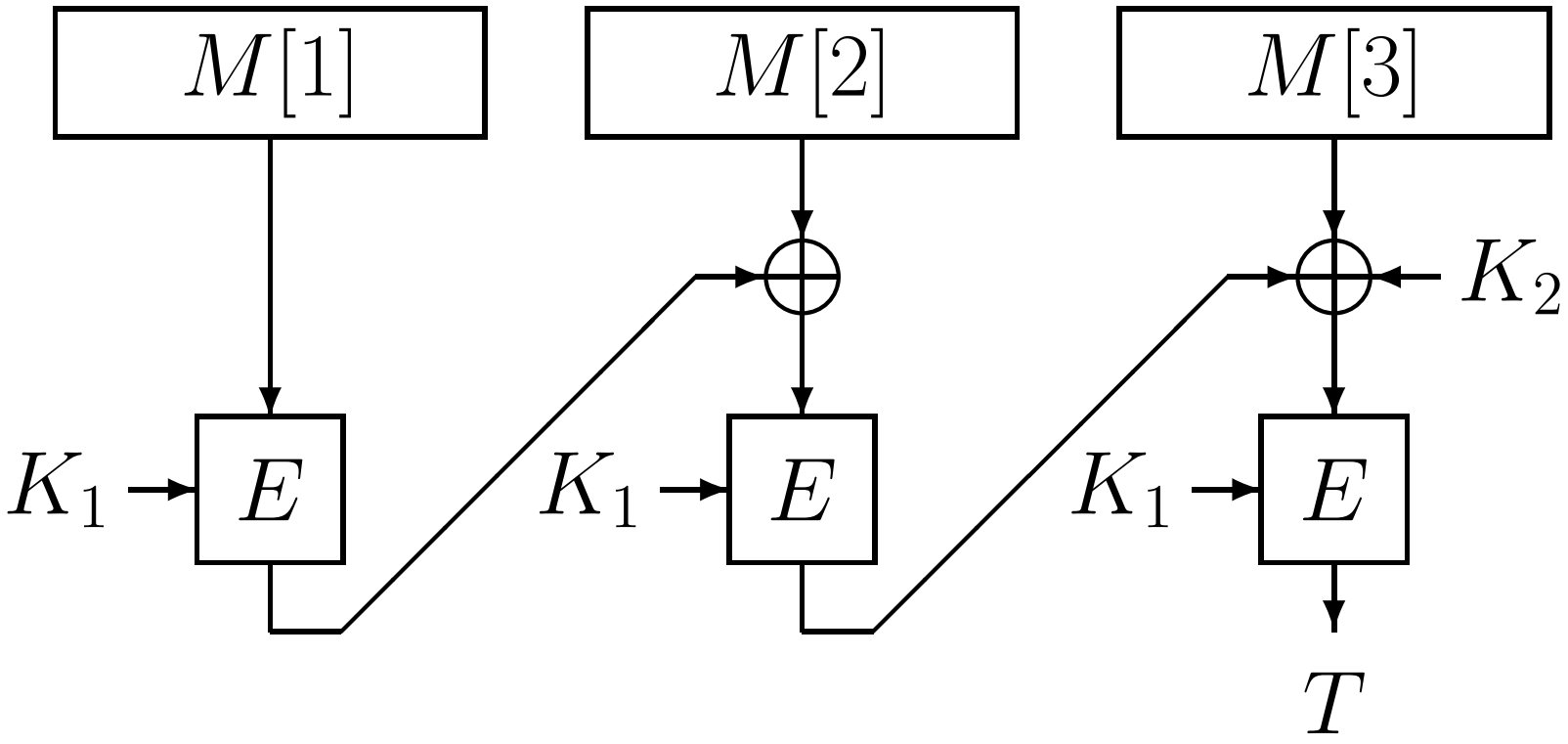
XCBC (Black and Rogaway, Crypto'00)

Case $|M|$ = a multiple of n



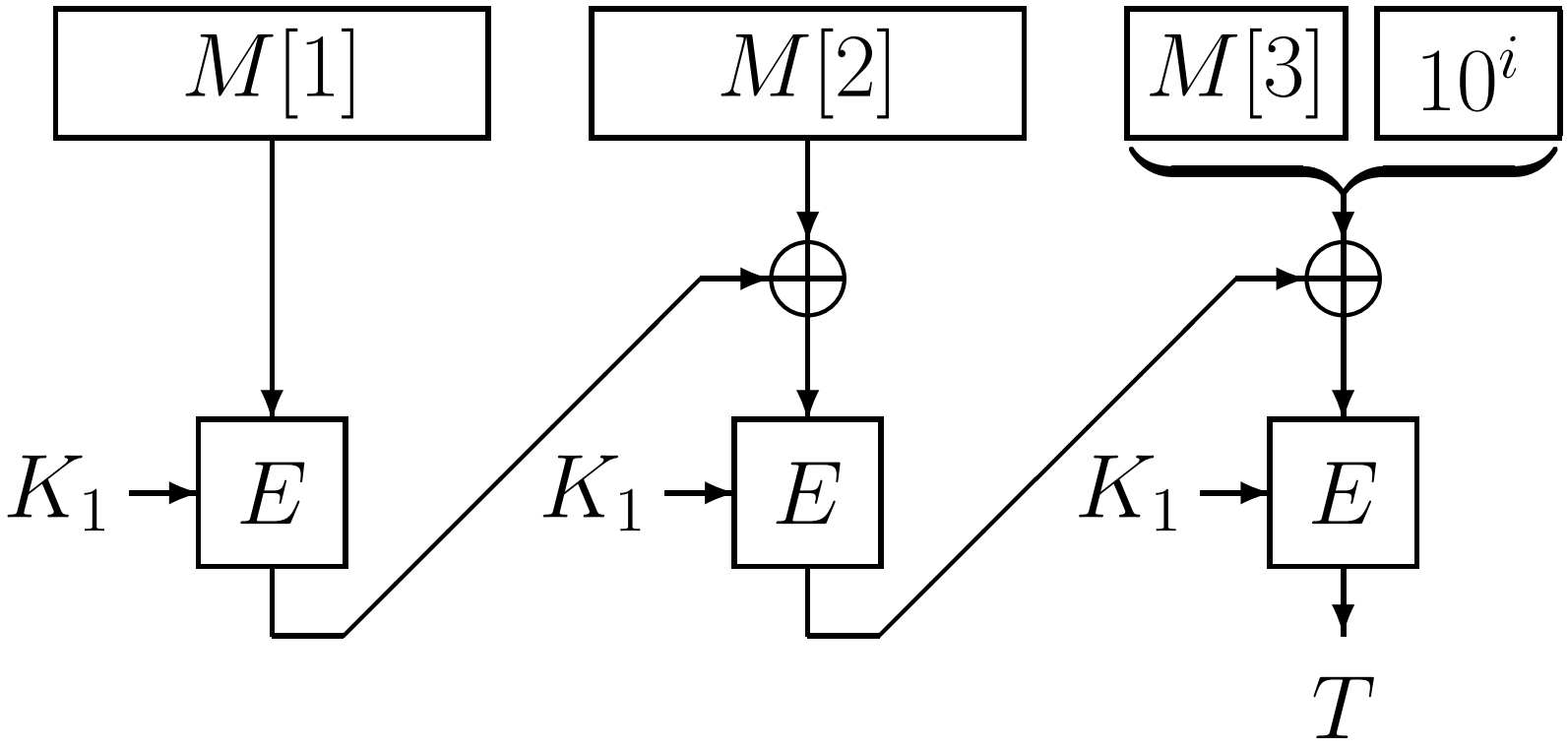
XCBC (Black and Rogaway, Crypto'00)

Case $|M|$ = a multiple of n



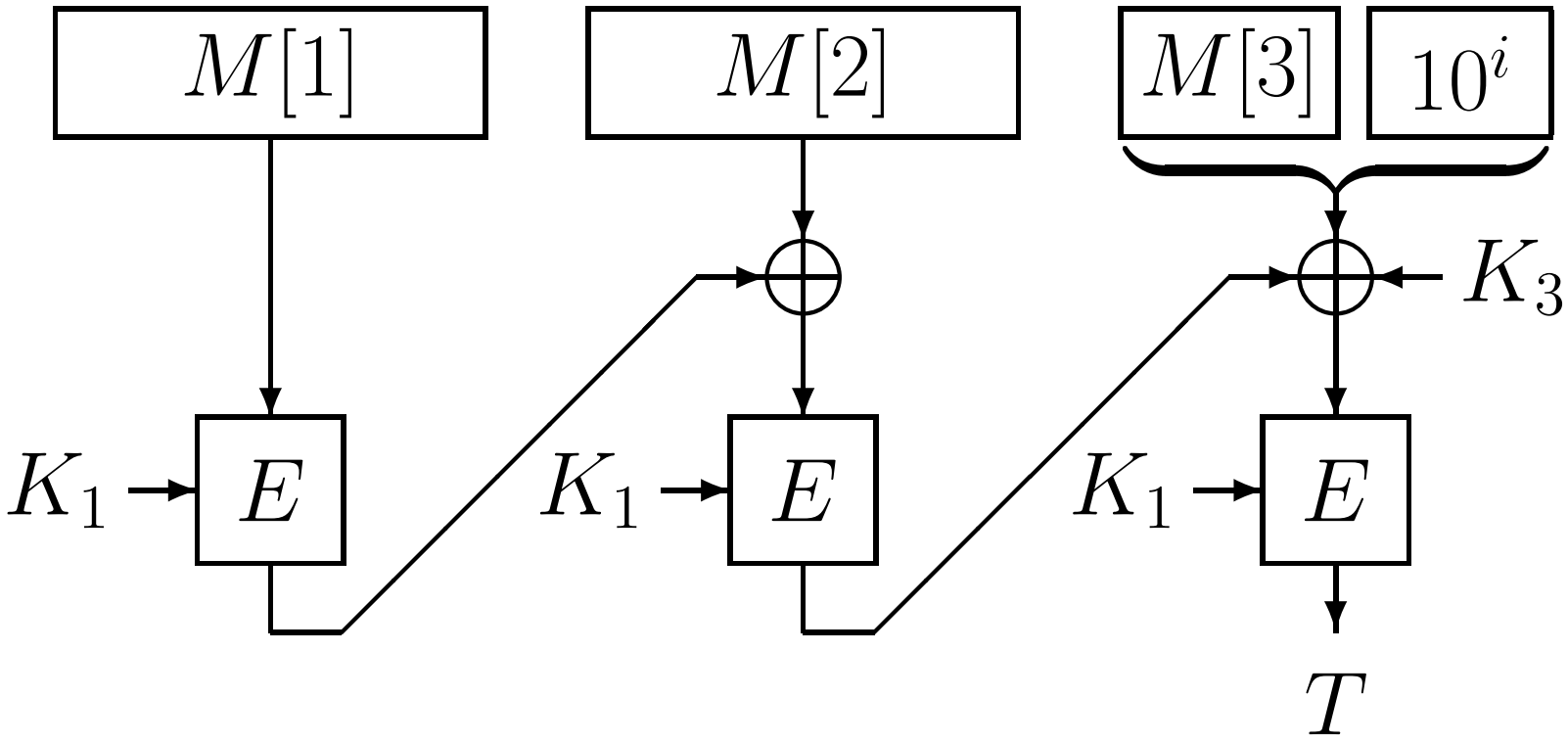
XCBC (Black and Rogaway, Crypto'00)

Case $|M| \neq$ a multile of n



XCBC (Black and Rogaway, Crypto'00)

Case $|M| \neq mn$



Advantages of XCBC

- No extra padding
- One key-scheduling

Disadvantage of XCBC

- **Three** keys ($k + 2n$ bits), K_1, K_2, K_3,

  where $|K_1| = k$.

TMAC and OMAC

- TMAC: $(K_1, K_2, K_3) \rightarrow (K_1,\ (K_2 \cdot \mathtt{u}),\ K_2)$,

  where $\mathtt{u} \in GF(2^n)$.

- OMAC: $(K_1, K_2, K_3) \rightarrow (K_1,\ (L \cdot \mathtt{u}^2),\ (L \cdot \mathtt{u}))$,

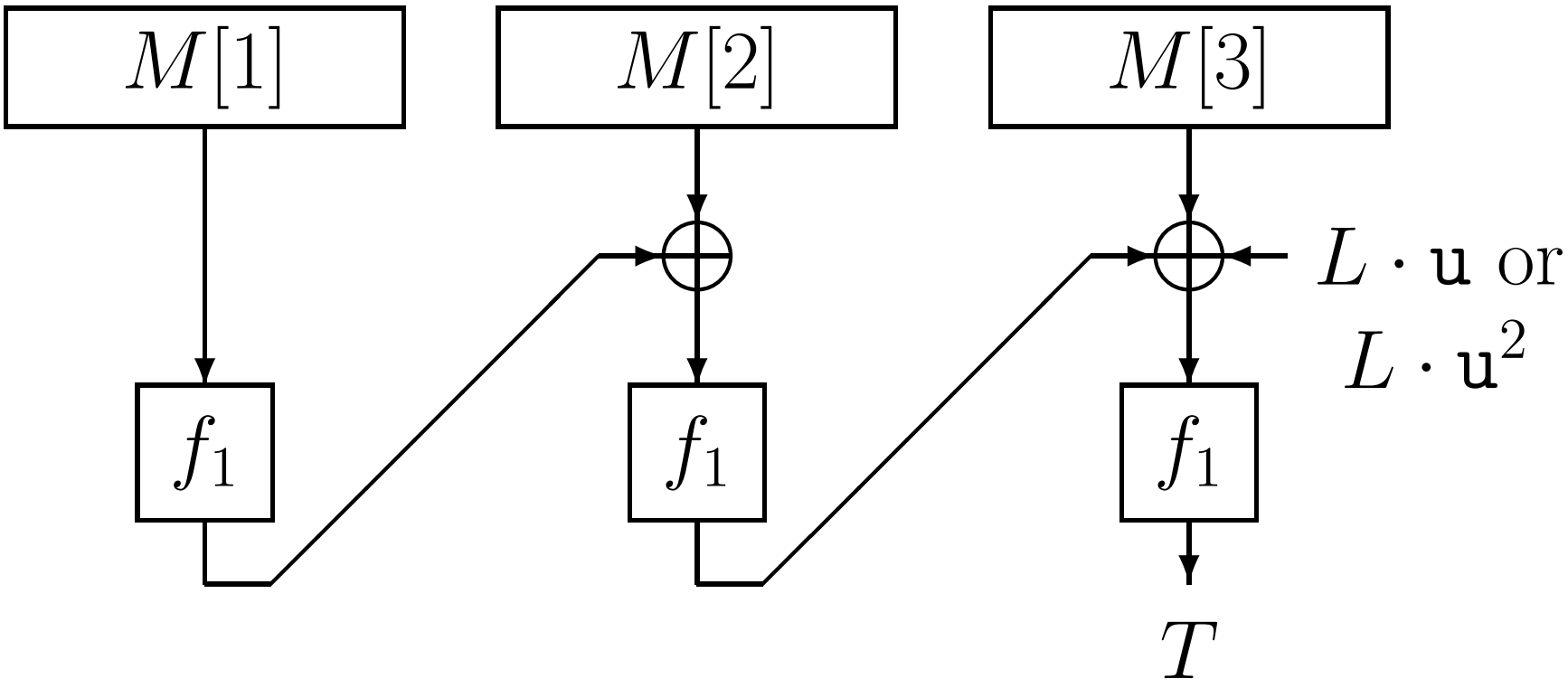
  where $L = E_{K_1}(0^n)$.

Comparison

	♯ of keys	size of keys
XCBC	3	$k + 2n$
TMAC	2	$k + n$
OMAC	1	k

Construction of OMAC

$$f_1 \xleftarrow{R} P, \quad L = f_1(0^n), \quad \mathtt{u} \in GF(2^n)$$



Ideal OMAC

- $f_1 \xleftarrow{R} \mathsf{Perm}$ is used for CBC-MAC part.
- Last block

$$= \begin{cases} P_2(x) = f_1(x \oplus L \cdot \mathtt{u}) & \text{if } |M| \text{ is a} \\ & \text{multiple of } n. \\ P_3(x) = f_1(x \oplus L \cdot \mathtt{u}^2) & \text{otherwise} \end{cases}$$

where $L = f_1(0^n)$.

Pseudorandomness of (f_1, P_2, P_3) ?

(f_1, P_2, P_3) and random (f_1, f_2, f_3)

are distinguishable

because $L = f_1(0^n)$.

$\Downarrow$

We need a new proof technique !!

Security of OMAC

(Theorem 4)

OMAC is secure if P is pseudorandomP.

(The security level $\approx$ XCBC)

NIST Recommends OMAC

http://csrc.nist.gov/CryptoToolkit/modes/

"NIST currently intends to specify the OMAC variation of the XCBC algorithm instead of the RMAC algorithm that was originally proposed in the first draft of SP 800-38B".

Implimentations of OMAC

- "Secure Programming Cookbook for C and C++"
  by John Viega and Matt Messir,
  published by O'Reilly (2003) ISBN 0-596-00394-3
- Brian Gladman: (C)
  http://fp.gladman.plus.com/AES/index.html

- Jack Lloyd: (C)

  http://botan.randombit.net/

- Paulo Barreto: (C++, Java)

  http://planeta.terra.com.br/informatica/paulobarreto/

Follow up work on OMAC

IEEE 802.11i standard (for Wireless LAN)

CCM = counter mode + CBC MAC

However,

Bellare, Rogaway and Wagner (ePrint)

pointed out the drwaback of CCM and proposed

EAX=counter mode + OMAC