OMAC (Long 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.

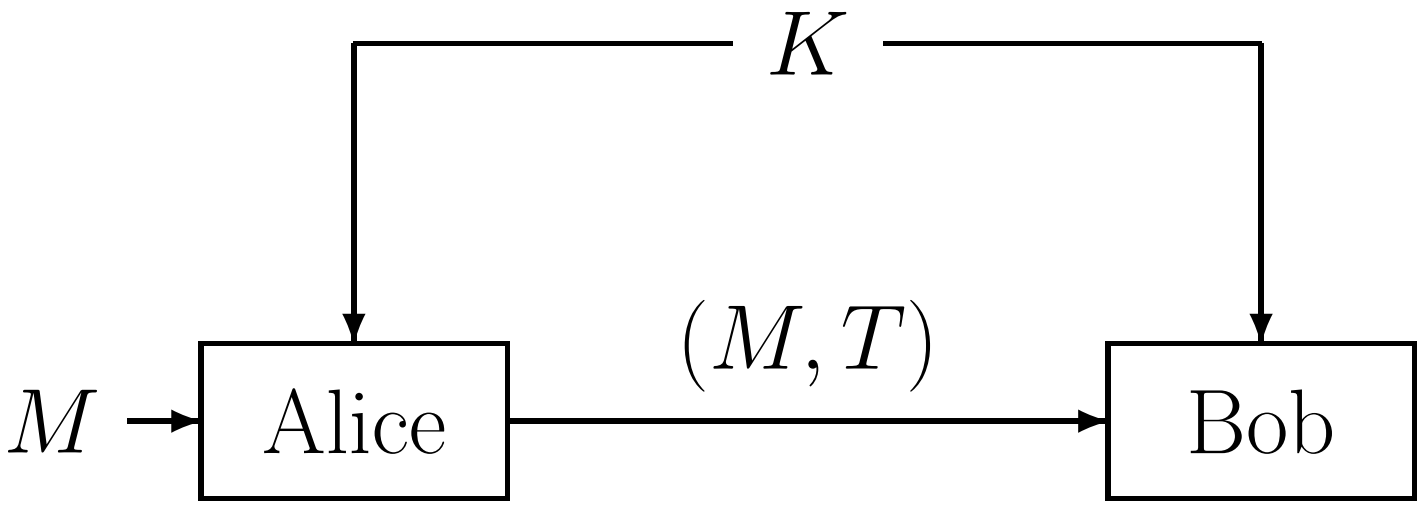
What is a MAC?

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)

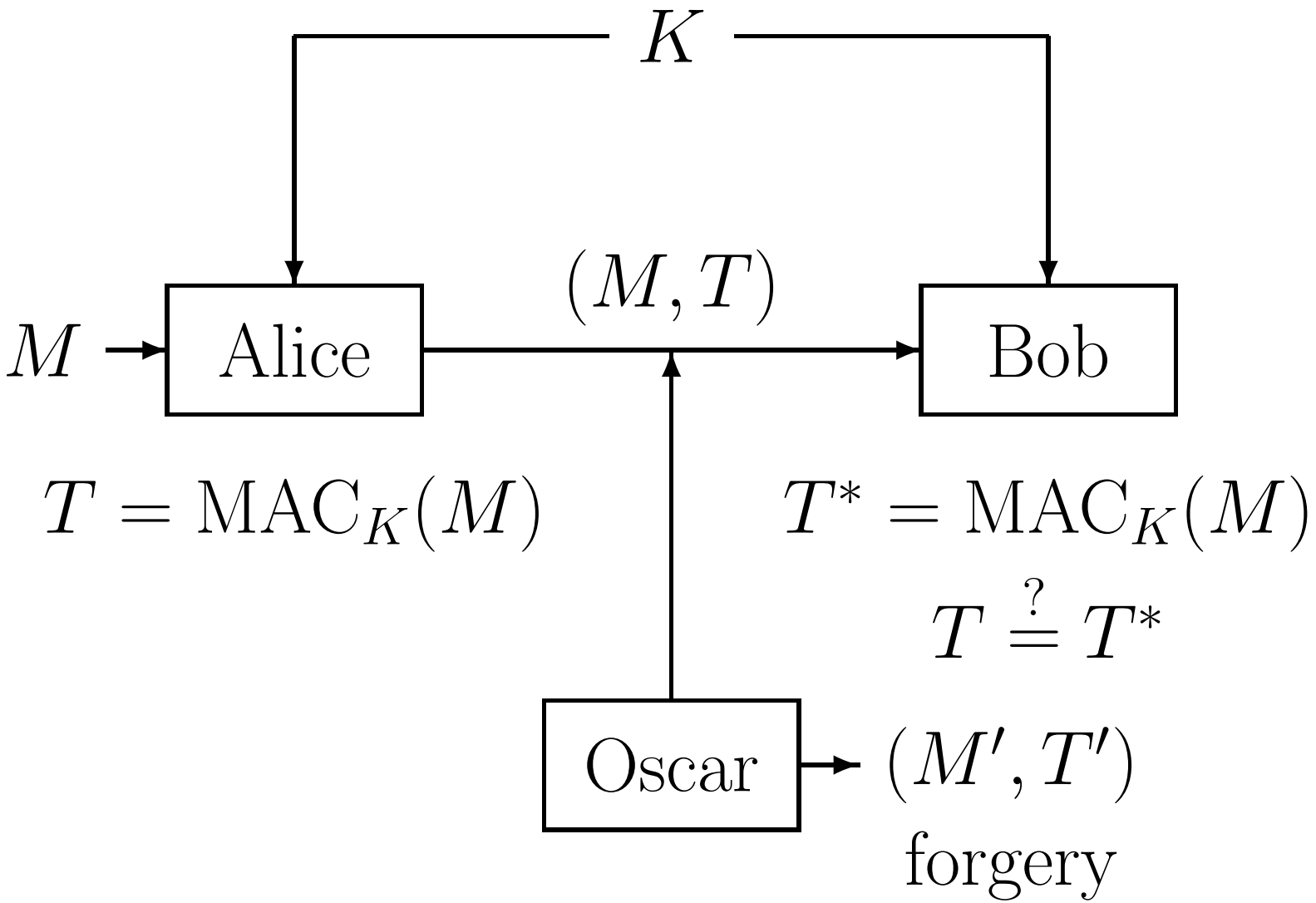
What is a MAC?



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

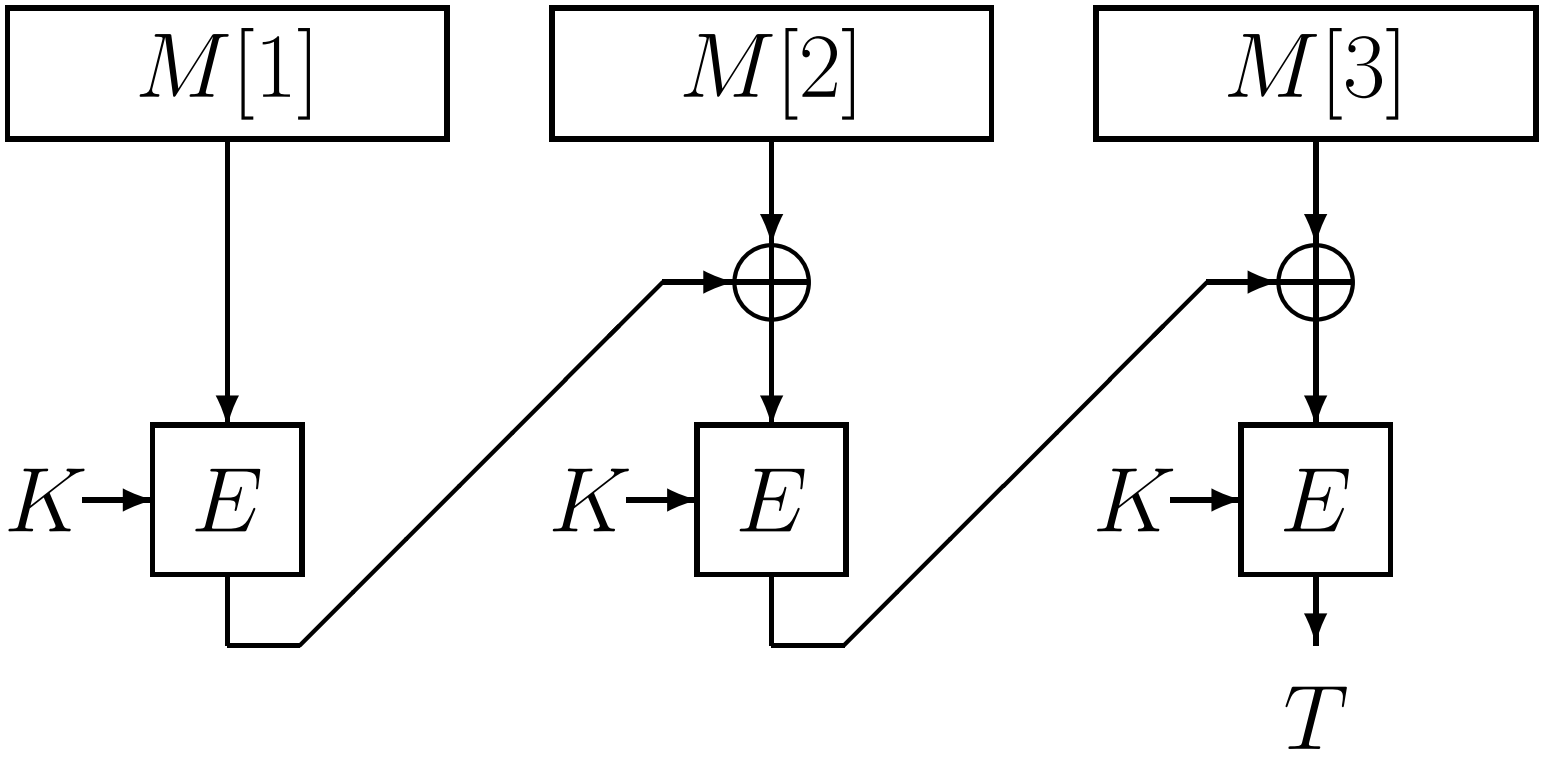
$$T \stackrel{?}{=} T^*$$

What is a MAC?

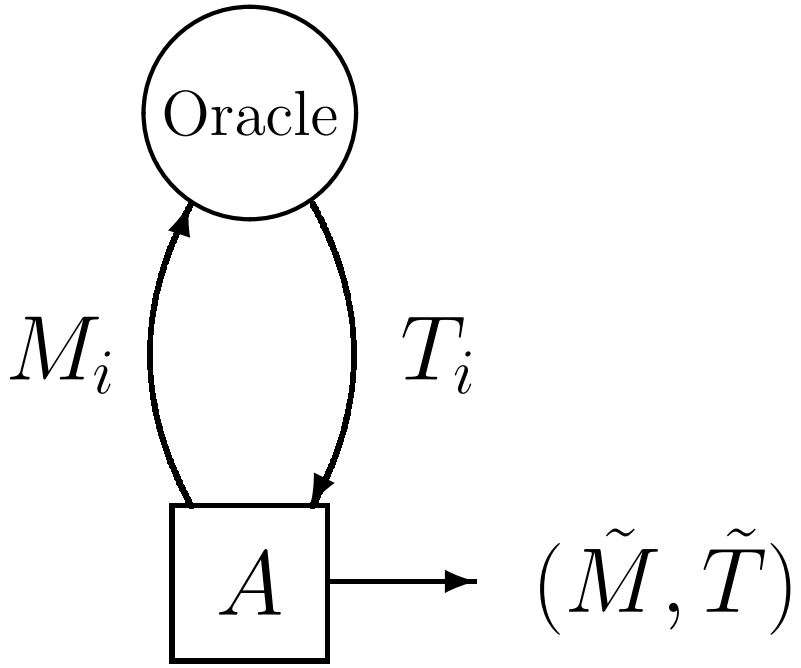

K
M
Alice
(M, T)
Bob
$T = \mathrm{MAC}_K(M)$
$T^* = \mathrm{MAC}_K(M)$
$T \stackrel{?}{=} T^*$
Oscar
(M', T')
forgery

CBC MAC

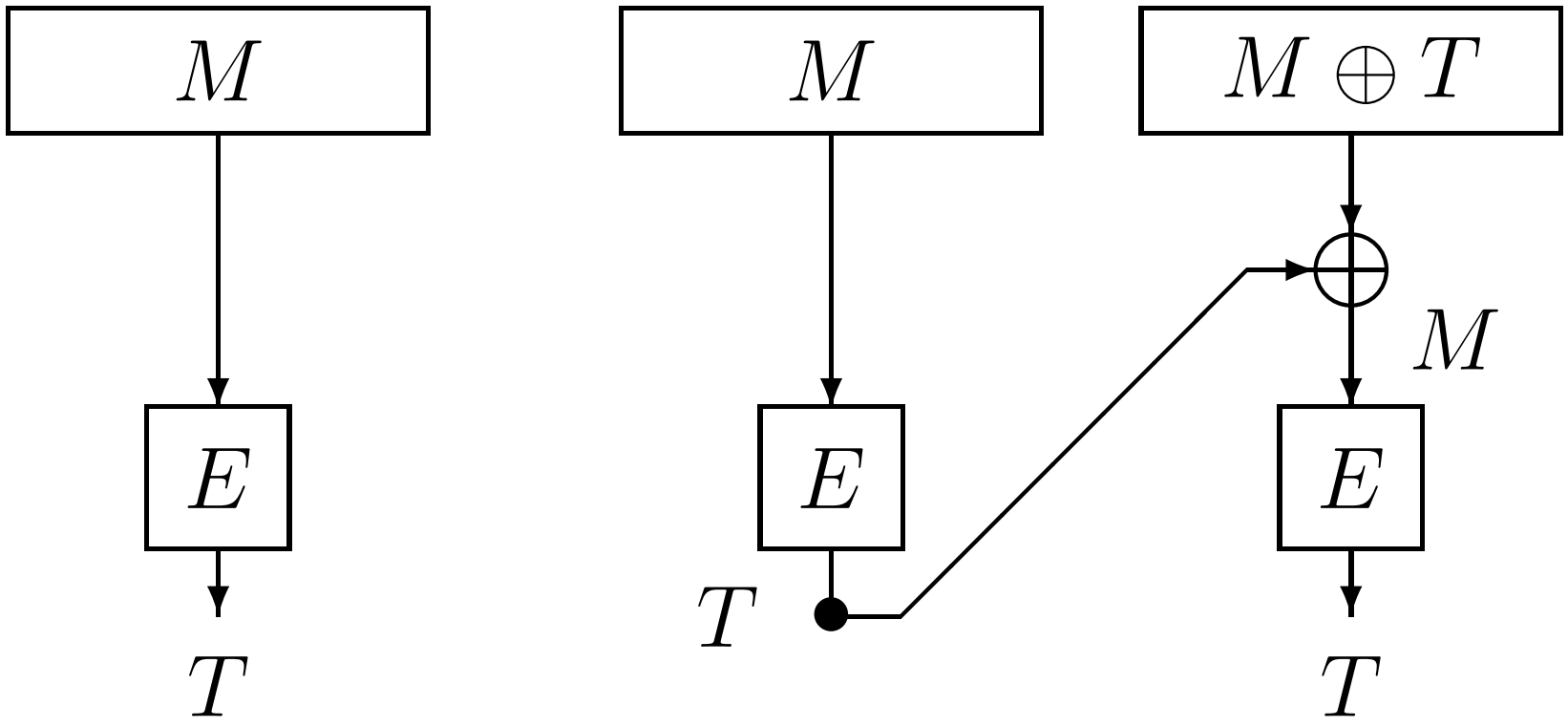
Block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$



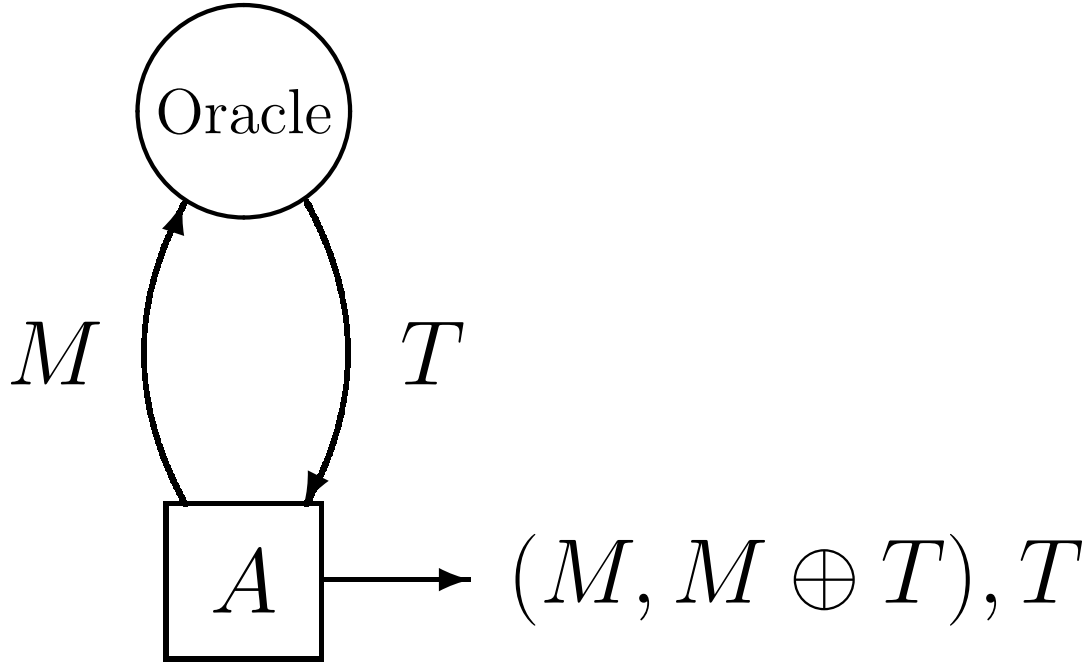
Chosen Message Attack



Attack on CBC MAC (1)

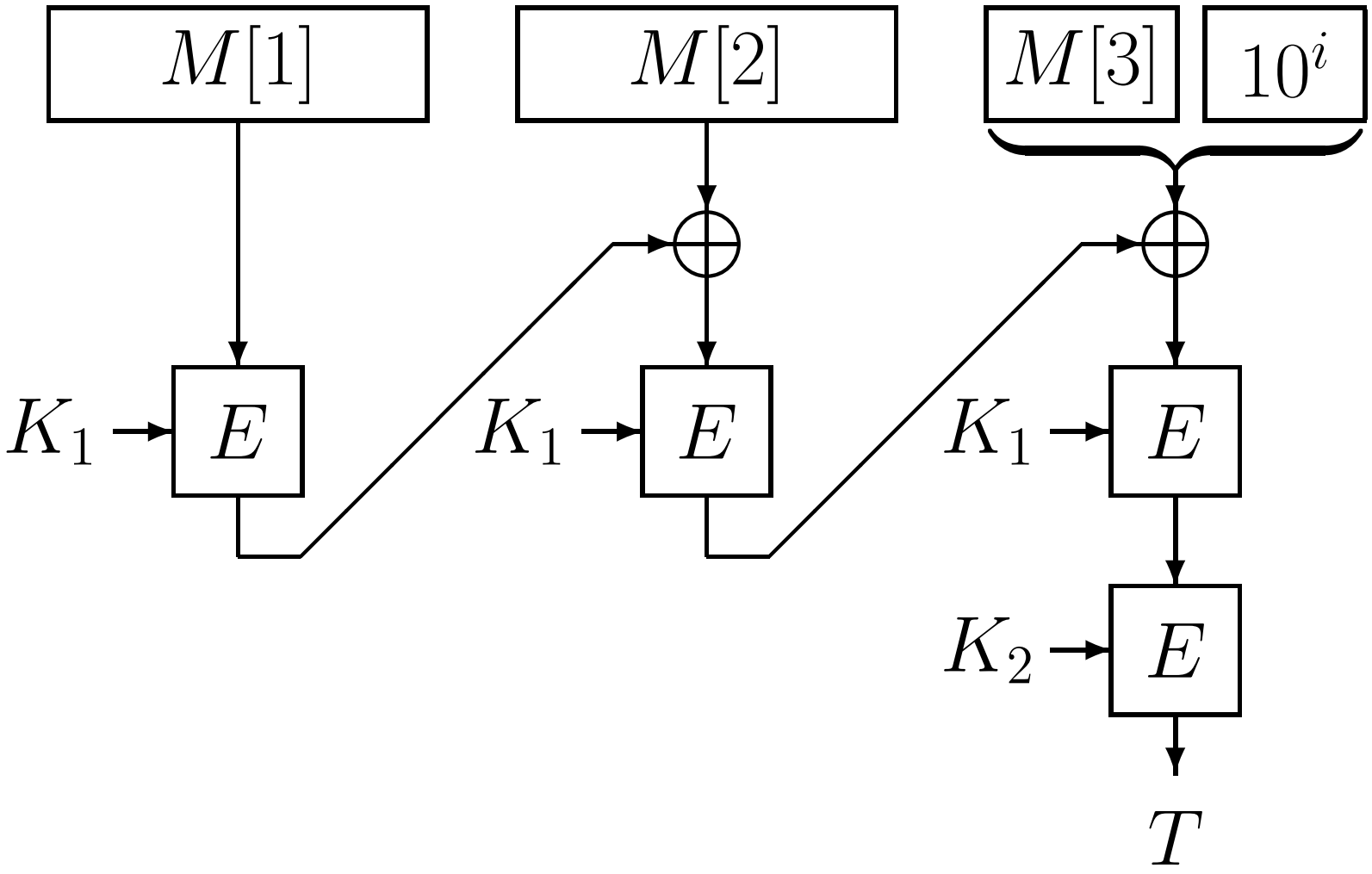


Attack on CBC MAC (2)



EMAC (Race Project)

Security is proved formally.



Psuedorandom Function

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

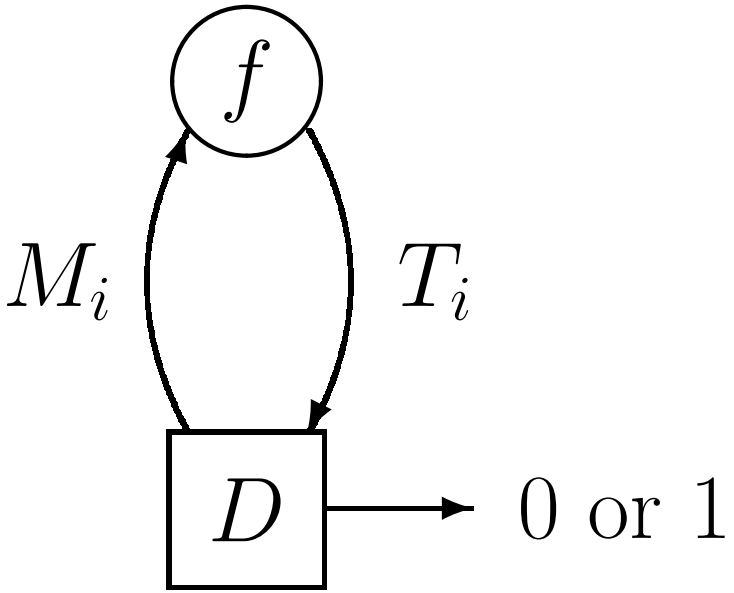
$$F \subset \mathsf{Random}$$

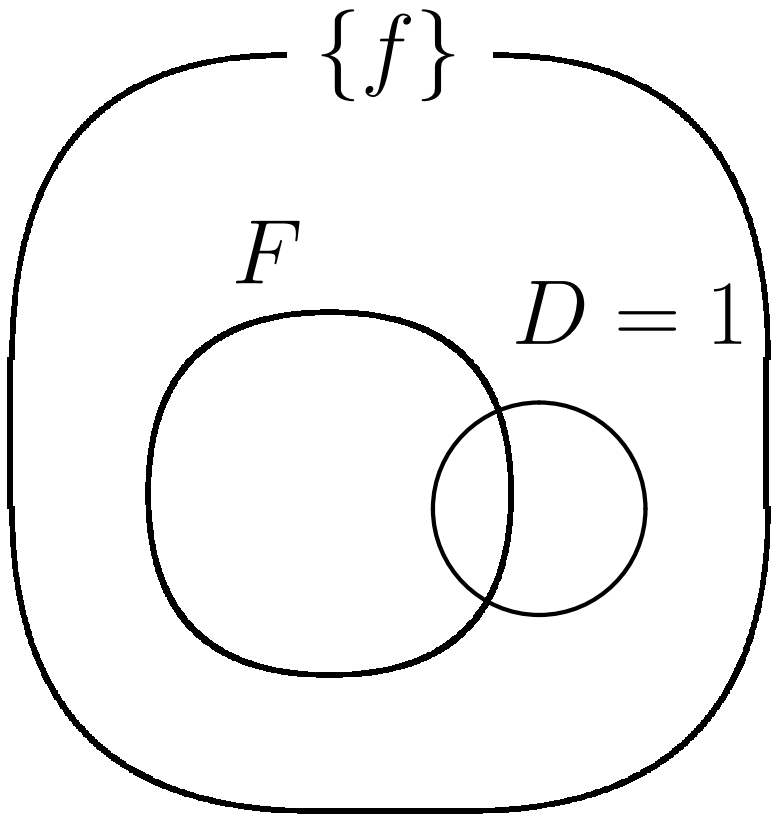
Informally,

F is pseudorandom if

F and Random are indistinguishable.

Distinguisher





Probability

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

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

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

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

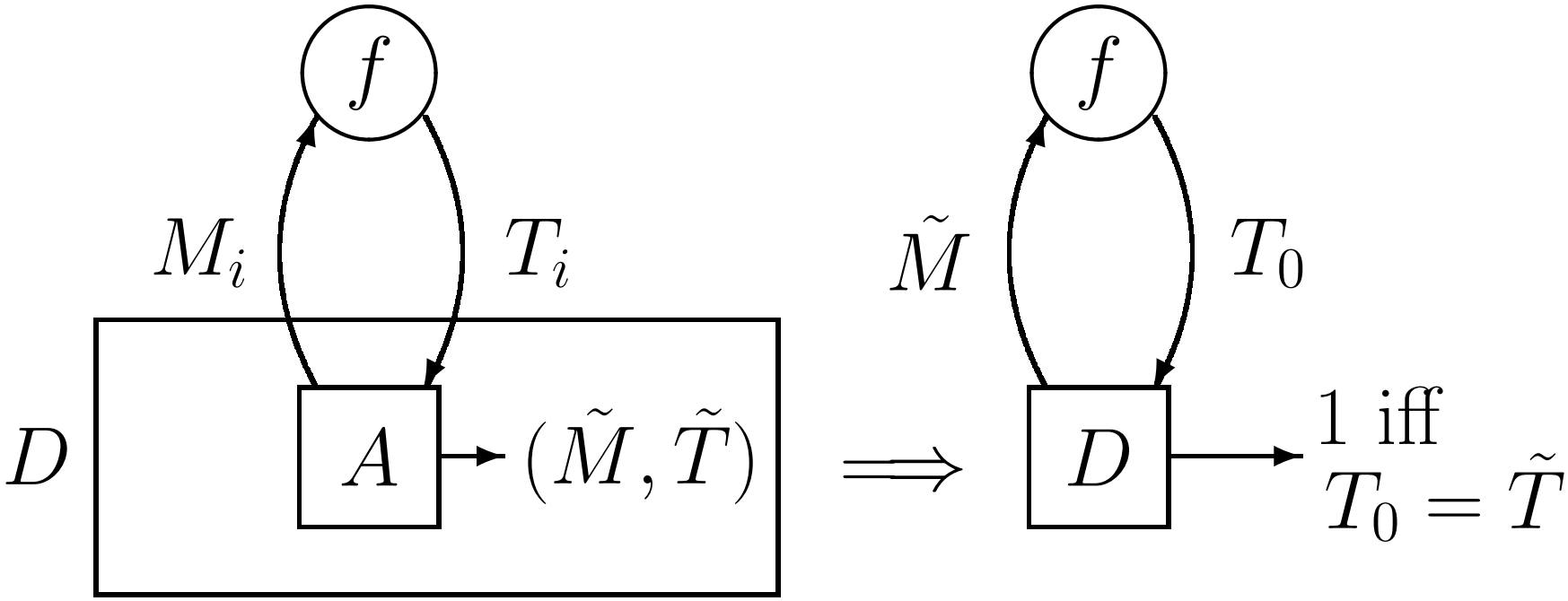
MAC scheme is (q, ϵ)-secure if

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

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

Proof (1)

$$\Pr(D = 1) = \Pr(A \text{ can forge}).$$



Proof (2)

1. $f \xleftarrow{R}$ Random: $\quad p_0 = \Pr(A \text{ can forge}).$

2. $f \xleftarrow{R} F$: $\quad p_1 = \Pr(A \text{ can forge}).$

Since F is $(q+1, \epsilon')$-random,

$$|p_1 - p_0| < \epsilon' \Longrightarrow p_1 < \epsilon' + p_0 = \epsilon' + \frac{1}{2^n} (= \epsilon).$$

(Question) What happens if $p_1 - p_0 < 0$?

For simplicity,

- F is Pseudorandom if

$$\epsilon = O\left(\frac{q^2\sigma^2}{2^n}\right)$$

- MAC is Secure if

$$\epsilon = O\left(\frac{q^2\sigma^2}{2^n}\right)$$

where $n \cdot \sigma = \max(|M_1|, \cdots, |M_q|)$.

Permutation

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

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

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: $f \longleftarrow P$ (pseudorandomP).

Ideal EMAC

$$f_1 \xleftarrow{R} \mathsf{Perm}, \quad f_2 \xleftarrow{R} \mathsf{Perm}.$$

$$T = f_2(CBC_{f_1}(M))$$

(Lemma 1) Ideal EMAC is pesudorandom.

$$\Downarrow$$

(Proposition 2) Ideal EMAC is secure.

Proof of Lemma 1

Assume that A queries $M_1, \cdots, M_q$.

$\mathsf{BAD} : CBC_{f_1}(\exists M_i) = CBC_{f_1}(\exists M_j)$

If $\neg\mathsf{BAD}$, then

$f_2(CBC_{f_1}(M_i))$ behaves at random.

It is proved that $\Pr(\neg\mathsf{BAD}) < \epsilon$.

Hence Ideal EMAC is pseudorandom.

Real EMAC

$$P \subset \mathsf{Perm}, \quad f_1 \xleftarrow{R} P, \quad f_2 \xleftarrow{R} P.$$

$$T = f_2(CBC_{f_1}(M))$$

(Lemma 2)

Real (f_1, f_2) and Random (f_1, f_2)

are indistinguishable if P is pseudorandomP.

(Proposition 3)

Real EMAC is secure if P is pseudorandomP.

(Proof)

Ideal EMAC is secure from Lemma 1.

Real EMAC and Ideal EMAC are indistinguishable

if P is pseudoramdom from Lemma 2.

Q.E.D.

Padding

$M \longrightarrow M \circ 10^i$

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

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

(Extra padding)

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

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

Drawback of EMAC

- Extra padding
- 2 key-schedulings

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

Improvements

1. XCBC

   Black and Rogaway (Crypto 2000)

2. TMAC

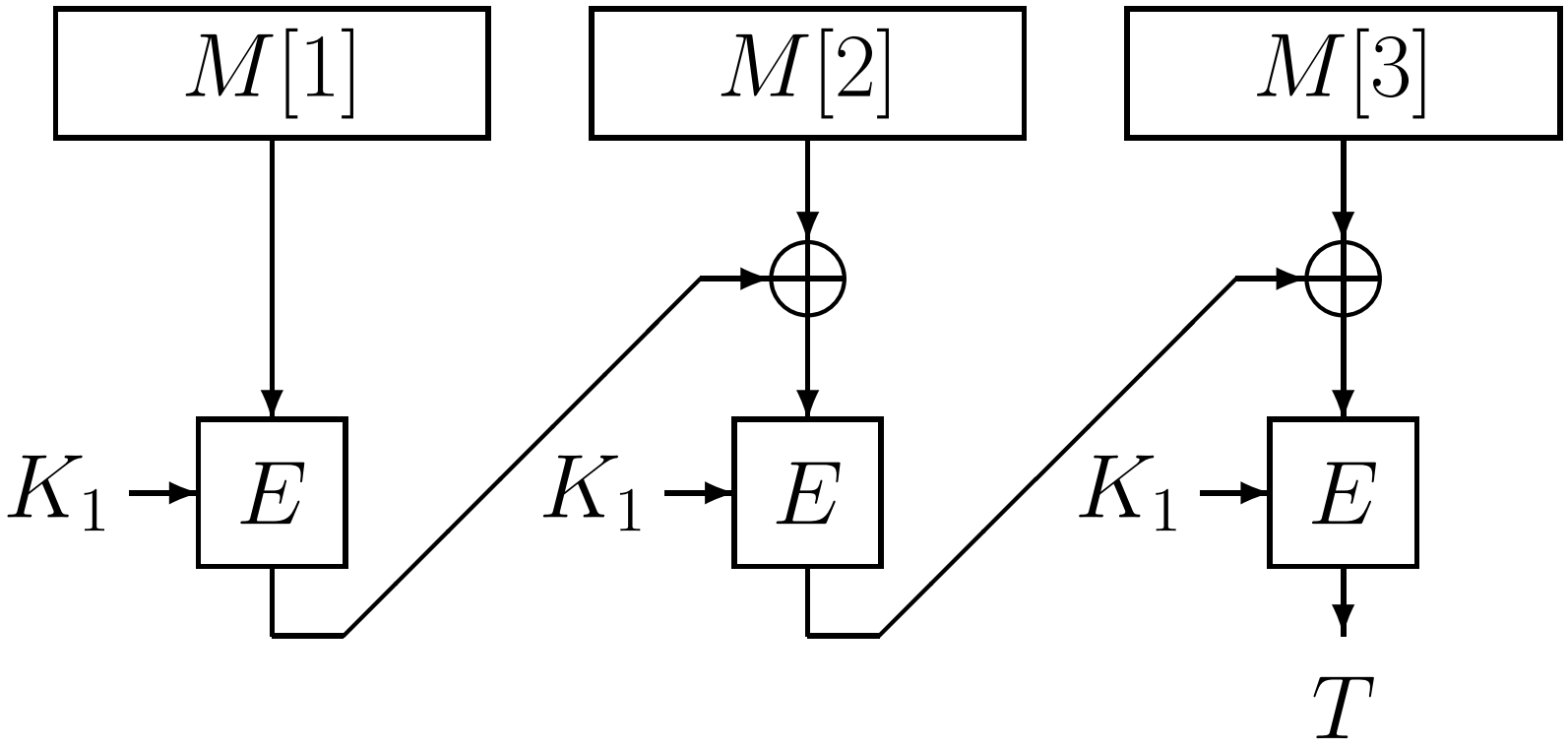
   Kurosawa and Iwata (CT-RSA 2003)

3. OMAC

   Iwata and Kurosawa (FSE 2003)

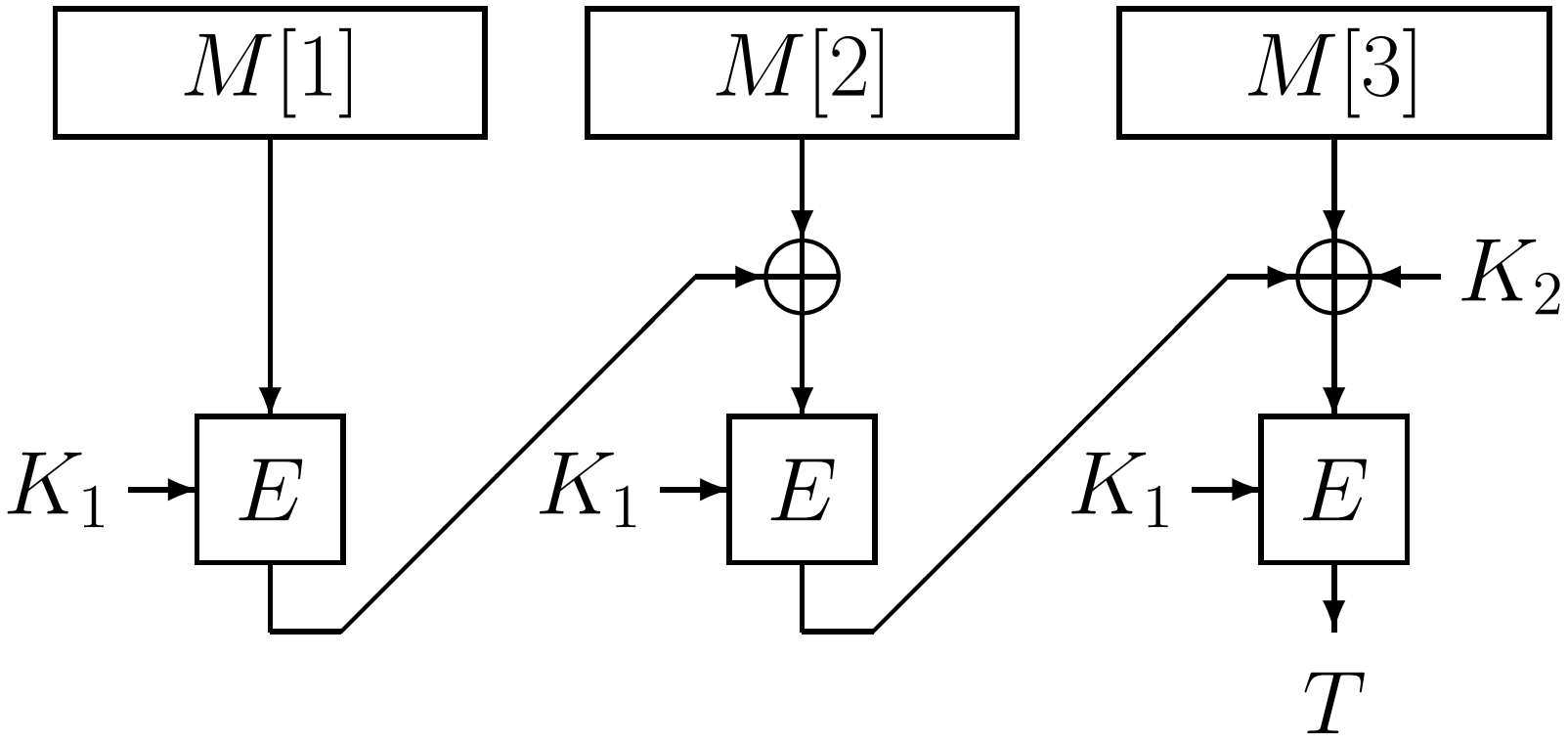
XCBC (Black and Rogaway, Crypto'00)

Case $|M| = mn$



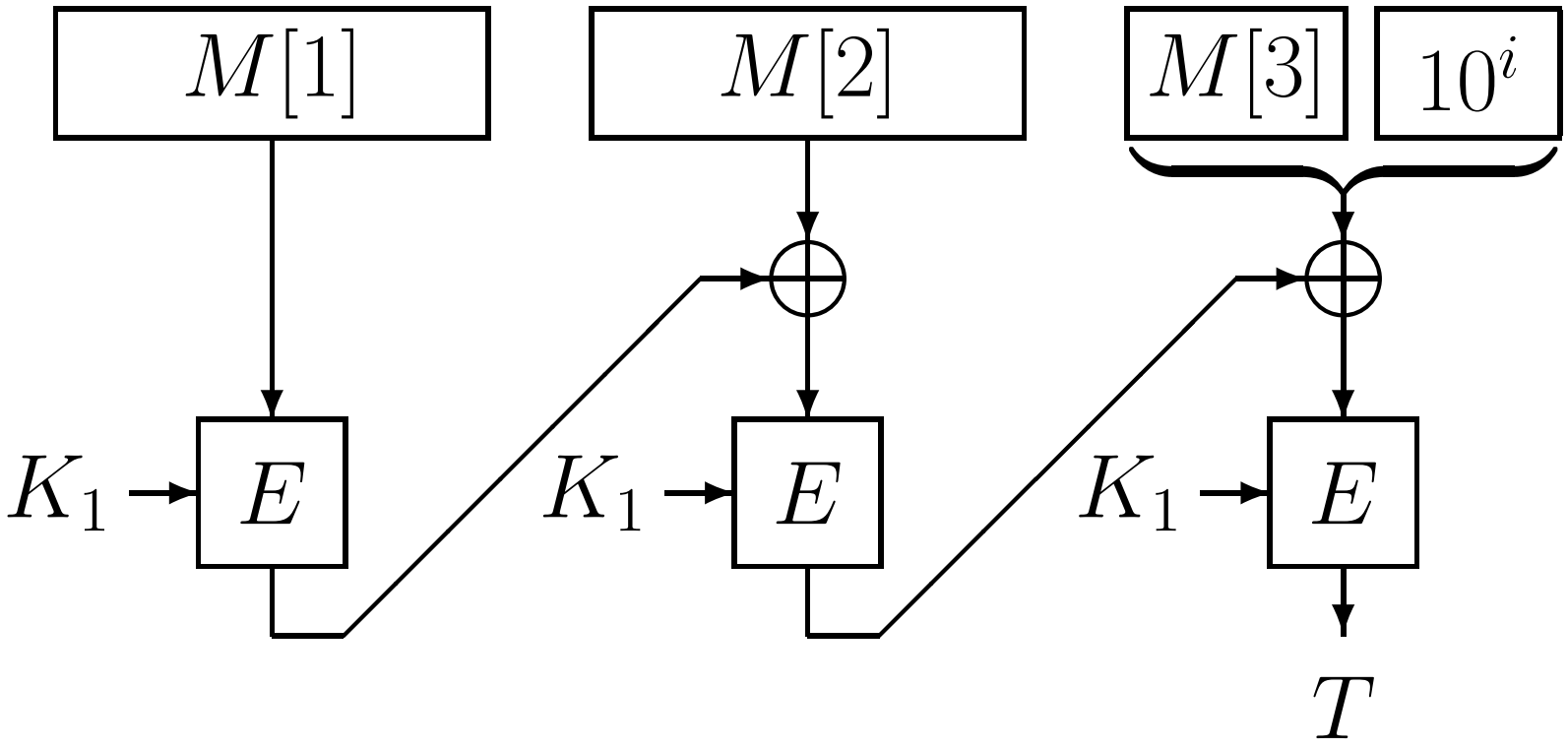
XCBC (Black and Rogaway, Crypto'00)

Case $|M| = mn$



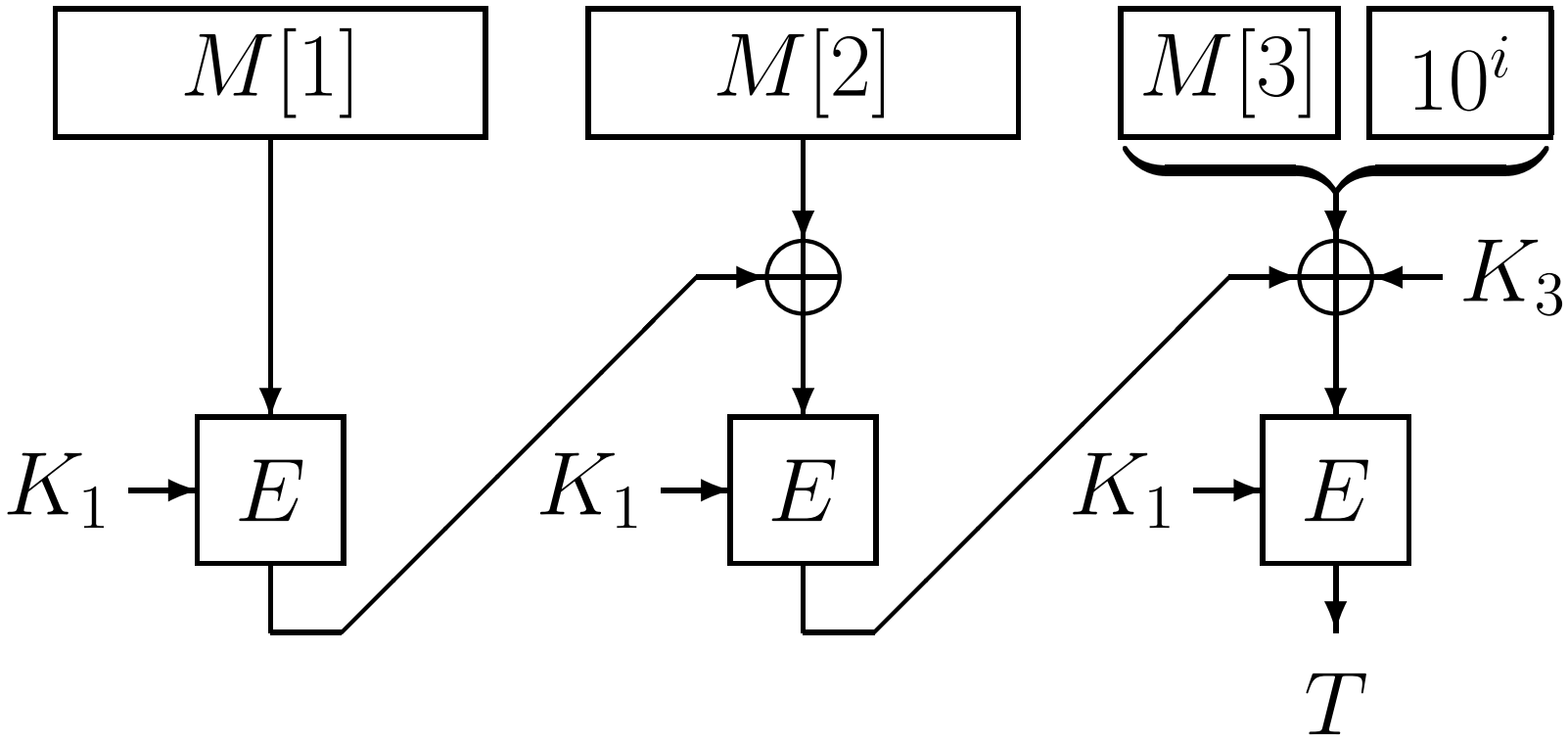
XCBC (Black and Rogaway, Crypto'00)

Case $|M| \neq mn$



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

FCBC

$$f_1 \xleftarrow{R} \mathsf{Perm}, \quad f_2 \xleftarrow{R} \mathsf{Perm}, \quad f_3 \xleftarrow{R} \mathsf{Perm}.$$

- f_1 is used for CBC MAC.
- Last block

$$= \begin{cases} f_2 & \text{if } |M| \text{ is a multiple of } n. \\ f_3 & \text{otherwise} \end{cases}$$

(Lemma 4) FCBC is pseudorandom.

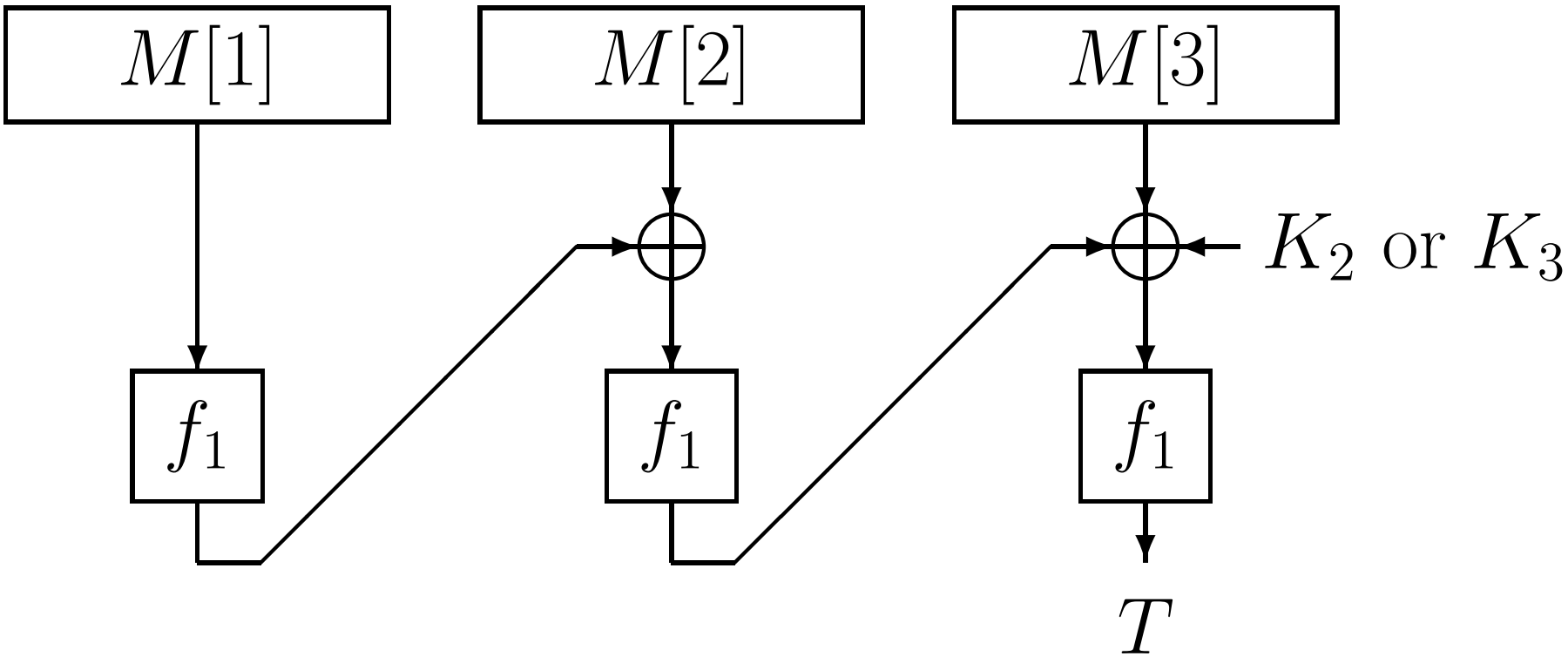
(Proof) Similar to Ideal EMAC.

$$\Downarrow$$

(Lemma 5) FCBC is secure.

Construction of XCBC

$$f_1 \xleftarrow{R} P.$$



Ideal XCBC

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

$$= \begin{cases} P_2(x) = f_1(x \oplus K_2) & \text{if } |M| \text{ is a multiple of } n. \\ P_3(x) = f_1(x \oplus K_3) & \text{otherwise} \end{cases}$$

Pseudorandomness of (f_1, P_2, P_3)

(Lemma 6)

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

are indistinguishable.

That is,

$$|\Pr(D^{f_1,P_2,P_3} = 1) - \Pr(D^{f_1,f_2,f_3} = 1)| < \epsilon.$$

Proof of Lemma 6

Suppose that D queries

$a_1, a_2, \cdots$ to f_1,

$b_1, b_2, \cdots$ to f_2 or $P_2(x) = f_1(x + K_2)$

$c_1, c_2, \cdots$ to f_3 or $P_3(x) = f_1(x + K_3)$.

BAD: The inputs to f_1 collide,

$$\exists a_i = \exists b_j \oplus K_2 \text{ or } \exists b_j \oplus K_2 = \exists c_k \oplus K_3$$

$$\text{or } \exists a_i = \exists c_k \oplus K_3.$$

If $\neg\mathsf{BAD}$, then

$$\begin{array}{cc} \text{semi-real} & \text{random} \\ \Pr(D^{(f_1,P_2,P_3)} = 1) & = \Pr(D^{(f_1,f_2,f_3)} = 1). \end{array}$$

Therefore,

If $\Pr(\mathsf{BAD}) < \epsilon$, then

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

are indistinguishable.

$$\Pr(\mathsf{BAD}) = \frac{|\{(K_2, K_3) \mid \mathsf{BAD} \text{ occurs}\}|}{|\{(K_2, K_3)\}|}$$

where BAD:

$$\exists a_i = \exists b_j \oplus K_2$$

$$\exists b_j \oplus K_2 = \exists c_k \oplus K_3$$

$$\exists a_i = \exists c_k \oplus K_3.$$

Hence $\Pr(\mathsf{BAD}) < \epsilon$.

Security of Ideal XCBC

(Proposition 4) Ideal XCBC is secure.

(Proof)

FCBC is secure from Lemma 5.

Ideal XCBC and FCBC are indistinguishable

from Lemma 6.

Q.E.D.

Security of XCBC

(Proposition 5)

XCBC is secure if P is pseudorandomP.

(Proof)

Ideal XCBC is secure from Proposition 4.

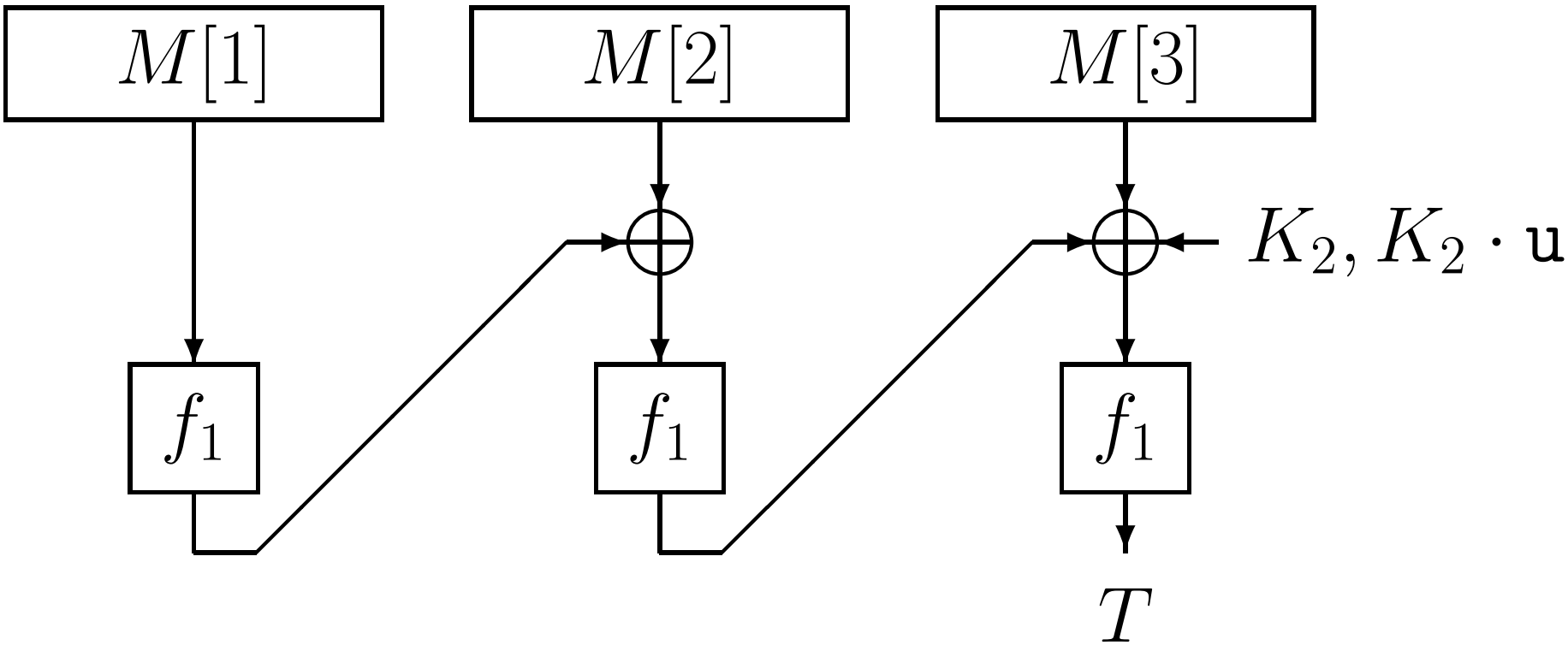
Q.E.D.

TMAC (Kurosawa and Iwata, RSA'03)

- XCBC has 3 keys ($k + 2n$ bits), K_1, K_2, K_3
- TMAC has 2 keys ($k + n$ bits), K_1, K_2.

Construction of TMAC

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



Ideal TMAC

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

$$= \begin{cases} P_2(x) = f_1(x \oplus K_2 \cdot \mathtt{u}) & \text{if } |M| \text{ is a} \\ & \text{multiple of } n. \\ P_3(x) = f_1(x \oplus K_2) & \text{otherwise} \end{cases}$$

Security of TMAC

(Theorem 1) Ideal TMAC is secure.

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

are indistinguishable.

$\Downarrow$

(Thorem 2)

TMAC is secure if P is speudorandomP.

About $GF(2^{128})$

Defined by $f(\mathtt{u}) = \mathtt{u}^{128} + \mathtt{u}^7 + \mathtt{u}^2 + \mathtt{u} + 1$.

For $a = a_{127} \cdots a_1 a_0 \in GF(2^n)$, let

$$(a \ll 1) = a_{126} \cdots a_1 a_0 0.$$

Then

$$a \cdot \mathtt{u} = \begin{cases} a \ll 1 & \text{if } a_{127} = 0, \\ (a \ll 1) \oplus 0^{120}10000111 & \text{otherwise.} \end{cases}$$

OMAC (Iwata and Kurosawa, FSE'03)

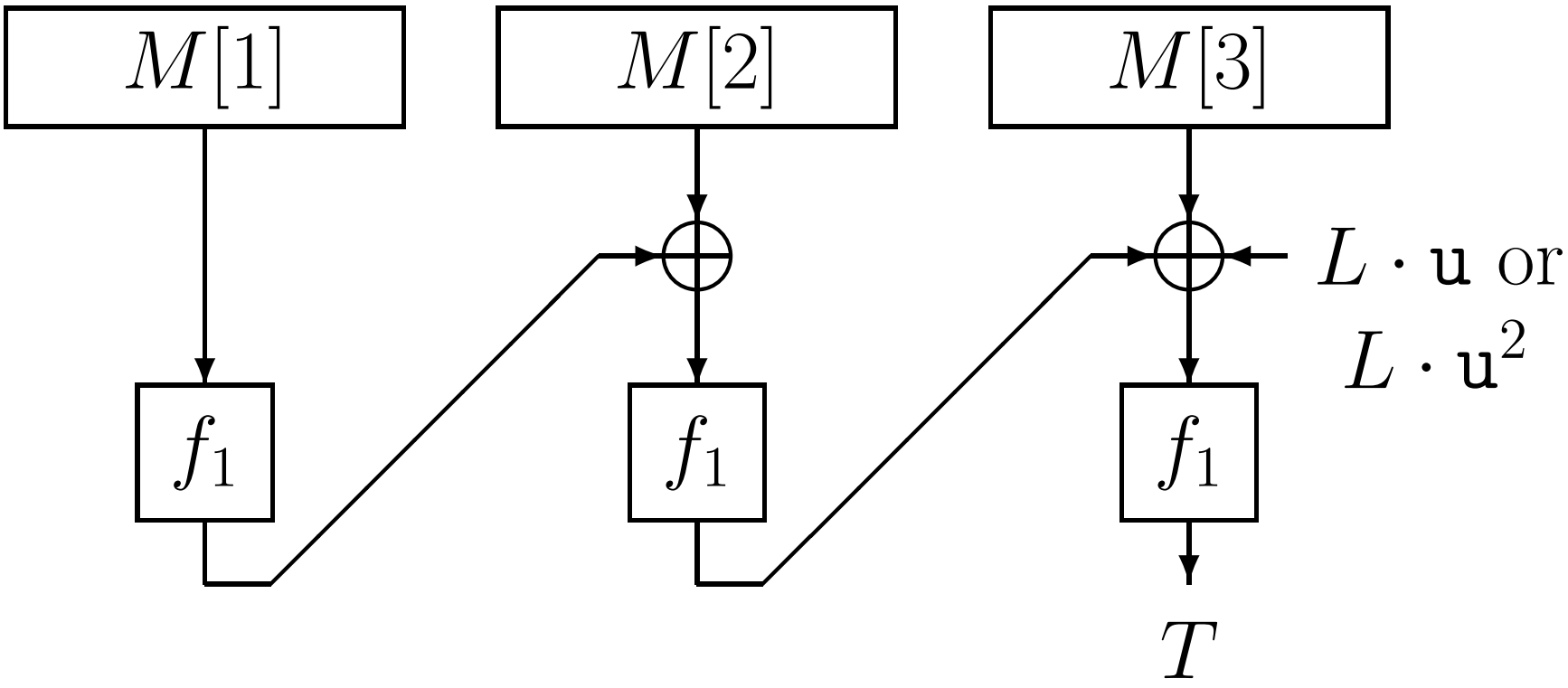
- XCBC has 3 keys ($k + 2n$ bits), K_1, K_2, K_3
- TMAC has 2 keys ($k + n$ bits), K_1, K_2.

$$\Downarrow$$

- OMAC has 1 key (k bits), K_1.

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.
- 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

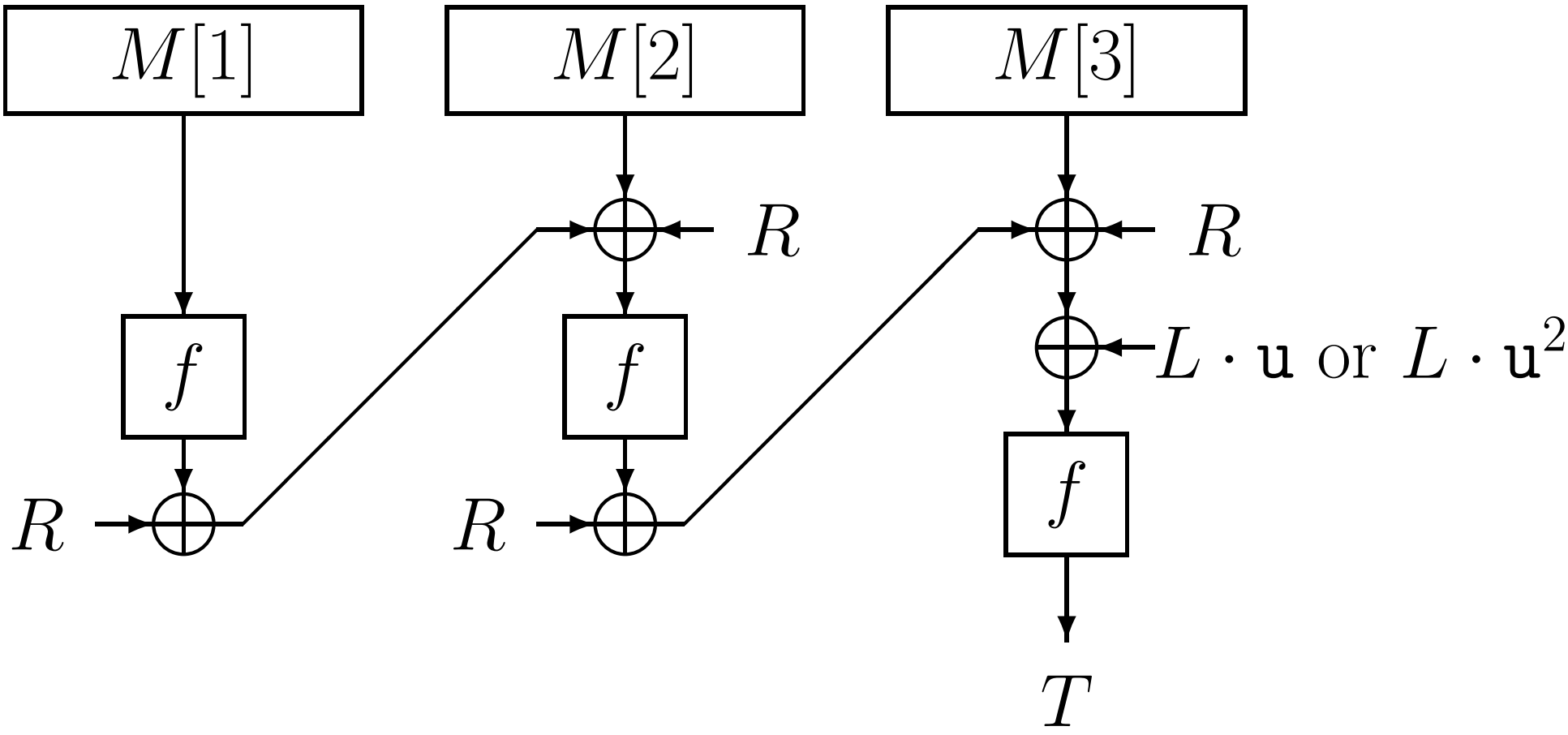
because $L = f_1(0^n)$.

$\Downarrow$

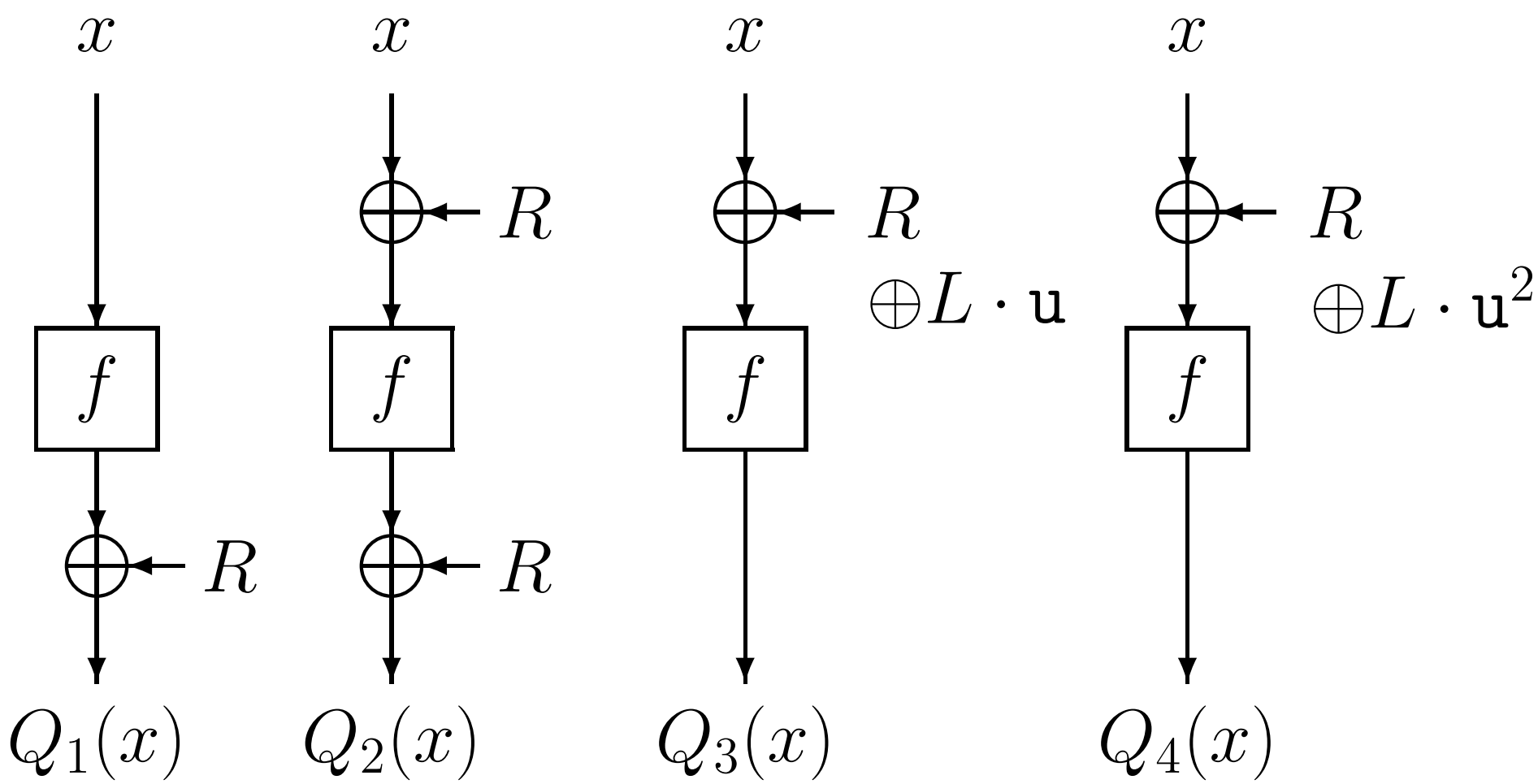
We need a new proof technique !!

Our Idea for Ideal OMAC

$$f \xleftarrow{R} \mathsf{Perm},\ R \xleftarrow{R} \{0,1\}^n,\ L = f(0^n).$$

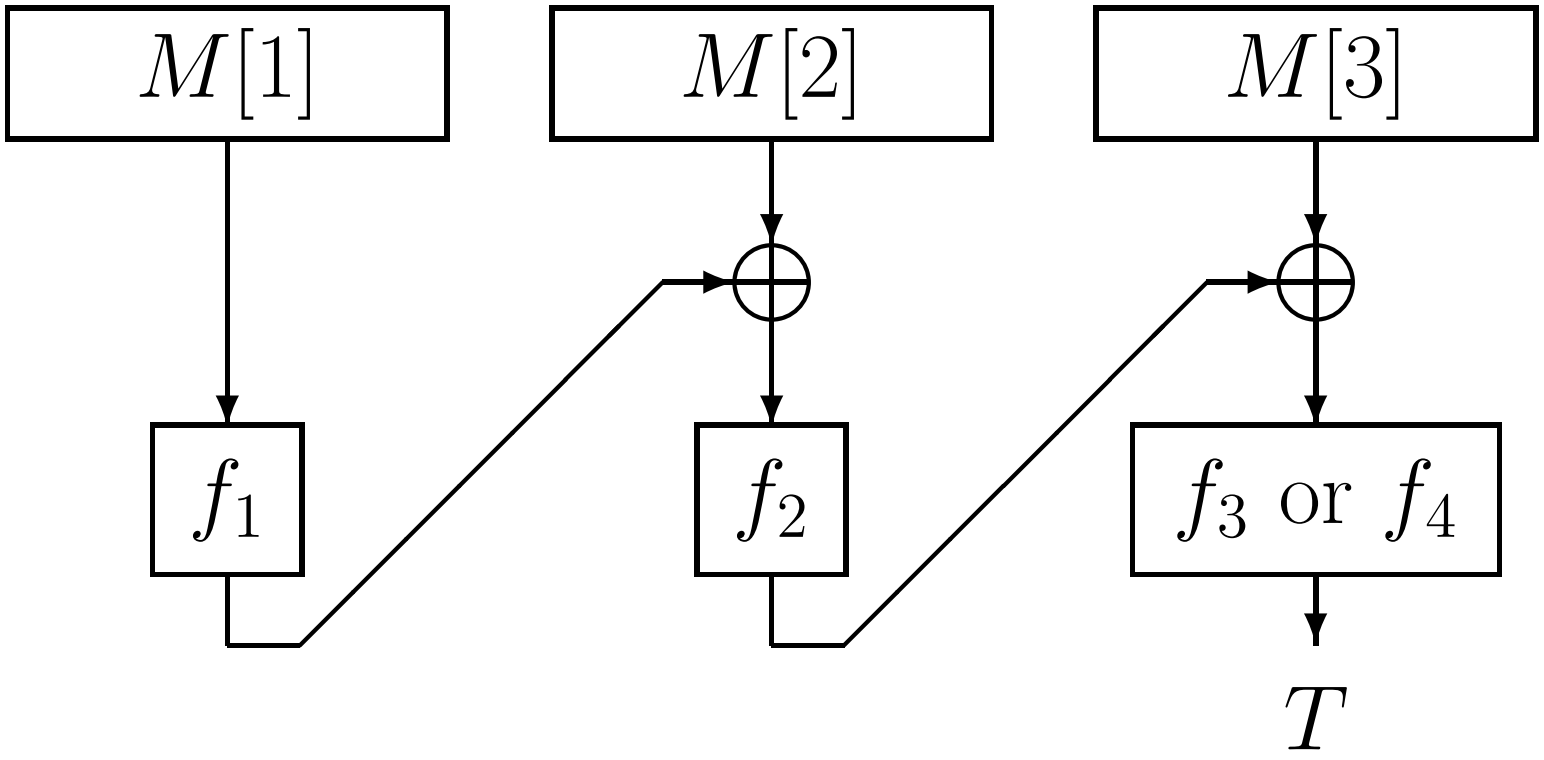


$Q_1, \cdots, Q_4$


x
f
R
$Q_1(x)$
x
R
f
R
$Q_2(x)$
x
R
$\oplus L \cdot \mathtt{u}$
f
$Q_3(x)$
x
R
$\oplus L \cdot \mathtt{u}^2$
f
$Q_4(x)$

MOMAC

$f_1, \cdots, f_4 \xleftarrow{R}$ Perm.



Security of MOMAC

(Lemma 7) MOMAC is pseudorandom.

(Proof) Similar to Ideal EMAC.

$$\Downarrow$$

(Lemma 8) MOMAC is secure.

Security of Ideal OMAC

(Theorem 3)

(Ideal OMAC) (MOMAC)

$(Q_1, \cdots, Q_4)$ and random $(f_1, \cdots, f_4)$

are indistinguishable.

(Corollary 1) Ideal OMAC is secure.

(Proof) MOMAC is secure from Lemma 8.

Proof of Theorem 3

$$y_0 = Q_1(0^n) = f(0^n) + R = L + R$$

For fixed y_0, L is random because R is random.

$\mathsf{BAD}_{i,j}$: The inputs to f collide for Q_i and Q_j.

For Q_3 and Q_4,

$$\exists x_i \oplus R \oplus L \cdot \mathtt{u} = \exists x_j \oplus R \oplus L \cdot \mathtt{u}^2$$

$$x_i \oplus x_j = L \cdot (\mathtt{u} + \mathtt{u}^2).$$

$$\Pr(\mathsf{BAD}_{i,j}) < \epsilon \text{ for any } (i,j).$$

Hence

$(Q_1, \cdots, Q_4)$ and random $(f_1, \cdots, f_4)$

are indistinguishable.

Q.E.D.

Security of OMAC

(Theorem 4)

OMAC is secure if P is pseudorandomP.

(Proof)

Because ideal OMAC is secure from Corollary 1.

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