OMAC: One-Key CBC MAC

February 25, 2003

Tetsu Iwata and Kaoru Kurosawa

Ibaraki University

Fast Software Encryption, FSE 2003, February 24–26, 2003, Lund, Sweden

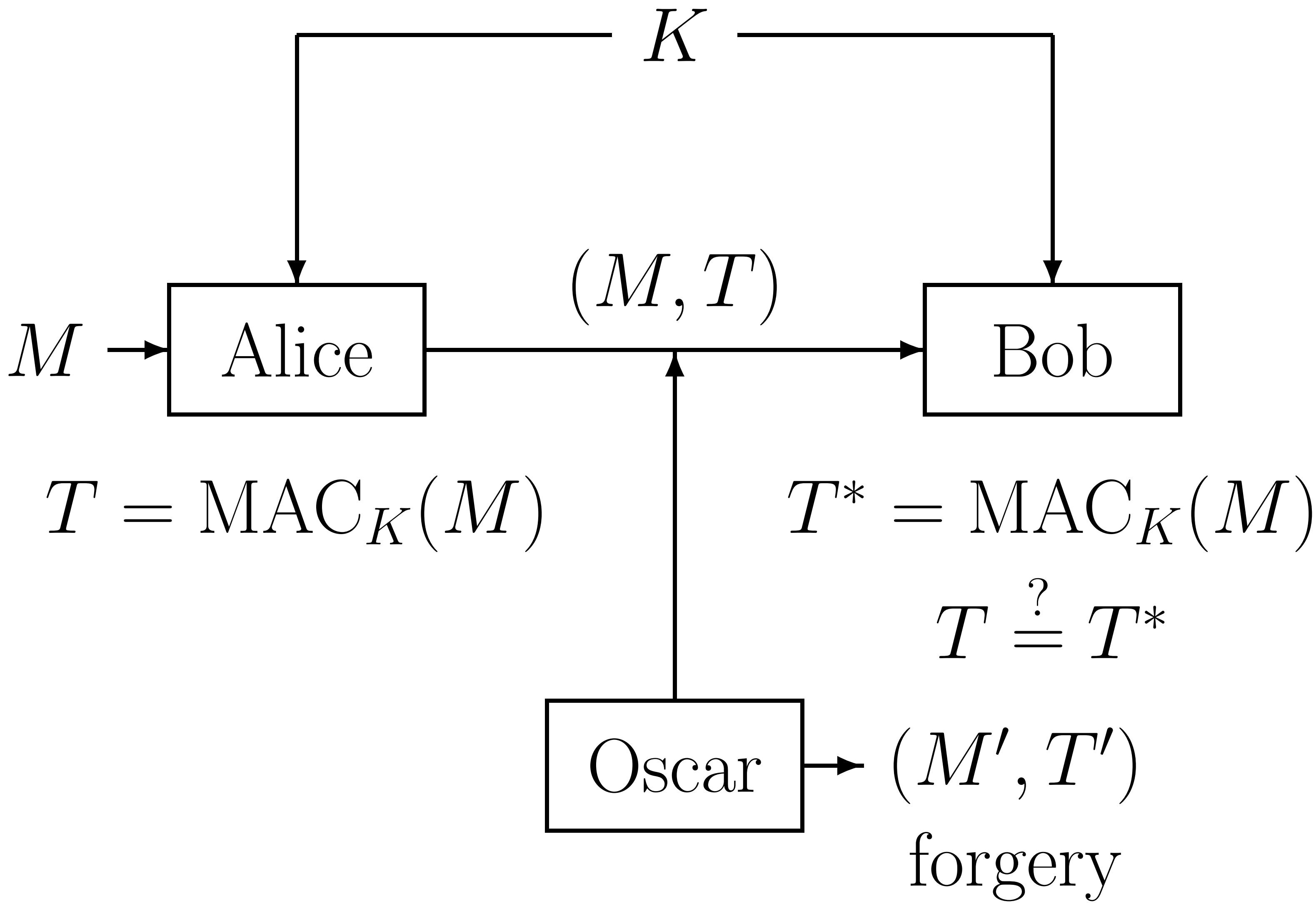
What is a MAC?

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.

$$\Downarrow$$

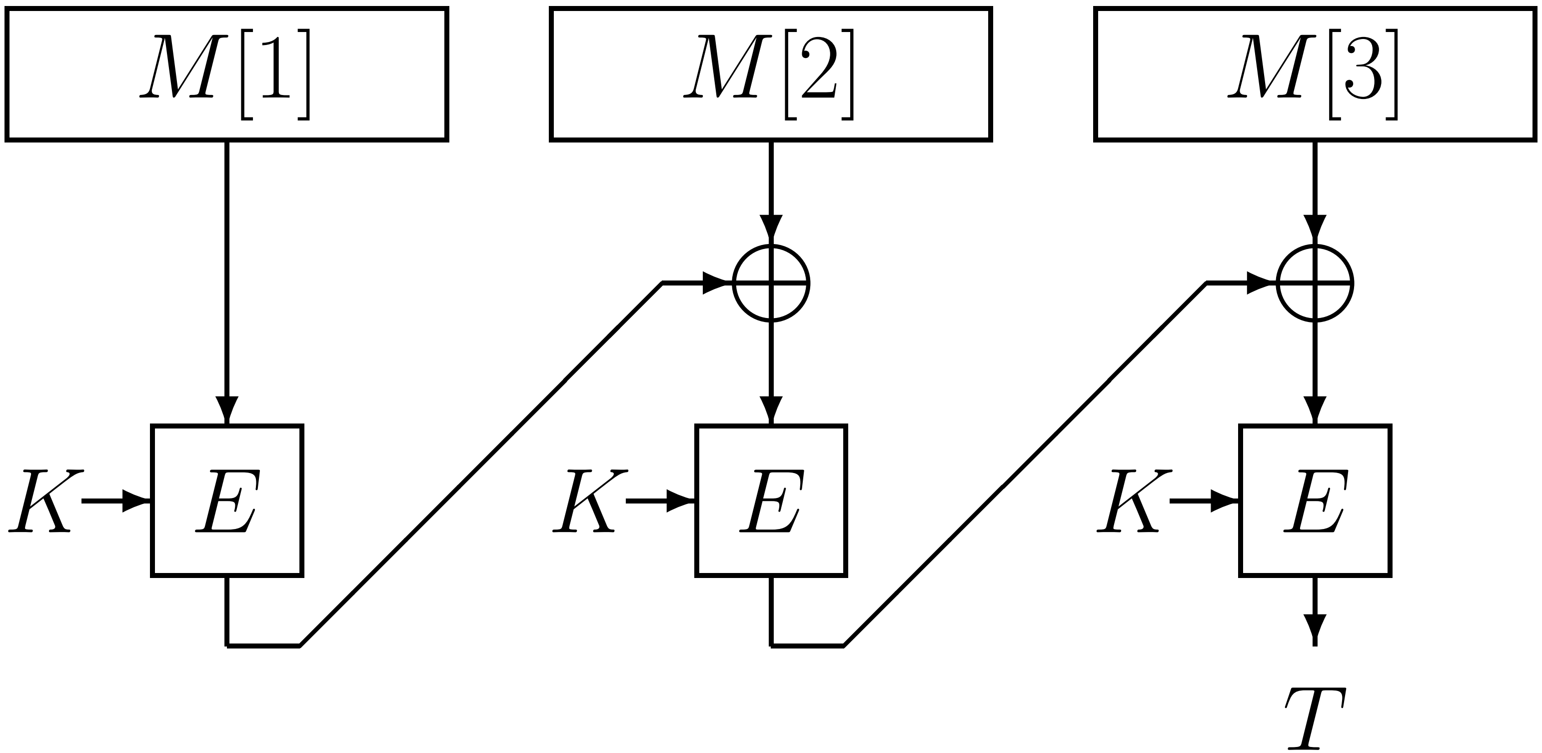
MAC (Message Authentication Code)

What is a MAC?


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



Problems of CBC MAC

- does not allow messages of **arbitrary bit length**

  (all messages must be a multiple of n bits)

- does not allow messages of **varying** lengths

  (otherwise **insecure**)

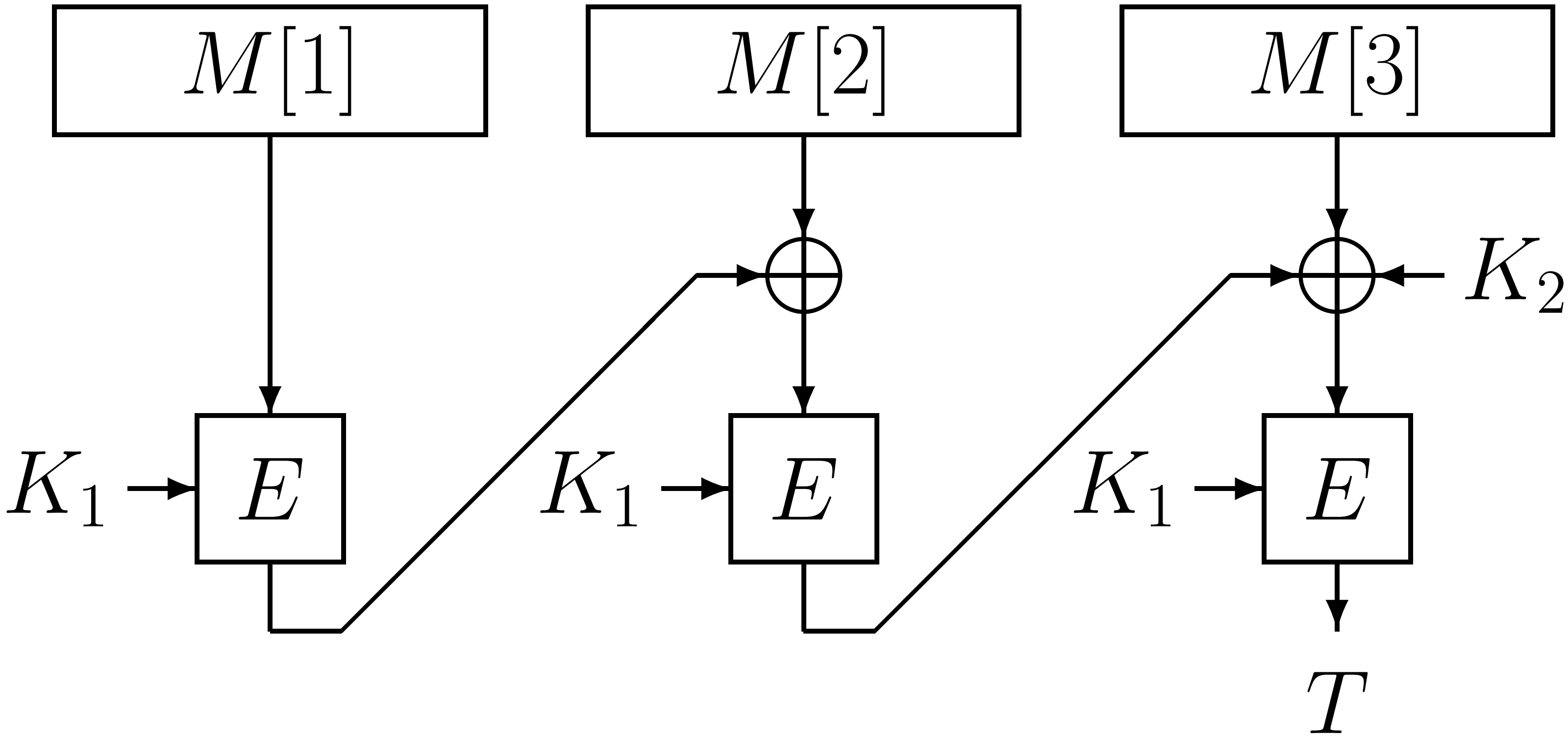
Previous Works

- ANSI X9.19 (Optional Triple-DES)
- MacDES [Knudsen, Preneel]
- EMAC [Race Project]

  (Analysis by [Petrank, Rackoff] and [Vaudenay])
- XCBC [Black, Rogaway]
- TMAC [Kurosawa, Iwata]

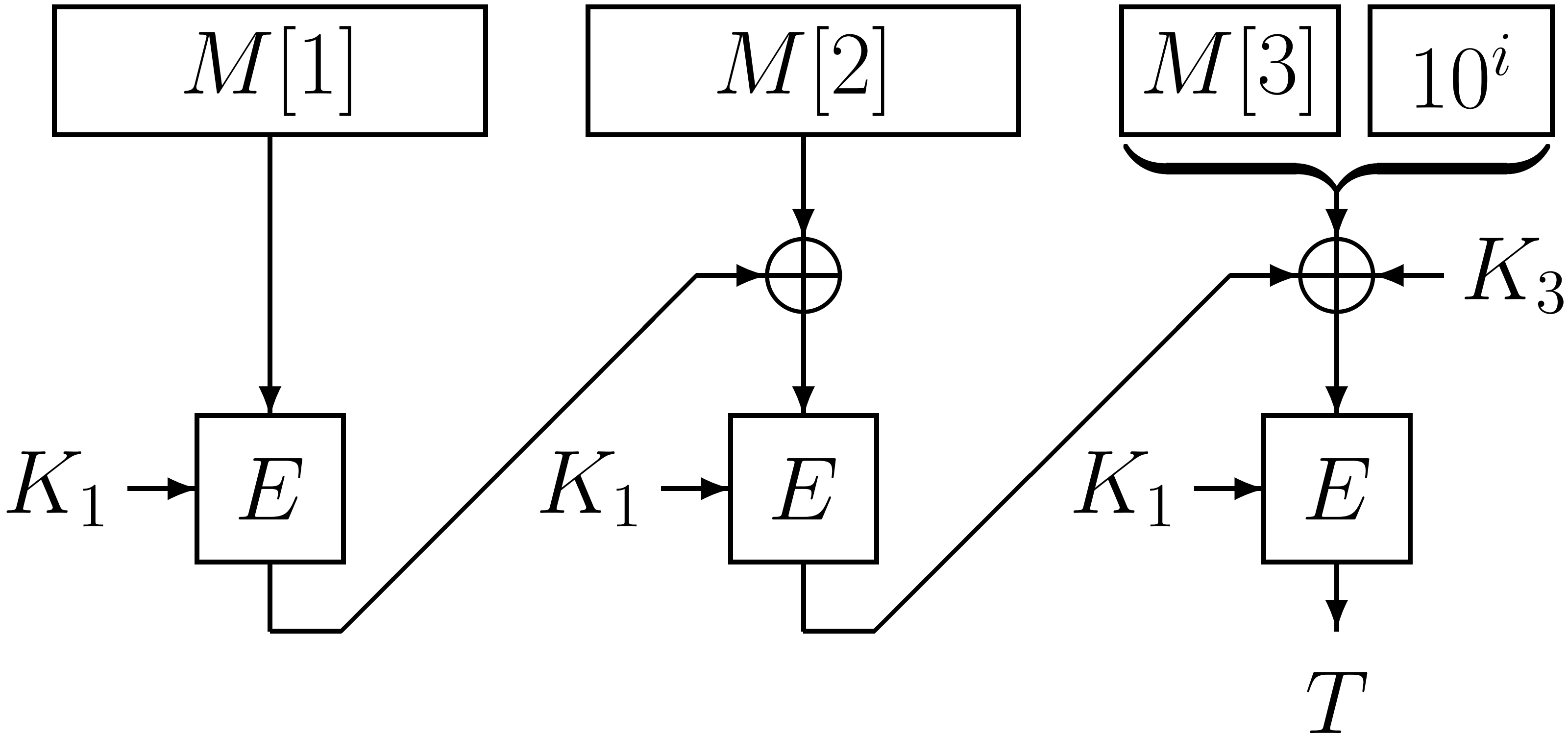
XCBC (Black and Rogaway, Crypto '00)

Case $|M| = mn$ $(m \geq 1)$



XCBC (Black and Rogaway, Crypto '00)

Case $|M| \neq mn$



Advantages of XCBC

- Correctly handles messages of **any** bit length
- Correctly handles messages of **varying** lengths

Disadvantage of XCBC

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

TMAC (Kurosawa and Iwata, RSA '03)

$$(K_1, K_2, K_3) \longrightarrow (K_1, K_2 \cdot \mathtt{u}, K_2)$$

Two keys ($k + n$ bits), K_1, K_2.

Still not optimal

Our Proposal: OMAC-family

One key (k bits) K

(with **small** cost and **without** security loss)

OMAC-family

- a block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$,

  (AES, Camellia, TDES, ...)

- an n-bit constant $\texttt{Cst}$, (arbitrarily)

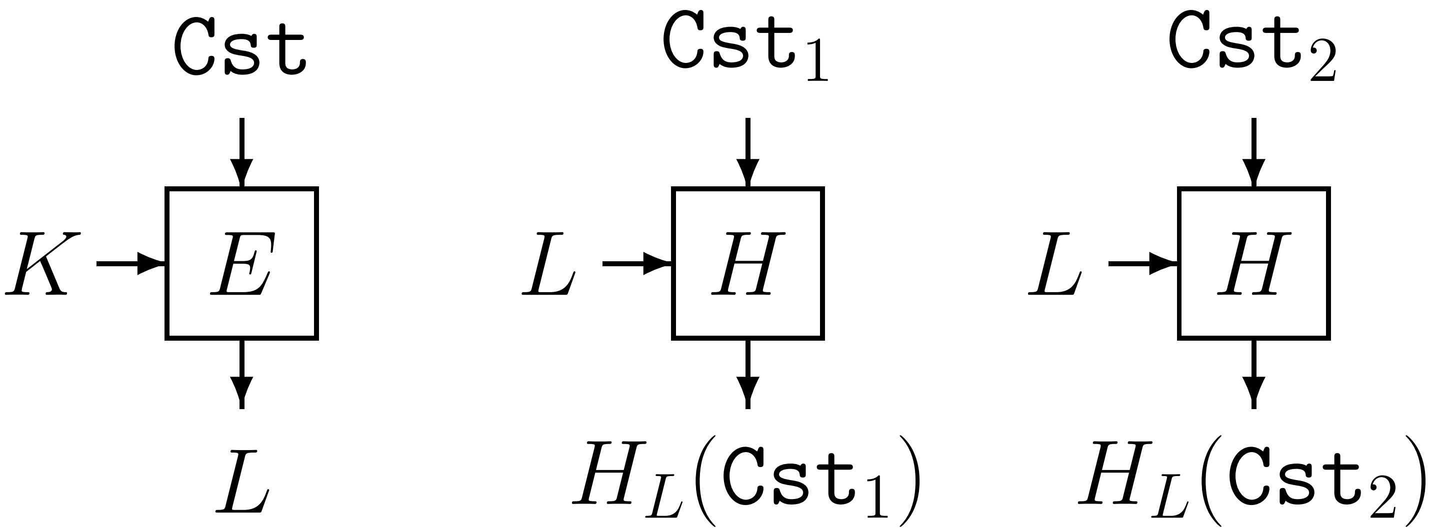
- a hash function $H : \{0,1\}^n \times X \to \{0,1\}^n$,

- two distinct constants $\texttt{Cst}_1$, $\texttt{Cst}_2 \in X$.

Conditions on H, $\mathtt{Cst}_1$ and $\mathtt{Cst}_2$

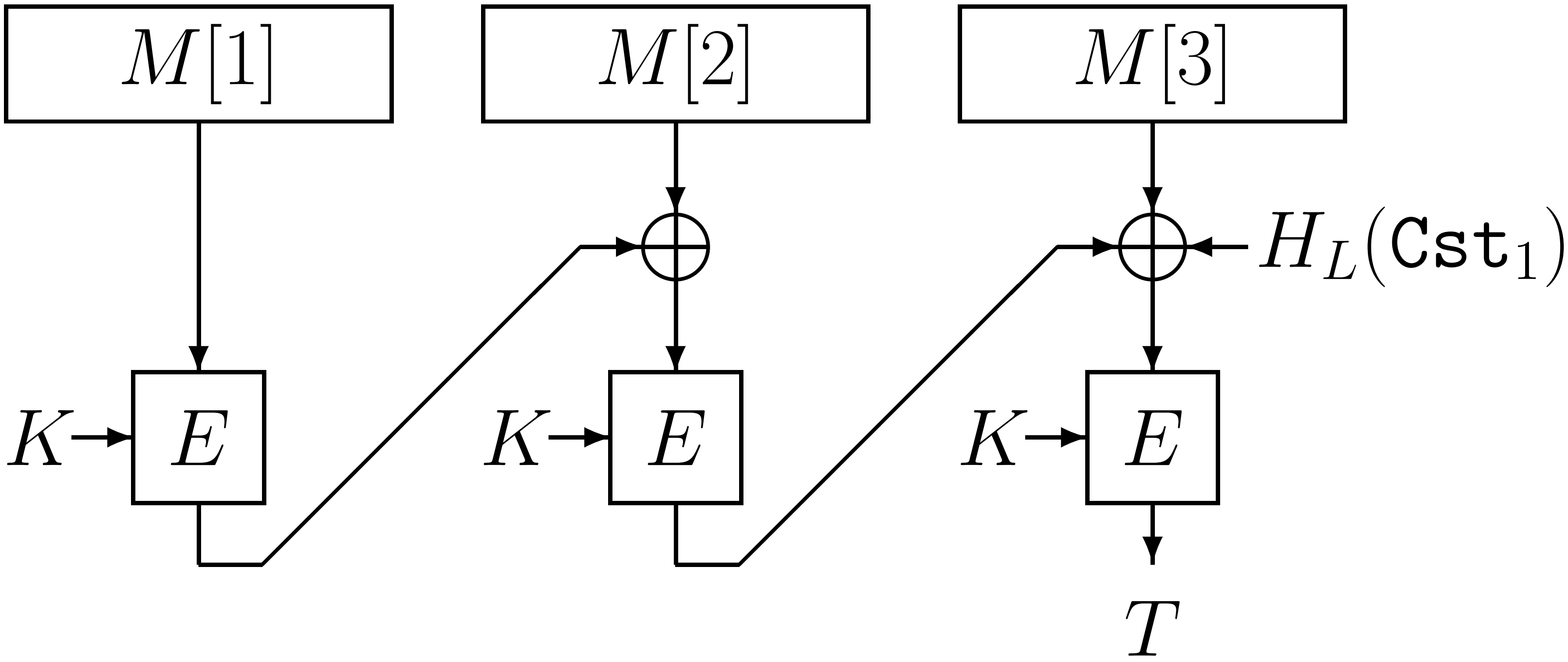
- $\forall y,\ \#\{L \mid H_L(\mathtt{Cst}_1) = y\} \leq \epsilon_1 \cdot 2^n$
- $\forall y,\ \#\{L \mid H_L(\mathtt{Cst}_2) = y\} \leq \epsilon_2 \cdot 2^n$
- $\forall y,\ \#\{L \mid H_L(\mathtt{Cst}_1) \oplus H_L(\mathtt{Cst}_2) = y\} \leq \epsilon_3 \cdot 2^n$
- $\forall y,\ \#\{L \mid H_L(\mathtt{Cst}_1) \oplus L = y\} \leq \epsilon_4 \cdot 2^n$
- $\forall y,\ \#\{L \mid H_L(\mathtt{Cst}_2) \oplus L = y\} \leq \epsilon_5 \cdot 2^n$
- $\forall y,\ \#\{L \mid H_L(\mathtt{Cst}_1) \oplus H_L(\mathtt{Cst}_2) \oplus L = y\} \leq \epsilon_6 \cdot 2^n$

OMAC-family: Set-up



OMAC-family

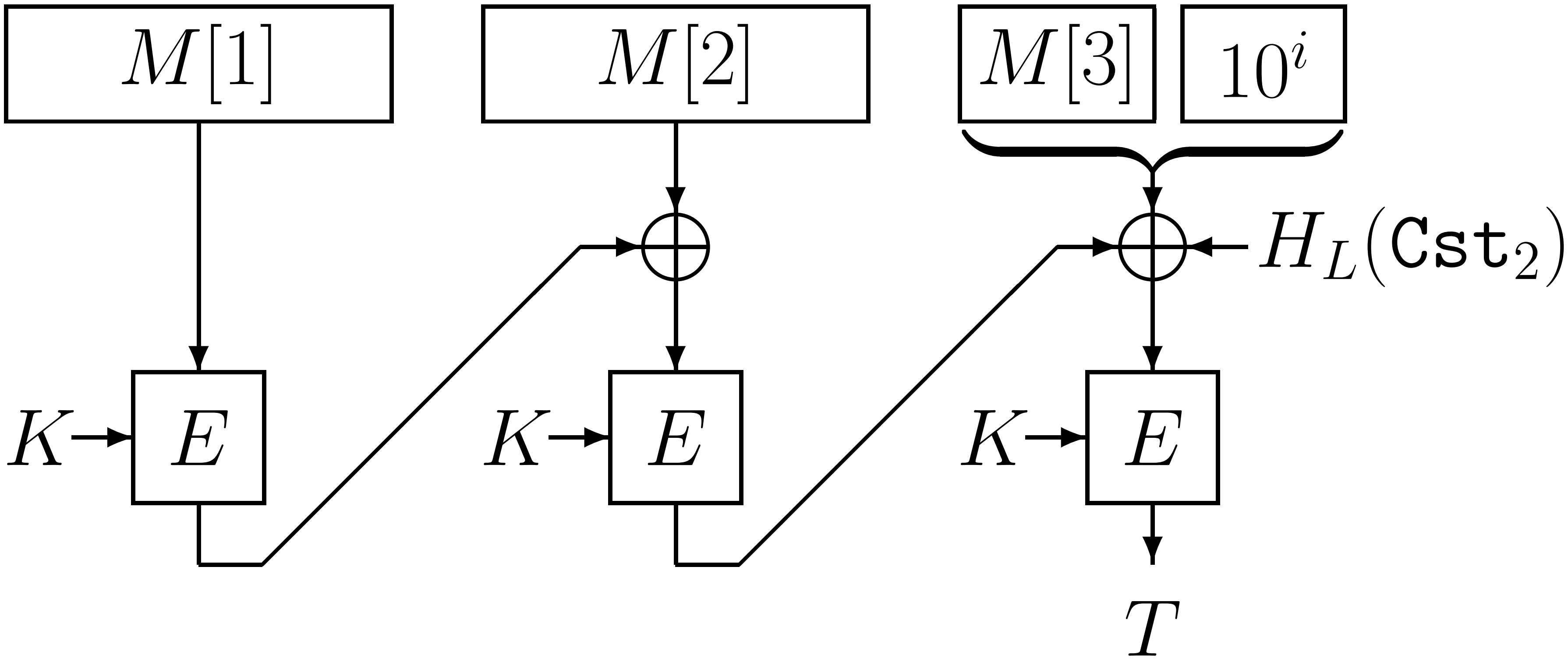
Case $|M| = mn$ $(m \geq 1)$



$$L = E_K(\mathtt{Cst})$$

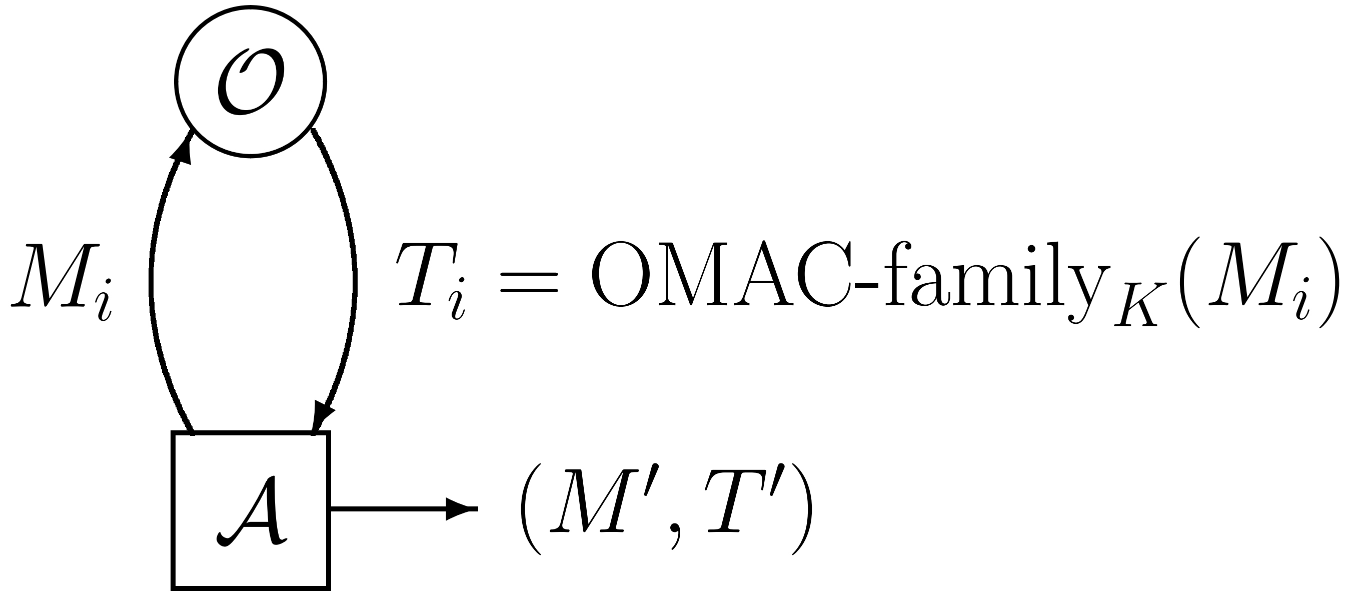
OMAC-family

Case $|M| \neq mn$



$$L = E_K(\mathtt{Cst})$$

Security of OMAC-family



- $\mathcal{A}$ forges if $T' = \text{OMAC-family}_K(M')$, $M' \neq M_i$
- $\mathtt{Adv}^{\mathsf{mac}}_{\text{OMAC-family}_K}(\mathcal{A}) \stackrel{\text{def}}{=} \Pr_K(\mathcal{A} \text{ forges})$

Theorem

Suppose that E is a random permutation P. Let $\mathcal{A}$ be an adversary which asks at most q queries, and each query is at most nm bits $(m \leq 2^n/4)$. Then

$$\mathtt{Adv}^{\mathsf{mac}}_{\text{OMAC-family}_P}(\mathcal{A}) \leq \frac{q^2}{2} \cdot \left(\frac{7m^2+2}{2^n} + 3m^2\epsilon \right) + \frac{1}{2^n}$$

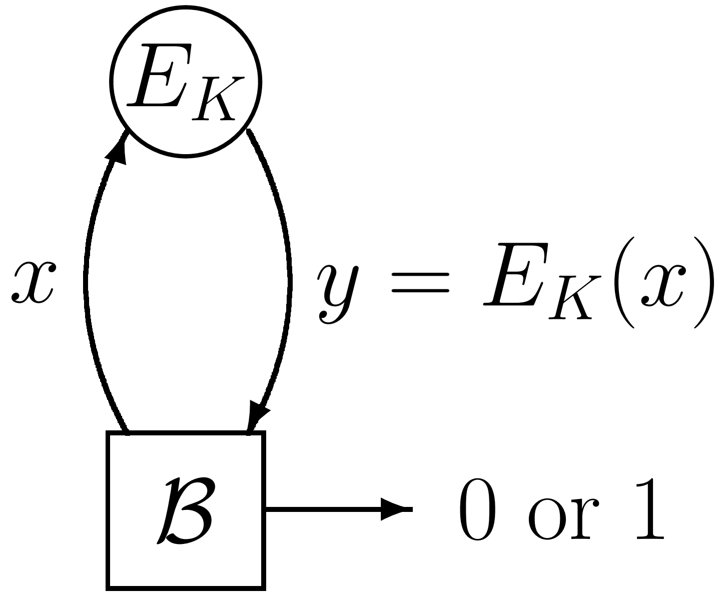
where $\epsilon = \max\{\epsilon_1, \ldots, \epsilon_6\}$.

Theorem (Cont.)

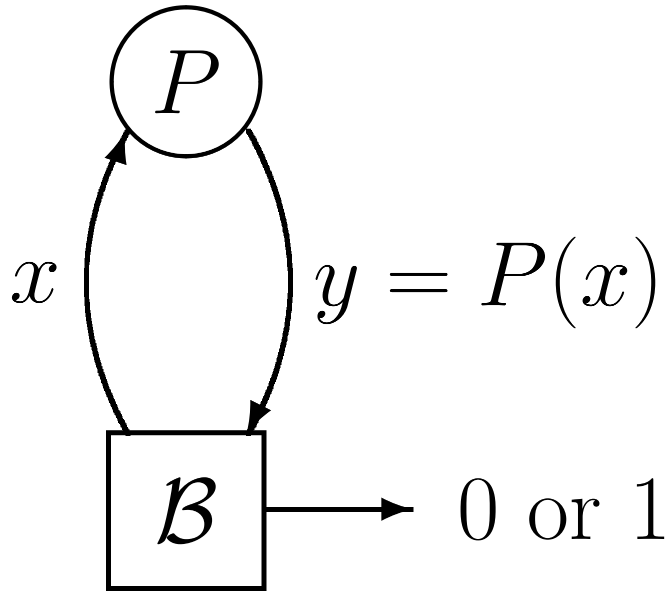
- If $\epsilon_i \approx 2^{-n}$, then OMAC-family is secure up to the birthday paradox limit.
- When E is a real block cipher (AES, Camellia, TDES), $\mathtt{Adv}_E^{\mathsf{prp}}(\mathcal{B})$ is added to the above bound.

Block Cipher Security (PRP)

Enc. Oracle



Random Perm. Oracle



$$\mathtt{Adv}_E^{\mathsf{prp}}(\mathcal{B}) \stackrel{\text{def}}{=} \left| \Pr_K(\mathcal{B}^{E_K} = 1) - \Pr_P(\mathcal{B}^P = 1) \right|$$

Examples of H, $\mathtt{Cst}_1$ and $\mathtt{Cst}_2$

Two Specifications: OMAC1, OMAC2

OMAC = OMAC1 and OMAC2

Proposed Specification: OMAC1

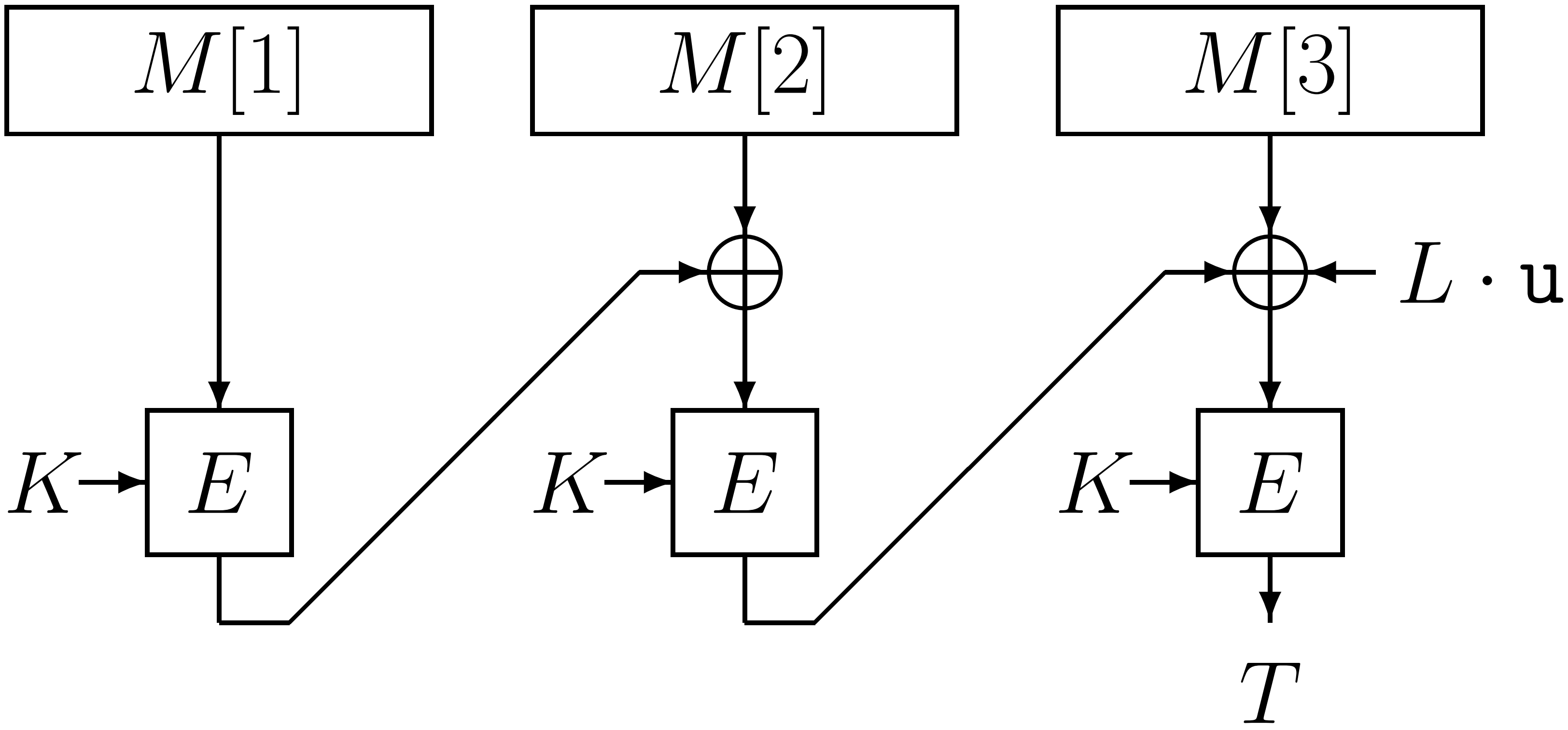
- $\texttt{Cst} = 0^n$,
- $H_L(x) = L \cdot x$ ("$\cdot$" over $\mathrm{GF}(2^n)$)
- $\texttt{Cst}_1 = \texttt{u}$,
- $\texttt{Cst}_2 = \texttt{u}^2$.

$$\Downarrow$$

$$\epsilon_1 = \cdots = \epsilon_6 = 2^{-n}$$

Proposed Specification: OMAC1

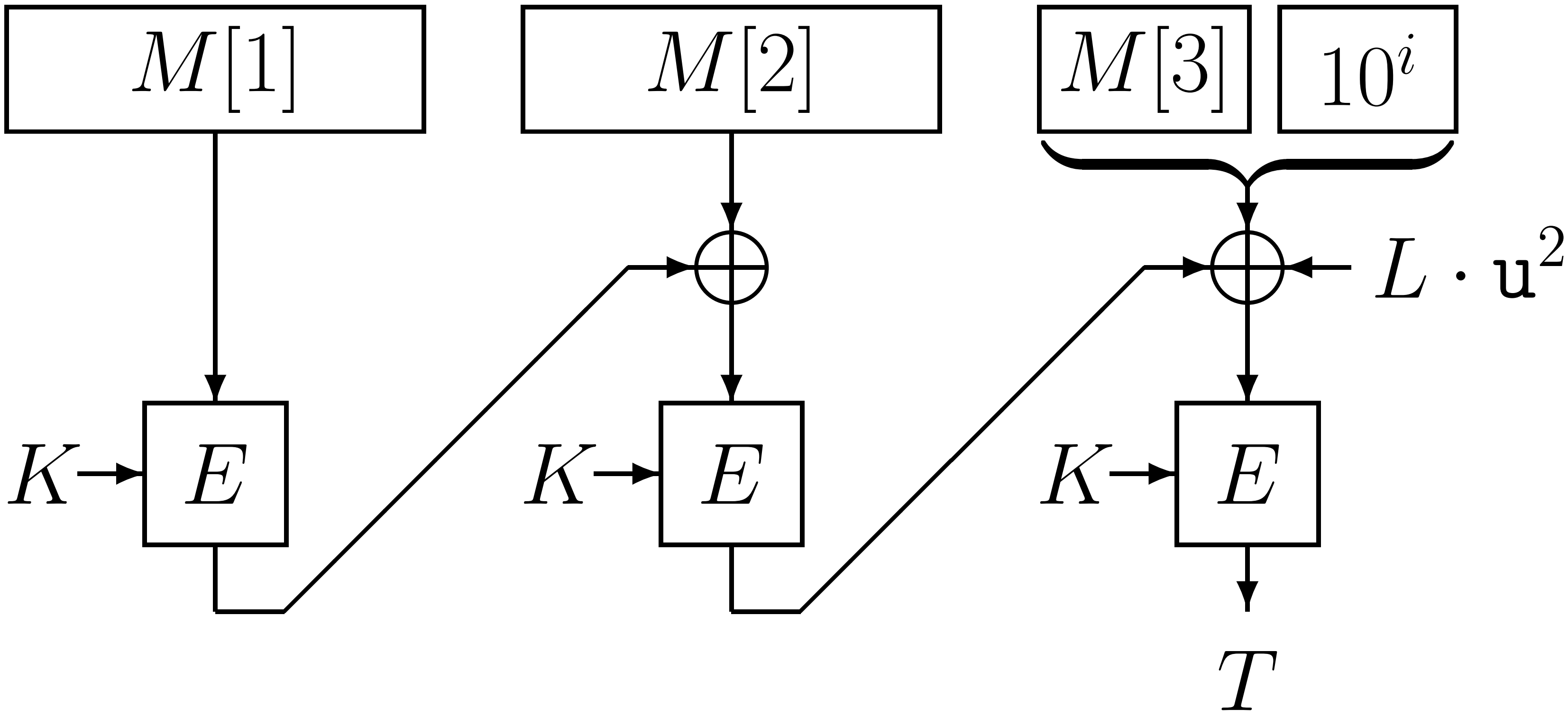
Case $|M| = mn$ $(m \geq 1)$



$$L = E_K(0^n)$$

Proposed Specification: OMAC1

Case $|M| \neq mn$



$$L = E_K(0^n)$$

$L \cdot \mathtt{u}$ and $L \cdot \mathtt{u}^2$

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

$$(n = 128)$$

$L \cdot \mathtt{u}^2 = (L \cdot \mathtt{u}) \cdot \mathtt{u}$ can be easily obtained from $L \cdot \mathtt{u}$.

Proposed Specification: OMAC2

- $\mathtt{Cst} = 0^n$,
- $H_L(x) = L \cdot x$ ("$\cdot$" over GF(2^n))
- $\mathtt{Cst}_1 = \mathtt{u}$,

——— same as OMAC1 ———

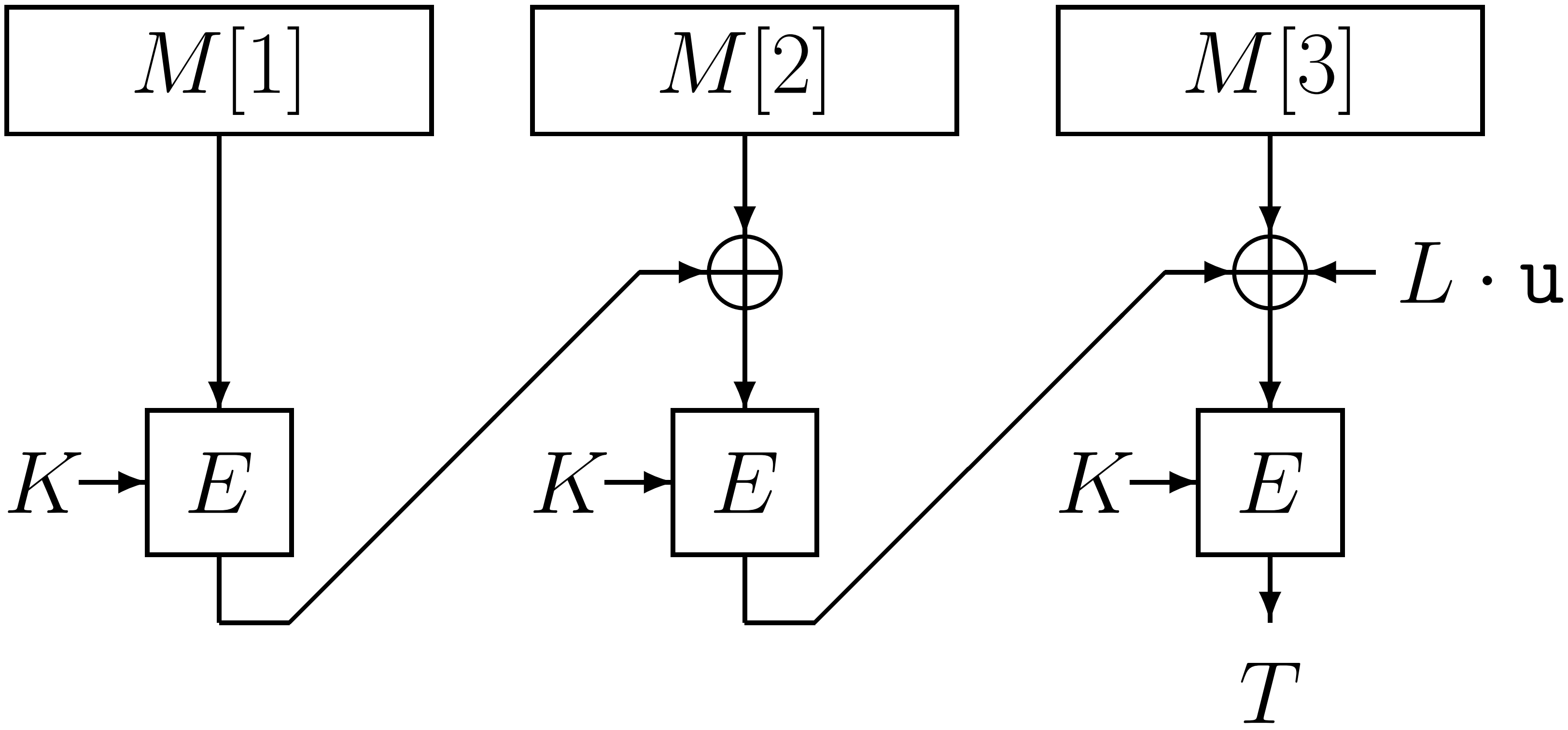
- $\mathtt{Cst}_2 = \mathtt{u}^{-1}$.

$$\Downarrow$$

$$\epsilon_1 = \cdots = \epsilon_6 = 2^{-n}$$

Proposed Specification: OMAC2

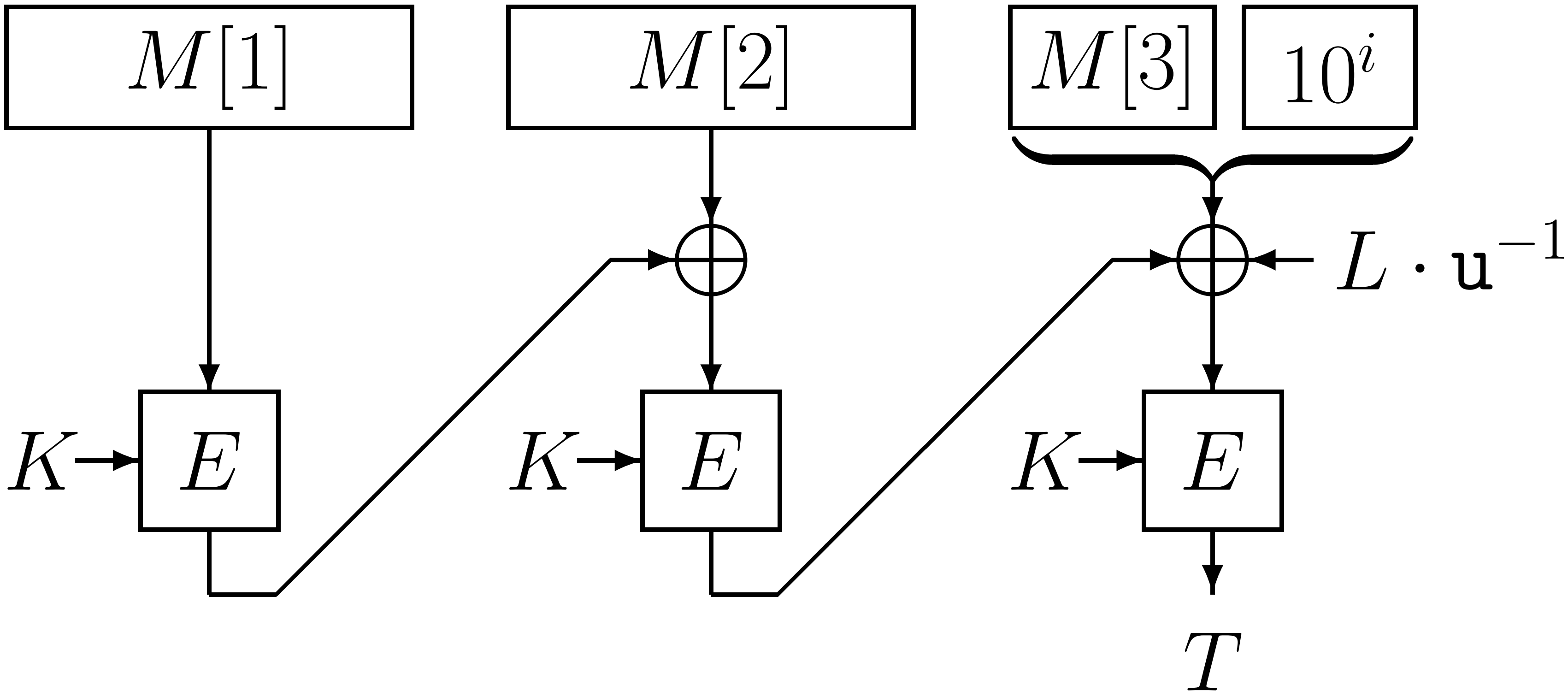
Case $|M| = mn$ $(m \geq 1)$



$$L = E_K(0^n)$$

Proposed Specification: OMAC2

Case $|M| \neq mn$



$$L = E_K(0^n)$$

$L \cdot \mathtt{u}^{-1}$

$$L \cdot \mathtt{u}^{-1} = \begin{cases} L \gg 1 & \text{if } L_0 = 0, \\ (L \gg 1) \oplus 10^{120}1000011 & \text{otherwise.} \end{cases}$$

$$(n = 128)$$

OMAC1: $L \cdot \mathtt{u}$, $L \cdot \mathtt{u}^2$

$$L \xrightarrow{\text{left shift}} L \cdot \mathtt{u} \xrightarrow{\text{left shift}} L \cdot \mathtt{u}^2$$

OMAC2: $L \cdot \mathtt{u}$, $L \cdot \mathtt{u}^{-1}$

$$\begin{array}{ccc} & \xrightarrow{\text{left shift}} & L \cdot \mathtt{u} \\ L & & \\ & \xrightarrow{\text{right shift}} & L \cdot \mathtt{u}^{-1} \end{array}$$

Efficiency Comparison

Name	K len.	$\#K$ sche.	$\#E$ invo.	$\#E$ pre.
XCBC	$k+2n$	1	$\lceil \lvert M \rvert / n \rceil$	0
TMAC	$k+n$	1	$\lceil \lvert M \rvert / n \rceil$	0
XCBC+`kst`	k	2	$\lceil \lvert M \rvert / n \rceil$	3 or 4
TMAC+`kst`	k	2	$\lceil \lvert M \rvert / n \rceil$	2 or 3
OMAC	k	1	$\lceil \lvert M \rvert / n \rceil$	1

`kst` $\cdots$ key separation technique

Conclusion

We proposed OMAC and proved its security.

Optimal key length **without** security loss

Questions?

Tetsu Iwata

iwata@cis.ibaraki.ac.jp

Kaoru Kurosawa

kurosawa@cis.ibaraki.ac.jp