Six Conditions in OMAC-family are Tight

February 24, 2003

Tetsu Iwata

Ibaraki University

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

What is OMAC-family?

- MAC (Message Authentication Code)
- Variant of CBC MAC

OMAC-family

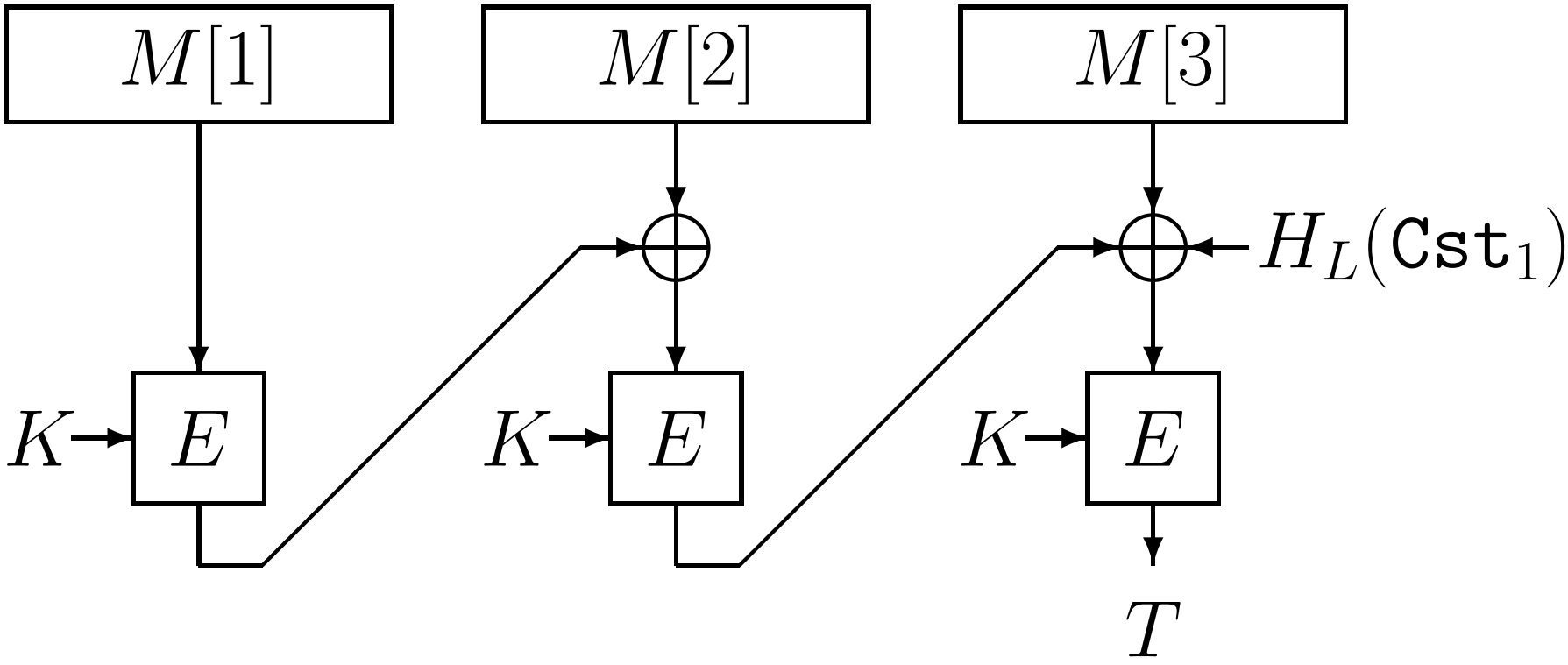
- a block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$,
- an n-bit constant $\texttt{Cst}$,
- a hash function $H : \{0,1\}^n \times X \to \{0,1\}^n$,
- two distinct constants $\texttt{Cst}_1, \texttt{Cst}_2 \in X$.

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

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

OMAC-family

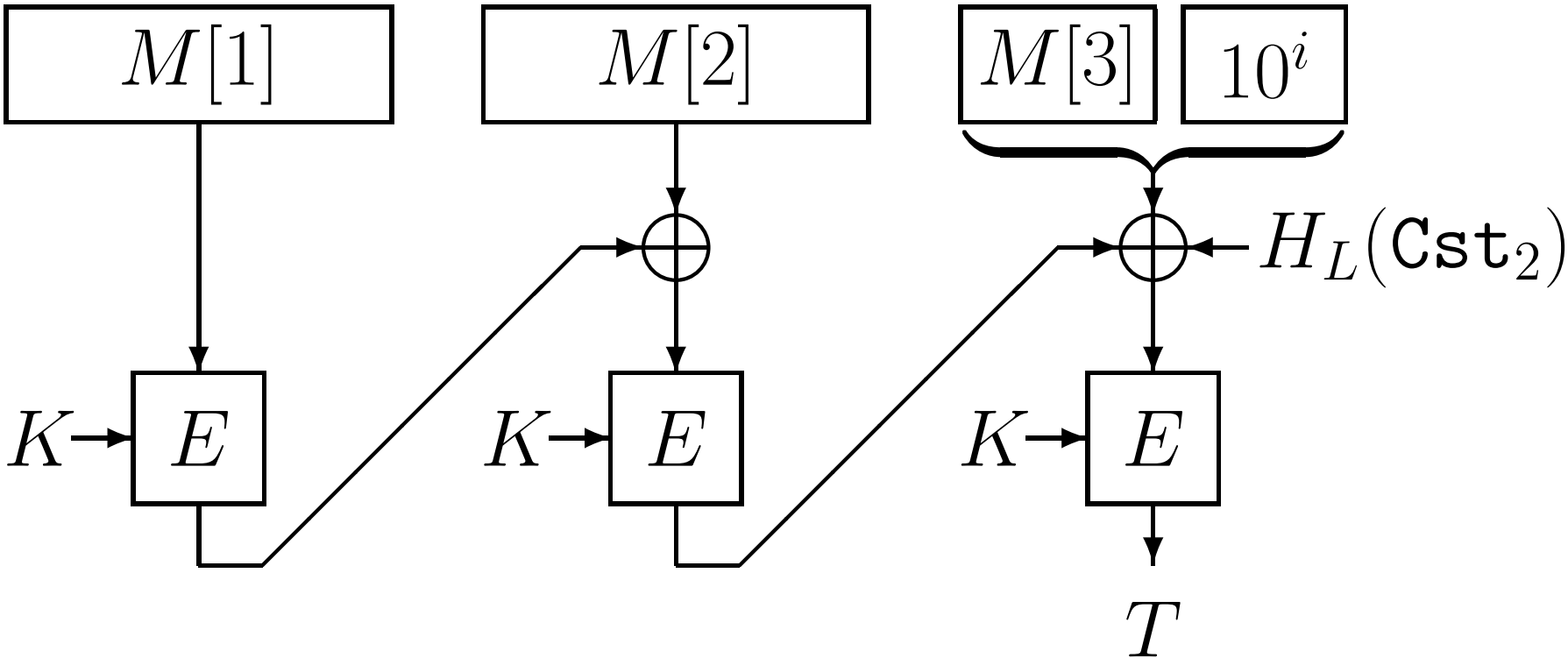
Case $|M| = mn$ $(m \geq 1)$



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

OMAC-family

Case $|M| \neq mn$



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

Six conditions are satisfied

Tomorrow $\Downarrow$ $\Uparrow$ This talk

OMAC-family is secure

$\surd\ \exists y,\ \#\{L \mid H_L(\texttt{Cst}_1) = y\} > \epsilon_1 \cdot 2^n$

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

The Attack

Algorithm $\mathcal{A}$

Step 1: $T \leftarrow \text{OMAC-family}_P(0^n)$

Step 2: Output $((y, T), T)$.

$$\Pr_P(\mathcal{A} \text{ success}) > \epsilon_1$$

Similar attack for conditions $2, \ldots, 6$.

Conclusion

Six conditions are satisfied

$$\Uparrow$$

OMAC-family is secure