SKLOIS
信息安全国家重点实验室

# Constructing Rate-1 MACs from Related-Key Unpredictable Block Ciphers: PGV Model Revisited

Liting Zhang, Wenling Wu, Peng Wang,
Lei Zhang, Shuang Wu and Bo Liang

中国科学院软件研究所
Institute of Software, Chinese Academy of Sciences

# Outline

- Background
  - MACs: definition, security and classification
  - Rate-1 MACs
  - MACs from unpredictable block ciphers
- Our Work
  - Attacks on current Rate-1 MACs
  - Assumption
  - Rate-1 MACs from PGV model
  - Relationships among them
- Summary and Future Work

# Background 1/7

Message Authentication Codes (MACs) provide

Data integrity protection,

Data origination authentication,

and are widely used (in Banking applications, Internet services, …)

A MAC algorithm includes:

1) A key generation algorithm $K \stackrel{\$}{\leftarrow} \mathrm{KG}$
2) A tag generation algorithm $T \stackrel{\$}{\leftarrow} \mathrm{TG}(K, M)$
3) A verification algorithm $d \leftarrow \mathrm{VF}(K, M, T)$

# Background 2/7

The security of a MAC algorithm $F=(\mathrm{KG},\mathrm{TG},\mathrm{VF})$ is evaluated by how unpredictable (or unforgeable) it is,

$$
\begin{array}{l}
\text{Experiment } \mathbf{Exp}_{F,\mathcal{A}}^{\mathrm{mac}} \\
K \xleftarrow{\$} \mathrm{KG}; \\
\text{while } \mathcal{A} \text{ makes a query } M \text{ to } \mathrm{TG}_K(\cdot), \text{ do} \\
\qquad \mathrm{Tag} \xleftarrow{\$} \mathrm{TG}_K(M); \text{ return Tag to } \mathcal{A}; \\
\text{if } \mathcal{A} \text{ makes a query } (M,T) \text{ to } \mathrm{VF}_K(\cdot,\cdot) \\
\quad \text{s.t. } \mathrm{VF}_K(M,T) \text{ returns } 1 \text{ and} \\
\qquad M \text{ was never queried to } \mathrm{TG}_K(\cdot); \\
\text{then return } 1 \text{ else return } 0.
\end{array}
$$

$$
\mathrm{Adv}_{F,\mathcal{A}}^{\mathrm{mac}} = \Pr[\mathbf{Exp}_{F,\mathcal{A}}^{\mathrm{mac}} = 1] \qquad \mathrm{Adv}_{F}^{\mathrm{mac}}(t,q,\mu) = \max_{\mathcal{A}}\{\mathrm{Adv}_{F,\mathcal{A}}^{\mathrm{mac}}\}
$$

# Background 3/7

## Different kinds of MACs

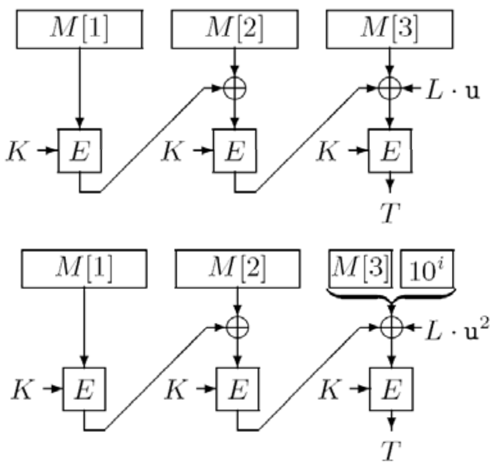
- Block-cipher-based
  OMAC, XCBC, PMAC, …
- Hash-function-based
  NMAC, HMAC, …
- Universal-hash-function-based
  UMAC, Poly1305-AES
- Dedicated MACs
  MAA, COMP-128, …

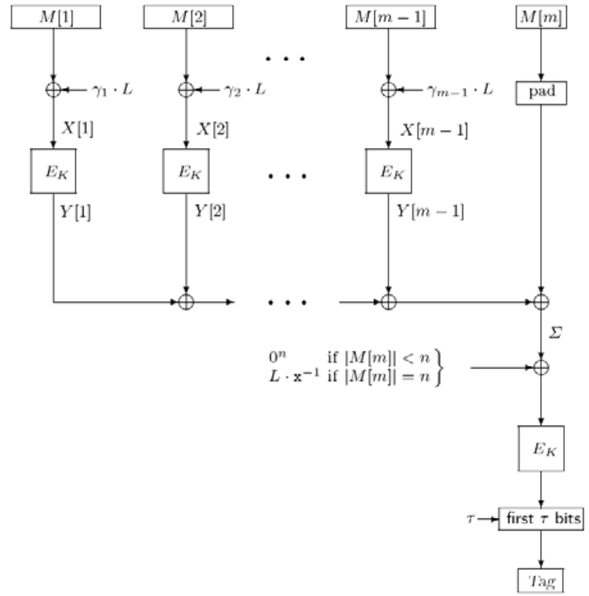
# Background 4/7

For the block-cipher-based MACs, its efficiency is mostly influenced by Rate.

$$\text{Rate} = \frac{\#\,\text{block-cipher invocations}}{\#\,\text{message blocks}}$$

Current Rate-1 MACs: OMAC, PMAC, …



# Background 5/7

For the block-cipher-based MACs, its security is mostly influenced by the security of E.

$$\mathbf{Adv}_{F[E]}^{\mathrm{prf}}(t,q,\mu) \le O(\sigma^2) \times \mathbf{Adv}_{E}^{\mathrm{prp}}(t',q',\mu')$$

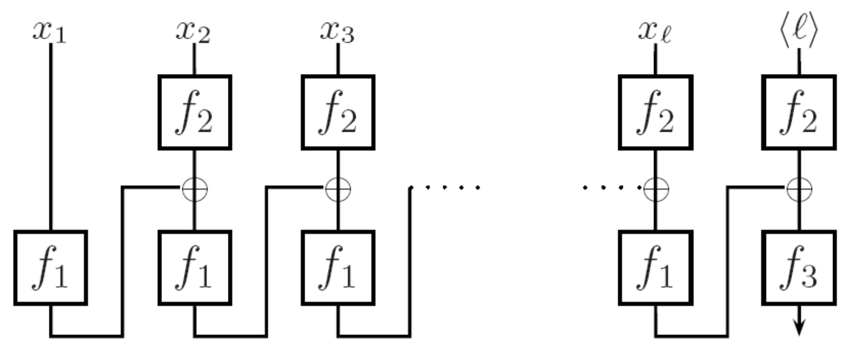
However,

A secure MAC needs only to be unpredictable (<< prf).

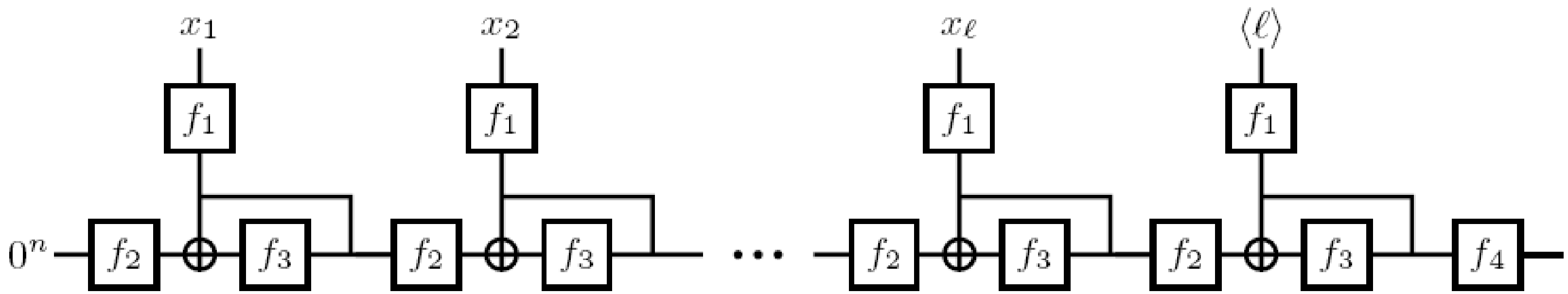
Reducing MAC security to the unpredictability of block ciphers is desirable and feasible.

Such constructions were first proposed by Dodis, et al

Enciphered CBC mode (EuroCrypt 2008)




SS-NMAC (Crypto 2009)



# Background 7/7

Summary of the current work

| Constructions | Requirements on E | Rate |
| --- | --- | --- |
| OMAC, TMAC, XCBC, PMAC, EMAC, GCBC, RAMC, f9, … | pseudorandom (prp) | 1 |
| Enciphered CBC mode | unpredictable | 2 |
| SS-NMAC | unpredictable | 3 |
| Other known MACs | prp | >1 |
| ??? | unpredictable | 1 |

# Our Work 1/12

All current rate-1 MACs may not be secure when instantiated with a related-key unpredictable block cipher E'.

$$E'(K, M) = \begin{cases} m_1||m_2||m_3||c, & \text{if } \mathrm{msb}_1(m_1) = 0, \\ m_1||c||m_3||m_4, & \text{if } \mathrm{msb}_1(m_1) = 1, \end{cases}$$

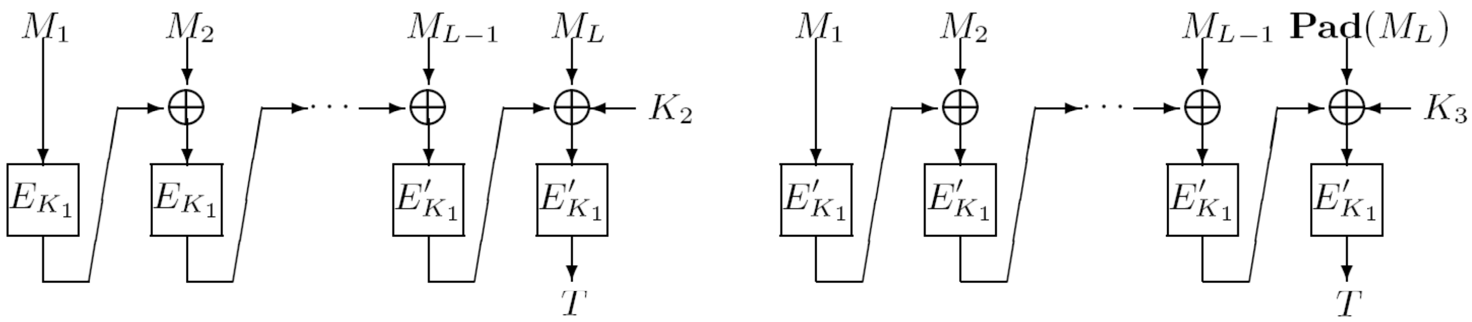
$M = m_1||m_2||m_3||m_4,\ |m_i| = n/4$ for $1 \leq i \leq 4$,

$c = \mathrm{CBC}[Q_K](m_1 m_2 m_3 m_4)$

$Q : \mathcal{K} \times \{0,1\}^{n/4} \to \{0,1\}^{n/4}$ is a block cipher with RK-PRP security.

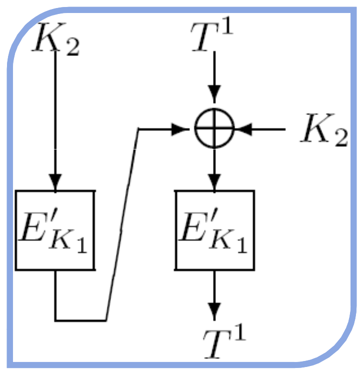
# Our Work 2/12

Example: XCBC[E'] is not secure.




1) Adversary $\mathcal{A}$ queries $\mathrm{XCBC}_{E'}(\cdot)$ with $0^n$, obtains the tag $T^1 = t_1^1 t_2^1 t_3^1 t_4^1$;
2) $\mathcal{A}$ queries $\mathrm{XCBC}_{E'}(\cdot)$ with $10^{n-1}$, obtains the tag $T^2 = t_1^2 t_2^2 t_3^2 t_4^2$;
3) $\mathcal{A}$ makes a forgery $(M', T^1)$, where

$$\begin{cases} M' = (t_1^1 t_2^1 t_3^1 t_4^2)\|T^1, & \text{if } \mathrm{msb}_1(t_1^1) = 0, \\ M' = (t_1^2 t_2^2 t_3^2 t_4^1)\|T^1, & \text{if } \mathrm{msb}_1(t_1^1) = 1. \end{cases}$$



Why are the current rate-1 MACs insecure when instantiated with E'?

The secrecy of chaining values can no longer be kept, which is fatal to their security as MACs.

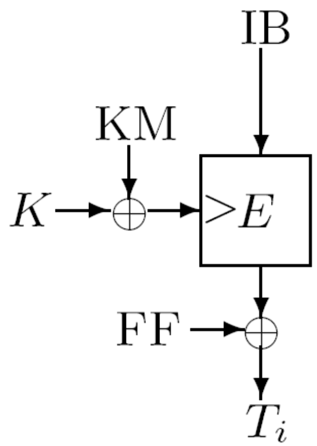
Assumption:

To study the security of MACs based on unpredictable block ciphers, assume all their chaining values are available to adversaries.

1) It explains why current rate-1 MACs are insecure when their block ciphers are only related-key unpredictable;
2) It explains why enciphered CBC and SS-NMAC are secure against Side Channel Attacks as long as their block ciphers are.

# Our Work 4/12

Under this assumption, we try to construct rate-1 MACs in keyed PGV model.




MAC $F_s(K, M)$ $\quad s = 1, 2, \cdots, 64$

$K \xleftarrow{\$} \mathcal{K}_E$;

**for** $i = 1$ **to** $l$ **do**

$\quad T_i \leftarrow f_s(K, M_i, T_{i-1})$

**return** $T_l$.

$$f(K, M_i, T_{i-1}) = E(K \oplus \mathrm{KM}, \mathrm{IB}) \oplus \mathrm{FF}$$

$K \xleftarrow{\$} \mathcal{K}_E$

IB, KM, FF$\in \{M_i, T_{i-1}, M_i \oplus T_{i-1}, \mathrm{Cst}\}$

$T_0 = \mathrm{Cst}$

# Our Work 5/12

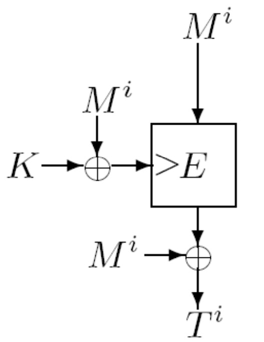
E is assumed to be unpredictable against a special kind of related-key attacks ($\Phi_K^{\oplus}$-restricted ).

Experiment $\mathbf{Exp}_{E,\mathcal{A}}^{\mathrm{rk-up}}$
$K \stackrel{\$}{\leftarrow} \mathcal{K}_E$;
while $\mathcal{A}$ makes a query $(\mathrm{KM}, M)$ to $E(K, \cdot)$, do
  $T \leftarrow E(\mathrm{KM} \oplus K, M)$; return $T$ to $\mathcal{A}$;
until $\mathcal{A}$ stops and outputs $(\mathrm{KM}', M', T')$ such that
  1) $E(\mathrm{KM}' \oplus K, M') = T'$;
  2) $(\mathrm{KM}', M')$ was never queried to $E(K, \cdot)$;
then return 1 else return 0.

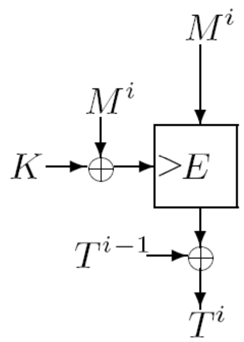
$$\begin{cases} \mathbf{Adv}_E^{\mathrm{rk-up}}(\mathcal{A}) \stackrel{\mathrm{def}}{=} \Pr[\mathbf{Exp}_{E,\mathcal{A}}^{\mathrm{rk-up}} = 1], \\ \mathbf{Adv}_E^{\mathrm{rk-up}}(t, q, \mu) \stackrel{\mathrm{def}}{=} \max_{\mathcal{A}}\{\mathbf{Adv}_E^{\mathrm{rk-up}}(\mathcal{A})\} \end{cases}$$

# Our Work 6/12

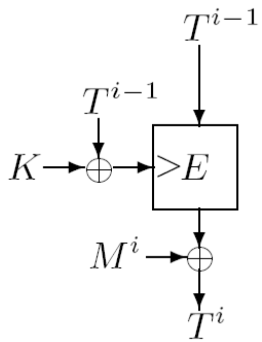
In keyed PGV model, we find some MACs are …



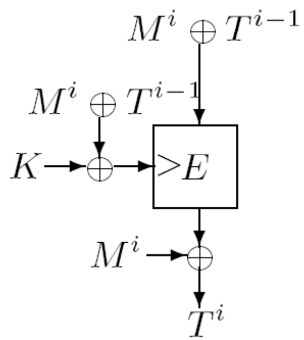

meaningless




vulnerable to fixed-M attack

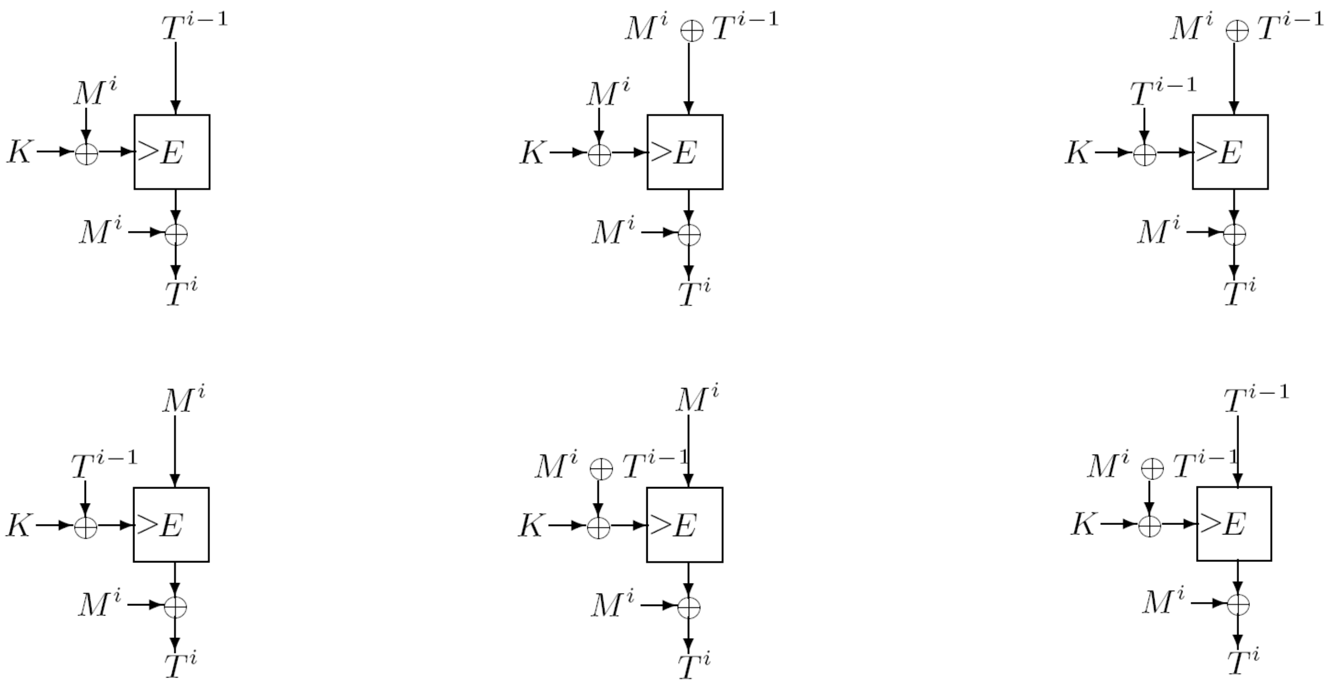



vulnerable to fixed-T attack




vulnerable to fixed-(M+T) attack

There are also some MACs secure, such like




$$\mathbf{Adv}^{\mathrm{mac}}_{F_s[E]}(t,q,\mu) \le (\sigma^2-\sigma+1)\mathbf{Adv}^{\mathrm{rk-up}}_{E}(t',q',\mu')$$

# Our Work 8/12

In total, we find in the keyed PGV model that

- \- Meaningless (15)
- 1 Vulnerable to fixed-M attack (6)
- 2 Vulnerable to fixed-T attack (6)
- 3 Vulnerable to fixed-(M+T) attack (13)

$f_i (i = 1, 2, \cdots, 24)$ can be used to construct secure MACs for prefix-free messages.

$f_i (i = 1, 2, 3, 4)$
$f_j (j = 5, 6, \cdots, 12)$
$f_k (k = 13, 14, \cdot, 20)$
can also be used to construct secure hash functions with different security levels.

| | | choice of IB | | | |
|---|---|---|---|---|---|
| choice of KM | choice of FF | $M_i$ | $T_{i-1}$ | $M_i \oplus T_{i-1}$ | Cst |
| $M_i$ | $M_i$ | – | $f_{17}$ | $f_{20}$ | – |
| | $T_{i-1}$ | 1 | $f_5$ | $f_8$ | 1 |
| | $M_i \oplus T_{i-1}$ | 1 | $f_7$ | $f_6$ | 1 |
| | Cst | – | $f_{15}$ | $f_{19}$ | – |
| $T_{i-1}$ | $M_i$ | $f_1$ | 2 | $f_4$ | 2 |
| | $T_{i-1}$ | $\boxed{f_{21}}$ | – | $\boxed{f_{24}}$ | – |
| | $M_i \oplus T_{i-1}$ | $f_3$ | 2 | $f_2$ | 2 |
| | Cst | $\boxed{f_{23}}$ | – | $\boxed{f_{22}}$ | – |
| $M_i \oplus T_{i-1}$ | $M_i$ | $f_9$ | $f_{12}$ | 3 | 3 |
| | $T_{i-1}$ | $f_{11}$ | $f_{10}$ | 3 | 3 |
| | $M_i \oplus T_{i-1}$ | $f_{14}$ | $f_{18}$ | 3 | 3 |
| | Cst | $f_{13}$ | $f_{16}$ | 3 | 3 |
| Cst | $M_i$ | – | 2 | 3 | – |
| | $T_{i-1}$ | 1 | – | 3 | – |
| | $M_i \oplus T_{i-1}$ | 1 | 2 | 3 | 3 |
| | Cst | – | – | 3 | – |

# Our Work 9/12

In total, we find in the keyed PGV model that

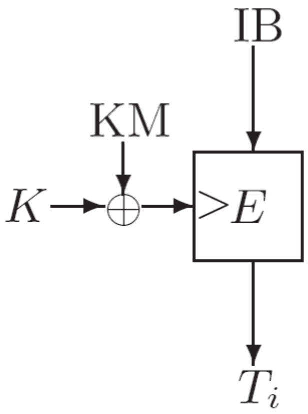
All MACs with a fixed key are unsatifying;

8 MACs may offer relatively high efficiency;

FF has no influence over the MAC security.

| choice of KM | choice of FF | choice of IB: $M_i$ | $T_{i-1}$ | $M_i \oplus T_{i-1}$ | Cst |
|---|---|---|---|---|---|
| $M_i$ | $M_i$ | – | $f_{17}$ | $f_{20}$ | – |
| $M_i$ | $T_{i-1}$ | 1 | $f_5$ | $f_8$ | 1 |
| $M_i$ | $M_i \oplus T_{i-1}$ | 1 | $f_7$ | $f_6$ | 1 |
| $M_i$ | Cst | – | $f_{15}$ | $f_{19}$ | – |
| $T_{i-1}$ | $M_i$ | $f_1$ | 2 | $f_4$ | 2 |
| $T_{i-1}$ | $T_{i-1}$ | $f_{21}$ | – | $f_{24}$ | – |
| $T_{i-1}$ | $M_i \oplus T_{i-1}$ | $f_3$ | 2 | $f_2$ | 2 |
| $T_{i-1}$ | Cst | $f_{23}$ | – | $f_{22}$ | – |
| $M_i \oplus T_{i-1}$ | $M_i$ | $f_9$ | $f_{12}$ | 3 | 3 |
| $M_i \oplus T_{i-1}$ | $T_{i-1}$ | $f_{11}$ | $f_{10}$ | 3 | 3 |
| $M_i \oplus T_{i-1}$ | $M_i \oplus T_{i-1}$ | $f_{14}$ | $f_{18}$ | 3 | 3 |
| $M_i \oplus T_{i-1}$ | Cst | $f_{13}$ | $f_{16}$ | 3 | 3 |
| Cst | $M_i$ | – | 2 | 3 | – |
| Cst | $T_{i-1}$ | 1 | – | 3 | – |
| Cst | $M_i \oplus T_{i-1}$ | 1 | 2 | 3 | 3 |
| Cst | Cst | – | – | 3 | – |

We refine the 24 secure MACs in Compact PGV model.




MAC $G_s(K, M)$
$K \xleftarrow{\$} \mathcal{K}_E$;
**for** $i = 1$ **to** $l$ **do**
    $T_i \leftarrow g_s(K, M_i, T_{i-1})$
**return** $T_l$.

$$g(K, M_i, T_{i-1}) = E(K \oplus \mathrm{KM}, \mathrm{IB})$$

$$K \xleftarrow{\$} \mathcal{K}_E$$

$$\mathrm{IB},\ \mathrm{KM} \in \{M_i, T_{i-1}, M_i \oplus T_{i-1}, \mathrm{Cst}\}$$

$$T_0 = \mathrm{Cst}$$

# Our Work 11/12

In Compact PGV model, we find

- Not meaningful (7)
3 Vulnerable to fixed-(M+T) attack (3)

| | choice of IB | | | |
|---|---|---|---|---|
| choice of KM | $M_i$ | $T_{i-1}$ | $M_i \oplus T_{i-1}$ | Cst |
| $M_i$ | – | $g_0$ | $g_5$ | – |
| $T_{i-1}$ | $g_1$ | – | $g_4$ | – |
| $M_i \oplus T_{i-1}$ | $g_2$ | $g_3$ | 3 | 3 |
| Cst | – | – | 3 | – |

$g_s(s = 0, 1. \cdots, 5)$ can be used to construct secure MACs for prefix-free messages.

Moreover, we find $g_s(s = 0, 1. \cdots, 5)$ are in fact equivalent to each other.

There exists 6 invertible 2*2 matrices over GF(2),

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, A_4 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, A_5 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, A_6 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

such that $\forall 0 \leq s1 \leq s2 \leq 5, \ \exists j \in \{1, 2 \cdots, 6\},$

$$(\mathrm{KM}_{s1}, \mathrm{IB}_{s1}) \times A_j = (\mathrm{KM}_{s2}, \mathrm{IB}_{s2})$$

# Our Work 12/12

The equivalence implies related-mode attacks on them.

-Users take the same key for $G_i, G_j, 0 \le i < j \le 5$;

-Adversaries can forge against $G_i$ after querying $G_j$.

A suggestion to break this equivalence:

For $s1 = (s2 + 3) \mod 6$, let $G_{s1}$ and $G_{s2}$ take distinct-and-fixed $T_0$.

# Summary and Future Work 1/2

- All current rate-1 MACs may not guarantee their security when instantiated with related-key unpredictable block ciphers;
- Assumption: Chaining values are available to adversaries;
  1) MACs secure under this assumption is secure against Side Channel Attacks as long as their underlying block ciphers are;
  2) The studies on MACs and hash functions are much more similar than before.

     black-box analysis → semi-white-box analysis
- In keyed PGV model, 24 rate-1 MACs are proved to be secure for prefix-free messages;
- Relationships among them are investigated.

# Summary and Future Work 2/2

Limitations:

1) rk-up ($\Phi_K^{\oplus}$-restricted) >> mac,

$$\mathbf{Adv}_{F_s[E]}^{\mathrm{mac}}(t, q, \mu) \leq (\sigma^2 - \sigma + 1)\mathbf{Adv}_E^{\mathrm{rk-up}}(t', q', \mu'),$$

2) The 24 MACs found here may not run faster than none rate-1 MACs, due to their large number of key schedules.

Question:

Is it possible to construct rate-1 MACs from only unpredictable block ciphers (not necessarily related-key secure)?

SKLOIS
信息安全国家重点实验室

# Thanks！

中国科学院软件研究所
Institute of Software, Chinese Academy of Sciences