Improved Collision Cryptanalysis of Authenticated Cipher MORUS

Tairong Shi*, Jie Guan, Junzhi Li and Pei Zhang
Information Science and Technology Institute, Zhengzhou, Henan, China
*Corresponding author

Abstract—MORUS is an authenticated stream cipher designed by Wu et al. and submitted for the third-round of the CAESAR competition. The collision properties of MORUS-640-128 are studied. We propose the necessary conditions for an internal state collision after two-step update, i.e., the Hamming weight of the input difference is at least 5 and the difference is distributed in at least three 32-bit words, which provide the theoretical support for MORUS’s resistance against collision attack.

Keywords—CAESAR; MORUS; collision cryptanalysis; partition method

I. INTRODUCTION

Authenticated encryption algorithm [1] combines encryption with authentication, providing both confidentiality and authenticity simultaneously and has been widely used in the security protocols such as SSL/TLS [2], etc. In order to accelerate the development of authentication encryption, CAESAR competition [3] merges. CAESAR is a large-scale cryptographic competition supported by the US National Institute of Standards and Technology (NIST) like AES [4], e-STREAM [5]. With the advance of the competition, authenticated cipher receives more attentions and develops rapidly. The third-round candidates own excellent performance on security and efficiency which are competitive and attract many researchers [6], [7], [8].

MORUS [9] is a notable family of authenticated stream ciphers designed by H. Wu and T. Huang, which has been selected as a third-round candidate of CAESAR competition. By adopting the idea of block cipher, MORUS uses 5 registers of equal length in its internal state and update each state successively. Three MORUS versions: MORUS-640-128, MORUS-1280-128, and MORUS-1280-256 are recommended with different internal state and key sizes. Mileva et al. [10] have proposed a distinguisher attack on MORUS in non-reuse setting. And Zhang et al. [11] researched on the confusion and diffusion properties of the initialization of MORUS. The research on MORUS is relatively limited currently.

Collision attack [12], [13] is a typical method used in attacking the message authentication. The basic technique is to inject a message difference at certain encryption (or processing the associated date) step and cancel it at a later step.

In this paper, we evaluate the security of authentication by theory deduction. Observations reveal that 32-bit word are not confused completely with internal state. Based on the feature that the 32-bit words in the state element are independent of each other, we utilize the partition method and propose the necessary conditions for an internal state collision after two-step update. There results imply that MORUS resists against collision attack in theory.

This paper is organized as follows. In Section 2, the description of MORUS is provided. In Section 3, the distribution of word difference is given. Section 4 discusses the lower bound of difference weight for collision. Section 5 concludes the paper.

II. DESCRIPTION OF MORUS

MORUS operates four phases: initialization, processing of the authenticated data, encryption, and finalization. In this paper we only focus on the processing of associated data and encryption and study the security of MORUS-640-128. MORUS takes a 128-bit key, a 128-bit nonce, and a tag length less than or equal to 128. More details of MORUS-640-128 can be found in [9]. All the “MORUS” in the rest of this paper refers to “MORUS-640-128”.

A. Notations

S’i : State at the beginning of i-th step, where i ≥ 0;
S’k : State at the beginning of k-th round at i-th step, where S’k = (S’k,0, S’k,1, S’k,2, S’k,3, S’k,4), 0 ≤ k ≤ 4;
S’k,j,i : The j-th element of the state S’k,i. S’k,j,i = (S’k,j,0, S’k,j,1, S’k,j,2, S’k,j,3, S’k,j,4), 0 ≤ j ≤ 4;
S’l,j,i : l-th 32-bit word of the S’k,j,i, where 1 ≤ l ≤ 4, 0 ≤ j ≤ 4;

& : Bit-wise AND;
<<< : Rotation to the left;
>>> : Rotation to the right;

[x] : The smallest integer not less than x;

Rotl(x,n) : Divide the 128-bit block x into four 32-bit words and rotate each word left by n bits,

Rotl+1(x,n) : Analogous to Rotl(x,n), divide the 128-bit x into four 32-bit words and rotate each word right by n bits;
B. The State Update Function of MOURS
MORUS uses five 128-bit registers in its internal state. This function consists of five rounds with similar operations that update the state $S$.

$S^{i+1} = \text{StateUpdate}(S', m_i)$ is given as follows:

Round 1:

$S_{1}^{1} = \text{Rotl}(S_{0,0}^{1} \oplus (S_{0,1}^{1} \& S_{0,3}^{1}) \oplus S_{0,2}^{1}, b_{1});$
$S_{1,2}^{1} = S_{1,2}^{1} \ll\ll w_{0};$
$S_{1,4}^{1} = S_{1,4}^{1};$
$S_{1,3}^{1} = S_{1,3}^{1};$
$S_{1,2}^{1} = S_{1,2}^{1};$
$S_{1,4}^{1} = S_{1,4}^{1};$

Round 2 to 5:

For $k=1$ to 4,

$S_{k,1}^{(k+5) \mod 5} = \text{Rotl}(S_{k,1}^{(k+5) \mod 5}, m_{k}, b_{k});$
$S_{k,2}^{(k+5) \mod 5} = S_{k,2}^{(k+5) \mod 5} \ll\ll w_{k};$
$S_{k,4}^{(k+5) \mod 5} = S_{k,4}^{(k+5) \mod 5};$
$S_{k,3}^{(k+5) \mod 5} = S_{k,3}^{(k+5) \mod 5};$
$S_{k,2}^{(k+5) \mod 5} = S_{k,2}^{(k+5) \mod 5};$

Generate $S^{i+1}$: For $k=0$ to 4: $S_{k}^{i+1} = S_{k}^{i}$.

The rotation constants $b_{1}, w_{1}, i = 0, \ldots, 4$ for each round are defined in [10].

C. Processing the Associated Data and Encryption
The processing the associated data $AD$ of MORUS can be described as follows. $adlen$ means bit length of the associated data, where $u = \lceil\text{adlen/128}\rceil$.

For $i=0$ to $u-1$: $S' = \text{StateUpdate}(S', AD)^{2b}$.

The encryption is described as follows. Let $msglen$ represents the length of plaintext and $v = \lceil\text{msglen/128}\rceil$.

For $i = 0$ to $v-1$:

$C_{i} = P \oplus S_{0,i}^{v} \oplus (S_{1,i}^{v} \ll\ll 96) \oplus (S_{2,i}^{v} \& S_{3,i}^{v});$
$S_{i}^{v+1} = \text{StateUpdate}(S_{i}^{v+1}, P);$
\( \Delta S^2_{i+1} = 00\beta 0 , \) where \( \beta = (\alpha \oplus \alpha') \ll 22 ; \)
\[ \Delta S^2_{i+1} = 0\gamma 0u , \] where \( \gamma = (\alpha \oplus \alpha') \ll 13 , u \) is unknown difference.

Because of \( \Delta S^2_{i+2} = \Delta S^2_{i} \oplus \Delta m_{i+1} \) and \( \Delta S^4_{i+2} = 0 , \) we get \( \Delta m_{i+1} = \Delta S^4_{i+1} = 0\gamma 0u . \)

Through update function, we know the presentation of \( \Delta S^4_{i+2} : \)
\[ \Delta S^4_{i+2} = \Delta S^2_{i+2} \oplus \Delta S^4_{i+1} \oplus \Delta S^2_{i+1} \oplus \Delta S^4_{i+1} \oplus \Delta S^2_{i+1} \]
\[ \oplus \Delta S^4_{i+1} \ggg 32 \]
\[ = 0u\beta 0 \oplus 0000 = 0u\beta 0 \]

To ensure \( \Delta S^2_{i+2} = 0 , \) we deduce \( \beta = 0 , \) namely \( \alpha \oplus \alpha' \ll 31 = 0 , \) then \( \alpha = 1_{22} \) must be established. Therefore we can deduce \( \alpha' = \alpha' = 1_{22} \) and \( \beta = \gamma = 0 , \) furthermore \( \Delta S^4_{i+2} = 0000 \), \( \Delta S^4_{i+2} = \Delta m_{i+1} = 000u . \)

Supposed \( \Delta S^4_{i+2} = 0 , \) we can get \( \Delta S^4_{i+2} = \Delta S^2_{i+2} \oplus \Delta S^4_{i+1} \oplus \Delta S^2_{i+1} \oplus \Delta S^4_{i+1} \oplus \Delta S^2_{i+1} \)
\[ = 0\alpha 00 \oplus 0000 \oplus 0000 = 0\alpha 0u = 0 \]

It contradicts to \( \Delta S^4_{i+2} = 0 . \) The above results also hold for \( \Delta m_i = 0\alpha 00 , \Delta m_i = 0\alpha 00 , \) and \( \Delta m_i = 0000 , \) so \( \text{WB}(\Delta m_i) \neq 1. \)

\[ \text{B. When } \text{WB}(\Delta m_i) = 2 \]

There are two cases:

Case 1 \( \Delta m_i = 0\alpha 0\gamma 0 , (\alpha' \neq 0, i = 1,2) \)
\[ \Delta S^4_{1} = \alpha' \alpha' \alpha' \alpha' 00 , \] where \( \alpha' \alpha' \alpha' \alpha' \ll 31,i = 1,2 ; \)
\[ \Delta S^4_{2} = 0\alpha 0\alpha' 00 , \] where \( \alpha' \alpha' \ll 7,i = 1,2 ; \)
\[ \Delta S^4_{3} = 0\beta \beta \beta \beta 0 , \] where \( \beta = (\alpha \oplus \alpha') \ll 22 , i = 1,2 ; \)
\[ \Delta S^4_{4} = \gamma \gamma \gamma \gamma u u u , \] \( \gamma = (\alpha \oplus \alpha') \ll 13,i = 1,2 . \) U refers to an unknown difference, \( \Delta m_{i+1} = \Delta S^4_{i+1} = \gamma \gamma \gamma \gamma u u u . \)

Now we analyze the \( \Delta S^2_{i+2} : \)
\[ \Delta S^2_{i+2} = \Delta S^4_{i+2} \oplus \Delta S^4_{i+1} \oplus \Delta S^4_{i+1} \oplus \Delta S^4_{i+1} \oplus \Delta S^4_{i+1} \]
\[ \oplus \Delta S^4_{i+1} \ggg 32 \]
\[ = u u u 0 \oplus 0000 = u u u 0 \]

To ensure \( \Delta S^4_{i+2} = 0 , \) we deduce \( \beta = 0 , \) it’s easy to get \( \alpha' = \alpha' = 1_{22} , \gamma = 0 . \) So \( \Delta S^4_{i+1} = 0\beta \beta 00 , \Delta S^4_{i+1} = \Delta m_{i+1} = \gamma \gamma \gamma \gamma u u u . \)

Supposed \( \Delta S^4_{i+2} = \Delta S^4_{i+2} = 0 , \) we can obtain
\[ \Delta S^4_{i+2} = \Delta S^4_{i+1} \oplus \Delta S^4_{i+1} \oplus \Delta S^4_{i+1} \oplus \Delta m_{i+1} \]
\[ = 0\beta \beta 00 \oplus 0000 = u \beta \beta \beta u \]

To ensure \( \Delta S^4_{i+2} = 0 , \) we deduce \( \beta = 0 , \alpha' = \alpha' = 1_{22} \) and \( \gamma = 0 . \) Therefore \( \Delta S^4_{i+1} = 0000 , \Delta S^4_{i+1} = \Delta m_{i+1} = 000u . \)

As for \( \Delta S^4_{i+2} , \) we get that
\[ \Delta S^4_{i+2} = \Delta S^4_{i+1} \oplus \Delta S^4_{i+1} \oplus \Delta S^4_{i+1} \oplus \Delta m_{i+1} \]
\[ = 0\beta \beta \beta 0 \oplus 0000 = 0\beta \beta \beta u \]

It contradicts to \( \Delta S^4_{i+2} = 0 . \) The above results also hold for \( \Delta m_i = 0\alpha 0\alpha' 0 , \Delta m_i = 0\alpha 0\alpha' 0 , \) and \( \Delta m_i = 0000 , \) so \( \text{WB}(\Delta m_i) \neq 1 . \)

Case 2 \( \Delta m_i = 0\alpha 0\gamma 0 , (\alpha' \neq 0, i = 1,2) \)
\[ \Delta S^4_{1} = \alpha' \alpha' \alpha' \alpha' 00 , \] where \( \alpha' \alpha' \alpha' \alpha' \ll 31, i = 1,2 ; \)
\[ \Delta S^4_{2} = \alpha' \alpha' \alpha' \alpha' 00 , \] where \( \alpha' \alpha' \ll 7, i = 1,2 ; \)
\[ \Delta S^4_{3} = \beta \beta \beta \beta 0 , \] where \( \beta = (\alpha \oplus \alpha') \ll 22 , i = 1,2 ; \)
\[ \Delta S^4_{4} = \gamma \gamma \gamma \gamma u u u , \gamma = (\alpha \oplus \alpha') \ll 13, i = 1,2 . \) U denotes unknown difference.

\( \Delta m_{i+1} = \Delta S^4_{i+1} = 0u0u . \)

Supposed \( \Delta S^4_{i+2} = \Delta S^4_{i+1} \oplus \Delta S^4_{i+1} \oplus \Delta m_{i+1} \)
\[ = \beta \beta \beta 0 \oplus 0000 = \beta \beta \beta u \]

To ensure \( \Delta S^4_{i+2} = 0 , \) we get \( \beta = \beta = 0 \) and \( \gamma = \gamma = 0 , \) therefore \( \Delta S^4_{i+1} = 0000 . \) Take consideration of \( \Delta S^4_{i+2} : \)
\[ \Delta S^4_{i+2} = \Delta S^4_{i+1} \oplus \Delta S^4_{i+1} \oplus \Delta S^4_{i+1} \oplus \Delta m_{i+1} = \alpha' \alpha' \alpha' \alpha' 00 \oplus 0000 \]
\[ = \alpha' \alpha' \alpha' \alpha' u u u = 0 \]

It contradicts to \( \Delta S^4_{i+2} = 0 . \) The same results also hold for \( \Delta m_i = 0\alpha 0\gamma 0 , \) so \( \text{WB}(\Delta m_i) \neq 2. \)

C. When \( \text{WB}(\Delta m_i) = 3 \)

Assume that \( \Delta m_i = (0\alpha , \alpha' , \alpha' , \alpha) (\alpha \\neq 0, i = 1,2,3) , \) we can deduce the followings.
\[ \Delta S^4_{1} = \alpha' \alpha' \alpha' \alpha' 00 , \] where \( \alpha' \alpha' \ll 31, i = 1,2,3 ; \)
\[ \Delta S^4_{2} = \alpha' \alpha' \alpha' \alpha' 00 , \] where \( \alpha' \alpha' \ll 7, i = 1,2,3 ; \)
\[ \Delta S^4_{3} = \beta \beta \beta \beta 0 , \] where \( \beta = (\alpha \oplus \alpha') \ll 22, i = 1,2,3 ; \)
\[ \Delta S^4_{4} = \gamma \gamma \gamma \gamma u u u , \gamma = (\alpha \oplus \alpha') \ll 13, i = 1,2,3 . \) U denotes unknown difference.

\( \Delta m_{i+1} = \Delta S^4_{i+1} = \gamma \gamma \gamma \gamma u u u . \)

We can obtain the internal state difference \( \Delta S^4_{i+2} \) as follows:
\( \Delta S_{i+2}^t = S_{i+1}^t \oplus \Delta S_{i+1}^t + S_i^t \oplus \Delta S_i^t + S_{i-1}^t \oplus \Delta S_{i-1}^t + S_{i-2}^t \oplus \Delta S_{i-2}^t + S_{i-3}^t \oplus \Delta S_{i-3}^t + S_{i-4}^t \oplus \Delta S_{i-4}^t \oplus \Delta S_{i-5}^t \rangle \ggg 32 = \text{\textit{iiiii}} \)

\( \Delta S_{i+1}^t = S_{i+1}^t \oplus S_i^t \oplus S_{i-1}^t \oplus S_{i-2}^t + S_{i-3}^t + \Delta S_i^t \oplus \Delta S_{i-1}^t \oplus \Delta S_{i-2}^t + \Delta S_i^t \oplus \Delta S_{i-1}^t \rangle \ggg 64 \oplus \Delta m_{i+1} = \text{\textit{iiiii}} \)

\( \Delta S_{i+2}^t = \Delta S_{i+1}^t + S_{i+1}^t \oplus \Delta S_i^t + S_{i-1}^t \oplus \Delta S_{i-1}^t + S_i^t \oplus \Delta S_{i-1}^t + \Delta S_i^t \oplus \Delta S_{i-1}^t + \Delta S_i^t \oplus \Delta S_{i-1}^t \rangle \oplus \Delta m_{i+1} = \text{\textit{iiiii}} \)

Each 128-bit element of \( \Delta S_{i+2}^t \) could be 0, therefore \( \text{WB}(\Delta m_i) = 3 \) is possible.

D. When \( \text{WB}(\Delta m_i) = 4 \)

We know \( \Delta m_i = (\alpha_i, \alpha_i, \alpha_i, \alpha_i) \) (\( \alpha_i \neq 0, i = 1, 2, 3, 4 \)). After one step update, each 32-bit word of \( \Delta S_i^t \) and \( \Delta S_{i-1}^t \) are non-zero, meanwhile, each 32-bit word of \( \Delta S_i^t \) and \( \Delta S_{i-1}^t \) is uncertain, through our analysis, each 128-bit element of \( \Delta S_{i+2}^t \) could be 0, therefore \( \text{WB}(\Delta m_i) = 4 \) is possible.

### V. CONCLUSIONS

In this work, we focus on the security of message authentication in MORUS. Through partition method, we found out the distribution of input difference is determined, namely \( \text{WB}(\Delta m_i) \geq 3 \). Finally, by experiments, we deduce the lower bound of difference is 5.

The new idea we used to find the distribution of word-oriented difference for collision is universal, which can be applied to other authenticated ciphers. Moreover, we will evaluate the ability of MORUS in resisting other attacks.

### ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (Grant No. 61572516, 61272041 and 61272488).

### REFERENCES


