Distinguishing and Forgery Attacks on Alred and Its AES-based Instance Alpha-MAC[⋆]

Zheng Yuan[1,2], Keting Jia[3], Wei Wang[3], and Xiaoyun Wang[⋆⋆2,3]

[1] Beijing Electronic Science and Technology Institute, Beijing 100070,China
[2] Center for Advanced Study, Tsinghua University, Beijing 100084, China
xiaoyunwang@mail.tsinghua.edu.cn
[3] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China

Abstract. In this paper, we present new distinguishers on MAC construction Alred and its specific instance Alpha-MAC based on AES, which is proposed by Daemen and Rijmen in 2005. For the Alred construction, we describe a general distinguishing attack which distinguishes it from a random function. Besides, the distinguisher is also applicable to the MACs based on CBC encryption mode and CFB mode. We also construct a two-round differential path for Alpha-MAC, which can be detected by our distinguisher. The complexity of the attacks is $2^{64.5}$ queries and the success rate is 0.63. If we double the number of chosen messages, the success rate can be up to 0.98. The distinguishing attacks can lead to forgery attacks with the same complexity and success rate.

Keywords: Distinguishing attack, Forgery attack, Alred construction, Alpha-MAC, AES

1 Introduction

Message Authentication Code (MAC) is a fixed length information used to ensure data integrity and authenticity, and is widely used in Internet community such as IPsec, SNMP, SSL, etc. MAC takes a secret key and a message of arbitrary length as input, and outputs a short digest. Many research groups have presented various approaches to construct MAC functions, for example, MAA [7], UMAC [3], OMAC [9], TMAC [12], XCBC [4], RMAC [10], NMAC [1], and HMAC [13], etc.

The MAC construction Alred and its instance Alpha-MAC were introduced by Daemen and Rijmen in FSE 2005 [6]. The Alred construction is an iterative MAC function using components of block ciphers. The secret key, which is used as the key of the block cipher, is applied in the initialization and the final transformation, respectively. And the internal state is changed by consecutive injections of message blocks. The Alpha-MAC is the Alred construction instantiated with AES [5]. Since the AES algorithm has been widely used in the

[⋆] This work is supported by 973 Project (No.2007CB807902).

[⋆⋆] To whom correspondence should be addressed.

real world, the Alpha-MAC can be easily implemented. Moreover, as the Alpha-MAC outperforms CBC-MAC with AES by a factor 2.5, it can achieve higher performance.

Daemen and Rijmen [6] proposed a set of security claims that the Alred construction is as strong as the underlying block cipher with respect to key recovery, and any forgery attack not involving internal collisions may be easily extended to a ciphertext guessing attack on the block cipher. Furthermore, they showed that for Alpha-MAC any colliding messages of the same size have to be at least 5 blocks long, and to construct such collisions seems intractable without any extra information except for the input-output pairs. Recently, Huang et al. [8] exploited the algebraic properties of the AES, constructed internal collisions, and found second preimages for Alpha-MAC, on the assumption that a key or an intermediate value is known. Biryukov et al. [2] proposed a side-channel collision attack on Alpha-MAC recovering its internal state, and mounted a selective forgery attack.

This paper introduces distinguishing and forgery attacks on the Alred construction and Alpha-MAC. There are two kinds of distinguishing attacks on MAC, which are the distinguisher-R and distinguisher-H attacks [11]. Distinguishing-R attack means distinguishing the MAC construction from a random function, and distinguishing-H attack identifies which cryptography primitive is embedded in the MAC construction.

Using the birthday paradox, Preneel and van Oorschot [14] introduced a general distinguishing-R attack on all iterate MACs, which detected the inner collision by appending one-block message with zero difference. Recently, new techniques to identify the underlying hash functions of MACs are presented in [16,15]. Wang et. al. [16] presented distinguishing-H attacks on HMAC/NMAC-MD5 and MD5-MAC, moreover, recovered partial key of the MD5-MAC. These motivate us to explore similar attacks on the Alred construction and Alpha-MAC.

First, we describe a distinguishing-R attack on the Alred construction with $2^{64.5}$ chosen messages, and the success probability is 0.63. By birthday paradox, we can get a specific difference in the state, which can be recognized with probability 1 by appending another message pair with the same difference. On the foundation of the distinguisher, we can forgery MACs with the same complexity and success probability. Although Preneel's attack can also be applicable to this construction, but the appended messages are the same, while in our attack, we can choose messages with difference. The distinguisher is also applicable to the MACs based on CBC and CFB encryption mode for block cipher. Combining the structural features of the Alpha-MAC with the algebraic properties of AES, a two-round differential path is constructed. Based on this, we propose a distinguishing-H attack on Alpha-MAC with $2^{64.5}$ choose messages and $2^{64.5}$ queries. The success rate of the attacks is 0.63, which can be improved by increasing the number of chosen messages. Besides, the above forgery attack is still feasible.

The paper is organized as follows. In section 2, we list the notations used in this paper and give a short description of the Alred construction and Alpha-MAC. Section 3 shows our new distinguishing attack and forgery attack on the Alred construction. The distinguishing and forgery attack on AES-based Alpha-MAC is introduced in the section 4. Finally, We conclude the paper in Section 5.

2 Backgrounds and Notations

In this section, we define the notations, and give a brief description of the Alred construction and Alpha-MAC.

2.1 Notation

f	:	the iteration function
x_i	:	the message word
y_i	:	the state after iteration i
k	:	the secret key
C	:	the output of MAC taking secret key K and message M as input
ΔA	:	the XOR difference of A and A'
n	:	the length of the state
l_w	:	the length of the message word
l_m	:	the length of the MAC output
$M\|N$	:	the concatenation of M and N

2.2 The Alred Construction

The MAC construction Alred [6] bases on an iterated block cipher. The length of the secret key equals to that of the underlying block cipher, and the message length is a multiple of l_w bits.

Denote the i-th message word as x_i, and the state after iteration i as y_i. For message $M = (x_1, x_2, \cdots, x_t)$, the construction is as follows.

1. Apply the block cipher to the state of all-zero block, i. e.,

$$y_0 = \mathrm{Enc}_k(0).$$

2. Perform an iteration for each message word. First, map the message word to an *injection input* which is used as a sequence of r round keys, then apply a sequence of r block cipher round functions to the state. For t message words,

$$y_i = f(y_{i-1}, x_i), i = 1, 2, \cdots, t.$$

3. Apply the block cipher to the state again, and truncate the first l_m bits of the state as the output. The final output C is

$$C = Trunc(\mathrm{Enc}_k(y_t)).$$

2.3 A Brief Description of Alpha-MAC

Alpha-MAC [6] is a specific instance of the Alred construction with AES as the underlying block cipher, where $l_w = 32$ and $r = 1$. Similar with AES, the Alpha-MAC supports key length of 128, 192 and 256 bits. The Alpha-MAC function is depicted in Figure 1.

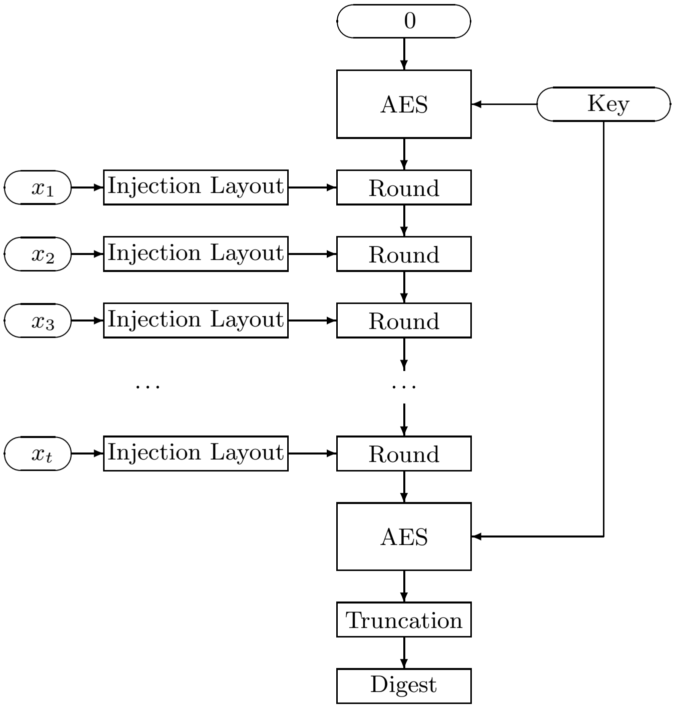

Fig. 1. The Construction of Alpha-MAC

The message padding method appends a single 1 followed by the minimum number of 0 bits such that the length of the result is a multiple of 32. For AES-128, the injection layout places the 4 bytes of each message word $x_i = (x_{i,0}, x_{i,1}, x_{i,2}, x_{i,3})$ into a 4×4 array with the form:

$$\begin{pmatrix} x_{i,0} & 0 & x_{i,1} & 0 \\ 0 & 0 & 0 & 0 \\ x_{i,2} & 0 & x_{i,3} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

which acts as the corresponding 128-bit round key. The Alpha-MAC round function consists of the four basic transformations of AES in the following order:

- AddRoundKey (AK): add the injection input to the state by XOR operation.

– SubBytes (SB): operate a non-linear byte substitution on each byte of the state independently using an 8×8 S-box.
– ShiftRows (SR): cyclically shift left the bytes in the last three rows of the state with different number of bytes, 1 for the second, 2 for the third and 3 for the fourth row.
– MixColumns (MC): multiply each column of the state with a matrix.

In this paper, we assume there is no truncation on the final output, i. e., $l_m = 128$.

2.4 The Outline of the Related Works

We recall the general distinguishing-R attack on all iterated MACs proposed by Preneel and van Oorschot [14], and the distinguishing-H attack on HMAC/NMAC-MD5 and MD5-MAC introduced by Wang et al. [16]. These attacks motivate us to explore the similar attacks on MACs based on block cipher.

Preneel et al. proposed a general forgery attack on MAC by birthday paradox, which is applicable to all deterministic iterated MACs, including MAA and CBC-MAC. They detected all the colliding pairs among $2^{(n+1)/2}$ known text-MAC pairs by birthday attack [17], where n is the bit length of the chaining variable. For each searched collisions, i. e., $MAC(k, M) = MAC(k, M')$, they appended one-block message N to identify whether it is an inner collision, according to the equation $MAC(k, M||N) = MAC(k, M'||N)$ holds or not. Once an inner collision is recognized, they can query the MAC with $M\|N'$, then they carried out a forgery, i. e., a new message $M'\|N'$ with a valid MAC. But the method can't distinguish the cryptographic primitives embedded in the MAC.

Wang et al. [16] introduced another interesting idea which can distinguish HMAC/NMAC-MD5 without the related-key setting and implement partial key recovery attack on MD5-MAC. The main idea of the distinguishing attack is: Firstly, they collect enough two-block message pairs $(M\|N, M'\|N)$ to guarantee the appearance of an expected inner near-collision in the first iteration. Then detect such a near-collision by changing the second block with another message N'. Once the expected inner near-collision is identified, the MAC is based on MD5.

3 Distinguishing and Forgery Attack on MAC Construction Alred

In this section, we present distinguishing and forgery attack on Alred construction. Enlightened by Wang et al.'s idea, we can get proper output difference as an inner near-collision by the birthday paradox, which can be detected with probability 1 by substituting the last different message pair with another message pair with the same difference.

3.1 Distinguishing Attack on Alred Construction

The iteration part of Alred construction bases on the round function of block cipher, taking the output of injection layout as the round key of block cipher and the state as the plaintext. The round function of block cipher usually combines the subkey with the plaintext by using XOR or modular addition operation, so the difference of states can be offset, if we choose messages smartly, which is the foundation of our attack. The details of the distinguisher are described in the following.

1. Randomly choose a structure $S = \{M^i | M^i = (x_1^i, x_2^i, \cdots, x_t^i)\}$ composed of $2^{(n+1)/2}$ different messages, and query the corresponding MAC value C^i.
2. By birthday paradox, a collision can be obtained, i. e., $C^a = C^b$.
3. Suppose x_j is the last unequal word in M^a and M^b, that is $M^a = (x_1^a, \cdots, x_j^a, x_{j+1}, \cdots, x_t)\}$, $M^b = (x_1^b, \cdots, x_j^b, , x_{j+1}, \cdots, x_t)\}$. We replace x_j^a, x_j^b with different $\overline{x_j^a}$ and $\overline{x_j^b}$, respectively, where $\overline{x_j^a} \oplus \overline{x_j^b} = x_j^a \oplus x_j^b$. Query the MACs with $(\overline{M^a}, \overline{M^b})$, where $\overline{M^a} = \{x_1^a, \cdots, x_{j-1}^a, \overline{x_j^a}\}$ and $\overline{M^b} = \{x_1^b, \cdots, x_{j-1}^b, \overline{x_j^b}\}$.
   - If $\overline{C^a} = \overline{C^b}$, we conclude that the MAC is Alred construction.
   - Else, it is a random function.

Note that t should be large enough to guarantee there is an inner near-collision at round $j-1, j \leq t$.

This attack requires about $2^{(n+1)/2}$ chosen messages and works with a probability of 0.63 by the birthday paradox. If we double the number of chosen text-MAC pairs, the success rate can be increased to 0.98.

Remark. With regard to MACs based on CBC encryption mode for block ciphers, e.g. CBC-MAC, OMAC, TMAC, etc., the iteration of MAC is defined as follows:

$$H_i = f(H_{i-1}, x_i) = E_k(H_{i-1} \oplus x_i).$$

The above attack can be applied similarly. Besides, the method also works for the MACs based on CFB mode, i. e.,

$$H_i = f(H_{i-1}, x_i) = E_k(H_{i-1}) \oplus x_i.$$

3.2 Forgery Attack on Alred Construction

The core of the above distinguisher is to detect the output difference of round $j-1$. Once the difference is identified, we can append message words with the same difference to extinguish it, and achieve a collision pair. Hence, we can construct a forgery attack easily with the same complexity and success rate as the distinguishing attack. The details are as follows:

Suppose (M^a, M^b) is the colliding pair detected in the above distinguishing attack. We can query the MAC oracle about $\widetilde{M^a}$, where $\widetilde{M^a} = (x_1^a, \cdots, x_{j-1}^a, \widetilde{x_j^a}, s)$, and s is an arbitrary message string. Then we construct the forgery of $\widetilde{M^b} = (x_1^b, \cdots, x_{j-1}^b, \widetilde{x_j^a} \oplus \Delta x_j, s)$.

4 The Distinguishing and Forgery Attack on Alpha-MAC

The adversary can obtain some information of the MAC construction in the above attack. Moreover, we introduce such a distinguishing attack that can recognize the Alpha-MAC from Alred based on a random function in this section. Some properties of the AES round function is described first, then a distinguishing-H and forgery attack is presented.

4.1 Two-Round Differential Path of Alpha-MAC

We summarize some useful properties of the underlying block cipher AES, and construct a two-round differential path of Alpha-MAC.

The differential path of AES is related to the distribution of *active bytes* in a round, where the difference of two states are nonzero. It's obvious that the steps SB and AK have no impact on the *active bytes*. The expansion of the *active bytes* is effected by the transformations SR and MC, where MC effects the number of *active bytes* in the state essentially. The MC transformation is a reversible linear transformation in Galois Field F_{2^8}, and has the following property.

Property 1. MixColumn has a *branch number* equal to 5 [5].

The *branch number* of a linear transformation L is $\min_{a \neq 0}(W(a)+W(L(a)))$, where $W(a)$ is the number of active bytes of a, and $W(L(a))$ is the number of active bytes after the linear transformation is applied to a. The property implies that sum of the active bytes in each column before and after MC transformation is lower bounded by 5.

Property 2. When the input difference of MC have 4 active bytes, i. e., $\{*, *, *, *\}$, the probability that its output difference has the form $\{*, 0, 0, 0\}$ is 2^{-24}, where $*$ denotes active bytes, and 0 denotes zero difference.

In Alpha-MAC, the i-th round function has two inputs, one is the state y_{i-1}, and another is the output of the injection layout which can be controlled by the message word x_i. According to the birthday paradox, there exists the state difference

$$\Delta y_{i-1} = \begin{pmatrix} * & 0 & 0 & 0 \\ 0 & * & 0 & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \end{pmatrix}.$$

Given such a starting point, a two-round collision differential path with probability 2^{-32} can be constructed as follows.

1. Choose a pair x_i, x_i' with difference $\Delta x_i = \{\alpha, 0, 0, 0\}$, where $\alpha \neq 0$, as the input messages of the i-th round.
2. After the round function, the state difference will have only one nonzero byte β with probability 2^{-24}. Because the AK and SB have no effect on the active bytes, the four active bytes in y_i changes into one column after SR, so that the probability is 2^{-24} according to Property 2.

3. Select a pair of (x_{i+1}, x'_{i+1}) with one byte nonzero difference γ. If $\gamma = \beta$, we obtain a collision. As the value of β is unknown, the probability of the collision is $(2^8 - 1)^{-1} = 255^{-1}$.

We depict the differential path in Fig. 2. The shaded boxes refer to the active bytes, while the white boxes denote the passive bytes with zero difference in the pair. We explore the mathematical property of the differential path, which is the basis for our distinguishing attack in the next.

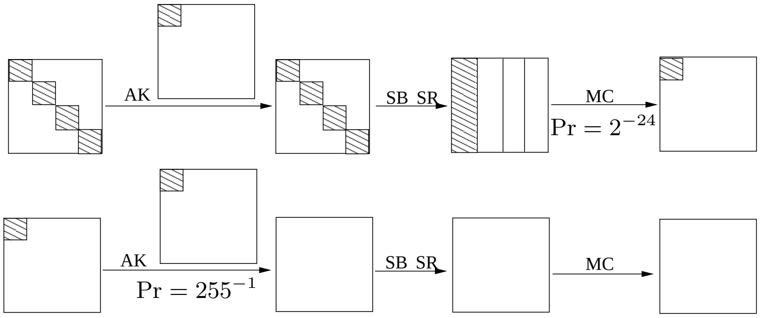

Fig. 2. Two-Round Differential Path

Property 3. Suppose (y_{i-1}, x_i, x_{i+1}) and $(y'_{i-1}, x'_i, x'_{i+1})$ follow such a differential path, replace the pair $(x_{i,0}, x'_{i,0})$ with $(\overline{x_{i,0}}, \overline{x_{i,0}} \oplus \delta)$, where $\delta \neq \alpha$ and the byte $\overline{x_{i,0}}$ traverses 256 values, then there exists a collision among the 256 values of $(\overline{y_{i+1}}, \overline{y'_{i+1}})$.

Proof. If (y_{i-1}, x_i, x_{i+1}) and $(y'_{i-1}, x'_i, x'_{i+1})$ follow such a differential path, there is one nonzero byte $\Delta x_{i+1,0}$ in the difference of x_{i+1}, so that the state difference before the MC transformation of round i is fixed, thus, the output difference of the $SB(y_{i-1,0} \oplus x_{i,0})$ is fixed, which is denoted as ϵ. According to the difference distribution of S-box in AES, for $\delta \neq \alpha$, we can get another input pair $(y_{i-1,0} \oplus \overline{x_{i,0}}, y'_{i-1,0} \oplus \overline{x_{i,0}} \oplus \delta)$, which leads to ϵ when $\overline{x_{i,0}}$ traverses 256 values.

4.2 Distinguishing Attack on Alpha-MAC

Inspired by the above two-round differential of Alpha-MAC and Property 3, the distinguishing attack on Alpha-MAC can be constructed naturally. We call the input difference of the two-round differential as the starting point. Combining with the idea of Wang et al.'s work, we can ensure the existence of the starting point by birthday attack, and identify the two-round differential through appending two message words with difference.

Reference [6] claims that an extinguishing differential in Alpha-MAC spans at least 5 message words. Hence, we choose a structure composed of $2^{64.5}$ messages with 5-word length. The first three words are used to guarantee the presence of the starting point, and the last two are used to detect the specific differential of Alpha-MAC. It is noted that for Alpha-MAC, only four bytes can be different in each message word. Thus, the structure is constructed as follows:

$$S = \{M^i \| M^i = (x_1^i, x_2^i, x_3^i, x_4^i, x_5^i)\},$$

where $(x_1^i, x_2^i, x_3^i, x_4^i, x_{5,0}^i)$ are randomly chosen, the rest bytes of x_5^i are fixed. The distinguisher works in the following manner:

1. Query the MAC with all the $2^{64.5}$ different messages in the structure S, and obtain the corresponding MAC values C^i.
2. According to the birthday paradox, a collision can be obtained among the $2^{64.5}$ C^i in step 1, i. e., $C^a = C^b$. Suppose corresponding messages are M^a and M^b, and denote the word difference of (x_4^a, x_4^b) and (x_5^a, x_5^b) as Δx_4 and Δx_5, respectively.
   - If $\Delta x_5 = 0$, conclude that the underlying function is a random function, because the collision path of Alpha-MAC spans at least 5 message words.
   - Else, randomly choose another pair of $(\overline{M^a}, \overline{M^b})$, where

     $$\overline{M^a} = (x_1^a, x_2^a, x_3^a, x_4^a, \overline{x_5^a}),\ \overline{M^b} = (x_1^b, x_2^b, x_3^b, x_4^b, \overline{x_5^b}),\ \Delta\overline{x_5} = \Delta x_5.$$

     Query the MAC with the new message pair $(\overline{M^a}, \overline{M^b})$.
     If they still collide, the MAC algorithm is Alred construction MAC, and goto step 3. Otherwise, we conclude that the MAC is a random function.
3. Let $\alpha \neq x_{4,0}^a \oplus x_{4,0}^b$, replace the pair $(x_{4,0}^a, x_{4,0}^b)$ with $(\overline{x_{4,0}}, \overline{x_{4,0}} \oplus \alpha)$, where the byte $\overline{x_{4,0}}$ traverses 256 values, and query their MAC values, respectively.
   - Examine whether there is at least one MAC pair colliding in the 256 values. If a collision appears, the Alred construction is concluded as a Alpha-MAC. Otherwise, the Alred construction is based on a random function.

Complexity Analysis. The probability that there is a collision among the $2^{64.5}$ messages is 0.63 according to the birthday paradox, so the complexity is $2^{64.5}$ queries and $2^{64.5}$ chosen messages in step 1. There is only 2 queries in the step 2. Step 3 needs 256 queries. So the total complexity is dominated by step 1, which is about $2^{64.5}$ queries.

Success Rate. Once the collision pair is found, the conclusion of the attack is correct according to the property of Alpha-MAC. Therefore, the success rate is 0.63. We can improve the success rate to 0.98 by doubling the size of the structure.

Remark: In fact, there can be no restriction on x_5 when construct the structure S, and the form of $(\overline{x_4^a}, \overline{x_4^b})$ in step 3 is various, according to the difference of Δx_5. For example, when the colliding pair satisfies that $x^a_{5,0} \oplus x^b_{5,0} \neq 0$, $x^a_{5,2} \oplus x^b_{5,2} \neq 0$, and $x^a_{4,1} \oplus x^b_{4,1} \neq 0$, we can replace $(x^a_{4,1}, x^b_{4,1})$ with $(\overline{x^a_{4,1}}, \overline{x^b_{4,1}})$, where $\overline{x^a_{4,1}} \oplus \overline{x^b_{4,1}} = x^a_{4,1} \oplus x^b_{4,1}$. If they still collide, we take it as a Alpha-MAC. Else, it is based on a random function.

4.3 Forgery Attack on Alpha-MAC

Similar with the forgery attack on the Alred Construction, we can construct a forgery attack on Alpha-MAC easily with the same complexity and success rate as the distinguishing attack, once we identify the internal collision caused by the differential path.

Suppose (M^a, M^b) is a colliding pair, we can query the MAC oracle with $\widetilde{M^a}$, where $\widetilde{M^a} = (x^a_1, \cdots, x^a_4, \widetilde{x^a_5}, s)$, and s is arbitrary message words string. Then we achieve a valid MAC value of $\widetilde{M^b} = (x^b_1, \cdots, x^b_4, \widetilde{x^a_5} \oplus \Delta x_5, s)$.

5 Conclusions

A distinguishing-R attack on the Alred construction is introduced in this paper on the illumination of Wang et al's idea [16]. There exists an expected difference in the state, which can be obtained by birthday attack. Once a collision has been detected, then the difference can be recognized with probability 1 by appending the different message pair with the same difference. The attack complexity is $2^{64.5}$ chosen messages and $2^{64.5}$ queries, and the success probability is 0.63. If we double the chosen messages, the success rate is up to 0.98. At the same time, we can forgery many MACs with the same complexity and successful probability on the basis of the distinguisher, as long as the chosen message difference is equivalent to the state difference, which has been confirmed at the distinguishing attack. Then, combining the structural features of the Alpha-MAC with the algebraic properties of AES, we construct a two-round differential path, and propose a distinguishing-H attack on Alpha-MAC with $2^{64.5}$ choose messages and $2^{64.5}$ MAC queries. The success rate of the attacks is 0.63, which can be improved by increasing the number of chosen messages as above. Both distinguishing attack can lead to forgery attack, where the appended messages may have difference.

References

1. M. Bellare, R. Canetti, H. Krawczyk, Keying Hash Functions for Message Authentication, CRYPTO 1996, LNCS 1109, pp. 1-15, 1996.
2. A. Biryukov, A. Bogdanov, D. Khovratovich, T. Kasper, Collision Attacks on AES-Based MAC: Alpha-MAC, CHES 2007, LNCS 4727, pp. 166-180, 2007.
3. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, P. Rogaway, UMAC: Fast and Secure Message Authentication, CRYPTO 1999, LNCS 1666, pp. 216-233, 1999.
4. J. Black, P. Rogaway, CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions, CRYPTO 2000, LNCS 1880, pp. 197-215, 2000.

5. J. Daemen, V. Rijmen, AES Proposal : Rijndae. The First Advanced Encryption Standard Candidate Conference. NIST AES Proposal, 1998.
6. J.Daemen, V. Rijmen, A New MAC Construction Alred and A Specific Instance Alpha-MAC. FSE 2005, LNCS 3557, pp. 1-17, 2005.
7. D. W. Davies, A Message Authenticator Algorithm Suitable for A Mainframe Computer. CRYPTO 1984, LNCS 196, pp. 393-400, 1985.
8. J. Huang, J. Seberry, W. Susilo, On the Internal Structure of Alpha-MAC. VIETCRYPT 2006, LNCS 4341, pp. 271-285, 2006.
9. T. Iwata, K. Kurosawa, OMAC: One-Key CBC MAC, FSE 2003, LNCS 2887, pp. 129-153, 2003.
10. E. Jaulmes, A. Joux, F. Valette, On the Security of Randomized CBC-MAC beyond the Birthday Paradox Limit: A New Construction, FSE 2002, LNCS 2365, pp. 237-251, 2002.
11. J. Kim, A. Biryukov, B. Preneel, S. Hong, On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0, and SHA-1. SCN 2006, LNCS 4116, pp. 242-256, 2006.
12. K. Kurosawa, T. Iwata, TMAC: Two-Key CBC MAC, CT-RSA 2003, LNCS 2612, pp. 265-273, 2003.
13. NIST, FIPS 198, The Keyed-Hash Message Authentication Code (HMAC), 2002.
14. B. Preneel, P. Oorschot, MDx-MAC and Building Fast MACs from Hash Functions. CRYPTO 1995, LNCS 963, pp. 1-14, 1995.
15. X. Wang, W. Wang, K. Jia, M. Wang, New Distinguishing Attack on MAC using Secret-Prefix Method. Submitted to FSE 2009.
16. X. Wang, H. Yu, W. Wang, H. Zhang, T. Zhan, Cryptanalysis on HMAC/NMAC-MD5 and MD5-MAC. Submitted to EUROCRYPT 2009.
17. G. Yuval, How to Swindle Rabin. *Cryptologia*, vol. 3, pp. 187-189, 1979.