IET Information Security

Research Article

IET Journals
The Institution of Engineering and Technology

Impossible differential cryptanalysis of MARS-like structures

ISSN 1751-8709
Received on 18th April 2014
Accepted on 24th October 2014
doi: 10.1049/iet-ifs.2014.0183
www.ietdl.org

Weijia Xue, Xuejia Lai ✉

Department of Computer Science and Engineering, Institute of Cryptology and Information Security, Shanghai Jiao Tong University, Shanghai 200240, People's Republic of China
✉ *E-mail: laix@sjtu.edu.cn*

Abstract: The MARS-like structure is a generalised Feistel structure. Unified impossible differential (UID) method is an effective method to discover impossible differential characteristics for block cipher structures. In this study, for a specific kind of MARS-like structure, the authors use UID to show that when n, the number of subblocks, is even, there always exist $3n-1$ rounds impossible differentials. Moreover, the authors prove that when n is odd, the MARS-like structure has impossible differentials for any number of rounds, which is a clear but interesting result.

1 Introduction

Impossible differential cryptanalysis was independently proposed by Biham *et al.* [1] and Knudsen [2]. It has been used to attack many block ciphers [3–5]. This cryptanalysis uses impossible differentials to discard the wrong keys and then process to find the right ones. Impossible differentials are one of the crucial tools to measure the resistance of the underlying block ciphers. When using this cryptanalysis strategy, the key step is to find the longest impossible differential.

Unified impossible differential (UID) method [6] is an improved method based on the previous U-method [7]. Both are used to find impossible differentials for block cipher structures. UID does not require the 1-Property for the encryption (decryption) characteristic matrix and can find more kinds of inconsistencies by improving the intermediate difference state expression. In the problem of automatically retrieving the impossible differentials of block ciphers using a Feistel structure [6] or an SPN structure [8], UID often reaches results at least as good as other techniques.

MARS [9] is one of the five finalists for AES. It is a kind of generalised Feistel structure designed to take advantage of the powerful operations supported in modern computers, resulting in a much improved security/performance trade-off over existing ciphers [9]. The MARS-like structure is defined in [10], and features more subblocks (branches) than the traditional MARS, which has only four.

Many works strive at discovering impossible differentials for MARS or MARS-like structures. An 11-round impossible differential chain of MARS-like structure is exhibited in [6] (mentioned as Gen-MARS there) using the UID method. In [11], using the matrix method, $2n-1$ rounds impossible differentials are found for an n subblocks MARS-like structure. The results in [12] provide $2n$ rounds impossible differentials for the MARS-like structure, while they do not require the round function to be bijective, which is to be contrasted with [6, 11]. We point out that the number of rounds, $2n+3$ for the MARS-like structure in Table 1 of [12] is not correct, although, when n is 4, $2n+3$ is 11, actually $3n-1$ is also 11 when n is 4, as described in [6]. In addition, Luo *et al.*, [6] only gave 11 when n is 4, not $2n+3$. Table 1 summarises the results. Some differential-based works on reduced versions of MARS, such as amplified boomerang attacks, differential attacks and differential meet-in-the-middle attacks, can be found in [13–17].

In this paper, we use the UID method to find impossible differentials for a specific kind of MARS-like structures. The number of rounds we worked out is $3n-1$ for even subblocks. Furthermore the case when n is odd, the structure has impossible differentials for any number of rounds.

The rest of this paper is organised as follows: Section 2 introduces some preliminaries. Section 3 focuses on finding impossible differentials for MARS-like structures. Section 4 concludes this paper.

2 Preliminaries

In this section, we introduce the MARS-like structure, the UID identity and how to find contradictions.

2.1 MARS-like structure

A MARS-like structure [10] with n subblocks is composed of r rounds, while the round function of every round is defined as follows:

Let $(X_1, X_2, \ldots, X_n)$ be the input of the round function, $(Y_1, Y_2, \ldots, Y_n)$ and k be the output and the round key

$$\begin{cases} Y_i = F_i(k, X_1) \oplus X_{i+1} \\ Y_n = X_1 \end{cases} \quad (1)$$

where $1 \le i \le n-1$ and F_i is a keyed permutation, actually a non-linear bijection.

We assume that all round functions F_i are the same for the subblocks in the rest of this paper. This assumption is reasonable for resource constrained devices, or just a misapplication of this structure.

The round function of a MARS-like structure with $n=4$ is shown in Fig. 1.

2.2 UID identity

We borrow the notation from [6]. UID identity is a $\langle L, M, R\rangle$ triple, whose value is the difference $L \oplus M \oplus R$, where L, M, R denote the XOR results of non-zero fixed differences, non-zero unknown differences and unknown differences, respectively. They are defined as follows:

Non-zero fixed difference. The difference is non-zero, fixed and denoted by l_i.

Non-zero unknown difference. The difference can be any value except zero and is denoted by m_i.

Table 1 Impossible differentials for MARS-like structures

No. of subblocks	No. of rounds	Round function	Source
4	11	bijective[a]	[6]
n	$2n-1$	bijective[a]	[11]
n	$2n$	any	[12]
n is even	$3n-1$	bijective[a]	Section 3.2
n is odd	Any	any[a]	Section 3.3

[a]The round function is the same for all subblocks.

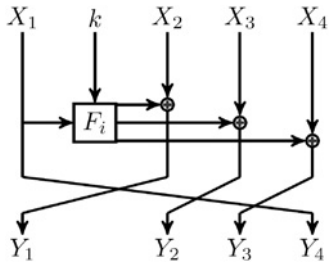

Fig. 1 *One round of a 4-subblock MARS-like structure*

Unknown difference. The difference can be any value and is denoted by r_i.

Table 2 shows different outputs of a non-linear bijective function, where m_j denotes a new non-zero unknown difference, whereas r_j means a new unknown difference.

2.3 Conflict detection

Each pair of plaintext and ciphertext differences is described using two UID vectors, whose components are the UID identities. Then, use the round function to get several intermediate difference vectors for each round. Thus, it is possible to detect whether there is a conflict between the encryption and decryption direction. If any conflict exists, we obtain an impossible differential chain.

To detect an inconsistency between two UID vectors, we need to search all over non-empty subsets of $\{1, 2, \ldots, n\}$, where n is the dimension of the UID vector, and the numbers in the subset represent the positions in the vector. In total, there are 2^n-1 non-empty subsets. For a subset, we XOR the UID components that appear in the subset to obtain a UID identity for each UID vector, and observe if there is a contradiction between the two results. If the two UID identities cannot be equal, we say they are inconsistent. For instance, two different non-zero fixed differences are unequal, and one zero difference cannot be equal to one non-zero difference (fixed or unknown). When an inconsistency is found, the traversal of subsets can stop.

For example, UID vectors $(\langle 0, m_1, 0\rangle, \langle 0, m_2 \oplus m_3, 0\rangle)$ and $(\langle 0, m_2, 0\rangle, \langle 0, m_1, 0\rangle)$ are inconsistent. Compare the XOR results of components of each (choose the subset $\{1, 2\}$), $\langle 0, m_1 \oplus m_2 \oplus m_3, 0\rangle$ and $\langle 0, m_1 \oplus m_2, 0\rangle$. For m_3 is a non-zero difference, the two results cannot be equal and we say that there is a conflict between the two UID vectors.

Note that in the ensuing paragraphs, for convenience, we omit the angles '$\langle\cdot\rangle$' when there is only one item in a UID identity. As the value of $\langle L, M, R\rangle$ is $L \oplus M \oplus R$, we can use ',' instead of '$\oplus$' in a UID identity and omit some '0' items. For example, UID vector $(0, m_1, \langle l_1, m_2\rangle, \langle m_1, m_2\rangle)$ stands for $(\langle 0, 0, 0\rangle, \langle 0, m_1, 0\rangle, \langle l_1, m_2, 0\rangle, \langle 0, m_1 \oplus m_2, 0\rangle)$.

Table 2 Non-linear bijection

Input	Output
0	0
l_i	m_j
m_i	m_j
Otherwise	r_j

3 Impossible differentials of MARS-like structures

In this section, we present the process and impossible differentials we find for the MARS-like structure which have four subblocks and extend to MARS-like structures with an even or odd number of subblocks.

3.1 Four-subblock case

Remind that from the encryption direction, the input (X_1, X_2, X_3, X_4) is turned into

$$(Y_1, Y_2, Y_3, Y_4) = (X_2 \oplus F(X_1), X_3 \oplus F(X_1), X_4 \oplus F(X_1), X_1)$$

by the round function, and from the decryption direction, the input (Y_1, Y_2, Y_3, Y_4) is decrypted into

$$(X_1, X_2, X_3, X_4) = (Y_4, Y_1 \oplus F(Y_4), Y_2 \oplus F(Y_4), Y_3 \oplus F(Y_4))$$

where $F(\cdot)$ is short for $F_i(k, \cdot)$ in Section 2.1.

Here, we consider the case where the plaintext and ciphertext differences are $(0, 0, 0, l_1)$ and $(l_1, 0, 0, 0)$, respectively.

From the encryption direction, after three rounds, the intermediate difference is $(l_1, 0, 0, 0)$, with no new UID identities. Let this intermediate difference be V_e.

Whereas from the decryption direction, the intermediate difference, after three rounds, turns into $(0, 0, 0, l_1)$. Then in the fourth round, l_1 goes through the non-linear bijective function F, and the output is m_1, thus the difference will be (l_1, m_1, m_1, m_1). In the fifth round, m_1 is turned into m_2 by F and the difference will be

$$(m_1, \langle l_1, m_2\rangle, \langle m_1, m_2\rangle, \langle m_1, m_2\rangle)$$

After the eighth round, the difference will be

$$(\langle l_1, m_2, r_1, r_2\rangle, \langle m_1, m_2, r_1, r_3\rangle, \langle m_1, m_2, r_2, r_3\rangle, \langle m_1, r_1, r_2, r_3\rangle)$$

which is the intermediate difference V_d. The process is described in Table 3.

When we choose the index subset $\{1, 2, 3\}$, this means XOR the first, second and third component of V_e and V_d, respectively. The result of the XOR operation of V_e is l_1 and that of V_d is

$$\begin{aligned} &l_1 \oplus m_2 \oplus r_1 \oplus r_2 \oplus m_1 \oplus m_2 \oplus r_1 \oplus r_3 \oplus m_1 \oplus m_2 \oplus r_2 \oplus r_3 \\ &\quad = l_1 \oplus m_2 \end{aligned}$$

Since m_2 is a non-zero difference, we observe an inconsistency between the two UID identities. We conclude that we obtain an 11-round impossible differential chain whose plaintext and ciphertext differences are $(0, 0, 0, l_1)$ and $(l_1, 0, 0, 0)$.

Table 3 Decryption process of $(l_1, 0, 0, 0)$

Round	Intermediate difference
8 (V_d)	$(\langle l_1, m_2, r_1, r_2\rangle, \langle m_1, m_2, r_1, r_3\rangle, \langle m_1, m_2, r_2, r_3\rangle, \langle m_1, r_1, r_2, r_3\rangle)$
7	$(\langle m_1, m_2, r_1\rangle, \langle m_1, m_2, r_2\rangle, \langle m_1, r_1, r_2\rangle, \langle l_1, m_2, r_1, r_2\rangle)$
6	$(\langle m_1, m_2\rangle, \langle m_1, r_1\rangle, \langle l_1, m_2, r_1\rangle, \langle m_1, m_2, r_1\rangle)$
5	$(m_1, \langle l_1, m_2\rangle, \langle m_1, m_2\rangle, \langle m_1, m_2\rangle)$
4	(l_1, m_1, m_1, m_1)
3	$(0, 0, 0, l_1)$
2	$(0, 0, l_1, 0)$
1	$(0, l_1, 0, 0)$
0	$(l_1, 0,0, 0)$

IET Inf. Secur., 2015, Vol. 9, Iss. 4, pp. 219–222

3.2 Even subblocks case

In this section, we discuss the case where the number of subblocks n is even. This can be seen as a generalisation of the 4-subblock case presented in Section 3.1.

The plaintext and ciphertext differences we choose for the example are (0, 0, … ,0, l_1) and (l_1, 0, 0, …, 0) and they both have n components.

The encryption process is such as that in the 4-subblock case, after $n-1$ rounds, the intermediate difference V_e is (l_1, 0, 0, …, 0).

From the decryption direction, after $n-1$ rounds, the ciphertext difference will become (0, 0, …, 0, l_1). Then, in the nth round, l_1 is changed to m_1 by F and the difference will be (l_1, m_1, m_1, …, m_1). In the $(n+1)$th round, m_1 is turned into m_2 and the difference will be

$$(m_1, \langle l_1, m_2\rangle, \langle m_1, m_2\rangle, \ \ldots, \langle m_1, m_2\rangle)$$

After that, in every round, with a one-position right rotation of the input difference vector, the right most component becomes the left most one and then, a new unknown difference r_i will be added (XOR) to all the $n-1$ components except the left most one. The decryption process is detailed in the Appendix. For example, after $n+2$ rounds, we obtain

$$(\langle m_1, m_2\rangle, \langle m_1, r_1\rangle, \langle l_1, m_2, r_1\rangle, \langle m_1, m_2, r_1\rangle, \ \ldots, \langle m_1, m_2, r_1\rangle)$$

and after $2n$ rounds, the difference will be

$$(\langle l_1, m_2, r_1, r_2, \ \ldots, r_{n-2}\rangle, \langle m_1, m_2, r_1, r_2, \ \ldots, r_{n-3}, r_{n-1}\rangle$$

$$\langle m_1, m_2, r_1, r_2, \ \ldots, r_{n-4}, r_{n-2}, r_{n-1}\rangle, \ \ldots, \langle m_1, m_2, r_1, r_3, \ \ldots, r_{n-1}\rangle$$

$$\langle m_1, m_2, r_2, r_3, \ \ldots, r_{n-1}\rangle, \langle m_1, r_1, r_2, \ \ldots, r_{n-1}\rangle)$$

which is V_d. Let (v_1, v_2, …, v_n) denote V_d, where

$$\begin{cases} v_1 = l_1 \oplus m_2 \oplus \bigoplus_{i=1}^{n-2} r_i \\ v_j = m_1 \oplus m_2 \oplus r_{n-j} \oplus \bigoplus_{i=1}^{n-1} r_i, j = 2, \ \ldots, n-1 \\ v_n = m_1 \oplus \bigoplus_{i=1}^{n-1} r_i \end{cases} \quad (2)$$

Here, $\bigoplus_{i=1}^{n}$ denotes the XOR result of a sequence of items.

In this case, we choose the subset $\{1, 2, \ldots, n-1\}$ for the intermediate differences. The XOR result of V_e is just l_1 and that of V_d is $\bigoplus_{k=1}^{n-1} v_k = v_1 \oplus \bigoplus_{k=2}^{n-1} v_k$. As n is even, in the part $\bigoplus_{k=2}^{n-1} v_k$, m_1, m_2 and $\bigoplus_{i=1}^{n-1} r_i$ all appear $n-2$ times and they are eliminated, thus

$$\bigoplus_{k=1}^{n-1} v_k = l_1 \oplus m_2 \oplus \bigoplus_{i=1}^{n-2} r_i \oplus \bigoplus_{j=2}^{n-1} r_{n-j} = l_1 \oplus m_2$$

Hence, the UID vectors are inconsistent, and we obtain a $(3n-1)$-round impossible differential chain. Note that this result is verified in the 4-subblock case, where $n=4$, hence we can obtain an 11-round impossible differential chain, which is in fact exactly the one presented in Section 3.1.

3.3 Odd subblocks case

We now focus on the case where the number of subblocks n is odd, which is in fact quite different from the former case.

Here we present a theorem:

Theorem 1: When the number of subblocks is odd, the MARS-like structure with the same round function (see F_i in Section 2.1) for the subblocks, has impossible differentials for any number of rounds.

Proof: Again we consider the ciphertext difference (l_1, 0, 0, …, 0), containing n components. Fortunately, the first $2n$ rounds of the decryption process are the same as that in the previous discussion. That is, in every round from the nth round, after a round rotation, a non-zero unknown difference m_1/m_2 or a new unknown difference r_i is added to all the $n-1$ components except the left most one. Assuming we obtain V_d after N rounds, here $N \gg 2n$, if we choose the subset as the universal set $\{1, 2, \ldots, n\}$, each unknown difference, m_1, m_2 and all r_i, will appear $n-1$ times in the result. For $n-1$ is even, all the unknown differences finally disappear, and the XOR result is l_1, that is only one known non-zero fixed difference. Now from the encryption direction, we choose (0, 0, …, 0, l_2) as the plaintext difference, with l_2 a non-zero fixed difference not equal to l_1. Similar to the decryption process, after any rounds, we obtain V_e. The XOR of all the components of V_e is l_2. Since l_1 and l_2 are not equal, there is a conflict between V_e and V_d. Then, we obtain an impossible differential whose length is exceedingly large no matter how many rounds the encryption process has. □

Moreover, it follows immediately from the fact that the XOR of all n components does not change after the round function, whether the round function is bijective or not. This allows for a very efficient distinguisher with one known plaintext.

Note although such case seldom occurs. Moreover, this result highlights the fact that the number of subblocks cannot be chosen arbitrarily.

4 Conclusion

In this paper, we exhibited impossible differentials for MARS-like structures with the same round function for the subblocks using the UID method. The number of rounds we worked out is $3n-1$ for the MARS-like structure featuring an even number n of subblocks. In the odd subblocks case, we can find impossible differentials for any number of rounds. Hence, we should pay more attention to the round function in the application of MARS-like structures, and MARS-like structures featuring an odd number of subblocks must not be used in practice. Whether the structure will be better by replacing the round rotation with some other permutations can be investigated in future work.

5 Acknowledgments

This work was supported by the National Natural Science Foundation of China (grant nos. 61073149, 61272440 and 61472251), and China Postdoctoral Science Foundation (grant nos. 2013M531174 and 2014T70417). The authors would like to thank the editor and the anonymous referees for their helpful comments and suggestions.

6 References

1 Biham, E., Biryukov, A., Shamir, A.: 'Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials'. Advanced Cryptol: Proc. EUROCRYPT'99, 1999, (LNCS, 1592), pp. 12–23

2 Knudsen, L.R.: 'DEAL - a 128-bit block cipher'. Technical Report 151, Department of Informatics, University of Bergen, Norway, February 1998. AES submission

3 Phan, R.C.W.: 'Impossible differential cryptanalysis of 7-round advanced encryption standard (AES)', *Inf. Process. Lett.*, 2004, **91**, (1), pp. 33–38

4 Wu, W., Zhang, W., Feng, D.: 'Impossible differential cryptanalysis of reduced-round ARIA and camellia', *J. Comput. Sci. Technol.*, 2007, **22**, (3), pp. 449–456

5 Tsunoo, Y., Tsujihara, E., Shigeri, M., Saito, T., Suzaki, T., Kubo, H.: 'Impossible differential cryptanalysis of CLEFIA'. FSE 2008, Fast Software Encryption, 2008, (LNCS, 5086), pp. 398–411

6 Luo, Y., Lai, X., Wu, Z., Gong, G.: 'A unified method for finding impossible differentials of block cipher structures', *Inf. Sci.*, 2014, **263**, pp. 211–220

7 Kim, J., Hong, S., Sung, J., Lee, S., Lim, J., Sung, S.: 'Impossible differential cryptanalysis for block cipher structures'. Proc. INDOCRYPT 2003, 2003, (LNCS, 2904), pp. 82–96

8 Xue, W., Lai, X.: 'Unified impossible differential cryptanalysis of ARIA', *China Commun.*, 2012, **9**, (8), pp. 129–134
9 Burwick, C., Coppersmith, D., DAvignon, E., *et al.*: 'MARS-a candidate cipher for AES'. NIST AES Proposal, 1998, vol. 268
10 Moriai, S., Vaudenay, S.: 'On the Pseudorandomness of top-level schemes of block ciphers'. Adv. Cryptol.: Proc. ASIACRYPT 2000, 2000, (LNCS, 1976), pp. 289–302
11 Kim, J., Hong, S., Lim, J.: 'Impossible differential cryptanalysis using matrix method', *Discrete Math.*, 2010, **310**, (5), pp. 988–1002
12 Bouillaguet, C., Dunkelman, O., Fouque, P.A., Leurent, G.: 'New insights on impossible differential cryptanalysis'. SAC 2011, Selected Areas in Cryptography, 2012, (LNCS, 7118), pp. 243–259
13 Biham, E., Furman, V.: 'Impossible differential on 8-round MARS' core'. Third AES Candidate Conf., 2000, pp. 186–194
14 Kelsey, J., Schneier, B.: 'MARS attacks! preliminary cryptanalysis of reduced-round MARS variants'. Third AES Candidate Conf., 2000, pp. 169–185
15 Kelsey, J., Kohno, T., Schneier, B.: 'Amplified boomerang attacks against reduced-round MARS and serpent'. FSE 2000, Fast Software Encryption, 2001, (LNCS, 1978), pp. 75–93
16 Pestunov, A.: 'Differential cryptanalysis of the MARS block cipher', *Prikladnaya Diskretnaya Matematika*, 2009, **2009**, (4), pp. 56–63
17 Gorski, M., Knapke, T., List, E., Lucks, S., Wenzel, J.: 'Mars attacks! Revisited'. Proc. INDOCRYPT 2011, 2011, (LNCS, 7107), pp. 94–113

7 Appendix

The decryption process of the ciphertext difference (l_1, 0, 0, …, 0) from the nth round to the $2n$th round is detailed below.

Round: Intermediate difference

$$n{:}(l_1, m_1, m_1, \ldots, m_1)$$

$$n+1{:}(m_1, \langle l_1, m_2\rangle, \langle m_1, m_2\rangle, \ldots, \langle m_1, m_2\rangle)$$

$$\begin{array}{r} (\langle m_1, m_2\rangle, \\ \langle m_1, r_1\rangle, \\ \langle l_1, m_2, r_1\rangle, \\ n+2{:}\ \langle m_1, m_2, r_1\rangle, \\ \langle m_1, m_2, r_1\rangle, \\ \vdots \\ \langle m_1, m_2, r_1\rangle) \end{array} \Bigg\} n-3$$

$$\begin{array}{r} (\langle m_1, m_2, r_1\rangle, \\ \langle m_1, m_2, r_2\rangle, \\ \langle m_1, r_1, r_2\rangle, \\ \langle l_1, m_2, r_1, r_2\rangle, \\ n+3{:}\ \langle m_1, m_2, r_1, r_2\rangle, \\ \langle m_1, m_2, r_1, r_2\rangle, \\ \vdots \\ \langle m_1, m_2, r_1, r_2\rangle) \end{array} \Bigg\} n-4$$

$$\ldots$$

$$\begin{array}{r} (\langle m_1, m_2, \bigoplus_{i=1}^{n-3} r_i\rangle, \\ \langle m_1, m_2, r_{n-3} \oplus \bigoplus_{i=1}^{n-2} r_i\rangle, \\ \vdots \\ 2n-1{:}\ \langle m_1, m_2, r_2 \oplus \bigoplus_{i=1}^{n-2} r_i\rangle, \\ \langle m_1, m_2, r_1 \oplus \bigoplus_{i=1}^{n-2} r_i\rangle, \\ \langle m_1, \bigoplus_{i=1}^{n-2} r_i\rangle, \\ \langle l_1, m_2, \bigoplus_{i=1}^{n-2} r_i\rangle) \end{array}$$

$$\begin{array}{r} (\langle l_1, m_2, \bigoplus_{i=1}^{n-2} r_i\rangle, \\ \langle m_1, m_2, r_{n-2} \oplus \bigoplus_{i=1}^{n-1} r_i\rangle, \\ \langle m_1, m_2, r_{n-3} \oplus \bigoplus_{i=1}^{n-1} r_i\rangle, \\ 2n{:}\ \vdots \\ \langle m_1, m_2, r_2 \oplus \bigoplus_{i=1}^{n-1} r_i\rangle, \\ \langle m_1, m_2, r_1 \oplus \bigoplus_{i=1}^{n-1} r_i\rangle, \\ \langle m_1, \bigoplus_{i=1}^{n-1} r_i\rangle) \end{array}$$

IET Inf. Secur., 2015, Vol. 9, Iss. 4, pp. 219–222