International Journal of Security and Its Application
Vol.11, No.1 (2017), pp.165-178
http://dx.doi.org/10.14257/ijsia.2017.11.1.14

Boomerang Analysis Method Based on Block Cipher

Fan Aiwan and Yang Zhaofeng

Computer School, Pingdingshan University, Pingdingshan, 467002 Henan province, China
{ Fan Aiwan} faw_1978@163.com

Abstract

This paper fused together the related key analysis and differential analysis and did multiple rounds of attack analysis for the DES block cipher. On the basis of deep analysis of Boomerang algorithm principle, combined with the characteristics of the key arrangement of the DES block cipher, the 8 round DES attack experiment and the 9 round DES attack experiment were designed based on the Boomerang algorithm. The experimental results show that, after the design of this paper, the value of calculation complexity of DES block cipher is only 2^{40} *and the analysis performance is greatly improved by the method of Boomerang attack.*

Keywords*: block cipher, DES, Boomerang, Computational complexity*

1. Introduction

With the advent of the information society, especially the extensive application of the Internet to break the traditional limitations of time and space, which brings great convenience to people. However, at the same time, a large amount of sensitive information is transmitted through the channel or computer network, especially the rapid development of e-commerce and e-government, more and more personal information such as bank accounts require strict confidentiality, how to guarantee the security of information is particularly important [1-2].

The essence of information security is to protect the information system or the information resources in the information network from various types of threats, interference and destruction, that is, to ensure the security of information [3]. Modern cryptography is one of the key technologies of information security has a very important foundation support [4].

Block cipher is the core element of many cryptographic systems, and it is an important technique to guarantee the confidentiality and integrity of information. The design and analysis of block cipher has always been a hot research topic in cryptography. How to design, analyze and evaluate the security of the algorithm is the key problem in this field [5].In order to ensure the security of cryptographic algorithm, the design of block cipher algorithm requires that the length of packet is long enough, the key amount is large enough, and the password transformation is complex enough. The existing block cipher is usually iterated block cipher, that is, by selecting simple password change (called round function), it is used to encrypt the transformation in the iterative method under the control of the key[6]. An iteration is called a round, the number of iterations is called the number of rounds of encryption, and the key is used for each iteration is called the round key. The mathematical essence of the block cipher analysis is that known plain text and the cipher text, for any round of the key. One of the important purposes of the iterative block cipher analysis is to analyze the number of rounds with a small time complexity and storage complexity, sometimes attack on the whole round of implementation of the password is very difficult, so use some kind of attack method to analyze the password with a low round attack, the result of the analysis can reflect the ability of the password to resist this

ISSN: 1738-9976 IJSIA

attack, which also has an important significance to the design and analysis of block cipher [7].

The effective degree of an attack method is usually measured by the time complexity, space complexity and the complexity of the data. The data complexity is the amount of data needed to carry out the attack, known the data complexity of plain text attack or chosen plain text attack, it is can be determined by using the number of plain text and cipher text pair that the have known or choose the needed to attack ; space complexity is the amount of storage required for the attack algorithm; time complexity is the implementation of the calculation steps needed in the attack ,usually represented by the number of encryption and decryption. If the key length of a block cipher is k , the time complexity of the attack is less than 2^k , then the attack is successful in theory [8].

At present, the common analysis methods of the security of the block cipher are: differential cryptanalysis method, linear attack method, brute force attack method. Ahmadian proposed differential analysis method for DES [9]. It is one of the most important and effective analysis methods of block cipher. Later there were some extension of the differential analysis method, including truncated differential cryptanalysis, high order differential cryptanalysis, impossible differential cryptanalysis [10].

The linear attack method proposed by Granger is to restore partial key by computing the probability of a linear relationship among the input bits, the output bits, and the key. It and the difference analysis method is an important index to measure the security of block cipher [11]. The method according with differential cryptanalysis are the important index to measure the security of block cipher.

Brute force attack method, which can be used for any block cipher, the attack complexity only depends on the block length and key length. Brute force attacks including exhaustive search attack, dictionary attack, look-up table attack [12].

In addition, the common attack method also including the meet-in-the-middle attack, the related-key attack, Square attack and so on. The Boomerang analysis method studied in this paper is one kind of differential cryptanalysis method, but the differential cryptanalysis method is the most effective analysis method of block cipher [13]. Boomerang attacks have also become an integral part of the security analysis of block cipher.

In the Boomerang attack method, need four sets of plain text data. In order to analyze the algorithm for more round, the encryption function E is divided into two parts E_0 and E_1 . When the differential characteristics of are poor, while the differential characteristics of A and B are good, connecting the two short high probability differential paths, the good attack effect can be achieved. Due to the Boomerang attack select plain text and adaptive selection of the cipher text to attack, making a lot of techniques for recovering the keys using the division can not be applied, the limitations is very large [14-15].

Ciet is proposed the expanded Boomerang attack, that is, the Amplified Boomerang attack. The attack applies to the plain text attack, the main idea is to encrypt a large number of clear text to find the four tuple in accordance with the Boomerang distinguisher [16].

Minematsu has improved the attack and proposed the Rectangle attack. It can greatly improve the probability of finding a division by using several differential paths simultaneously [17].

Boomerang attacks are often combined with the relevant key, as the related key Boomerang attack. Since then, the article on the Boomerang attacks emerge in endlessly, which is make a great contribution to the security analysis of block cipher.

In this paper, we will design a new Boomerang attack strategy for the DES block cipher system, in order to investigate the performance of the Boomerang method for the security analysis of block cipher.

2. Analysis Theory of Boomerang Method

Boomerang attack is a kind of attack method based on difference analysis, and it is a kind of attack algorithm which is chosen to be adapted to the cipher text attack. In the Boomerang attack method, in order to analyze the more round of the algorithm, connect the two short high probability of the differential path.

First, define a block cipher algorithm, this algorithm can be described as follows:

$$F = F_1 \circ F_0 \tag{1}$$

In the formula, F_0 represents the first half of the encryption, F_1 represents the last half of the encryption, and both F_0 and F_1 are reversible. There is a difference result $\beta \to \gamma$ in F_0, the probability is p, the calculation is as follows:

$$p = \Pr(\beta \to \gamma) \tag{2}$$

There is a difference result $\eta \to \varepsilon$ in F_1^{-1},the probability is q, the calculation is as follows:

$$q = \Pr(\eta \to \varepsilon) \tag{3}$$

For the plain text four tuple Q_a, Q_b, Q_c, Q_d, after encrypted, get the cipher text D_a, D_b, D_c, D_d.

Enter the following vertical differential:

$$Q_a \oplus Q_b = Q_c \oplus Q_d = \beta \tag{4}$$

After a transfer to the output horizontal differential:

$$D_a \oplus D_b = D_c \oplus D_d = \eta \tag{5}$$

In this way, the two large probability events are linked together.

If F_0 has a difference $\beta \to \gamma$ in plain text pair Q_a, Q_b, then:

$$\begin{cases} Q_b = Q_a \oplus \beta \\ F_0(Q_b) = F_0(Q_a) \oplus \gamma \end{cases} \tag{6}$$

At the same time, F_1^{-1} has a difference $\eta \to \varepsilon$ in the cipher text pair Q_a, D_c and Q_b, D_d then:

$$\begin{cases} D_a \oplus D_c = \eta \\ D_b \oplus D_d = \eta \\ F_1^{-1}(D_a) \oplus F_1^{-1}(D_c) = F_0(Q_a) \oplus F_0(Q_c) = \varepsilon \\ F_1^{-1}(D_b) \oplus F_1^{-1}(D_d) = F_0(Q_b) \oplus F_0(Q_d) = \varepsilon \end{cases} \tag{7}$$

Then, for plain text pair Q_c and Q_d, F_0^{-1} must has a difference $\gamma \to \beta$.When the above conditions are fully established, the middle value of the first half after encrypted, as follows:

$$\begin{aligned} Y_c \oplus Y_d &= F_0(Q_c) \oplus F_0(Q_a) \\ &= [F_0(Q_a) \oplus F_0(Q_b)] \oplus [F_0(Q_a) \oplus F_0(Q_c)] \oplus [F_0(Q_c) \oplus F_0(Q_d)] \\ &= [F_0(Q_a) \oplus F_0(Q_b)] \oplus [F_1^{-1}(D_a) \oplus F_1^{-1}(D_c)] \oplus [F_1^{-1}(D_c) \oplus F_1^{-1}(D_d)] \\ &= \gamma \oplus \varepsilon \oplus \varepsilon \\ &= \gamma \end{aligned} \quad (8)$$

Need to pay attention to is that the essential condition of the above type establishment is F_0^{-1} must has the difference $\gamma \to \beta$,only when the difference condition is established, the plain text pair Q_c, Q_d and original plain text Q_a, Q_b have the same difference. This is why it is called the Boomerang attack, which is the reason why the fly to attack the attack: When the encryption begins, choose a plain text difference properly, after the decryption will still get the same express difference.

The Boomerang attack process is as follows:

(1)Randomly select the plain text pair Q_a and Q_b, $Q_b = Q_a \oplus \beta$, encrypt Q_a and Q_b,will get $D_a = F(Q_a), D_b = F(Q_b)$;

(2)Calculate $D_c = D_a \oplus \eta$, $D_d = D_b \oplus \eta$, decrypt D_c and D_d , will get $Q_c = F^{-1}(D_c)$, $Q_d = F^{-1}(D_d)$;

(3)Check whether $Q_c \oplus Q_d = \beta$ is established.

The probability of the four tuple to pass the Boomerang distinguisher is:

$$\sum_{\gamma} \Pr^2[\beta \to \gamma] \sum_{\eta} \Pr^2[\eta \to \varepsilon] = p^2 q^2 \quad (9)$$

For a random permutation of N bits, the probability of the four tuple is 2^{-n}. So, as long as the choice of good probability of the differential path with $p^2 q^2 > 2^{-n}$, so that, you can use the Boomerang distinguisher to restore the key.

3 Analysis of Key Rules for DES Algorithm

DES is a block cipher encryption algorithm used to protect the security of its products, which is a typical digital encryption standard. It is one of the most popular and widely used block cipher in the world, has played a significant role in promoting the development and application for cryptography theory. DES uses the key with the length of 64 bits and the plain text with the encrypted length of 64 bits, get the cipher text with the length of 64 bits and the number of encryption rounds are 16. The encryption process is shown in figure 1:

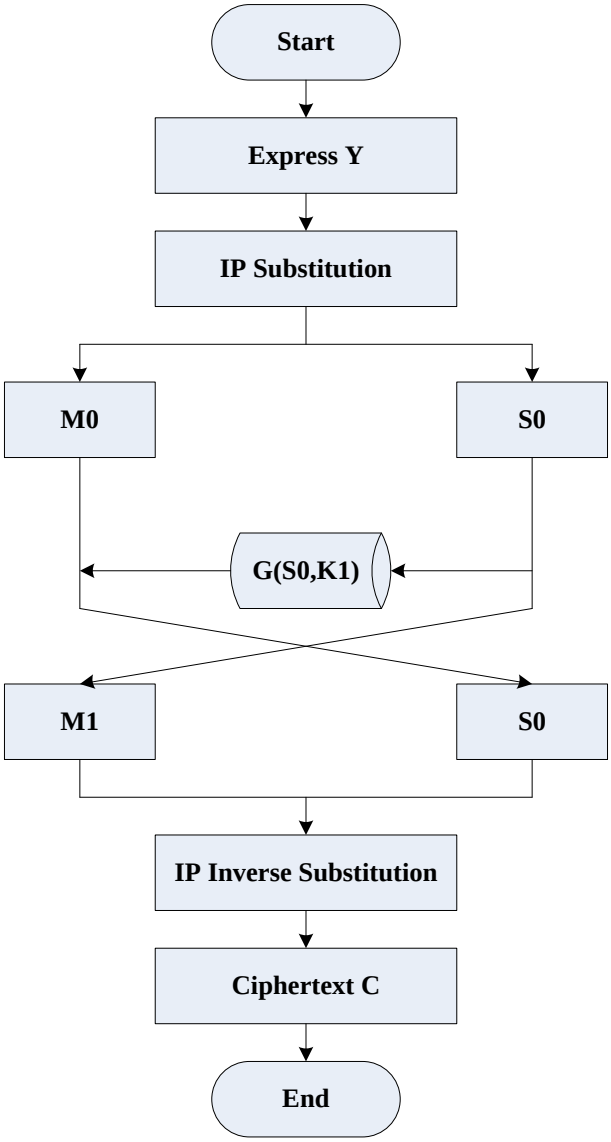

Figure 1. Encryption Flow Chart of DES Algorithm

The cipher text Y after a fixed initial replacement IP, obtain $y_0 = M_0 S_0$. Among them, M_0 is the first 32 bits of y_0, S_0 is the last 32 bits of y_0. And then after the 16 round of the same operation:

$$\begin{aligned} M_i &= S_{i-1} \\ S_i &= M_{i-1} \oplus g(S_{i-1}, K_i) \end{aligned} \tag{10}$$

Finally, the $S_{16}M_{16}$ is obtained by the initial inverse permutation IP^{-1} to obtain the cipher text D. Among them, $1 \le i \le 16$, $\oplus$ represents XOR operation between the two bit string . K_i is a 48 bit round key in $g(S_{i-1}, K_i)$,which is the function of the main key K.

The function of IP and IP^{-1} is only used to disrupt the order of the original bit string.

First, the 32 bits of S_{i-1} after an extended function F becomes a bit string of 48 bits, then XOR with round key K_i, that is:

$$C = F(S_{i-1}) \oplus K_i \tag{11}$$

Then the resulting 48 bit string C is divided into 8 bit strings with length of 6:

$$C = C_1C_2C_3C_4C_5C_6C_7C_8 \tag{12}$$

Put each C_j into one T_i, each T_i of which is a 16 rows 4 columns matrix.

Suppose there exists a bit string with a length of 6, that is $C = C_1C_2C_3C_4C_5C_6$, put such a bit string into the corresponding T_j. The decimal number C that corresponding to $C_1C_2C_3C_4$ determine the column of T_j, then output D_j of $T_j(C_j)$ is the number corresponding to the l row the d column of the matrix T_j. D_j is a bit string of length 4. The outputs D_j of 8 T_j are combined into a 32 bit string $D_1D_2D_3D_4D_5D_6D_7D_8$, and finally the results of $g(S_{i-1}, K_i)$ can be obtained by a fixed permutation.

4. Design, Experiment and Results of DES Block Cipher for Boomerang 8 Rounds Attack

In order to verify the validity of the Boomerang method for the analysis of the DES block cipher, we first design a 8 round related key attack device.

See the 8 rounds of DES algorithm F as two parts, F_0 and F_1, so $F = F_0 \circ F_1$.There exists an input difference β and an output difference γ in F_0; and exists an input difference ε and an output difference η in F_1.

(1)The structure of F_0

F_0 consists of the first 4 rounds. The input difference, that is, the plain text difference β and the related key difference ΔK_{ab}. At this point, the input difference of the fourth round of the g function on the right side is also $0x20000000 \oplus \Delta K_4^{22}$, and there exists the same input difference at T_1 and T_4, which is 000100.The output difference distribution of T_1 is observed when the input difference is 000100: 0011 appeared 6 times; 0101 appeared 10 times; 0110 appeared 10 times; 0111 appeared 6 times; 1001 appeared 4 times ; 1010 appeared 6 times ; 1011 appeared 4 times ; 1100 appeared 2 times ; 1101 appeared 8 times ; 1110 appeared 6 times ; 1111 appeared 2 times.

So the probability of the difference of the output of the T_1 is equal to sum of the probability when both of the two are 0011, 0101, ... , 1111, that is $\frac{6^2 + 10^2 + \cdots + 2^2}{64^2} = 0.109$. By the same way, we can calculate the probability of T_4 is $\frac{544}{64^2} = 0.133$.

At this point, the output difference γ of F_0 only in T_1 and T_4 have difference, and the rest are 0. The probability of have the equal value γ is $\frac{448\times 544}{2^{24}} \approx 2^{-6}$.

(2)The structure of F_1

F_1 consists of 5-8 rounds. Because D49 does not appear in the 5 and 7 rounds , select the relevant key difference $\Delta K_{ac} = f_{49}$. Here, f_{49} represents only the 49 of component is 1, the rest of the components are 0, it is a binary vector with 64 dimensional .

Select the input differential $\varepsilon = 0x00020000000000$ of F_1. In the 5 round, because there is no D49 in K_5, the key difference is 0 and A's right 32 bits also have no difference, the input and output difference of T in the g function are 0. After the operation of XOR and exchange , the output difference of the 5 round are, $\Delta M_5 = 0x00000000$, $\Delta S_5 = 0x00020000$.

The use order of the 6 round key is D03, D44, D27, D17, D42, D10, D26, D50, D60, D02, D41, D35, D25, D57, D19, D18, D01, D51, D52, D59 , D58, D49, ……, D22. Among these, D29 appeared in the 22 place.

The 22 bit of the key corresponds to the 15 bit of the right input, offset the key difference and the differential of ΔS_5, get the output difference of the 6 round, that is, the output difference of the 7 round are $\Delta M_6 = 0x00020000$, $\Delta S_6 = 0x00000000$.

In the 7 round, the D49 is not appear in the key order, so there is no difference in the 7 round sub key , and there is no difference in the right input ΔS_6, so the

There is no difference, so the 8 round of the seventh input, the input and output difference of 8 T_j are 0 in the 7 round.

On the right side of the input of the 8 round has a 1 bit difference in the15 bit, after the extension is the 22 bit, that is, the 1 bit of T_4. The key use sequence: D36 , D41, D60, D50, D10, D43, D59, D18, D57, D35, D09, D03, D58, D25, D52, D51, D34, D19, D49, ……, D53, D49 at the 19 bit, that is, the first bit of T_4. Both are gathered in T_4, namely the input difference of T_4 is 100100. When the input difference is 100100, the number of the output difference 0001, 0010, 0100, 0111, 1000, 1011, 1101, 1110 of T_4 is the highest, which is 6 times. The output difference is 1000, after the P replacement, the output difference of the 8 round function is 0x00000040.So the output difference of the 8 round function is $\Delta M_8 = 0x00020000$, $\Delta S_8 = 0x00000040$, that is, the output difference of F_1 is $\eta = 0x0002000000000040$.

The probability of the above event is $\frac{6}{64}$. The probability of both sides of the rectangle is $\frac{36}{64^2} = \frac{9}{2^{10}} \approx 2^{-6.8}$, so the probability of the entire 8 rounds related key Boomerang attack distinguisher is about $2^{-6}\times 2^{-6.8} = 2^{-12.8}$.

Experimental results from the 5 round attack to the 8 round attack are shown in Figure 2.

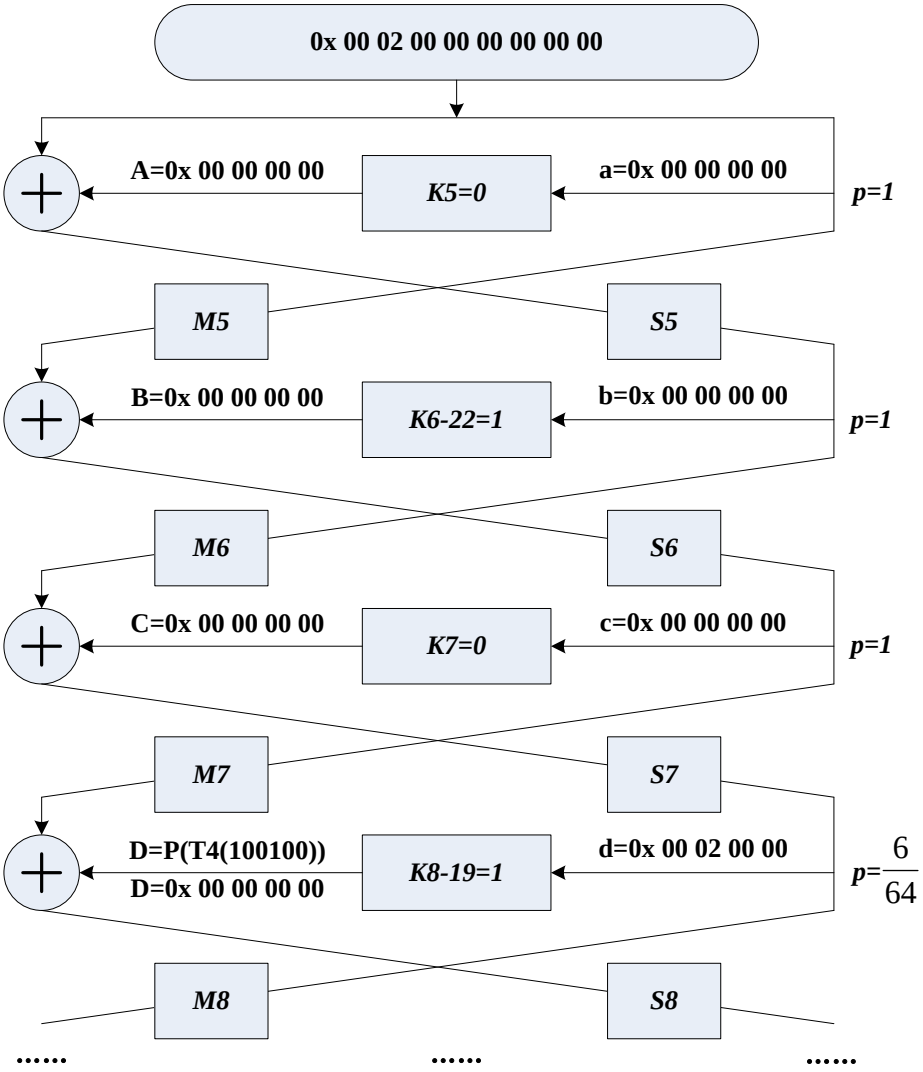

Figure 2. Experimental Results of the 8 Rounds Attacks

5 Design, Experiment and Results of DES Block Cipher for Boomerang 8 Rounds Attack

In this section experiment, further increase the 8 round attack to the 9 round of attacks.

The use of sub key order in the 9 round is D57, D33, D52, D42, D02, D35, D51, D10, D49, ……, D4, D49 appears at the 9 bit. The input ΔS_8 on the right side of the 9 round has a bit difference in the 26 bit, and after the extension is the 39 bit. So, in the 9 round, the input difference only at the T_2、 T_7 are not 0, are 001000.

In the 9 round , when the input difference of T_2 is 001000, 1100 appears the most times in the output difference, which are 16 times, after the P permutation ,occurs in the 2 bit and the 13 bit, the occurrence probability is $\frac{16}{64}$. When the input difference of T_7 is 001000, 1100 also appears the most times in the output difference, which are 12 times, after the P permutation ,occurs in the 22 bit and the 32 bit, the

occurrence probability is $\frac{12}{64}$. After permutation, the output difference of the 9 round function is 0x40080401.

The difference on the left side of the cipher text is $\Delta M_9 = \Delta S_8 = 0x00000040$, the right side is $\Delta S_9 = \Delta S_8 \oplus g(\Delta S_8, \Delta K_9) = 0x400a0401$, so take the difference $\eta = 0x00000040400a0401$. So far, the probability of the establishment of related-key differential path is $2^{-12.8} \times \left(\frac{16}{64}\right)^2 \times \left(\frac{12}{64}\right)^2 \approx 2^{-21.7}$ in the whole 9 rounds, .

In this paper, the experimental process if the 9 round attack design is as follows:

(1) Data acquisition

The number of $D_a = (A, Y_a)$ is 2^{28}, here A is a fixed value of 32 bits, Y_a takes an arbitrary 32 bits value. Use K_a decrypt the plain text Q_a which is corresponds to the D_a .

Give an increment to Q_a, that is $Q_b = Q_a \oplus (0x2000000000000000)$, use the key $K_b = K_a \oplus f_{52}$ encrypt Q_b get D_b.

The number of $D_c = (A \oplus 0x00000040, Z_c)$ is 2^{28}, here A is the same as above. take 2^{28} arbitrary 32 bits value for Z_c. Use $K_c = K_a \oplus f_{49}$ decrypt D_c get the corresponding plain text Q_c.

Give an increment to Q_c, that is $Q_d = Q_c \oplus (0x2000000000000000)$, use the key $K_d = K_a \oplus f_{52} \oplus f_{49}$ encrypt Q_d get D_d.

(2) First screening

From the above D_a and D_c, each select one. Check whether the corresponding D_b and D_d meet $D_b \oplus D_d$ in the left half at this time , like 0x00000040, If there are not satisfied then discard D_a、D_b、D_c、D_d. If satisfied, then retain. As the left half of the $D_b \oplus D_d$ such as 0x00000040, the probability is 2^{-32}. So the probability of obtaining the expected result of this step is $2^{56} \times 2^{-32} = 2^{24}$.

(3) Screening again

Because the difference on the left side of the 8 round is $\Delta M_8 = 0x00020000$, after the 9 round, the right side difference is the XOR between the output difference of the g function and 0x 00020000, that is:

$$D_a^R \oplus D_c^R = g(D_a^M, K_a) \oplus g(D_c^M, K_c) \oplus 0x00020000$$

Then $D_a^R \oplus D_c^R = g(A, K_a) \oplus g(A \oplus 0x00000040, K_c) \oplus 0x00020000$ is a constant. In other words, $D_a^R \oplus D_c^R$ in the right side of all of the correct four tuple cipher text are equal. In the rest of the 2^{24} four tuples, respectively, get the value of $D_a^R \oplus D_c^R$. If the times of equal number greater than or equal to 2 $2^{24} \times 2^{-21.7} \approx 4$, it is thought that these four tuple are correct.

(4)Recovery key

According to these four tuple and $g(A, K_a) \oplus g(A \oplus 0x00000040, K_c) = D_a^R \oplus D_c^R$, we can know the input and output

difference of T_2, T_7 in the 9 round, so we get a key alternative set of T_2 and T_7, respectively.

In the 9 round, The output difference 1100 appeared 16 times when the input difference of T_2 is 001000, after P permutation, occurs in the 2 bit and the 13 bit. The output difference 1001 appeared 10 times, probability is $\frac{10}{64}$, after P permutation, occurs in the 13 bit and the 18 bit. The output difference 1010 appeared 12 times when the input difference of T_7 is 001000, and the output difference 0111 appeared 10 times, the probability is $\frac{10}{64}$, after P permutation, occurs in the 7 bit、the 12 bit and the 22 bit. Change the right side value of η, the left side is still 0x 00000040, make the right value is $g_7 + g_{12} + g_{13} + g_{18} + g_{22}$, there are $2^{24} \times 2^{-12.7} \times \left(\frac{10}{64}\right)^2 \times \left(\frac{10}{64}\right)^2 \approx 1.5$ correct pairs, that is, the number of correct four tuple is at least 1, once again, obtaining a key alternative set of T_2 and T_7, the common element in the set of the before and after two times is the key of T_2 and T_7 in the 9 round . If it is still can not determined, then change the output difference of T_2 and T_7, finally determine the key of T_2、 T_7 are D51, D10, D49, D27, D01, D60, D47, D07, D20, D14, D29, D38.

From these correct four tuple ,we know the input and output difference of T_4 in the 8 round, obtaining the key of T_4 in the 8 round are D49, D27, D26, D17, D44, D02. The obtaining key in the two times has 2 bit coincidence, that are D49, D27, so get a total of 16 bit key. Even if the rest of the infinite search, the complexity is only 2^{40}. So the whole attack process need encrypt and decrypt operation for 2^{31} times. So far, it is known that the analysis performance of the Boomerang method based on the DES block cipher is much better than that of the method has appeared (At present, the minimum computational complexity of this method is 2^{119}).

In this paper, the experimental results of the 9 rounds attacks are shown in Figure 3.

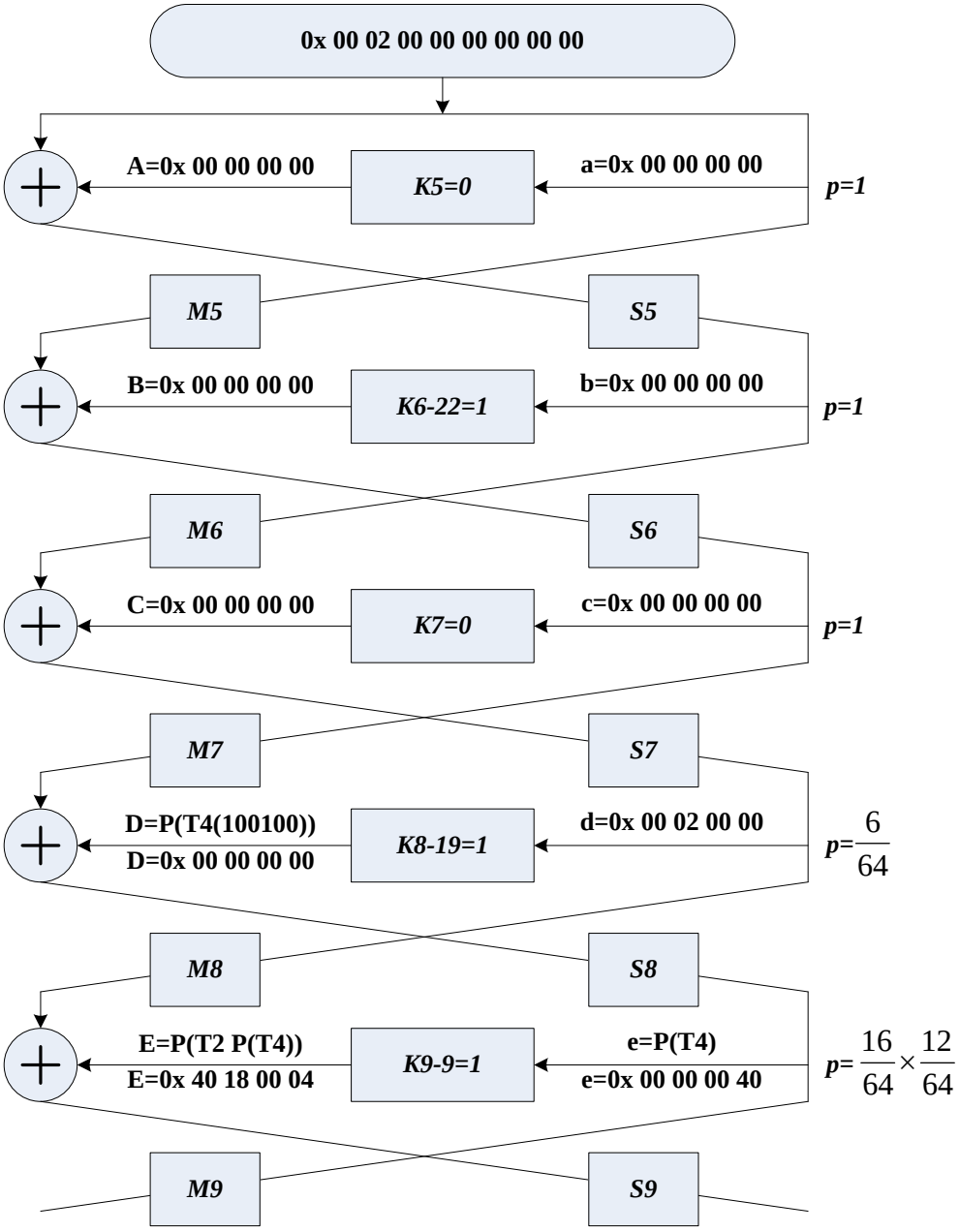

Figure 3. Experimental Results of the 9 Rounds Attacks

6. Conclusion

In this paper, the analysis of the DES block cipher is successfully realized by the combination of the key analysis and the difference analysis. According to the DES key layout algorithm, the sub key of each round is getting back by the original key. According to the use order and the number of bits not appearing of each round of key, set the plain text difference and key difference properly to get the DES related key difference path. On the basis of DES related key difference analysis, using the Boomerang analysis method, the related key Boomerang attack of the 9 round DES is obtained. Construct a 8 round distinguisher for DES, and plus one round after the 8 round distinguisher, using the related key Boomerang attack method to analyze the 9 round DES. The complexity of the attack time is about 2^{31} times of the encryption

and decryption operation, the data complexity is 2^{40}, which is much better than the appeared Boomerang attack method.

Appendix

This paper is a revised and expanded version of a paper entitled [Research on Boomerang Analysis Method Based on Block Cipher] presented at The 9th International Conference on Security Technology (SecTech 2016), 24-26 November 2016，Jeju Island, Korea.

References

[1] Kelsey J,Kohno T,Schneuer B.Amplified Boomerang attacks againgst reduced-round MARS and serpent[C]. In: Schnier B, ed. Proc. of the Fast Software Encryption, Berlin: Springer-Verlag, 75-93**.(2001)**
[2] Alex Biryukow. The Boomerang Attack on 5 and 6-Round Reduced AES[C]. Proceedings of AES4 Conference, Lecture Notes in Computer Science, Springer-Verlag, 111-120. **(2004)**
[3] X.Y Wang, H.Yu. How to Break MD5 and Other Hash Functions[C]. Advances in Cryptology EUROCRYPT, Berlin: Springer, 19-35. **(2005)**
[4] Bozhan Su, Wenling Wu, Shuang Wu, and Le Dong. Near-collisions on the reduced-round compression functions of skein and blake[J]. In Swee-Huay Heng,Rebecca N. Wright, and Bok-Min Goi, editors, CANS, volume 6467 of Lecture Notes in Computer Science, 124-139. **(2010)**
[5] Andrey Bogdanov, Christian Rechberger. A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Light weight Block Cipher KTANTAN[J]. Selected Areas in Cryptography, 229-240. **(2010)**
[6] P Rogaway, M Bellare, J Black. OCB: A block-cipher mode of operation for efficient authenticated encryption[J]. ACM Transactions on Information and System Security, 6(3): 196-205. **(2015)**
[7] TP Berger, J Francq, M Minier, G Thomas. Extended Generalized Feistel Networks using Matrix Representation to Propose a New Lightweight Block Cipher: Lilliput[J]. IEEE Transactions on Computers, 1-5. **(2016)**
[8] Bo Xu, Zhiping Peng, Fangxiong Xiao, Antonio Marcel Gates, Jian-Ping Yu. Dynamic deployment of virtual machines in cloud computing using multi-objective optimization
[9] [9] Ahmadian Z., Salmasizadeh M., Aref M.R. Biclique cryptanalysis of the full-round KLEIN block cipher[J]. Iet Information Security, 9(5): 294-301. **(2015)**
[10] W Yi, S Chen. Multidimensional zero-correlation linear cryptanalysis of the block cipher KASUMI[J]. Iet Information Security, 10(4): 215-221. **(2016)**
[11] R Granger, P Jovanovic, B Mennink, S Neves. Improved Masking for Tweakable Blockciphers with Applications to Authenticated Encryption[C]. International Conference on Advances in Cryptology, 111-115. **(2016)**
[12] A Baysal, S Şahin. Conference Paper: RoadRunneR: A Small And Fast Bitslice Block Cipher For Low Cost 8-bit Processors[J]. Discover the World's Research, 10(5): 13-18. (2015)
[13] A Baysal, S Şahin. RoadRunneR: A Small And Fast Bitslice Block Cipher For Low Cost 8-bit Processors[J]. Lightsec, 79-85**.(2015)**
[14] R Beaulieu, S Treatman-Clark,D Shors, B Weeks. The SIMON and SPECK lightweight block ciphers[J]. Design Automation Conference, 1-6. **(2015)**
[15] BJ Mohd, T Hayajneh, AV Vasilakos. A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues[J]. Journal of Network & Computer Applications, 58(C): 73-93. **(2015)**
[16] M Ciet, AJ Farrugia, FT Paun. Systems and methods for implementing block cipher algorithms on attacker-controlled systems[J]. Dissertations & Theses Gradworks, 12(6): 71-80. **(2015)**
[17] K Minematsu. Building blockcipher from small-block tweakable blockcipher[J]. Designs Codes & Cryptography, 74(3): 645-663. **(2015)**

Authors

Fan Aiwan, an associate professor in Computer School of Pingdingshan University, who was born in 1978 in Neixiang County, Henan Province, China. He received the M.S. degree of Computer Application Technology in Xi'an Electronic and Science University in 2009. He is mainly engaged in the research of network information security and cloud computing security.

Yang Zhaofeng, an associate professor in Computer School of Pingdingshan University, who was born in 1978 in Xiangcheng County, Henan Province, China. He received the M.S. degree of Computer Application Technology in Xi'an Electronic and Science University in 2010. He is mainly engaged in the research of network information security and cloud computing security.