UDC 004.056.5
SRSTI 81.93.29

CRYPTOGRAPHIC ATTACK TO ENCRYPTION ALGORITHM "AL01" BY THE BOOMERANG METHOD

K.S .Sakan[1,2], K.T.Algazy[1,2]
[1]Institute of Information and Computational Technologies SC MES RK, Almaty, Kazakhstan,
[2]Kazakh National University named after al-Farabi, Almaty, Kazakhstan
E-mail: kairat_sks@mail.ru, kunbolat@mail.ru

Abstract. This paper describes the implementation of a cryptographic attack by the boomerang method on the "AL01" block symmetric algorithm, one of the encryption algorithms which are developed at the Institute of information and computational technologies of the SC MES RK.

This method allowed for successful attacks on many ciphers previously recognized as resistant to classical differential cryptanalysis. There are modifications of this cryptanalysis method: an amplified boomerang attack and a rectangle attack (this method is covered in this paper). In some cases, the use of this attack method can significantly reduce the amount of required data. Also this attack is applicable to algorithms with a heterogeneous structure of rounds. As with the method of differential cryptanalysis, the practical application of the boomerang attack is limited by the high requirements for processing time and data volume. Taking into account the basic properties of the differential cryptanalysis and based on the conclusions of other scientific works, the necessary minimum number of a set of quartets of open and corresponding closed texts is determined. The article concludes that the proposed cryptographic algorithm is highly resistant to this type of cryptographic attack.

Keywords: symmetric encryption algorithms, requirements for encryption algorithms, basic methods of cryptanalysis, boomerang attack.

Introduction. The strength of an encryption algorithm is its permissible degree of resistance to differential cryptographic attacks. There are certainly resistant (or theoretically persistent), provably resistant, and presumably resistant crypto algorithms. Similarly, one can distinguish between the stability of the crypto algorithm itself, the stability of the protocol, and the stability of the key distribution generation algorithm [1]. Supposedly resistant crypto algorithms are based on the complexity of solving a particular mathematical problem that is not reduced to well-known. Examples are the ciphers GOST 28147-89, AES, FEAL [2].

The boomerang attack is a cryptographic attack on a block cipher based on differential cryptanalysis methods. The attack algorithm was published in 1999 by UC Berkeley professor David Wagner, who used it to crack the COCONUT98, Khufu, and CAST-256 ciphers. Further, this method has found wide theoretical application in reliability assessments in many block ciphers. The boomerang method allows to attack some of the algorithms that are resistant to classical differential cryptanalysis, significantly reducing the amount of data required for analysis.

Cryptographic attack to encryption algorithm "AL01". The main point of the study is to find the sets of open quartets and their corresponding ciphertexts, and their minimum necessary layer to continue the analysis. As you know, the data encryption block of the "AL01" algorithm consists of the following transformations: linear transformation - bitwise addition operation (XOR), nonlinear transformation S-replacement block. As already described in the scheme of the encryption algorithm "AL01", the number of rounds is eight [3]. When using a boomerang attack, the completes scheme of algorithm E *is* divided into two consecutive parts of equal complexity: into two parts, 2 round seach E_0 and E_1, such that $E = E_0 \circ E_1$, where $\circ$ - operation of concatenation. We can this structure describe in function form: $E(M) = E_1\big(E_0(M)\big)$.

The basic idea behind the boomerang attack is to use two short effective differentials instead of one long differential, trying to do better than the traditional differential attack [4]. Let the function E_0 has differential characteristic $\alpha \to \beta$ with probability p, and the function $E_1 : \gamma \to \delta$ with probability q. This work uses a rectangle-style boomerang attack, but the name of the boomerang attack is saved.

Figure 1 shows a rectangular boomerang structure with E_0 and E_1, quartets plaintext ciphertext quartets and related differentials, α, β, γ and δ. The essence of the analysis is to find the correct quartets of texts, the analysis of which will lead to finding the secret key. By a correct quartet of texts, we will call a pair of a quartet of open and closed texts (P_1, P_2, P_3, P_4) and (C_1, C_2, C_3, C_4), for which the difference of the sum modulo 2 of the plain text P_1 and P_2, coincides with the difference of the sum modulo 2 of the plaintext P_3 and P_4, and at the same time the sum modulo 2 of the two corresponding closed texts C_1 and C_3 coincides with the difference of the sum mod 2 of the plain text C_2 and C_4. The adversary encrypts a set of plaintext pairs with a difference α and collects quartets that satisfy the requirements $P_1 \oplus P_2 = P_3 \oplus P_4 = \alpha$ and $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$. In this case, the following three conditions must be met, namely [5]:

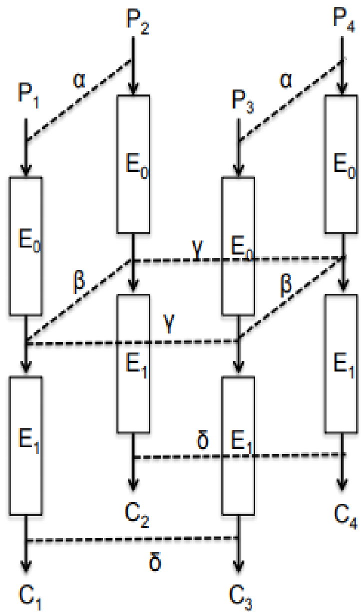

Fig 1. Rectangle-style boomerang

$$E_0(P_1) \oplus E_0(P_2) = E_0(P_3) \oplus E_0(P_4) = \beta,$$

$$(P_1) \oplus E_0(P_3) = \gamma,$$

$$C_1 \oplus C_3 = C_2 \oplus C_4 = \delta.$$

The probability of success of a boomerang attack is determined by a simple estimate $p_0 \geq Pr(\alpha \to \beta) * Pr(\gamma \to \delta) = pq$. It was noted that the probability of p and q can be increased by using multiple characteristic differentials with respect to E_0 and E_1:

$$\hat{p} = \sqrt{\sum\nolimits_{\gamma} Pr^2 (\alpha \to \beta)},$$

$$\hat{q} = \sqrt{\sum\nolimits_{\gamma} Pr^2 (\gamma \to \delta)}.$$

It is known that if the with the length of the encryption block n-bit the in equality is:

$$\hat{p}\hat{q} > 2^{-n/2},$$

then ciphertexts can be distinguished from random texts. Further, the number of correct quartets t is calculated by the formula:

$$t = N^2 2^{-n} \hat{p}^2 \hat{q}^2,$$

where N is the number of plain text quartets.

We consider a truncated version of the analysis of the algorithm: the number of rounds will be two, according to the first round, functions E_0, on the second - E_1. As mentioned above, the "AL01" algorithm uses two primitives: linear – addition 2 modulo (XOR operation) and nonlinear – S-box, which maps one byte to another byte. One round consists of 16 rows, where each byte of the row is defined as the value of the S-box, the input parameter of which is the result of the XOR operation to two bytes of the previous row and the round key. The main primitive that affects the differentials is the S-box. Further, we will consider the change in the differential after each series.

Consider the worst case: the best suitable differential characteristic is when α is the difference between the plaintext P_1 and P_2 is minimal and differs with only one last bit:α=0x00000000000000000000000000000001. Taking into account the algorithm scheme and performing the S-box differential analysis, after each row we obtain the probability of obtaining the necessary characteristics for the analysis (Table 1) [6].

Table 1. Probability of obtaining the necessary characteristics for analysis

Round No	Series	The effective number of unequal S-blocks	Probability
Round 1	Series 1	2	$\frac{4}{256} = 2$
	Series 2	3	2^{-12}
	Series 3	4	2^{-18}
	Series 4	5	2^{-24}
	Series 5	6	2^{-30}
	Series 6	7	2^{-36}
	Series 7	8	2^{-42}
	Series 8	9	2^{-48}
	Series 9	10	2^{-54}
	Series 10	11	2^{-60}
	Series 11	12	2^{-66}
	Series 12	13	2^{-72}
	Series 13	14	2^{-78}
	Series 14	15	2^{-84}
	Series 15	16	2^{-90}
	Series 16	16	2^{-192}
	p- overall probability after Round 1		2^{-192}

We carry out the same procedure for the 2nd round with respect to the suitable differential $E_0(P_1)$ and $E_0(P_3)$. Here, we also assume that the best differential:

$$\gamma = E_0(P_1) \oplus E_0(P_3) = 0x00000000000000000000000000000001.$$

e.g. $E_0(P_1)$ and $E_0(P_3)$ is minimal and differs with only one last bit.

Taking into account the symmetry of E_0 and E_1, we obtain the probability $q = 2^{-192}$. Since the computing power of the computer does not allow us to consider all possible variants of differentials, we restrict ourselves to $\hat{p} = p$ and $\hat{q} = q$.

Therefore, the probability of success of a rectangle-type boomerang attack is extremely small:

$$p_0 \geq Pr(\alpha \to \beta) * Pr(\gamma \to \delta) \approx pq \approx 2^{-392}.$$

Now let us determine the number of required plaintext quartets N to obtain one correct quartet. Assuming that $t = 1$, we calculate

$$N^2 2^{-n} \hat{p}^2 \hat{q}^2 = 1.$$

Since the length of the encryption block is n=128, it follows that $N = 2^{455}$. For at least one correct quartet for two-round "AL01" algorithm will need about 2^{455} quartets plaintext. Given that this estimate is carried out before the two-round algorithm, the subsequent analysis steps do not make sense, since the complexity of the calculation and the number of optimal numbers of correct quartets increase rapidly with increasing rounds.

Conclusion. Summing up, it shows that the complexity of the analysis on two rounds becomes greater than the complexity of a complete search and it makes no sense to apply the analysis. Therefore, it is considered that the proposed "AL01" encryption algorithm is cryptographically resistant to the attack by the boomerang method. Our results showed that the attack poses no threat to the full-round "AL01" algorithm, but helps us understand the differential behavior and its strength in a boomerang attack.

As well as for the method of differential cryptanalysis, the practical application of this attack in terms of computational complexity is strictly limited by high requirements for processing time and data volume. Therefore, the boomerang attack was mainly applied to ciphers with the least number of rounds when evaluating the strength of algorithms. The algorithm is a theoretical achievement of evaluating algorithms.

The presented works were carried out at the expense of the funding of the grant funding project AP08856426 for scientific research for 2020-2022 years "Development and research of an encryption algorithm and creation of a software and hardware complex for its implementation".

Reference:

1. Rostovtsev A. G., Mikhailova N. V. Methods of cryptanalysis of classical ciphers//. A. G. Rostovtsev, N. V. Mikhailova - M.: Nauka, 1995. 208 p.

2. Introduction to Cryptanalysis. Cryptanalysis of symmetric cryptosystems: block ciphers //2012.url:https://docplayer.ru/36057626-Vvedenie-v-kriptoanaliz-kriptoanaliz-simmetrichnyh-kriptosistem-blochnye-shifry.html(in Russian)

3. Report of scientific-research work «Development of software and software-hardware means for cryptographic protection of information during its transmition and storage in general-purpose infocommunication systems and networks», BR05236757, 2020.

4. D. Wagner, The boomerang attack in Fast Software Encryption, FSE'99 (L. R. Knudsen, ed.), vol. 1636 of Lecture Notes in Computer Science, pp. 156–170, Springer-Verlag, 1999.

5. J. Chen, A. Miyaji, Differential Cryptanalysis and Boomerang Cryptanalysis of LBlock, International Conference on Availability, Reliability and Security CD-ARES 2013: Security Engineering and Intelligence Informatics, pp 1-15, volume 8128, Regensburg, Germany, September 2-6, 2013.

6. Dyusenbayev D.S., Sakan K.S., Cryptographic attack on the "Qamal" algorithm using the boomerang method // Materials of the international scientific-practical conference "Actual problems of information security in Kazakhstan". – 2020. – P. 123-129 (in Russian).