Scientific and Practical Cyber Security Journal (SPCSJ) 2(3): 42-46 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

CRYPTOGRAPHIC ANALYSIS OF RIJNDAEL-LIKE CIPHER

Kovalov S., Maslova N., Psel V.
Donetsk National Technical University, Pokrovsk, Ukraine

ABSTRACT. The algorithm of linear-algebraic cryptanalysis of Rijndael-like cipher is proposed. The approach connected with the allocation of round differentials is considered. The description and justification of the algorithm are fulfilled, the requirements are formulated, the general model is described. The parameters for increasing the speed algorithm are specified.

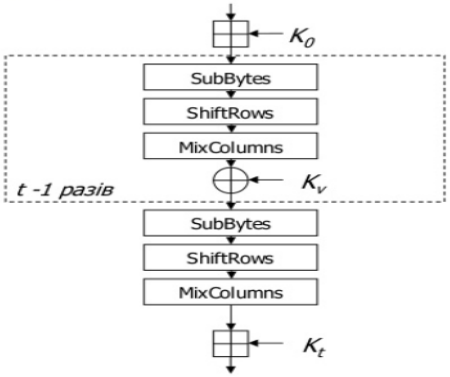
KEYWORDS: Linear Cryptanalysis; Algebraic Cryptanalysis; Differentials; Cipher; Algorithm

INTRODUCTON

The task of analyzing the reliability of cryptographic algorithms is one of the topical problems of information security. In connection with continuously improving technologies, this issue is under the constant supervision of specialists.

In 2015 Ukraine introduced a new national cryptographic standard for the block symmetric conversion of DSTU 7624: 2014 [1]. The standard defines the structure of the Kalyna cipher and the modes of its operation and supports the block size and the length of the encryption key 128, 256 and 512 bits.

The model has a Square-like SPN-structure. Analogues of this structure are used in algorithms AES / Rijndael, Whirlpool, Stribog, Kuznyechik “Grasshopper” block cipher and a number of others. In addition to the block cipher, DSTU 7624: 2014 defines the modes of operation corresponding to ISO 10116: 2006, includes additional features that are oriented to modern cryptographic protection systems, provides for the possibility of effective implementation on most modern software or hardware and software platforms.
At the heart of the standard is a cyclic transformation, built on the basis of tables of substitution (S-blocks) and multiplication by an MDS-matrix over a finite field. Figure 1 shows one of the main cipher blocks - the algorithm of the encryption function [2].



$$T_{l,k}^{(K)} = \eta_l^{(K_t)} \circ \psi_l \circ \tau_l \circ \pi_l' \circ$$
$$\circ \left(\prod_{v=1}^{t-1} \left(\kappa_l^{(K_v)} \circ \psi_l \circ \tau_l \circ \pi_l' \right) \right) \circ \eta_l^{(K_0)}$$

Fig. 1 – The scheme of encryption function of the algorithm Kalyna

The use of this design allows to provide provable cryptographic stability to linear, integral, differential and other types of cryptanalysis [3,4] with 6 cycles for 128-bit, 7 cycles for 256-bit and 9 cycles for 512-bit block. Each additional cycle provides an exponential increase in the complexity of cryptanalysis. The developers of the Kalyna cipher have increased the number of cycles to 10, 14 and 18 for blocks of 128, 256 and 512 bits to provide a guaranteed margin of safety.

Thus, at the present stage the symmetric encryption standard of DSTU 7624: 2014 is resistant to most known types of cryptographic attacks. But taking into account the constant development and improvement of methods of cryptanalysis and the emergence of new types of attacks, works on finding possible vulnerabilities and methods of neutralizing them should continue uninterruptedly.

In the paper it is proposed to consider the possibility of applying, combined linear-algebraic crypto analysis to one of the models of the Kalyna cipher (block length 128, key length 128).

Analysis of cryptographic algorithms requires large computing power, which is not always available to researchers at the initial stages of development. The possibility of timely research to accelerate decision-making processes is often of great importance. Therefore, the option of working out ideas on simplified models, that preserve the main features of the main cipher, is perspective at the initial stages of algorithm development.

For example, the purpose and features of applying a simplified version of the AES-cipher are described in [5]. The authors called the mini-AES cipher and used it to determine the basic characteristics of a complete filter.

There are known [6] studies of a number of cryptographic indices of the "reduced" model of the Kalyna cipher, conducted by the developers of the new standard. An input 16-bit block of plaintext P consisting of a sequence of four nibbles $P = (p_0, p_1, p_2, p_3)$, which is represented as a 2×2 matrix, was taken for the study. The encryption involves all the basic operations of the standard: Sbox, ShiftRows and MixColumns, as well as XORRoundKey and AddRoundKey. Their ordered multiple application to realizations consisting of 4 and 10 cycles is considered.

To obtain the cyclic subkeys, a special procedure was used. The procedure uses the original master key and constant to form three new key states. Then, using the shift procedure, circular keys were generated.

The differential and linear properties of the cipher are investigated. It was concluded that the computational volume for constructing a linear table of approximations turns out to be substantially larger than when determining the maximum of the total differential. It is associated with the bit size of the input to the cipher n as 2^{2n} and performing a full calculation for even a single key and for 16-bit data blocks is computationally difficult [6].

DESCRIPTION OF THE STUDY

Algorithm Kalyna cipher, as well as AES, refers to Rijndael-like codes and is based on operations on polynomials in finite fields. To form the substitution table n_i, which is similar to the S-box substitution table in the AES cipher, the same finite field is used, Gf (2^8), and for the introduction of diffusion, the SP network. Therefore, crypto analysis techniques that are relevant for the AES encryption standard are also applicable for the Kalyna cipher analysis.

For analysis, the basic version of the standard is taken, in which the size of the encryption unit is 128 bits. The key length is the same as the block length. The general form of encryption includes 10 rounds and the use of four main functions of the algorithm. To construct a mathematical model, was used the rules of the algebra of finite fields and the decomposition of polynomials.

The main problem with cryptanalysis of AES cipher is the impossibility of combining several rounds into one due to the operation of decomposing a polynomial over a finite field. A number of crypto analysts, among them Bruce Schneier and Alex Biryukov, created attacks on the cipher, which were based on linear crypto analysis, and showed the speed of 245 operations for a 10-round cipher. But for a fully round AES, they turned out to be weak [7]. However, combining such attacks with an algebraic approach looks very promising, because in this case, the replacement function using the S-box will not just be a "black box", but a full-featured mathematical function that can be simplified.

The goal of the proposed algorithm [8] is to find special truncated differentials that represent the difference between additions modulo 2 and 2^8 [8].

$$(a \oplus b)' = ((a+b)_{mod\ 256} - \partial)' = \frac{a' \otimes b'}{\partial'}, \quad (1)$$

where $\partial = (a+b)_{mod\ 256} - (a \oplus b)$

Suppose that round keys, open text and differentials are in some way interconnected. Each byte of the key is added to the cipher repeatedly (see Figure 1). The plain text bytes that were encrypted in the previous round each time are different. The differential is also different. If, say, in the round i, the differential dif is equal to d, which corresponds to one of the set of key bytes Ki, and in the round j of dif will equal e, which corresponds to one of the set of key bytes Kj, then the byte of the resultant key will lie on the intersection of the sets Ki and Kj. As a result of multiple intersection of resulting sets, we get all the required bytes of the key.

Differentials, as the difference between the sum modulo 2^8 and the sum modulo 2 between certain key bytes and plain text, will be sorted in ascending order. This is due to the fact that the zero differential has a high probability of appearance, as shown in Figure 2.

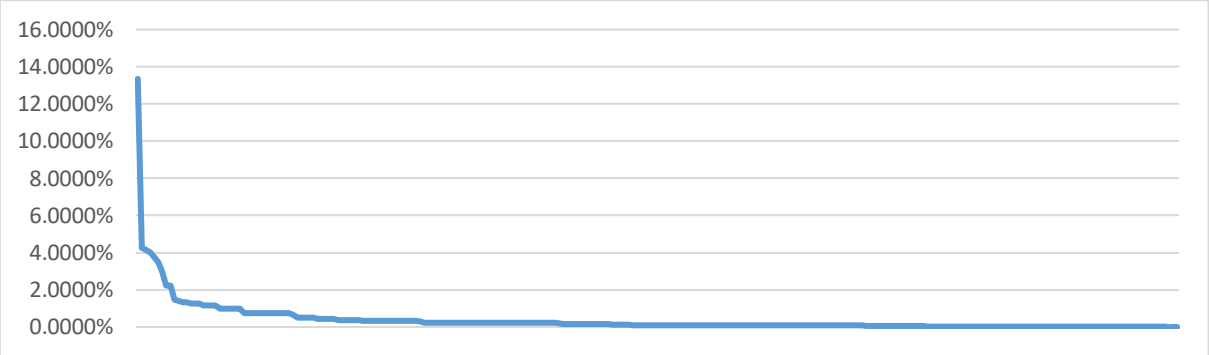


Fig. 2 – Range of frequencies used differentials

In addition, for each of the plain text bytes, not all differentials can exist in principle, and therefore they will not need to be checked. For example, for the plain text byte 0x38, the value dif = 0 will occur for as many as 32 key variants, the value of the differential equal to one of the elements of the set {16, 32, 48, 64, 80, 96, 112} will occur 24 times, whereas the value of {240, -224, - 208, -192, -176, -160, -144} - 8 times, which in total gives the expected 256 different bytes of the key. As a result, instead of 256 key values, you should check only 15 differentials.

In all, for all possible plain text - key pairs, 255 variants of different differentials are possible, and, it should be noted, these differentials can only be even numbers.

So, the introduction of operation (1) in a number of cases makes it possible to increase the effectiveness of the attack. If the probability of finding each of the bytes is 1/256, then the probability of occurrence of the 0th differential will be 10-14%. Finding such a differential for each of the rounds, and knowing the plain text and the encrypted text, you can find the key.

The algorithm for constructing the list of differentials requirements:
- the possibility for one iteration to obtain the differential for the selected byte and vice versa, to find the next byte corresponding to the chosen differential;
- the ability to quickly move to the next differential in the list;
- the order of the list of differentials in descending probability of its appearance.

The general model of the algorithm is as follows:
1. For each byte of plain text, select possible differentials, and order them in the descending order of probability.

2. Select the first of the array of differentials obtained and find the corresponding possible variants of the encrypted text for it. Is necessary save the possible keys for this purpose.
3. Take the received byte of the encrypted text as a plain text option and in the next round select the possible differentials and their corresponding keys.
4. From the entire list of keys for the second round, leave only those keys that are obtained from the other bytes of the other rounds.
5. Repeat this operation until the encryption rounds are over (in this case, if there is one key left - it is correct, if we have several keys left, we will just check them for the correctness of the search on other pairs of encrypted - plain text). If no keys remain, select the next possible differential and repeat steps 2-5.
The operation is repeated until we find the desired key

CONCLUSIONS

So, the algorithm of linear-algebraic crypto analysis of Rijndael-like cipher Kalyna is proposed. The approach connected with the allocation of round differentials is considered.
It is argued that this algorithm has higher performance (in comparison with direct search) for the following reasons:
some keys are excluded from the list of available ones before all rounds of encryption are completed, becouse its are impossible for the selected differentials;

- the differentials are sorted in order of decreasing probability of their appearance, due to which the first differentials cover the maximum possible set of possible keys;
- the keys that remain after the completion of the round-trip search, are no verified.

The demonstrated approach significantly reduces the computational complexity of the procedure of direct search with $2^{8^{16}} = 2^{128}$ (for 16 bytes) to $2^{8^{15}} = 2^{120}$operations. If we consider that in each of the block lines is enough to find all the keys except the last, then the complexity of such an attack on the cipher will be no more $2^{8^{12}} = 2^{96}$ operations.

REFERENCES

1. Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev, Oleksandr Kuznetsov, Yurii Gorbenko, Oleksandr Dyrda, Viktor Dolgov, Andrii Pushkaryov, Ruslan Mordvinov, Dmytro Kaidalov. DSTU 7624:2014. National Standard of Ukraine. Information technologies. Cryptographic Data Security. Symmetric block transformation algorithm. Ministry of Economical Development and Trade of Ukraine, 2015 (in Ukrainian)

2. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. https://eprint.iacr.org/2015/650.pdf

3. Принципи побудови і основні властивості нового національного стандарту блокового шифрування України / Р. Олійников, І. Горбенко, О. Казимиров, В. Руженцев, Ю. Горбенко // Захист інформації, том 17, №2, квітень-червень 2015, С.142-157

4. Казимиров А.В. Алгебраические свойства схемы разворачивания ключей блочного симметричного шифра «Калина» / А.В.Казимиров, Р.В.Олейников // Радіоелектронні і комп'ютерні системи, 2010б №5(46), С.61-66, https://www.khai.edu/csp/nauchportal/Arhiv/REKS/2010/REKS510/Kazimir.pdf

5. Raphael Chung-Wei Phan, Mini Advanced Encryption Standard (Mini-AES): A Tested for Cryptanalysis Students, Cryptologia, XXVI (4), 2002

6. Долгов В.И. Криптографические свойства уменьшенной версии шифра «Калина» / В.И.Долгов, Р.В. Олейников, А.Ю. Большаков, А.В. Григорьев, Е.В. Дробатько // Прикладная радиоэлектроника, 2010, Том 9, № 3, С.349-354

7. Alex Biryukov and Dmitry Khovratovich. Related-key Cryptanalysis of the Full AES-192 and AES-256 / Biryukov A., Khovratovich D. // University of Luxemburg.

8. Псьол В. О. Алгебраїчний аналіз шифрів, оснований на криптографічних перетвореннях в алгебрі полів Галуа / В. О. Псьол, Н. О. Маслова // Матеріали сьомої міжнародної науково-технічної конференції «Моделювання і комп'ютерна графіка» (МіКГ-2017). – С. 108–111