NOVATEUR PUBLICATIONS
JournalNX- A Multidisciplinary Peer Reviewed Journal
ISSN No: 2581 - 4230
VOLUME 6, ISSUE 5, May -2020

DEVELOPMENT OF A MODEL FOR APPLYING CORRELATION CRYPTANALYSIS TO FILTERING GENERATORS

ABDURAKHIMOV BAKHTIYOR FAYZIEVICH
Professor, Doctor of Physics and Mathematics,
National university of Uzbekistan,
+998935143137, a_bakhtiyor@mail.ru

BOYKUZIEV ILKHOM MARDANAKULOVICH
PhD Student, National university of Uzbekistan,
+998909779300, salyut2017@gmail.com

SHONAZAROV SOATMUROD KULMURODOVICH
Teacher, Termez state university,
+998996760166, sshoh1989@mail.ru

ZIYAKULOVA SHAKHNOZA ABDURASULOVNA
Teacher, Termez state university,
+998905208923, shahnozaziyaqulova@gmail.com

ABSTRACT:

This article is devoted to problems of cryptanalysis. Cryptographic analysis results, got from using of correlation cryptanalysis method to algorithm of the flow crypto operation, founded on register of the shift with feedback, were presented in work. For estimation of the flow crypto operation algorithm's crypto stability by correlation cryptanalysis method, number of important tasks was defined, purposes and problems of the study were determined. As a result of defined tasks decision, mathematical model and software of correlation cryptanalysis method to flow crypto operation to filtering LILI-128 – were developed. Results has shown, that characteristic of correlation immunity of filtering functions, used in filtering generator, provide stability to correlation cryptanalysis method. Execution with big probability of stat-analogical function, defined in process of cryptanalysis, raises the efficiency of cryptanalysis.

Proposed mathematical model and software can be used for estimation of stability of the algorithm of the flow crypto operation to correlation cryptanalysis, as well as in scholastic purpose.

KEYWORDS: cryptanalysis, stream ciphers, shift registers, LILI-128, filtering, correlation

INTRODUCTION:

Ensuring information security requires relatively fast cryptographic tools, not only as the exchange of documentary information transmitted over the network increases, but also as the exchange of multimedia, that is, video and audio, increases. Therefore, the use of stream encryption algorithms in local and global networks has become an urgent problem[1,2].

When analyzing stream encryption algorithms, in contrast to block encryption algorithms, although many original ideas and directions for creating stream encryption cryptographic algorithms were developed in this area, there is no single way to express their commonality[3].

Therefore, it is important to conduct research in the field of continuous encryption algorithms and modern methods for assessing their cryptographic strength.

Due to the design features of continuous encryption algorithms, the most common type of attack is a correlation attack. If a non-linear function transfers information about its internal components to the output, the work required to open such a system is greatly reduced. However, such a function is always available[4]. According to this axiom, correlation attacks use the correlation between a sequence leaving an encryption scheme and a sequence leaving registers[5,6,7].

METHODOLOGY:

2.0 Correlation cryptanalysis method for filter generators

There are several methods of correlation cryptanalysis applied to continuous encryption algorithms based on filter generators. Underlying these approaches is the use of linear statanalogs of the filtering function.

Suppose that in a filter generator there is a linear feedback shift register of length n, $\varphi(x_1,...,x_n) = c_n x_1 \oplus … \oplus c_1 x_n$ is the feedback function of the register, $C(D) = c_n D^n \oplus … \oplus c_1 D \oplus 1$ is its characteristic multiplication, and f $(x_1,...,x_n)$ is a filtering function, let the linear statanology of the function f(x) be $l(x) = x_{i1} \oplus x_{i2} \oplus … \oplus x_{ik} \oplus b$. The probability that the function f (x) and its statonology coincide with l(x) is: Prob{f(x) = l(x)} = 1/2 + a/2 [5]. Where $a = \max_{v \in Z_2^n} |S'f\,(v)|$ – is the maximum value of the normalized modulus of the Fourier coefficient. We call this given generator 1st generator. Filter generator with a similar shift register, but with a filter function l(x). This generator is called the 2nd generator. The following symbols {y(t)} and {y'(t)} denote the output sequences generated by the generators 1 and 2, respectively, when the initial filled state is the same (Figure 1).

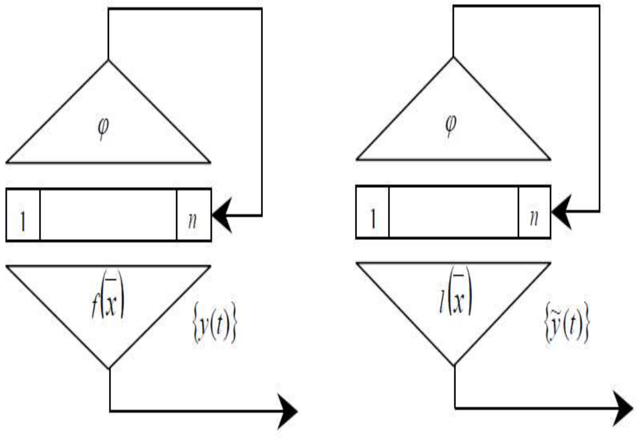

Figure 1. Scheme of 1st and 2nd generators

$l(x) = x_{i1} \oplus x_{i2} \oplus … \oplus x_{ik} \oplus b$ depending on the value of the free variable b (b =0 ва b = 1) in linear stanology, the operation of the 2nd generator can be expressed using one of the schemes shown in the figure 2.

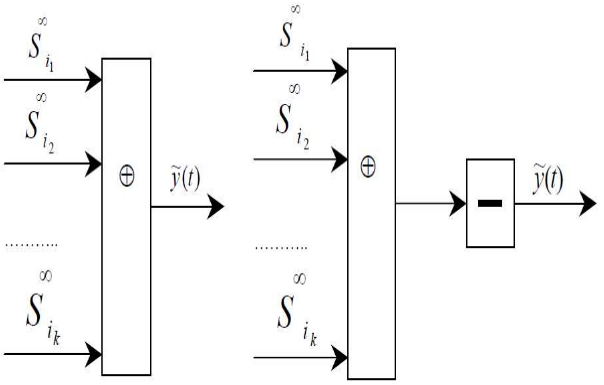

Figure 2. Operating status of 2nd generator

The series S_{ij}^{∞}} are different recurrence sequences formed by one shift register with a feedback function $\varphi(x_1,...,x_n)$, length n. From the known results on the linear complexity of the sum of linear recurrence sequences and the linear complexity of inverted sequences, it can be seen that the length of the sequence {y'(t)} is n, and the feedback function is still equal to $\varphi(x_1,...,x_n) = c_n x_1 \oplus … \oplus c_1 x_n$ or length n + 1 and multiplication of the characteristic

$C'(D) = c_n D^{n+1} \oplus (c_n \oplus c_{n-1}) D^n \oplus (c_{n-1} \oplus c_{n-2}) D^{n-1} \oplus … \oplus (c_2 \oplus c_1) D^2 \oplus (c_1 \oplus 1) D \oplus 1$ (1)

which is made using offset sizes. Where c_i is the coefficient of the feedback $\varphi(x_1,...,x_n)$ function.

Thus, instead of the 2nd generator, we can take a look at the equivalent 3-generator (Figure 3). Therefore, in the case b = 0, the register length is L=n, and the feedback function is φ'(x) = φ(x), and in the case b = 1, the register length is L=n+1, and the coefficient of the feedback function C'(D) is determined from the characteristic coefficient of the polynomial. Then the output sequences of 2nd generators and 3rd generators coincide and are equal to {y'(t)}, and then the following equation holds for the elements of the output sequences of 1st generators and 2nd generators: Prob{ y(t)= y'(t)} = 1/2 + a/2.

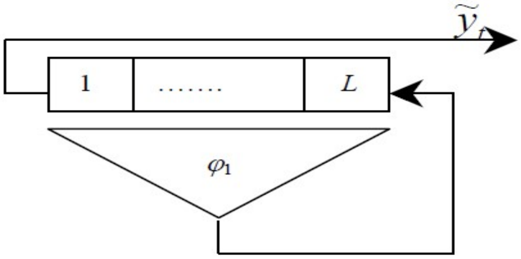

Figure 3. Scheme of generator 3

If the 1st generator is used to encrypt some “ordinary” information and the parameter a is large enough, the 3rd generator can be used as a decoder, and errors can be eliminated depending on the capabilities of the language.

Consider a situation that has the form: The feedback function of the above approach the 1st generator $\varphi(x_1,...,x_n)$ is unknown, and the filter function f(x) is as follows: $f(x_1,...,xn) = x_1*x_2*…*x_m \oplus x_{m+1} \oplus x_{m+2} \oplus … \oplus x_n$.
Where m ≤ n, n is the length of the displacement dimensions. The linear statonology of the function f(x) is the function $l(x_{m+1},…,x_n) = x_{m+1} \oplus x_{m+2} \oplus … \oplus x_n$ with the probability of coincidence $\text{Prob}\{f(x) = l(x)\} = 1 - 2^{-m}$. In particular, for m ≥ 5, the probability is Prob{f(x) = l(x)} > 0,969.

Thus, if the filtering function f(x) in a 1st generator is replaced by its linear statistical analog, the resulting 2nd generator is equivalent to a 3rd generator, i.e. there is an n-length shift register with the same feedback function as before. In this case, the bits of the output sequence {y'(t)} of the 3rd generator correspond to the bits of the sequence {y(t)} with a probability of $1 – 2^{-m}$. In this case, assuming that all 2n bits of the sequence {y(t)} correspond to bits of the sequence {y'(t)}, we can construct a feedback linear displacement register (3rd generator) at the output of the 1st generator. Then this generator is used as a decoder with the correct decryption probability of $1 – 2^{-m}$. Therefore, if the function f(x) has certain properties, the operation of the 1st generator can be completely restored, that is, the unknown feedback function and the initial state of the register can be determined. As a rule, to assess the reliability of the continuous encryption algorithm, the cryptanalyst is informed about the gamma sequence and internal structure of the generator, which come from a generator of a certain length. That is, the length of the register used in the generator, the feedback, and the appearance of the filter function are known.

Based on this, using the two above approaches, the method of correlation cryptanalysis is applied to the filter generator as follows.

Example 1. Let the above 1 be a generator (Figure 4). It is known that this generator has an offset register of length 7 and a filter function f(x) as follows:

$$f(x) = x_1 \oplus x_2 * x_3 * x_4 * x_5 * x_6 \oplus x_7$$

The φ feedback function is as follows:

$$\varphi(x_1,…,x_7) = x_1 \oplus x_2 \oplus x_3 \oplus x_6$$

The initial filled state of the generator is unknown.

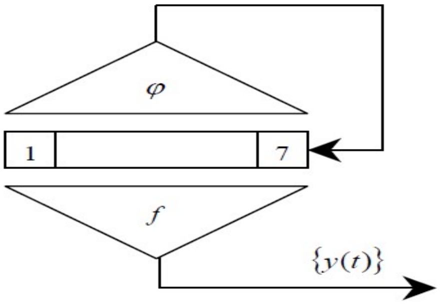

Figure 4. Filtering generator

However, at least 14 consecutive bits of the output sequence {y(t)} are specified, let be: 00101001110010. The purpose of the analysis is to find the initial state of the register.

The linear statanology of the filter function f(x) is the function $l(x) = x_1 \oplus x_7$. Since m = 5 for this function, the probability of matching the filtering function f(x) and its linear statanology is $P\{f(x) = l(x)\} = 1–2^{-m} = 1 – 2^{-5} \approx 0{,}969$. In this case, the length of the register of the generator 2 corresponds to the length of the register of the generator 1, which is equal to 7. Therefore, the bit of the output sequence of the 2nd generator {y'(t)} corresponds to the corresponding bit of the output sequence of the 1st generator {y(t)} with a probability $p = 1 – 2^{-5} \approx 0{,}969$.

Feedback function of the 2nd generator is $\varphi(x_1,\dots,x_7) = x_1 \oplus x_2 \oplus x_3 \oplus x_6$. Accordingly, its characteristic multiplicity is as follows:

$$C(D) = D^7 \oplus D^6 \oplus D^5 \oplus D^2 \oplus 1 \qquad (2)$$

In this case, it is possible to completely restore the full operation of the 1st generator, that is, the initial state of the registers. To do this, it is used to coordinate the entire internal state of the shift register in the 2nd generator (including the initial filled state) with the corresponding internal state of the register in the 1st generator. The sequence leaving the 2nd generator is the sequence {y'(t)}. In this case, all 14 bits of the sequence {y'(t)} correspond to the corresponding bits of the sequence {y(t)}, and corresponds to register filling in the 2nd generator at time t $x(t) = (x_t, x_{t+1},\dots,x_{t+6})$, we get:

$$y(t) = y'(t) = l(x(t)) = l(x_t, x_{t+1},\dots,x_{t+6}) = x_t \oplus x_{t+6} \qquad (3)$$

However, for all t > 6, the following recurrence expression is suitable in accordance with $\varphi(x_1,\dots,x_7) = x_1 \oplus x_2 \oplus x_3 \oplus x_6$: $x_t = x_{t-7} \oplus x_{t-6} \oplus x_{t-5} \oplus x_{t-2}$.

The result is a system of linear equations that determines the initial values $x_0, \dots , x_6$ of 1st and 2nd generators.

The output bits of the 2nd generator sequence y'(t) are calculated using a linear filter $l(x) = x_1 \oplus x_7$.

Thus, the following system of equations (4) is suitable:

$$\begin{aligned} x_0 \oplus x_6 &= 0;\\ x_1 \oplus x_7 &= 0;\\ x_2 \oplus x_8 &= 1;\\ x_3 \oplus x_9 &= 0; \qquad (4)\\ x_4 \oplus x_{10} &= 1;\\ x_5 \oplus x_{11} &= 0;\\ x_6 \oplus x_{12} &= 0. \end{aligned}$$

Выражая значения $x_7 ,\dots, x_{12}$ через $x_0 ,\dots, x_6$, можно создать следующую систему уравнений (5):

$$\begin{aligned} &x_7 = x_0 \oplus x_1 \oplus x_2 \oplus x_5 ;\\ &x_8 = x_1 \oplus x_2 \oplus x_3 \oplus x_6 ;\\ &x_9 = x_2 \oplus x_3 \oplus x_4 \oplus x_7 = x_2 \oplus x_3 \oplus x_4 \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_5 = x_3 \oplus x_4 \oplus x_0 \oplus x_1 \oplus x_5;\\ &x_{10} = x_3 \oplus x_4 \oplus x_5 \oplus x_8 = x_3 \oplus x_4 \oplus x_5 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_6 = x_4 \oplus x_5 \oplus x_1 \oplus x_2 \oplus x_6;\\ &x_{11} = x_4 \oplus x_5 \oplus x_6 \oplus x_9 = x_4 \oplus x_5 \oplus x_6 \oplus x_3 \oplus x_4 \oplus x_0 \oplus x_1 \oplus x_5 = x_6 \oplus x_3 \oplus x_0 \oplus x_1; \quad (5)\\ &x_{12} = x_5 \oplus x_6 \oplus x_7 \oplus x_{10} = x_5 \oplus x_6 \oplus x_7 \oplus x_{10} = x_5 \oplus x_6 \oplus x_7 \oplus x_4 \oplus x_5 \oplus x_1 \oplus x_2 \oplus x_6 =\\ &= x_7 \oplus x_4 \oplus x_1 \oplus x_2 = x_0 \oplus x_1 \oplus x_2 \oplus x_5 \oplus x_4 \oplus x_1 \oplus x_2 = x_0 \oplus x_5 \oplus x_4. \end{aligned}$$

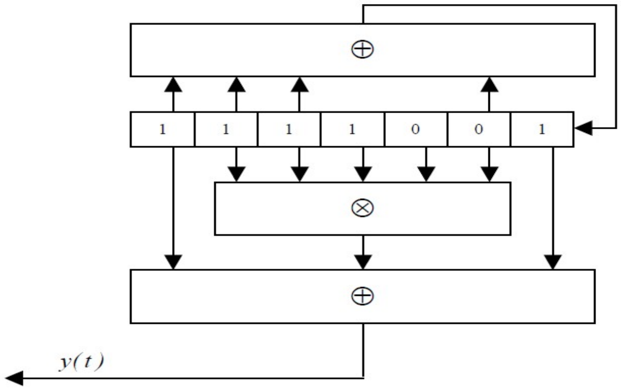

Figure 5. Generator filter's structure

As a result, we have a system of linear equations (6) that connects the values $x_0, \dots, x_6$ with the initial signs y'(t).

$x_0 \oplus x_6 = 0;$

$x_0 \oplus x_2 \oplus x_5 = 0;$

$x_1 \oplus x_3 \oplus x_6 = 1;$

$x_0 \oplus x_1 \oplus x_4 \oplus x_5 = 0;$ (6)

$x_1 \oplus x_2 \oplus x_5 \oplus x_6 = 1;$

$x_0 \oplus x_1 \oplus x_3 \oplus x_5 \oplus x_6 = 0;$

$x_0 \oplus x_4 \oplus x_5 \oplus x_6 = 0.$

Solving these equations, unknown values can be determined as follows: $x_0 = 1$, $x_1 = 1$, $x_2 = 1$, $x_3 = 1$, $x_4 = 0$, $x_5 = 0$, $x_6 = 1$. Therefore, the initial position of the shift register in the 1st generator is (1111001). After checking, can see that the result is correct. As a result, the initial circuit of generator 1 will be as shown in Figure 5.

2.2 Using correlation immunistic function in filter generators

The use of the correlation-immune function as a filtering function in filtering generators does not significantly affect the complexity of cryptanalysis. This is because filter generators use a single register.

Theorem 1. Assume that the key current generator is a filter generator that uses the Boolean function of correlation immunity as a filter function. In this case, it is possible to create a filter generator that has the same shift register (that is, the register length and feedback function are the same), but the filter function is not correlation-immune, in which the developed sequence corresponds to the output sequence from the primary generator (initial state register will be different) [5].

Proof. Suppose that the length of the register of the primary generator is n, the feedback function is $\varphi(x_1,\dots,x_n) = c_n x_1 \oplus \dots \oplus c_1 x_n$, and the filter function is $f(x_1,\dots,x_n)$. x_t is the state in which the first register cell is filled at time t, y_t is the symbol of the output sequence generated from the original generator at the same time. In this case, the internal state of the displacement register at time t is $X(t) = (x_t, x_{t+1}, \dots, x_{t+n-1})$, and the resulting sequence is $y_t = f(x_t, x_{t+1}, \dots, x_{t+n-1}) = f(X(t))$.

In this case, the vector $X(t+1) = (x_{t+1}, x_{t+2}, \dots, x_{t+n})$ corresponding to the internal state of the register at the next instant of time is related to the vector X(t) by the following relation: $X(t+1) = (x_{t+1}, x_{t+2}, \dots, x_{t+n}) = A^* X(t)$.

Where the matrix A (n x n) looks like this:

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ c_n & c_{n-1} & c_{n-2} & \dots & c_2 & c_1 \end{pmatrix} \quad (7)$$

Then $X(t) = A^* X(0)$, where X(0) is the initial state of the shift register.

Therefore, $g(x_1,\dots,x_n)$ is a construction of a function that is not related to correlation, and the initial state of the register can be chosen so that a filter generator with the same offset sizes and filter function $g(x_1,\dots,x_n)$ creates the same sequence as the original generator. To do this, we need to find a matrix D of size (n x n), firstly, this matrix must be connected with the matrix A, and secondly, the function $f(D^{-1}X)$, $X = (x_1,\dots,x_n)$ is not must be correlation-immune. As such a matrix, we can choose a polynomial matrix from the matrix:

$$D = d_0E + d_1A + d_2A^2 + \dots + d_kA^k. \quad (8)$$

In this case, we consider a filter generator with the same shift register as before, but with the filter function $g(x_1,\dots,x_n) = f(D^{-1}X)$ and the initial state $X' = D^*X(0)$. If we define the internal state vector of the generator generated by X'(t) at time t, then $X'(t) = D^*X(t)$. Since both generators use the same feedback function and the matrices A and D are interconnected, we can obtain the following equation: $X'(t) = A^t {}^*X'(0)=A^{t*}D^*X(0)=D^*A^{t*}X(0)= D^*X(t)$. The output sequence of the new generator at time t is: $z_t = g(X'(t)) = f(D^{-1} X'(t)) = f(D^{-1}DX(t)) = f(X(t)) = y_t$.

As we can see, both generators work the same way, so cryptanalysis of the second generator (with the function of non-immune correlation filtering) leads to cryptanalysis of the primary cryptosystem.

2.3 Correlation cryptanalysis method for algorithm LILI -128

The LILI-128 algorithm is a continuous synchronous cipher based on classic controlled shift registers[5,12]. The generator can be divided into two subsystems based on the functions they perform: the clock control subsystem and data generation subsystem.

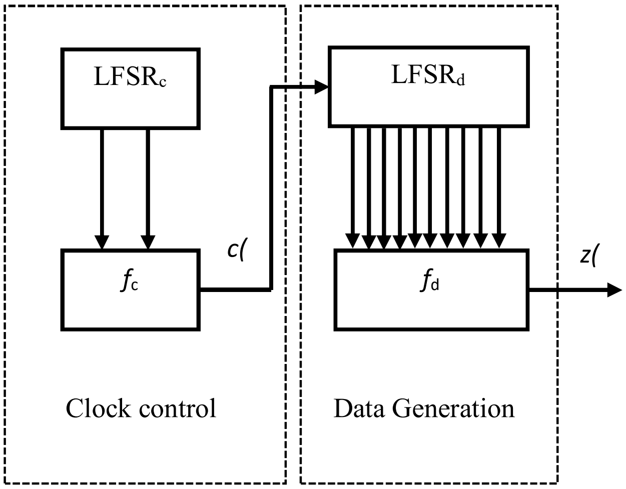

Figure 6. Overview of LILI-128 keystream generators

The length of the control register is L_c = 39 bits, f_c - the function is as follows: $f_c(x_{12}, x_{20}) = 2(x_{12}) + x_{20} + 1$
The feedback polynomial of the $LFSR_c$ is chosen to be the primitive polynomial: $h(x) = x^{39} + x^{35} + x^{33} + x^{31} + x^{17} + x^{15} + x^{14} + x^2 + 1$.

The length of the $LFSR_d$ register is L_d= 89 bits, The feedback polynomial of $LFSR_d$ is given as follows:: $h(x) = x^{89} + x^{83} + x^{80} + x^{55} + x^{53} + x^{42} + x^{39} + x + 1$.

The filtering function of the LILI-128 algorithm is kept secret. The input to the filter function includes values in 10 cells (0, 1, 3, 7, 12, 20, 30, 44, 65, 80) of the $LFSR_d$ register.

The LILI-128 algorithm participated in the NESSIE European competition, in which it was found that the complexity of its evaluation by the method of correlation cryptanalysis is 2^{71}. To carry out the method of correlation cryptanalysis discussed above and to obtain certain results, we work without looking at the subsystem for controlling the movement of the circuit.

Since the filter function of the LILI-128 algorithm is hidden, we must choose the filter function ourselves. The degree of nonlinearity of this filter function must be non-zero. The reason is that if the degree of non-linearity of the function is zero, its initial state can be determined, since the number of registers is equal to one. For this reason, the degree of nonlinearity as a filtering function is different from zero, and it is recommended to use a correlated immunistic function. One of these functions is the following function:

$$f(x) = x_9 \oplus x_{24} \oplus x_{45} * x_{59} * x_{49} * x_{77} * x_{82} * x_{86} * x_{88} \oplus x_{89}$$

Therefore, in this case, the method of correlation cryptanalysis for the filter generator can be applied in the sequence of steps described in Example 1.

RESULTS:

Summarizing the above results, in general, we can propose a model for applying the method of correlation cryptanalysis for filtering stream encryption algorithms.

In general, the method of correlation cryptanalysis for filtering stream encryption algorithms is based on the following sequence of steps:

Step 1. The combination function used in the continuous encryption algorithm is the degree of nonlinearity. If the nonlinearity level is zero, the function used is considered intolerable. Otherwise the second step is taken;

Step 2. The correlation immunity levels of the combining function used in the continuous encryption algorithm are. If the correlation immunity level is zero, the function used is considered intolerable. Otherwise proceed to the third step;

Step 3. All available statanalog functions of the combinatorial function are searched. Statanalog is selected from the features that are linear;

Step 4. Using the statanalog function as a filtering function, a system of linear equations is constructed using the known gammas and feedback polynomials;

Step 5. By solving a system of structured linear equations, the initial state of the register is determined.

CONCLUSION:

In general, several factors influence the application of the method of correlation cryptanalysis to continuous encryption algorithms with a filtering generator.

The use of the correlation immunization function as a filter function in filter generators cannot completely exclude the implementation of the correlation cryptanalysis method.

The use of the immunization function with non-zero correlation in filtering generators increases the generator's resistance to the method of correlation cryptanalysis.

REFERENCES:

1) Stallings V. Cryptography and network protection: principe and practice. - M., Ed. Williams House, 2001. - 672 p.
2) Shannon K. Communication Theory in Secret Systems // In the book. Works on information theory and cybernetics. - M., IL, 1963.
3) Xarin Y.S., Bernik V.I., Matveyev G.V., Agiyevich S.V. Mathematical and computer foundations of cryptology: a Training manual. - Minsk, LLC New knowledge, 2003. - 382 p.
4) Asoskov A.V., Ivanov M.A. Stream ciphers, M: Kudits-Obraz, 2003, 336 p.
5) Gorbenko I.P., Potiy A.V., Izbenko Y.A. Analysis of stream encryption schemes presented at the NESSIE European contest. Harkov National University of Radio Electronics, 2005. - 17 p.
6) Jukov A.YE. Strength analysis of stream encryption systems. The manual on the course "Cryptographic Methods of Protecting Information." Moscow State Technical University. 2003.– 23 p.
7) Stasev Y.V, Potiy A.V, Izbenko Y.A. The study of cryptanalysis methods for stream ciphers. Taganrog: Izvestiya TRTU, 2005, - 250 p.
8) Akbarov D.YE. Cryptographic methods of information security and their application. - Tashkent, “Uzbekistan Markasi” publishing house, 2009. - 432 p.
9) Ivanov M. Cryptographic methods of storing information in computer systems and networks. - M., «Kudits-Obraz», 2001, - 368 p.
10) Babenko L.K, Ishukova YE.A. Differential cryptanalysis potochnix cipher. Izvestiya YuFU, 2009. 232 - 238 p.
11) Shnayyer B. Applied cryptography. Protocols, algorithms, source texts in C language. - M., Ed. TRIUMPH, 2003 .-- 816 b.
12) http://www.cryptonessie.org.
13) http://www.cryptography.ru.