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 COMBINATORIAL 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 discusses the application of the method of correlation cryptanalysis for stream encryption algorithms based on shift registers with feedback. To evaluate the cryptographic stability of the stream encryption algorithm by the method of correlation cryptanalysis, the correlation cryptanalysis method was applied to the Geffe combinatorial algorithm, stream encryption algorithm A5, and a mathematical model was developed to apply the correlation cryptanalysis method to combinatorial generators. This model serves as the basis for evaluating the stream encryption algorithm by the method of correlation cryptanalysis.

KEYWORDS: stream ciphers, shift registers, adder, Geffe, A5, register, primitive polynomial, correlation

INTRODUCTION:

The fact that electronic information exchange is becoming the main means of exchanging documents requires the connection of computer systems to a local network or the global Internet. The security of organizations and individuals connected to the network depends on the level of security of information transmitted on the network. 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].

Unlike block ciphers, stream ciphers prevent encryption of information about each element of the information stream in the cryptosystem, and the main advantage is high-speed encryption of information close to the access speed. Therefore, continuous ciphers allow real-time encryption and transmission without delay, regardless of the amount of information, flow rate.

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:

2.1 Application of the method of correlation cryptanalysis to the Geffe generator

The cryptanalysis process is based on the search for the initial state of the generator registers, that is, the key, with the sequence leaving the generator.

The main idea, principles and application of the method of correlation cryptanalysis for combined generators can be seen on the example of this cryptanalysis method.

This generator was proposed by P.R.Geffe in 1973 and is based on a 3-line shift feedback register. The length of the generator shift registers should be simple, and the polynomial feedback should be primitive.

When applying the method of correlation cryptanalysis to the Geffe generator, the main goal of the analysis process is to find the secret key, which is part of the key sequence generated by the generator. For this, a statistical function is used. The statonology of a function is a function whose outputs correspond to the outputs of a given function with a certain probability. When a function looks like this: $f(x_1,...,x_n) = x_1*x_2*...*x_m \oplus x_{m+1} \oplus x_{m+2} \oplus...\oplus x_n$ (here, m ≤ n, n – dimension length shift register), linear statanalog function f(x) with probability

$$P\{f(x) = l(x)\} = 1 - 2^{-m} \quad (1)$$

function $l(x_{m+1},...,x_n) = x_{m+1} \oplus x_{m+2} \oplus...\oplus x_n$.

$f(x_1,x_2,x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3$ - combining function of a Geffe generator. In any case, the probability of coincidence function f (x) and its statistics $l_i(x)$ equally: $P\{f(x) = l(x)\} = 1 - 2^{-m} = 1 - 2^{-2} = 3/4$. Linear statonology of this function $l_i(x)$ are the following functions x_1, x_3, $x_2 \oplus x_3$ and $x_1 \oplus x_2 \oplus 1$. The definition of a linear statistical analog of these functions by the probability of convergence is given in table 1. In this table, the values of l_i are highlighted, which overlap with the values of the function f (x).

Table 1.

x_1	x_2	x_3	$f = x_1x_2 \oplus x_2x_3 \oplus x_3$	$l_1 = x_1$	$l_2 = x_3$	$l_3 = x_2 \oplus x_3$	$l_4 = x_1 \oplus x_2 \oplus 1$
0	0	0	0	**0**	**0**	**0**	1
0	0	1	1	0	**1**	**1**	**1**
0	1	0	0	**0**	**0**	1	**0**
0	1	1	0	**0**	1	**0**	**0**
1	0	0	0	1	**0**	**0**	**0**
1	0	1	1	**1**	**1**	**1**	0
1	1	0	1	**1**	0	**1**	**1**
1	1	1	1	**1**	**1**	0	**1**

Example 1. Define the statanological function of a function $f(x_1,x_2,x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3$.

The truth table of function $f(x_1,x_2,x_3)$ выглядит следующим образом: $S(f) = \{0,1,0,0,0,1,1,1\}$. According to expression 1, the function and its statonology correspond to probability 3/4. Therefore, we consider a function whose truth table S '(f) = {0,1,1,0,0,1,1,0,0} corresponds to S (f) with a

probability of 3/4. The algebraic normal form (ANF) of this function is constructed as follows:

l: $\neg x_1 \neg x_2 x_3 + \neg x_1 x_2 \neg x_3 + x_1 \neg x_2 x_3 + x_1 x_2 \neg x_3 = (x_1+1)(x_2+1)x_3+(x_1+1)(x_3+1)\ x_2 + (x_2+1)x_1 x_3 + + x_1 x_2 (x_3+1) = x_1 x_2 x_3 + x_2 x_3 + x_1 x_3 + x_3 + x_1 x_2 x_3 + x_2 x_3 + x_1 x_2 + x_2 + x_1 x_2 x_3 + x_1 x_3 + x_1 x_2 x_3 + + x_1 x_2 =$ **$x_2 + x_3$**.

It turns out that the statanological function of the function $f(x_1,x_2,x_3)$ is $l=x_2 \oplus x_3$.

It should be noted that finding the secret key of the Geffe generator requires consideration of the O(2L1+L2+L3) options by finding all possible key options, where L_i is the length of the corresponding registers.

The following possible model of the Geffe generator operation is considered. At each time t at the input of the function $f(x_1,x_2,x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3$ free random variables $x_1(t)$, $x_2(t)$, $x_3(t)$ are set, each of which takes values 0 and 1 with equal probability. Then the quantity $k(t) = f(x_1(t), x_2(t), x_3(t))$ is a random variable, and the probability of its coincidence with $x_1(t)$ and $x_3(t)$, respectively, expression 1, is $P\{k(t) = x_1(t)\} = P\{k(t) = x_3(t)\} = 3/4$. However, for all $\tau \neq t$ $P\{k(t) = x_1(\tau)\} = Prob\{k(t) = x_3(\tau)\} = ½$ if $|\tau - t|$ less than the length of the period of the sequences from LFSR-1 and LFSR-3.

This hypothesis is a fairly accurate representation of the pseudo-random property of a sequence derived from a linear feedback shift register[5,16].

Based on this assumption, it is possible to determine the initial state of each register independently of each other. The first step is to check all the initial variations of the first register. For all these variants with the t -bit of the output sequence generated using this register and the initial value, the frequency of coincidence of the output sequence k(t) of the generator known to us is calculated.

If the coincidence frequency is less than the indicated value C, then this initial filling is not accepted, but if it is large, it is added to the list of possible options. The value of the C-boundary value is determined by certain statistical methods. The initial state of the third register is also determined similarly to the first register.

The initial state of the second register is determined as follows. If $\{x_1(t)\}$ and $\{x_3(t)\}$ are the actual initial states of the first and third registers, then the initial state of the second register, $x_2(t)$, is defined as one value for each time t. False variants of the initial state of the second register are discarded along with false variants of the initial state of the first and third registers, which were not omitted in the first stage.

Thus, the method requires the sequential selection of $2^{L1} + 2^{L2} + 2^{L3}$ variants. This value is significantly less than $2^{L1+L2+L3}$ when considering all possible options for large values of the register length L_i. For example, if the length of the generator registers is $L_1 = 31$, $L_2 = 33$, $L_3 = 35$ bits, then the total number of options is $2^{99} \sim 6{,}3*10^{29}$, as a result of the correlation attack this value can be reduced to $2^{31}+2^{33}+2^{35} \sim 4{,}5*10^{10}$.

The above approach is used in cryptanalysis of most combined generators.

Example 2. Let the Geffe generator shift register and its initial position be as shown in Figure 1. The sequences generated in the first 10 measures using these registers are $\{\{x_1(t)\}=\{0100111010\}$, $\{x_2(t)\}=\{1100110011\}$ and $\{x_3(t)\}=\{0111001011\}$ respectively. In this case, the sequence from the generator: $\{k(t)\}=\{0111111010\}$. The correspondence frequency is calculated by the symbols of the sequence $\{k(t)\}$ and the corresponding symbols of the unfolded sequences of the first and third registers in nonzero initial states.

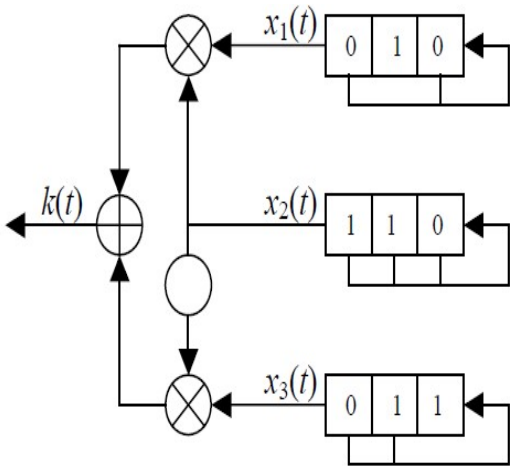

Figure 1. A special case of the Geffe generator

The corresponding calculation results are shown in table 2. To the right and left of the first row are the values of the sequence {k(t)}. The left part of the next line shows the initial state of the first register, the corresponding sequence and the frequency of correspondence with the characters of the sequence of characters {k(t)} created by the first registers. The right side of the table shows the analog values for the third register.

Table 2.

LFSR–1			LFSR–3		
{k(t)} = 0111111010		C	{k(t)} = 0111111010		C
(001)	0011101001	0,6	(001)	0010111001	0,6
(011)	0111010011	0,7	(010)	0101110010	0,8
(111)	1110100111	0,4	(101)	1011100101	0,3
(110)	1101001110	0,5	(011)	0111001011	0,7
(101)	1010011101	0,3	(111)	1110010111	0,4
(010)	0100111010	0,8	(110)	1100101110	0,5
(100)	1001110100	0,4	(100)	1001011100	0,4

If C = 0.7 is chosen as the limit, vectors (011) and (010) are possible options for the initial state of the first register, and vectors (010) and (011) are for the third register.

Determine the initial state of the second register. The outgoing sequences of the second register corresponding to various initial states are shown in Table 3 together with the selected sequences of the first and third registers. By comparing the bits of a known sequence {k(t)} with sequences developed using the first and third registers, the signs of the outgoing sequences of the second register are determined. Bits whose values are not indicated in the table are marked with a "*", and the bits of the sequence under study are in opposite positions "?" marked with a symbol.

Table 3.

Initial state	LFSR-2 Output	Determination of the outputs of registers 1 and 3 and the outputs of register 2 through the gamma k(t)	
(001)	0011001100	0111111010 = {k(t)} 0111**0**1011 –LFSR–1 output 0101110010 –LFSR–3 output **1*0*?**0 –LFSR–2 output	0111111010 = {k(t)} 0111**0**10011 –LFSR–1 output 0111**0**1011 –LFSR–3 output ****?10**? –LFSR–2 output
(011)	0110011001		
(110)	1100110011		
(100)	1001100110		
(010)	0101010101	0111111010 = {k(t)} 0**0**0111010 –LFSR–1 output 0**1**1110010 –LFSR–3 output **?0**1*** –LFSR–2 output	0111111010 = {k(t)} 0100111010 –LFSR–1 output 0111001011 –LFSR–3 output **0011***1–LFSR–2 output
(101)	1010101010		
(111)	1111111111		

As can be seen from the table, the only consistent option for all registers is (010), (110), (011) respectively for the initial states of the first, second and third registers, and they correspond to the initial state of the registers.

2.2 Correlation Immune Properties of Functions

The concept of correlation immunity initially arose as a feature of these combinatorial functions, which did not allow the application of the above approach. Accordingly, some concepts are described below.

Definition 1. $f(x)$, $x \in GF(2^n)$ the Boolean function has a correlation immunity of the indicators of level "k" (CI (k) – defined, here $1 \le k < n$), if $U_{\alpha}^{\wedge}(f) = 0$ - for all that satisfy the condition $1 \le Wt(\alpha) \le k$ [13].

Where $Wt(\alpha)$ - is the "Heming weight" for the vector "α" (that is, the number of units in the vector $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$). $U_{\alpha}^{\wedge}(f)$ - replacement of Walsh-Hadamard.

Therefore, if the given level of correlation immunity of this function $f(x)$ is "k", then the value of the function $Y = f(x)$ is considered statistically independent in any component $x \in GF(2^n)$ of the argument "k".

In general, $f(x)$, $x \in GF(2^n)$, a function can have a correlation immunity level k = n-1, that is, no more.

Example 3. Rate the given $f(x) = x_1 + x_2 + x_4$ (n = 4) function in accordance with the general requirements given above. The truth table of the function $f(x)$: $S(f) = \{0,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1\}$.

This function is a balanced Boolean function, because the number of zeros and ones in the values of the function is 8, that is, it is evenly distributed.

The degree of algebraic nonlinearity is $\deg(f)$ =1.

The Walsh-Hadamard substitution of the function $f(x)$ is calculated as follows:

$$U_{\alpha_1}^{\wedge}(f) = \sum_{x \in GF(2^4)} (-1)^{f(x) \oplus <\alpha_1, x_1>} = (-1)^{f(x_0) \oplus <\alpha_1, x_0>} + (-1)^{f(x_1) \oplus <\alpha_1, x_1>} +$$
$$+ (-1)^{f(x_2) \oplus <\alpha_1, x_2>} + (-1)^{f(x_3) \oplus <\alpha_1, x_3>} + (-1)^{f(x_4) \oplus <\alpha_1, x_4>} +$$
$$+ (-1)^{f(x_5) \oplus <\alpha_1, x_5>} + (-1)^{f(x_6) \oplus <\alpha_1, x_6>} + (-1)^{f(x_7) \oplus <\alpha_1, x_7>} +$$
$$+ (-1)^{f(x_8) \oplus <\alpha_1, x_8>} + (-1)^{f(x_9) \oplus <\alpha_1, x_9>} + + (-1)^{f(x_{10}) \oplus <\alpha_1, x_{10}>} +$$
$$+ (-1)^{f(x_{11}) \oplus <\alpha_1, x_{11}>} + (-1)^{f(x_{12}) \oplus <\alpha_1, x_{12}>} + (-1)^{f(x_{13}) \oplus <\alpha_1, x_{13}>} +$$
$$+ (-1)^{f(x_{14}) \oplus <\alpha_1, x_{14}>} + (-1)^{f(x_{15}) \oplus <\alpha_1, x_{15}>} = 0$$

(2)

Similarly, the following results were obtained for the remaining values of the α - vector:

$U_{\alpha_2}^{\wedge}(f) = 0$, $U_{\alpha_3}^{\wedge}(f) = 0$, $U_{\alpha_4}^{\wedge}(f) = 0$, $U_{\alpha_5}^{\wedge}(f) = 0$, $U_{\alpha_6}^{\wedge}(f) = 0$,

$U_{\alpha_7}^{\wedge}(f) = 0$, $U_{\alpha_8}^{\wedge}(f) = 0$, $U_{\alpha_9}^{\wedge}(f) = 0$, $U_{\alpha_{10}}^{\wedge}(f) = 0$, $U_{\alpha_{11}}^{\wedge}(f) = 0$,

$U_{\alpha_{12}}^{\wedge}(f) = 0$, $U_{\alpha_{13}}^{\wedge}(f) = 0$, $U_{\alpha_{14}}^{\wedge}(f) = 16$, $U_{\alpha_{15}}^{\wedge}(f) = 0$, $U_{\alpha_{16}}^{\wedge}(f) = 0$

The maximum value of this calculated Walsh-Hadamard replacement is 16. Where: $\alpha_1 = (0, 0, 0, 0)$, $\alpha_2 = (0, 0, 0, 1)$, $\alpha_3 = (0, 0, 1, 0)$, $\alpha_4 = (0, 0, 1, 1)$, $\alpha_5 = (0, 1, 0, 0)$, $\alpha_6 = (0, 1, 0, 1)$, $\alpha_7 = (0, 1, 1, 0)$, $\alpha_8 = (0, 1, 1, 1)$, $\alpha_9 = (1, 0, 0, 0)$, $\alpha_{10} = (1, 0, 0, 1)$, $\alpha_{11} = (1, 0, 1, 0)$, $\alpha_{12} = (1, 0, 1, 1)$, $\alpha_{13} = (1, 1, 0, 0)$, $\alpha_{14} = (1, 1, 0, 1)$, $\alpha_{15} = (1, 1, 1, 0)$, $\alpha_{16} = (1, 1, 1, 1)$.

According to the formula for calculating the degree of nonlinearity,

$$N(f) = 2^{4-1} - \frac{1}{2} \cdot \max_{\alpha_i \in GF(2^3)} \left| U_{\alpha_i}^{\wedge}(f) \right| = 2^3 - \frac{1}{2} \cdot 16 = 0 \quad (3)$$

that is, the degree of nonlinearity of this function is zero. In general, for these functions

with 4 arguments, the maximum level of nonlinearity should be 4 [8].

Using the above definition, the following results were obtained for all "α" vectors with heme weights 1, 2, 3, and 4, respectively:

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 16, 0, 0,

$Wt(\alpha)$ = 1 => $U_{\alpha_i}^{\wedge}(f)$: 0, 0, 0, 0;

$Wt(\alpha)$ = 2 => $U_{\alpha_i}^{\wedge}(f)$: 0, 0, 0, 0, 0, 0;

$Wt(\alpha)$ = 3 => $U_{\alpha_i}^{\wedge}(f)$: 0, 0, 16, 0;

$Wt(\alpha)$ = 4 => $U_{\alpha_i}^{\wedge}(f)$: 0. (4)

Therefore, the level of correlation immunity of this function is 2.

Example 4. Rate the given $f(x) = x_1 * x_2 * x_4$ (n = 4) function in accordance with the general requirements given above. The truth table of the function $f(x)$:

$S(f) = \{0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1\}$.

This function is not balanced, because the number of zeros in the values of the function is 14, and the number of units is 2, which is not evenly distributed.

The degree of algebraic nonlinearity is $\deg(f)$=3.

The Walsh-Hadamard substitution of the function $f(x)$ is as follows:

$U_{\alpha 1}^{\wedge}(f) = 12$, $U_{\alpha_2}^{\wedge}(f) = 4$, $U_{\alpha_3}^{\wedge}(f) = 0$,

$U_{\alpha_4}^{\wedge}(f) = 0$, $U_{\alpha_5}^{\wedge}(f) = 4$, $U_{\alpha_6}^{\wedge}(f) = -4$,

$U_{\alpha_7}^{\wedge}(f) = 0$, $U_{\alpha_8}^{\wedge}(f) = 0$, $U_{\alpha_9}^{\wedge}(f) = 4$,

$U_{\alpha_{10}}^{\wedge}(f) = -4$, $U_{\alpha_{11}}^{\wedge}(f) = 0$,

$U_{\alpha_{12}}^{\wedge}(f) = 0$, $U_{\alpha_{13}}^{\wedge}(f) = -4$,

$U_{\alpha_{14}}^{\wedge}(f) = 4$, $U_{\alpha_{15}}^{\wedge}(f) = 0$, $U_{\alpha_{16}}^{\wedge}(f) = 0$

The maximum value of this calculated Walsh-Hadamard replacement is 16. Where: α_1 = (0, 0, 0,0), α_2 = (0, 0, 0, 1), α_3 = (0, 0, 1, 0), α_4 = (0, 0, 1, 1), α_5 = (0, 1, 0, 0), α_6 = (0, 1, 0, 1), α_7 = (0, 1, 1,0), α_8 = (0, 1, 1, 1), α_9 = (1, 0, 0, 0), α_{10} = (1, 0, 0, 1), α_{11} = (1, 0, 1, 0), α_{12} = (1, 0, 1, 1), α_{13} = (1, 1, 0,0), α_{14} = (1, 1, 0, 1), α_{15} = (1, 1, 1, 0), α_{16} = (1, 1, 1, 1).

According to the formula for calculating the degree of nonlinearity,

$$N(f) = 2^{4-1} - \frac{1}{2} \cdot \max_{\alpha_i \in GF(2^3)} \left| U_{\alpha_i}^{\wedge}(f) \right| = 2^3 - \frac{1}{2} \cdot 12 = 2$$

that is, since the degree of nonlinearity of this function is 2.

Using the above definition, the following results were obtained for all "α" vectors with heme weights 1, 2, 3, and 4, respectively:

12, 4, 0, 0, 4, -4, 0, 0, 4, -4, 0, 0, -4, 4, 0, 0,

$Wt(\alpha)$ = 1 => $U_{\alpha_i}^{\wedge}(f)$: 4, 0, 4, 4;

$Wt(\alpha)$ = 2 => $U_{\alpha_i}^{\wedge}(f)$: 0, -4, 0, -4, 0, -4;

$Wt(\alpha)$ = 3 => $U_{\alpha_i}^{\wedge}(f)$: 0, 0, 4, 0;

$Wt(\alpha)$ = 4 => $U_{\alpha_i}^{\wedge}(f)$: 0.

Therefore, the level of correlation immunity of this function is 0.

Comparing the results of the above calculations for a given function, we can say that the concepts of nonlinearity and correlation immunity are theoretically contradictory concepts. That is, the level of correlation immunity of functions with a maximum level of non-linearity was minimal, or, conversely, the level of correlation-immunistic functions with a minimum level of non-linearity was the maximum value.

The Geffe correlation analysis is an example of determining the unknown key (in this case, the initially filled state of the registers) "in parts"[6,9]. It follows that a non-zero correlation between the values at the output of the function and their individual inputs allows you to independently check the initial state of each individual register. Although the use of the correlation immunization function as a combined function in combinatorial generators does not completely exclude the possibility of a correlation analysis, although it does not allow to restore the initial state of each register

individually. In accordance with the property of the Fourier spectrum obtained from the Parseval equation, the zero correlation of these functions provides a high correlation of one linear function with another linear function. The following example considers the correlation analysis of the combination generator with the correlation-immunist combination function.

Suppose that the combinatorial function of a generator with three shift registers has the form $f(x_1,x_2,x_3) = x_1 \oplus x_1x_2 \oplus x_1x_3$ is a correlation-immunistic function.The Fourier spectrum of this function is as follows in the standard order: {1/2, 0, 0, -1/2, 0, 1/2, 1/2, 0}. Thus, this function has a nonzero correlation with the following functions $x_2 \oplus x_3$, $x_1 \oplus x_3$ ва $x_1 \oplus x_2$ If at each time t at the input of the function $f(x_1,x_2,x_3) = x_1 \oplus x_1x_2 \oplus x_1x_3$, random variables are introduced taking the values 0 and 1, with equal probability $x_1(t)$, $x_2(t)$, $x_3(t)$, and if the random variable k(t) is determined from the equation $k(t) = f(x_1(t), x_2(t), x_3(t))$,then the probability is $Prob\{k(t) = x_1(t) \oplus x_2(t)\} = 3/4$. In this case, we get $Prob\{k(t) = x_1(\tau)\} = x_2(\tau)\} = 1/2$ from the pseudo-random property of the sequences coming out of the linear feedback shift register for all $\tau \neq t$ if $|\tau - t|$ the value is less than the length of the period of the sequences from LFSR-1 and LFSR-2. Based on these considerations, you must first consider all the initial cases of the first and second registers. The output sequence designed for each of these options is the frequency with which the known generator sequence k(t) corresponds to the output sequence. If the matching frequency is less than C, the initial state corresponding to this sequence is reset, otherwise it is added to the list of possible options. The initial value of the third register is determined separately. The sequence developed by the third register must correspond to the sequence created by the first and second registers. False variants of the initial cases of the third register according to the signs of the known outgoing sequence $k(t) = f(x_1(t), x_2(t), x_3(t))$ of the first and second registers are deleted together with false parameters that are not deleted in the first step. In general, this method requires a consistent selection of $O(2^{L1+L2}) + O(2^{L3})$ options. In the case of $L_i = L$, this method requires testing of $\sim 2^{2L}$ variants. This value is greater than $\sim 2^{L}$ when using the combined function without correlation immunization, but less than $\sim 2^{3L}$ when considering all options [6].

As the above example shows, using the correlation immunization function as a combined function does not completely exclude the possibility of a correlation attack on the algorithm, but complicates it.

2.3 Correlation cryptanalysis method for stream encryption algorithm A5

The combined function used in the A5 algorithm used only the linear XOR operation. The truth table for this function is given in table 4.

Table 4.

$\alpha(\alpha_1,\alpha_2,\alpha_3)$	x_1	x_2	x_3	$f = x_1 \oplus x_2 \oplus x_3$
000	0	0	0	0
001	0	0	1	1
010	0	1	0	1
011	0	1	1	0
100	1	0	0	1
101	1	0	1	0
110	1	1	0	0
111	1	1	1	1

The truth table of the function $f(x) : S(f) = \{0,1,1,0,1,0,0,1\}$.

The levels of nonlinearity and correlation immunity of this function are calculated below.

This function is a balanced function, because the number of zeros and ones is 4, i.e. it is evenly distributed.

The degree of algebraic nonlinearity is $\deg(f)$ =1.

The Walsh-Hadamard substitution of the function $f(x)$ is calculated as follows:

$U_{\alpha_1}^{\wedge}(f) = 0$, $U_{\alpha_2}^{\wedge}(f) = 0$, $U_{\alpha_3}^{\wedge}(f) = 0$, $U_{\alpha_4}^{\wedge}(f) = 0$, $U_{\alpha_5}^{\wedge}(f) = 0$, $U_{\alpha_6}^{\wedge}(f) = 0$, $U_{\alpha_7}^{\wedge}(f) = 0$, $U_{\alpha_8}^{\wedge}(f) = 8$

The maximum value of this generated Walsh-Hadamard replacement is 8. Where: $\alpha_1 = (0, 0,0)$, $\alpha_2 = (0, 0, 1)$, $\alpha_3 = (0, 1, 0)$, $\alpha_4 = (0, 1, 1)$, $\alpha_5 = (1, 0, 0)$, $\alpha_6 = (1, 0, 1)$, $\alpha_7 = (1, 1,0)$, $\alpha_8 = (1, 1, 1)$.

According to the formula for calculating the level of nonlinearity,

$$N(f) = 2^{3-1} - \frac{1}{2} \cdot \max_{\alpha_i \in GF(2^3)} \left| U_{\alpha_i}^{\wedge}(f) \right| = 2^2 - \frac{1}{2} \cdot 8 = 0 \quad (5)$$

that is, the degree of nonlinearity of this function is zero.

Using Definition 1, the following results were obtained for all "α" Heming weight vectors equal to 1, 2, 3, respectively:

0, 0, 0, 0, 0, 0, 0, 8

$Wt(\alpha)$ = 0 => $U_{\alpha_i}^{\wedge}(f)$: 0;

$Wt(\alpha)$ = 1 => $U_{\alpha_i}^{\wedge}(f)$: 0, 0, 0;

$Wt(\alpha)$ = 2 => $U_{\alpha_i}^{\wedge}(f)$: 0, 0, 0; (6)

$Wt(\alpha)$ = 3 => $U_{\alpha_i}^{\wedge}(f)$: 8;

Therefore, the level of correlation immunity of this function is 2.

The results show that the nonlinearity of the combined function used in algorithm A5 is zero. He has a correlation immunity level of 2. According to Table 4, the generator output coincides with the outputs of the registers with the probability P{k(t) = $x_1(t)$} = $x_2(t)$ = $x_3(t)$} = ½. These results mean that when f (x_1,x_2,x_3) = $x_1 \oplus x_2 \oplus x_3$ is used as a combined function in algorithm A5, the aforementioned method of correlation cryptanalysis is inefficient. Therefore, the A5 algorithm is considered resistant to the method of correlation cryptanalysis.

However, you can use the method of correlation cryptanalysis if the combining function uses functions that provide a relationship between the output of the generator and the output of the registers with a probability greater than ½. As such a union function, we can take the function f (x_1,x_2,x_3) = $x_1x_2 \oplus x_2x_3 \oplus x_1x_3$. The truth table for this function is shown in table 5 below.

Table 5

x_1	x_2	x_3	f (x_1,x_2,x_3) = x_1 $x_2 \oplus x_2$ $x_3 \oplus$ x_1x_3	l_1 = x_1	l_2 = x_3	l_3 = x_3
0	0	0	0	**0**	**0**	**0**
0	0	1	0	**0**	**0**	1
0	1	0	0	**0**	1	**0**
0	1	1	1	0	**1**	**1**
1	0	0	0	1	**0**	**0**
1	0	1	1	**1**	0	**1**
1	1	0	1	**1**	**1**	0
1	1	1	1	**1**	**1**	**1**

As can be seen from table 5, the output of the combinatorial function and the output of the registers correspond with probabilities P{k(t) = $x_1(t)$} = $x_2(t)$ = $x_3(t)$} = ¾. Therefore, if the function f (x1, x2, x3) = x1x2 $\oplus$ x2x3 $\oplus$ x1x3 is used as a combined function in the A5 algorithm, the correlation cryptanalysis method can be used to determine the initial state of the registers R1, R2, R3 using the sequence of steps in Example 2.

RESULTS:

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

The sequence of stages of applying the method of correlation cryptanalysis to combinatorial algorithms for stream encryption:

Step 1. The level of nonlinearity and the levels of correlation stability of the union function used in the stream encryption algorithm are calculated. If the level of nonlinearity is zero, and the level of correlation security is high, the algorithm is considered resistant to the method of correlation cryptanalysis, and the analysis process is completed. Otherwise, go to the second step;

Step 2. Search for all possible statistical functions of a combinatorial function. If the function has statistical analogs equal to x_1, x_2 or x_3, proceed to the next step, otherwise the algorithm is considered resistant to the method of correlation cryptanalysis, and the analysis process ends;

Step 3. Using the control function, the outputs of the registers with respect to various initial states are taken separately;

Step 4. The outputs of the registers corresponding to a given output frequency of the generator are divided, the remaining parameters are omitted.

Step 5. Crossing the possible variants of the registers, the variants of the initial state of the registers are determined.

CONCLUSION:

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

An increase in the number and length of registers in combinatorial generators, as well as the use of a correlation immunistic function with a low degree of nonlinearity as a combinatorial function, increases the complexity of the method of correlation cryptanalysis.

The function used in the Geff generator is considered unacceptable for the method of correlation cryptanalysis, since it passes information about the output of the registers. Provides resistance to the method of correlation cryptanalysis thanks to the linear function used in algorithm A5.

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.