ISSN 2278-3091
Volume 9 No.2, March -April 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse48922020.pdf
https://doi.org/10.30534/ijatcse/2020/48922020

Some aspects with the use of improved slide attack to the standard Encryption algorithm GOST 28147-89

Akhmedov B.B.[1],Aloev R.D.[2],
[1] National university of Uzbekistan, Uzbekistan, shirin07@ya.ru
[2] National university of Uzbekistan, Uzbekistan,aloevr@mail.ru

ABSTRACT

The article demonstrates the mechanism of using slide attack method to provide security assessment of the standard encryption algorithm GOST 28147-89 when uses weak keys.
The main objective of a slide attack is to search for slide pairs and the optimal choice Δ is the difference between keys and slide pairs. Because of using addition $mod2^{32}$ in the encryption algorithm GOST 28147-89 shows that, a slide attack can be implemented only with $\Delta = 0$ and $\Delta = 2^{31}$ to keep unchanged Δ the difference with probability p = 1 until the end of the rounds.For fixed S-blocks of standard encryption algorithm GOST 28147-89, to determine slide pairs which supply four round particularity and satisfy term of combined slide attack are carried out by using experimental software.
Analysis of experiments indicate that,it's impossible to give conclusion to determine slide pairs which satisfy terms of the attack along with not influence changing stability number of rounds, round keys, cryptographic operations during implementation slide attack cryptanalysis methods for four round particularity of the algorithm.
It is also revealed that, it is possible to fully determine the key using one or two slide pairs, and vice versa, that it is impossible to determine the real key using slide pairs.
For this reason, it has been shown that it is unpredictable to determine the number of slide pairs needed to effectively perform the slide attack.

Key words: cryptography, block cipher, plaintext(PT), cipher text(CT), slide attack, complementation slide attack.

1.INTRODUCTION

The study showed that the identified shortcomings of symmetric data encryption algorithms using linear, differential and linear differential methods of cryptanalysis can be eliminated by increasing the number of rounds [3,5,6,7,9,13,14,15]. This situation necessitates research on the use of the Slide Attack cryptanalysis method, which does not depend on the number of rounds.
In present there are following types of "Slide attack":
1. A usual slide attack and an attack based on known-plaintext (PT) to encryption processes with single-frame self-similarities;
2. Improved sliding techniques sliding with a twist and the complementation slide attack to encryption processes with two-round self-similarities.
3. Combined slide attack on encryption processes with four-round self-similarity.
There are organized appropriate experiences about first and second methods and got results. For example, you can bring a slide attack to the S-DES and DES ciphering algorithm based on the Feistel network and the results obtained from them[1,2,4].
The corresponding results were also obtained on the use of a slide attack on the foundations of selected plaintexts and a slide attack using additions to the symmetric encryption algorithm GOST 28147-89[4,9,10,11,12]. In the algorithm GOST 28147-89, together with the key, the S-block is a secret parameter, and during the study, the transformation of S-blocks recommended for use in the Central Bank of the Russian Federation was chosen[8].

2. THE MAIN PART

The combined slide attack method is applied to four round self-similarity encryption algorithms based on the Feistel network. This attack method contains the combined use of two methods, that is, a sliding with a twist and the complementation slide attack. In this case, the requirements and conditions for sliding with a twist and the complementation slide attack are maintained. Including, for a slide attack using the additions of introducing the difference between the slide pairs and keys and their conservation with probability equal to one until the end of the rounds. In the encryption algorithm GOST 28147-89, the round keys are added in the $mod2^{32}$ to the 32-bit value of the right part of the message included in each round. Based on this, the difference between the keys is also determined using the $mod2^{32}$, which, in turn, should provide the difference between the texts.
For instance, in order to carry out slide attack based on complementation, it must be saved with possibility p=1 till the end of encrypting process and differences must be equal according to requirement find slide couples;

$$\Delta = (K_0 + K_1) mod 2^{32} \text{ва } \Delta = (L' + R) mod 2^{32} (1)$$

There are shown that this action only can be used when slide attack based on $\Delta=0$ and $\Delta = 2^{31}$ and there must be kept difference between keys and entire texts when it is used in simple XOR operation in encrypting process. Here when $\Delta=0$ there is $K_0 = K_1$, simple slide attack will be appeared. In this

case it becomes equal with previous researches[4,9,10,11]. In the second case there $K_0 - K_1 = K_1 - K_0 = 2^{31}$is appropriate for $\Delta = 2^{31}$, there appeared continuous connection between keys. So this method only can be used when $\Delta = 2^{31}$. Here when $0 < K_0 < 2^{31} K_1 \geq 2^{31}$ and when $K_0 \geq 2^{31}$
$0 < K_1 < 2^{31}$.
A slide attack with a twist is applied to two-round self-similarities of the encryption algorithm and finds keys in these two rounds. If there are ignored initial and final permutations which are usually used in block encrypting processes, it could be continued like encrypting process using part keys of decipherment process and using part keys for encrypting process which is made in the Feystel system. This similarity makes it possible to use an attack with a comparison of the decryption process with a delay of one round to the encryption process. In this case in every rounds with exception of the first round of encrypting and the last round of decipherment slide pairs correspond to each other.
According to results of the analysis, the usage of combinative slide attack method will be continued by the following scheme(Figure 1).

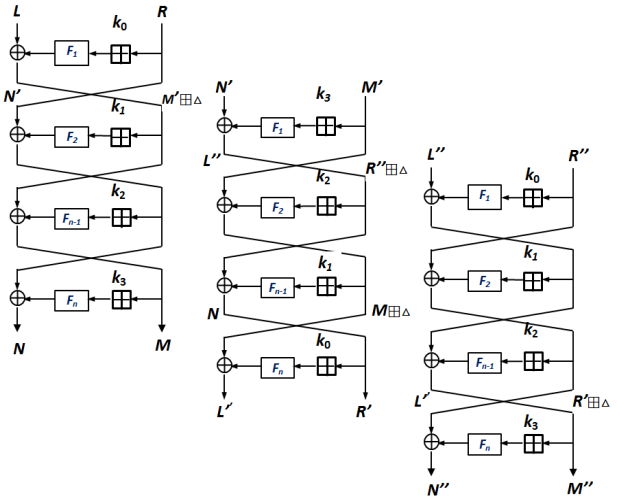

Figure 1: The scheme of the combinative slide attack process

In this work the usage of parallel account technology potentialities is required to GOST 28147-89 algorithm when there used combinative slide attack cryptanalysis method scheme. In spite of this there analysed the following keys by choosing in order to check it right or wrong:
$K_0 = 16777216_{10} = 01000000_{16} =$
$00000001000000000000000000000000_2$
$K_1 = 16778241_{10} = 01000401_{16} =$
$00000001000000000000010000000001_2$
$K_2 = 2164260864_2 = 81000000_{16} =$
$10000001000000000000000000000000_2$
$K_3 = 2164261889_2 = 81000401_{16} =$
$10000001000000000000010000000001_2$
Slide attack consists of two stages, in the first one delaying second decipherment process to a round it becomes alternative to encrypting process and there appeared equation which makes difference $\Delta = K_3 - K_1 = K_1 - K_3$
In the second stage the second encrypting process delays to a round and becomes alternative to decipherment process. In this case there also appears equation which proves delta difference. In these two cases
$\Delta = \Delta' = 2^{31} = 80000000_{16} = 2147483648_{10} =$
$= 10000000000000000000000000000000_2$ is proved.
As an example the following slide pairs will be analysed (Table 1)

Table 1: Slide pairs.

Quantities of plaintext in two and sixteen reckoning systems			Quantities of ciphertext in two and sixteen reckoning systems		
L	0011100100100110 1000101000100010	39268A22	N	0011001101001101 0001100010001110	334D188E
R	0000000100000000 0000000000000000	01000000	M	1101011101100110 0111101100010101	D7667B15
N'	0000000100000000 0000000000000000	01000000	L'	0100000101111110 0011101000100000	417E3A20
M'	0000001000000000 0000000000000000	02000000	R'	0011001101001101 0001100010001110	334D188E
L''	0000001000000000 0000000000000000	02000000	N''	1001101110110111 0110001100101111	9BB7632F
R''	0011101000111110 1111101101100010	3A3EFB62	M''	0100000101111110 0011101000100000	417E3A20

2.1 The first process of using slide attack forfirst round.

1) Analysing 1-situation(Table 1), in this case slide pairs are taken as following:
PT1= $39268A2201000000_{16}$
PT1: $L=(39268A22)_{16}=$
$00111001001001101000101000100010_2$
$R=(01000000)_{16}= 00000001000000000000000000000000_2$
PT2= 0100000002000000_{16}
PT2: $N' =(01000000)_{16}$
$=00000001000000000000000000000000_2$
$M' =(02000000)_{16} = 00000010000000000000000000000000_2$
PT3=$020000003A3EFB62_{16}$
PT3: $L'' =(02000000)_{16} =$
$00000010000000000000000000000000_2$
$R'' = (3A3EFB62)_{16} =$
$00111010001111101111101101100010_2$
CT1= $334D188ED7667B15_{16}$
CT1: $N = (334D188E)_{16}=$
$00110011010011010001100010001110_2$
$M = (D7667B15)_{16}= 11010111011001100111101100010101_2$
CT2 = $417E3A20334D188E_{16}$
CT2: $L' =(417E3A20)_{16} =$
$01000001011111100011101000100000_2$
$R' =(334D188E)_{16}= 00110011010011010001100010001110_2$
CT3=$9BB7632F417E3A20_{16}$
CT3: $N'' =(9BB7632F)_{16} =$
$10011011101101110110001100101111_2$
$M'' =(417E3A20)_{16} =$
$01000001011111100011101000100000_2$
In the first stage slide pairs are given by the following requirement:
1-requirement: $R = N'$
PT1= $39268A2201000000_{16}$
PT1: $L=(39268A22)_{16}=$
$00111001001001101000101000100010_2$
$R=(01000000)_{16}= 00000001000000000000000000000000_2$
PT2= 0100000002000000_{16}
PT2: $N'=(01000000)_{16} =$
$00000001000000000000000000000000_2$

$M'=(02000000)_{16}$ = 00000010000000000000000000000000$_2$
Represented slide pairs satisfies completely slide attack requirement. In the next stage there made attack by help of slide pairs. In the 2-figure(Figure 2) there given that slide pairs situated in the first round.

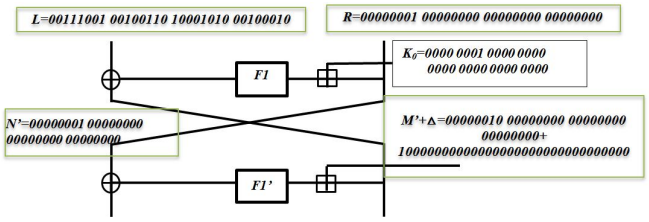

Figure 2: Situating slide pairs in the first round

Here 1st round$L\oplus F(R,K_0)=M'+\Delta\Rightarrow$
$F(R,K_0)=(M'+\Delta)\oplus L$=(00000010000000000000000000000000 00$_2$+10000000000000000000000000000000$_2$)
$\oplus$00111001001001101000101000100010$_2$=
10111011001001101000101000100010$_2$
F(R,K_0)= 10111011001001101000101000100010$_2$
F(R,K_0)>>11=(10111011001001101000101000100010$_2$)>>11=(01000100010101110110010011010001$_2$)
=(445764D1)$_{16}$=(4,4,5,7,6,4,13,1)$_{10}$
$S^{-1}(F(R,K_0))=(R+K_0)$ mod 2^{32}=
01000100010101110110010011010001$_2$)= (445764D1)$_{16}$
=(4,4,5,7,6,4,13,1)$_{10}$= (0,2,0,0,0,0,0,0)$_{10}$=
(00000010000000000000000000000000)$_2$
K_0=
$S^{-1}(F(R,K_0))$-$R(mod2^{32})$=(00000010000000000000000000000000– 00000001000000000000000000000000)$(mod2^{32})$ =
00000001000000000000000000000000$_2$=16777216$_{10}$ =
01000000$_{16}$=16777216$_{10}$

2.2 The first process of using slide attack forlast round

Take slide pairs by the last round (Figure 3) cipher texts, that is:
CT1= 334D188ED7667B15$_{16}$
CT1: N = (334D188E)$_{16}$=
00110011010011010001100010001110$_2$
M = (D7667B15)$_{16}$= 11010111011001100111101100010101$_2$
CT2= 417E3A20334D188E$_{16}$
CT2: L'=(417E3A20)$_{16}$ =
01000001011111100011101000100000$_2$
R'=(334D188E)$_{16}$= 00110011010011010001100010001110$_2$

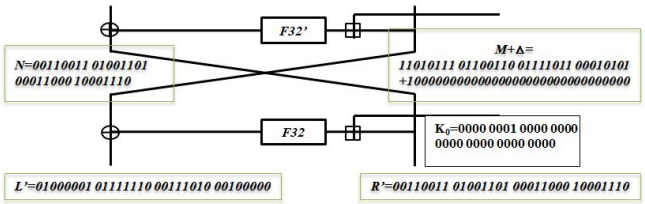

Figure 3: The analysis of the last round first slide pairs

32-round$L'\oplus F(R',K_0)=M+\Delta\Rightarrow$ $F(R',K_0)=(M+\Delta)\oplus L'$=
=(11010111011001100111101100010101$_2$+10000000000000000000000000000000$_2$)$\oplus$01000001011111100011101000100000$_2$=00010110000110000100000100110101$_2$
$F(R',K_0)$>>11=(00010110000110000100000100110101$_2$)>>11= (00100110101000101100001100001000$_2$) =
(26A2C308)$_{16}$ = (2,6,10,2,12,3,0,8)$_{10}$
$S^{-1}(F(R',K_0)$= 00100110101000101100001100001000$_2$)=
$(R'+K_0)$ mod 2^{32}
$S^{-1}(F(R',K_0)$= 00100110101000101100001100001000$_2$) =
(2,6,10,2,12,3,0,8)$_{10}$) =(3,4,4,13,1,8,8,14)$_{10}$ =
(00110100010011010001100010001110)$_2$=877467790$_{10}$
$K_0=S^{-1}(F(R',K_0))$-$R'(mod2^{32})$=
(00110100010011010001100010001110$_2$ –
00110011010011010001100010001110$_2$) $(mod2^{32})$ =
00000001000000000000000000000000$_2$= 16777216$_{10}$
$K_0(32\text{-}round)$=00000001000000000000000000000000$_2$=16777216$_{10}$=01000000$_{16}$.
So in both cases the keys became equal, this shows that used keys in the first round of encrypting process and the last round of decipherment process are equal.
In the second stage, slide pairs are taken respectively by the following requirement:
1-requirement: $M' = L''$ PT2= 0100000002000000$_{16}$
PT2: N'=(01000000)$_{16}$ =
00000001000000000000000000000000$_2$
M'=(02000000)$_{16}$ = 00000010000000000000000000000000$_2$
PT3= 020000003A3EFB62$_{16}$
PT3: L''=(02000000)$_{16}$ =
00000001000000000000000000000000$_2$
R''= (3A3EFB62)$_{16}$ =
00111010001111101111101101100010$_2$
2- requirement: $L' = M''$CT2= 417E3A20334D188E$_{16}$
CT2: L'=(417E3A20)$_{16}$ =
01000001011111100011101000100000$_2$
R'=(334D188E)$_{16}$= 00110011010011010001100010001110$_2$
CT3= 9BB7632F417E3A20$_{16}$
CT3: N''=(9BB7632F)$_{16}$ =
10011011101101110110001100101111$_2$
M''=(417E3A20)$_{16}$ =
01000001011111100011101000100000$_2$

2.3 The secondprocess of using slide attack forfirst round.

Represented slide pairs satisfies completely slide attack requirement. In the next stage there made attack by help of slide pairs. In the 4-figure(Figure 4) there given that slide pairs situated in the first round

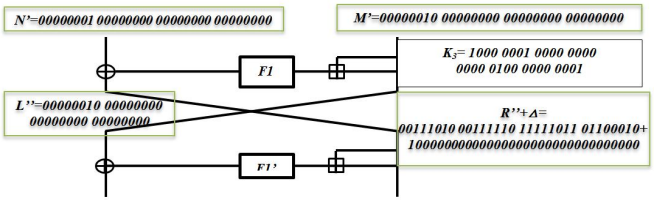

Figure 4: Situating slide pairs in the first round

Here 1-round $N'\oplus F(M',K_3)=R''+\Delta\Rightarrow$ $F(M',K_3)=$
$(R''+\Delta)\oplus N'$=(00111010001111101111101101100010$_2$
+10000000000000000000000000000000$_2$) $\oplus$
00000001000000000000000000000000$_2$
=10111011001111101111101101100010$_2$
$F(M',K_3)$= 10111011001111101111101101100010$_2$

$F(M',K_3)$>>11=(10111011001111110111110110110 0010_2)>>11= ($0110110001010111011001111101111_2$) $=(6,12,5,7,6,7,13,15)_{10}$
$S^{-1}(F(M',K_3))= (M'+K_3) \bmod 2^{32}$
$S^{-1}(F(M',K_3)$= ($0110110001010111011001111101111_2$) $=(6,12,5,7,6,7,13,15)_{10}$= $(8,3,0,0,0,4,0,1)_{10}$ = $(10000011000000000000010000000001)_2$=$2197816321_{10}$
K_3= $S^{-1}(F(M',K_3))$-$M'(mod2^{32})$=(1000001100000000000000100000000001 – 00000010000000000000000000000000)$(mod2^{32})$ = $1000000100000000000010000000001_2$ =2164261889_{10}
K_3*(1-round)*= $1000000100000000000010000000001_2$ = 2164261889_{10}= 81000401_{16}

2.4 The second process of using slide attack forlast round.

Take slide pairs by the last round (Figure 5) cipher texts, that is:
CT2= $417E3A20334D188E_{16}$
CT2: $L'=(417E3A20)_{16}$ = $01000001011111100011101000100000_2$
$R'=(334D188E)_{16}$= $00110011010011010001100010001110_2$
CT3=$9BB7632F417E3A20_{16}$
CT3: $N''=(9BB7632F)_{16}$ = $10011011101101110110001100101111_2$
$M''=(417E3A20)_{16}=01000001011111100011101000100000_2$

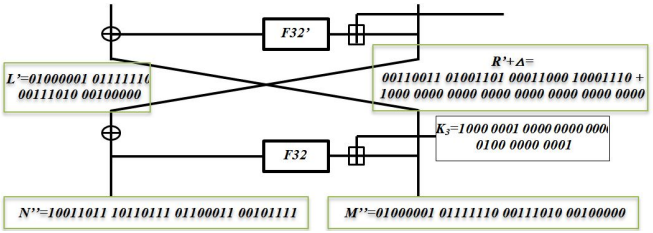

Figure 5: The analysis of the last round first slide pairs

Here 32-round$N'' \oplus F(M'',K_3)=R'+\Delta \Rightarrow F(M'',K_3)=$ $(R'+\Delta) \oplus N''=$ $=(00110011010011010001100010001110_2$+$10000000000000000000000000000000_2)\oplus$ $10011011101101110110001100101111_2$=$00101000111110100111101110100001_2$
$F(M'',K_3)$>>11=($00101000111110100111101110100001_2$)>>11= ($01110100001001010001111101001111_2$) $=(7,4,2,5,1,15,4,15)_{10}$
$S^{-1}(F(M'',K_3)=)= (M''+K_3) \bmod 2^{32}$
$S^{-1}(F(M'',K_3)$= $01110100001001010001111101001111_2$) $=(7,4,2,5,1,15,4,15)_{10}$ = $(12,2,7,14,3,14,2,1)_{10}$ =$(11000010011111100011111000100001)_2$=$3263053345_{10}$
K_3= $S^{-1}(F(M'',K_3))$-$M'')(mod2^{32})$=(1100001001111110001111100010000 1_2 – $0100000101111110001110100010000 0_2$) $(mod2^{32})$ = $1000000100000000000010000000001_2$ =2164261889_{10}
K_3*(32-round)*=$1000000100000000000010000000001_2$ =2164261889_{10}=81000401_{16}
So in the second stage keys became equal, this shows that used keys in the first round of decipherment process and the last round of encrypting process are equal. $\Delta = K_3 - K_1 = K_1 - K_3 \Delta' = K_2 - K_0 = K_0 - K_2$
Using these equations rest keys are found as following:
$\Delta = 2^{31} = 2147483648and\Delta' = 2^{31} = 2147483648$
$K_1=(K_3-\Delta) \bmod 2^{32}$ =(2164261889-2147483648)$mod2^{32}$=16 778241_{10} =01000401_{16}
$K_2=(K_0-\Delta) \bmod 2^{32}$ =(16777216-2147483648) $mod2^{32}$=2164260864_{10}=81000000_{16}
There analysed 2^{24} texts on a basis of above mentioned combinative slide attack algorithm, and determined 2^{12} slide pairs. It is defined from analysis that, not all determined slide pairs can make possibility to find round keys correctly. In the following table there given slide pairs which round keys are found correctly in them (Table 2).

Table 2: Slide pairs which round keys are found correctly in them.

Plaintext values in hexadecimal notation		Ciphertext values in hexadecimal notation		Round keys
1 – slide pair				k0=01000000
PT1	39268A2201000000	CT1	9A67C3E76350D606	k1=0100005F
PT2	0100000002000000	CT2	9B51F38C9A67C3E7	k2=81000000
PT3	020000003A27E362	CT3	F366B6E69B51F38C	k3=8100005F
2 -slide pair				k0=01000000
PT1	39268A2201000000	CT1	F83436882EB0C65F	k1=01000101
PT2	0100000002000000	CT2	2E388FC1F8343688	k2=81000000
PT3	020000003A5EFB62	CT3	8D175E462E388FC1	k3=81000101
3 -slide pair				k0=01000000
PT1	39268A2201000000	CT1	71579F26696493A6	k1=01000201
PT2	0100000002000000	CT2	1416C48771579F26	k2=81000000
PT3	020000003A56FB62	CT3	B95FD2CA1416C487	k3=81000201
4 -slide pair				k0=01000000
PT1	39268A2201000000	CT1	334D188ED7667B15	k1=01000401
PT2	0100000002000000	CT2	417E3A20334D188E	k2=81000000
PT3	020000003A3EFB62	CT3	9BB7632F417E3A20	k3=81000401
5 -slide pair				k0=01000000
PT1	39268A2201000000	CT1	F4A23B652D8E1ADE	k1=01000001
PT2	0100000002000000	CT2	FD24A330F4A23B65	k2=81000000
PT3	020000003A26FB62	CT3	F022C44DFD24A330	k3=81000001

For GOST 28147-89 standard symmetric encryption algorithm has been found slide pairs which can satisfy the terms of the combinational slide attack and with the help of combinational slide attack and obtained positive results.

3. CONCLUSION

After finding effective slide pairs for the encryption algorithm, you can find the corresponding bits of the round keys. Due to spending much more time for the process of calculation slide pairs, we use Δ value in advance.
To determine all the bits of the private key, it is enough to select several plaintext and corresponding ciphertext, as well as determined several slide pairs for a given mask.
In general, based on the above information, we can conclude that the generated necessary slide pairs for conducting slide attacks will take a lot of time. This leads to the fact that the effectiveness of slide attacks depends on an effective solution to this problem.
Implementation of cryptanalysis methods of slide attack indicate that, it's impossible to give general conclusion to determine slide pairs which satisfy terms of the attack along with not influence changing stability number of rounds, round keys, cryptographic operations during implementation slide attack cryptanalysis methods for four round particularity of the algorithm.

For the algorithm GOST 28147-89, based on various keys, 2^{18} texts were analyzed using a 32-bit Galois generator out of 2^{32} possible selected plaintexts.

As a result, about 2^6 and 2^5 slide pairs have been found for two different keys, and enough half of them to find private key to get positive result.

It is important to note that only with the help of one or two slide pairs you can completely find the private key, and vice versa, it's impossible to find private key using all of the slide pairs.

For this reason, it is not possible to determine in advance the number of slide pairs needed to effectively use the slide attack.

Because of using addition mod2^{32} in the encryption algorithm GOST 28147-89, $\Delta$the difference between round keys and slide pairswhich is the main condition of the combined slide attack doesn't always kept until the end of rounds.

As a result, it's possible to implement slide attack to standard encryption algorithm GOST 28147-89when these terms $\Delta = 0$ and $\Delta = 2^{31}$ have been done.

For $\Delta = 0$, equality of keys leads to implement successfully common slide attack and only one case, $\Delta = 2^{31}$this method may be used to find private key.

REFERENCES

1. A. Biryukov, D. Wagner **"Advanced Slide Attacks"** in Advanced Cryptology pp. 589-606, EUROCRYPT 2000.
2. A. Biryukov, D. Wagner "**Slide Attacks**" in Proceeding of Fast Software Encryption. Springer-Verlag 1999.
3. Ishukova Y. A. **Development and research of algorithms for analysing the strength of block encryptions using differential cryptanalysis method**.
4. Akhmedov B. B. **The principles of the usage of slide attack cryptanalysis method**.// "Practical mathematics and information security" scientific-technic conference materials. 2014 year, pp. 311-317.
5. Babenko L.K., Ishukova Ye.A. **Analysis of simmetric cryptsystems**// News of YuFU. Technic sciences, №12, 2012, pp. 136-147.
6. Sattarov A.B. **The principles of the usage algebraic cryptanalysis method to evaluate cryptdurability of encrypting algorithms**. // " Practical mathematics and burning problems of information technologies – Al-Xorazmiy 2014" International scientific conference collection №2, 2014, pp. 47-51.
7. Babenko L.K., Ishukova Ye.A. **Contemporary algorithms of block encrypting and method of their analysis**. – M., "GeliosARV", pp. 2006.-376.
8. **State standard union SSR. Information processing systems. Crytographic protection. Cryptographic transformation algorithm GOST 28147-89**. IPK Publishing standards of Moscow,1989.
9. Kuryazov D.M., Akhmedov B.B., Sattarov A.B. "**Assessment of the resistance of block symmetric encryption algorithms to modern cryptanalysis methods**". Manual. Tashkent.: "Aloqachi". 2017,p. 228.
10. Akhmedov B.B. "**Application of a slide attack on the foundations of selected plaintexts to the algorithm GOST 28147-89**". Information communications: Networks, Technologies, Solutions, AK:TTE №3 (47)/2018, pp. 46–51.
11. Akhmedov B.B. "**Some aspects of using slide attack using additions to Feistel-based encryption algorithms**.", Uzbek Journal Of the problems of informatics and energetics. 2018. – №3, pp. 43–49.
12. Babenko L.K., Ischukova E.A., Alekseev D.M. **Implementing of slide pairs' searching for encryption algorithm Magma with using MPI technology**. Scientific bulletin. 2015 №3(5), pp. 38-49. DOI: 10.17117/nv.2015.03.038.
13. Kuryazov D.M. **Algorithm for ensuring message confidentiality using elliptic curves**, International Journal of Advances in Computer Science and Technology, Vol. 9(1), February, pp. 295-298, 2020. https://doi.org/10.30534/ijacst/2020/44912020.
14. Koduru P.R. **Information Security Using Hilbert With Hash Value**, International Journal of Advanced Trends in Computer Science and Engineering, 8(5),September - October 2019, 2507- 2511. https://doi.org/10.30534/ijacst/2019/96852019.
15. Deepti Sehrawat.**A Review on Performance Evaluation Criteria and Tools for Lightweight Block Ciphers**, International Journal of Advanced Trends in Computer Science and Engineering, 8(3), May - June 2019, 630 – 639. https://doi.org/10.30534/ijacst/2019/47832019.