International Journal of Informatics, Information System and Computer Engineering

Unique Aspects of Usage of the Quadratic Cryptanalysis Method to the GOST 28147-89 Encryption Algorithm

Bardosh Akhmedov, Rakhmatillo Aloev*

University of Uzbekistan named after Mirzo Ulugbek Tashkent, Uzbekistan
*Corresponding Email: shirin07@ya.ru

ABSTRACTS

In this article, issues related to the application of the quadratic cryptanalysis method to the five rounds of the GOST 28147-89 encryption algorithm are given. For example, the role of the bit gains in the application of the quadratic cryptanalysis method, which is formed in the operation of addition according to mod232 used in this algorithm is described. In this case, it is shown that the selection of the relevant bits of the incoming plaintext and cipher text to be equal to zero plays an important role in order to obtain an effective result in cryptanalysis.

ARTICLE INFO

Article History:
Submitted/Received 15 Mar 2022
First Revised 02 Jun 2022
Accepted 18 Aug 2022
Available online 01 Oct 2022
Publication Date 01 Dec 2022

Keywords:
GOST 28147-89,
selected plaintext,
quadratic approximation,
correlation matrix,
quadratic cryptanalysis

1. INTRODUCTION

In order to verify and evaluate the strength of encryption algorithms the possibilities of linear, differential, linear-differential, algebraic, and correlation cryptanalysis are used. Many works are devoted to improving applications of linear cryptanalysis. Several linear approximations simultaneously for one combination of key bits (Kaliski & Robshaw, 1994; Quisquater, 2004) can be used to increase the efficiency of the linear cryptanalysis method. A method for improving the LC method (in particular, for the cipher LOKI91) is proposed, which suggests taking into account the probabilistic behavior of some bits instead of their fixed values when approximating (Sakurai & Furuya, 1997).

2. LITERATURE REVIEW

2.1. Linear Cryptanalysis

A series of works is devoted to the issues of the resistance of various encryption algorithms to the linear cryptanalysis method. In (Chee et al., 1994), L.Knudsen considered the issues of constructing Feistel-type encryption schemes that are resistant to linear and differential cryptanalysis methods. V.Shorin, V.Zheleznyakov and E.Gabidulin proved in 2001 that the Russian algorithm GOST

DOI: https://doi.org/10.34010/injiiscom.v3i2.8445
p-ISSN 2810-0670 e-ISSN 2775-5584

28147-89 is resistant to these methods (with no less than five rounds of encryption in linear cryptanalysis and seven rounds in a different one).

A large number of works are devoted to the study of various classes of approximating functions and to the construction of functions that are most difficult to such approximations. In these papers, bent functions (Logachev et al., 2004; Dobbertin & Leander, 2004; Chee et al., 1994) are considered, which are Boolean functions from an even number of variables that are maximally distant from the set of all linear functions in the Hamming metric, as well as their generalizations: semi-bent functions (Dobbertin & Leander, 2005), partially bent functions (Qu et al., 2000), Z−bent functions (Pfitzmann, 2003), homogeneous bent functions (Kuzmin et al., 2006), hyper best functions (Carlet & Gaborit, 2006; Youssef, 2007; Kuz'min et al., 2008; Knudsen & Robshaw, 1996). The main idea of using linear cryptanalysis of nonlinear approximations (Knudsen & Robshaw, 1996) is to enrich the class of approximating functions (of m variables) with nonlinear functions and increase the quality of approximation due to this. In this case, the cryptanalyst has to deal with the difficulties of choosing nonlinear approximations and combining nonlinear approximations of individual rounds.

2.2. GOST 28147-89 encryption algorithms

In the GOST 28147-89 encryption algorithm (Kuryazov et al., 2017; Vinokurov) mod232 addition operation is used, and this operation, by its nature, the value of each resulting bit is connected to the values of the incoming bits below it in order. The mathematical model of each bit of the result of this operation can be expressed as follows:

$$p_{32} = (x_{32} + k_{32}) \bmod 2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

$$p_{31} = (x_{31} + k_{31} + q_{32}) \bmod 2 \quad \ldots\ldots\ldots\ldots\ldots..(2)$$

$$p_2 = (x_2 + k_2 + q_3) \bmod 2 \quad ...\ldots\ldots\ldots\ldots\ldots..(3)$$

$$p_1 = (x_1 + k_1 + q_2) \bmod 2 \quad \ldots\ldots\ldots\ldots\ldots\ldots....(4)$$

The general mathematical model of addition operation according to mod232 can be expressed as follows (Kuryazov et al., 2017):

$$p_i = (x_i + k_i + q_{i+1}) \bmod 2, i = \overline{32\ldots1},\ q_{33} = 0$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(5)$$

here, qi –addition of sum of all i-bits.

In this case, when applying the linear cryptanalysis method, considering the influence of the bit in each position of the block to be reflected with the output bits, the problem of building a Boolean function for each bit of the result of the addition operation according to mod232 was considered. An overview of this function is as follows (Kuryazov et al., 2017).

$$p_i = x_i \oplus k_i \oplus q_{i+1}, \quad q_i = x_i \wedge k_i \oplus q_{i+1} \wedge (x_i \oplus k_i),$$
$$i = \overline{32\ldots1},\ q_{33} = 0.(2)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(6)$$

Based on the results of the research on the mod232 addition operation used in the GOST 28147-89 encryption algorithm, the schematic view of one round of this algorithm is as follows (Fig. 1) (Kuryazov et al., 2017).

3. METHOD

3.1. A. Quadratic relations of a special form

In previous works, correlation matrix values for linear and quadratic dependences and appropriate approximation equations with probability r=7/8 were obtained for GOST 28147-89 algorithm S box. These equations are effectively used in linear cryptanalysis to find key bits with high probability (Akhmedov & Aloev, 2020; Akhmedov, 2021). These equations are shown in Table 1.

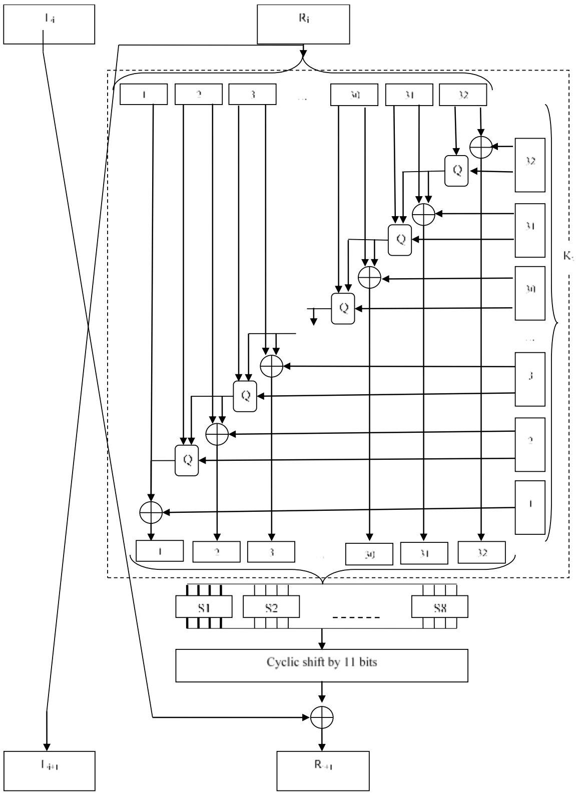

Fig. 1. Schematic view of one round of GOST 28147-89 encryption algorithm

3.2. Quadratic cryptanalysis

With these approximation equations, a modification of the GOST 28147-89 algorithm, that is, using the XOR operation instead of the mod232 addition operation, was used for the 5th round of quadratic cryptanalysis, and the corresponding results were obtained (Akhmedov & Aloev, 2020; Akhmedov, 2021).

Based on the quadratic cryptanalysis conducted for the 5th round of the GOST 28147-89 algorithm, the addition operation according to mod232 is used for the S block reflections, when conducting cryptanalysis based on the correlation matrices of linear and quadratic connections, the fact that some bits of the plaintext and ciphertext are equal to zero ensures the formation of an effective approximation relationship.

4. RESULTS AND DISCUSSION

Based on the concepts presented above, the quadratic dependence approximation equations in Table 1 determined for the correlation matrices for the S3-block are analyzed.

1-round: For S3 block 〚(p〛_1⊕p_3)(p_2⊕p_4)⊕p_1⊕p_3=c_3 with probability p=12/16 the position of variables in the round reflection of the approximation equality, according to 11-bit left cyclic shift and addition of left-side appropriate bits {(P(41) ⊞ K1(9))⊕(P(43) ⊞ K1(11))}*{(P(42) ⊞ K1(10))⊕(P(44) ⊞ K1(12))} ⊕ (P(41) ⊞ K1(9))⊕(P(42) ⊞ K1(10)) =Y1(32)⊕P(32) will have the form. In order not to encounter the problem of addition from the sum of bits in this equality, it is necessary to choose plaintexts that satisfy the condition P(42)=P(43)=P(44)=P(45)=0. Since the addition of the sum of P(41) and K1(9) in this block does not affect equality, it can be obtained in the form P(41) ⊞K1(9)=P(41)⊕K1(9). In this case

(P(41)⊕K1(9)⊕K1(11))*(K1(10)⊕K1(12)) ⊕

P(41)⊕K1(9)⊕K1(10))=Y1(32)⊕ P(32) (3)

The equation is formed.

Table 1. Cloud Users' Responsibility Types of Attacks

№	Approximation equations	Possibility	Exclusion
S1	$p_1 \oplus p_4 = c_1c_2 \oplus c_2c_3 \oplus c_1c_4 \oplus c_3c_4 \oplus c_1 \oplus c_4$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_2 \oplus p_4 = c_1c_3 \oplus c_1c_4 \oplus c_2c_3 \oplus c_2c_4 \oplus c_1 \oplus c_3$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_1 \oplus p_3 = c_2 \oplus c_3 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_1 \oplus p_3 = c_2 \oplus c_3 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_1 \oplus p_3 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_1 \oplus c_3 \oplus 1$	P = 1/8	Δ=3/4
S2	$p_1 \oplus p_3 \oplus p_4 = c_1 \oplus c_4 \oplus 1$ $p_1 \oplus p_2 = c_1 \oplus c_2 \oplus c_4$ $p_1 \oplus p_2 \oplus p_3 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_2 \oplus c_3$ $p_1p_2 \oplus p_1p_4 \oplus p_2p_3 \oplus p_3p_4 \oplus p_2 \oplus p_3 = c_1 \oplus c_2 \oplus c_4$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_4 \oplus p_3 = c_3 \oplus c_4 \oplus 1$	P = 1/8	Δ=3/4
S3	$p_1 \oplus p_4 = c_1 \oplus c_3$ $p_2 \oplus p_3 \oplus p_4 = c_1 \oplus c_3 \oplus c_4$ $p_2 \oplus p_3 = c_1 \oplus c_2 \oplus c_3 \oplus 1$ $p_1 \oplus p_3 = c_1c_2 \oplus c_2c_3 \oplus c_1c_4 \oplus c_3c_4 \oplus c_1 \oplus c_2 \oplus 1$ $p_4 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_2 \oplus c_4 \oplus 1$ $p_1 \oplus p_4 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_3 \oplus c_4$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_1 \oplus p_3 = c_1 \oplus c_2 \oplus 1$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_2 \oplus p_4 = c_1 \oplus c_3$ $p_1p_2 \oplus p_1p_4 \oplus p_2p_3 \oplus p_3p_4 \oplus p_1 \oplus p_4 = c_1 \oplus c_2 \oplus c_3$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_1 \oplus p_3 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_1 \oplus c_3 \oplus 1$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_1 \oplus p_3 = c_1c_2 \oplus c_1c_3 \oplus c_2c_4 \oplus c_3c_4 \oplus c_3 \oplus c_4$	P = 1/8	Δ=3/4

Table 1 (Continue). Cloud Users' Responsibility Types of Attacks

№	Approximation equations	Possibility	Exclusion
S4	$p_3 = c_1 \oplus c_2 \oplus c_3 \oplus c_4 \oplus 1$ $p_1 \oplus p_3 \oplus p_4 = c_1$ $p_2 \oplus p_4 = c_3 \oplus 1$ $p_3 \oplus p_4 = c_1c_2 \oplus c_2c_3 \oplus c_1c_4 \oplus c_3c_4 \oplus c_2 \oplus c_3$ $p_3 \oplus p_4 = c_1c_2 \oplus c_1c_3 \oplus c_2c_4 \oplus c_3c_4 \oplus c_1 \oplus c_3$ $p_1 \oplus p_2 \oplus p_3 \oplus p_4 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_1 \oplus c_2 \oplus 1$ $p_1 \oplus p_2 \oplus p_4 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_3 \oplus c_4$ $p_1p_2 \oplus p_1p_4 \oplus p_2p_3 \oplus p_3p_4 \oplus p_2 \oplus p_3 = c_4 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_2 \oplus p_4 = c_3 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_1 \oplus p_2 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_1 \oplus c_3 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_1 \oplus p_2 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_1 \oplus c_3 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_3 \oplus p_4 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_2 \oplus c_4$	P = 1/8	Δ=3/4
S5	$p_3 = c_1 \oplus c_2 \oplus c_3 \oplus c_4$ $p_1 \oplus p_2 \oplus p_3 \oplus p_4 = c_1c_2 \oplus c_2c_3 \oplus c_1c_4 \oplus c_3c_4 \oplus c_1 \oplus c_2$ $p_1p_2 \oplus p_1p_4 \oplus p_2p_3 \oplus p_3p_4 \oplus p_1 \oplus p_4 = c_1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_2 \oplus p_4 = c_1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_3 \oplus p_4 = c_1 \oplus c_2 \oplus c_3 \oplus 1$	P = 1/8	Δ=3/4

Table 1 (Continue). Cloud Users' Responsibility Types of Attacks

№	Approximation equations	Possibility	Exclusion
S6	$p_3 \oplus p_4 = c_1 \oplus c_3 \oplus c_4$ $p_1 \oplus p_2 \oplus p_3 = c_3$ $p_3 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_2 \oplus c_3 \oplus 1$ $p_1 \oplus p_2 \oplus p_4 = c_1c_2 \oplus c_2c_3 \oplus c_1c_4 \oplus c_3c_4 \oplus c_2 \oplus c_3 \oplus 1$ $p_3 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_1 \oplus c_2 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_2 \oplus p_4 = c_1 \oplus c_3 \oplus c_4$	P = 1/8	Δ=3/4
S7	$p_2 \oplus p_3 \oplus p_4 = c_2 \oplus c_4$ $p_1 \oplus p_4 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_1 \oplus c_3 \oplus 1$ $p_3 \oplus p_4 = c_1c_2 \oplus c_1c_4 \oplus c_2c_3 \oplus c_3c_4 \oplus c_1 \oplus c_2 \oplus 1$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_1 \oplus p_3 = c_2 \oplus c_3 \oplus 1$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_2 \oplus p_4 = c_3$ $p_1p_2 \oplus p_2p_3 \oplus p_2p_3 \oplus p_3p_4 \oplus p_1 \oplus p_2 = c_2 \oplus c_3 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_2 \oplus p_4 = c_3$ $p_1p_3 \oplus p_2p_3 \oplus p_1p_4 \oplus p_2p_4 \oplus p_1 \oplus p_3 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_1 \oplus c_3 \oplus 1$	P = 1/8	Δ=3/4
S8	$p_1 \oplus p_3 = c_1 \oplus c_4 \oplus 1$ $p_2 = c_1 \oplus c_2$ $p_2 \oplus p_3 = c_2 \oplus c_3 \oplus c_4 \oplus 1$ $p_1 \oplus p_2 \oplus p_4 = c_1 \oplus c_2 \oplus c_3 \oplus c_4 \oplus 1$ $p_1 \oplus p_3 = c_1c_2 \oplus c_2c_3 \oplus c_1c_4 \oplus c_3c_4 \oplus c_2 \oplus c_3$ $p_2 = c_1c_2 \oplus c_1c_4 \oplus c_2c_3 \oplus c_3c_4 \oplus c_1 \oplus c_2$ $p_1 \oplus p_4 = c_1c_2 \oplus c_1c_4 \oplus c_2c_3 \oplus c_3c_4 \oplus c_3 \oplus c_4$	P = 1/8	Δ=3/4

2-round: In block S8, the equality $p_4=c_1\oplus c_2\oplus c_4\oplus 1$ has probability p=12/16, the variables in the approximation equality have the appearance $P2(32)\boxplus K2(32)=Y2(18)\oplus Y2(19)\oplus Y2(21)\oplus$

$P(18)\oplus P(19)\oplus P(21)\oplus 1$ according to the position of the round reflection, a cyclic left shift of 11 bits, and the addition of left-side appropriate bits. Since the value P2(32) in this parity represents the last bit, it is not affected by the summation, and since no other incoming text and key bits are involved, the addition $P2(32)\boxplus K2(32)$ is not involved. In this case, equation

$$P2(32)\oplus K2(32)=Y2(18)\oplus Y2(19)\oplus Y2(21)\oplus P(18)\oplus P(19)\oplus P(21)\oplus 1 \qquad (4)$$

Will appear Y1(32) = P2(32) as a result of combining equations 3 and 4 according to compatibility, the following equation results:

$$Y2(18)\oplus Y2(19)\oplus Y2(21)=(P(41)\oplus K1(9)\oplus$$

$$K1(11))*(K1(10)\oplus K1(12))\oplus P(41)\oplus K1(9)\oplus$$

$$K1(10))\oplus P(32)\oplus P(18)\oplus P(19)\oplus P(21)\oplus$$

$$K2(32)\oplus 1 \qquad (5)$$

3-round: In S3 block $(p_1\oplus p_3)(p_2\oplus p_4)\oplus p_1\oplus p_3=c_3$ with probability p=12/16 the variables in the approximation equality have the appearance of $\{(C(41)\boxplus K5(9))\oplus(C(43)\boxplus K5(11))\}*\{(C(42)\boxplus K5(10))\oplus(C(44)\boxplus K5(12))\}\oplus(C(41)\boxplus K5(9))\oplus(C(42)\boxplus K5(10))=Y5(32)\oplus C(32)$ according to the position in the round reflection, 11-bit left cyclic shift and addition of the left appropriate bits. In order not to encounter the problem of addition from the sum of bits in this equality, it is necessary to choose plaintexts that satisfy the condition S(42)=S(43)=S(44)=S(45)=0. Since the addition of the sum of S(41) and K5(9) in this block does not affect equality, it can be obtained in the form $S(41)\boxplus K5(9)=S(41)\oplus K5(9)$. In this case

$(S(41)\oplus K5(9)\oplus K5(11))*(K5(10)\oplus K5(12))\oplus S(41)\oplus$

$K5(9)\oplus K5(10))=Y5(32)\oplus S(32)$ (6) results in equality.

4-round: In block S8, the equality $p_4=c_1\oplus c_2\oplus c_4\oplus 1$ has probability p=12/16, the variables in the approximation equality have the appearance of $P4(32)\boxplus K4(32)=Y4(18)\oplus Y4(19)\oplus Y4(21)\oplus C(18)\oplus C(19)\oplus C(21)\oplus 1$ according to the position of the round reflection, 11-bit left cyclic shift and addition of the left-side appropriate bits. Since the value P4(32) in this parity represents the last bit, it is not affected by the summation, and since no other incoming text and key bits are involved, the addition $P4(32)\boxplus K4(32)$ is not involved.

In this case $P4(32)\oplus K4(32)=Y4(18)\oplus Y4(19)\oplus Y4(21)\oplus S(18)\oplus S(19)\oplus S(21)\oplus 1$ (7)

equality is formed. According to Y5(32)=P4(32), combining equations 6 and 7 results in the following equation:

$$Y4(18)\oplus Y4(19)\oplus Y4(21)=(C(41)\oplus K5(9)\oplus$$

$$K5(11))*(K5(10)\oplus K5(12))\oplus C(41)\oplus K5(9)\oplus$$

$$K5(10))\oplus C(32)\oplus C(18)\oplus C(19)\oplus C(21)\oplus$$

$$K4(32)\oplus 1 \qquad (8)$$

5 and 8 equations $Y4(18)\oplus Y4(19)\oplus Y4(21)=Y2(18)\oplus Y2(19)\oplus$

Y2(21) based on

$$(P(41) \oplus K1(9) \oplus K1(11)) * (K1(10) \oplus K1(12)) \oplus P(41) \oplus K1(9) \oplus K1(10)) \oplus P(32) \oplus P(18) \oplus P(19) \oplus P(21) \oplus 2(32) \oplus 1 = (C(41) \oplus K5(9) \oplus K5(11)) * (K5(10) \oplus K5(12)) \oplus C(41) \oplus K5(9) \oplus K5(10)) \oplus K4(32) \oplus C(32) \oplus C(18) \oplus C(19) \oplus C(21) \oplus 1$$

and this results the following:

$$(P(41) \oplus K1(9) \oplus K1(11)) * (K1(10) \oplus K1(12)) \oplus K1(9) \oplus K1(10) \oplus K2(32) \oplus (C(41) \oplus K5(9) \oplus K5(11)) * (K5(10) \oplus K5(12)) \oplus C(41) \oplus K5(9) \oplus K5(10)) \oplus K4(32) = P(32) \oplus P(18) \oplus P(19) \oplus P(21) \oplus C(32) \oplus C(18) \oplus C(19) \oplus C(21) \qquad (9)$$

The problem with sum-of-bits does not arise due to the fact that parity in general satisfies the following conditions:

$$\begin{cases} P(41) = P(42) = P(43) = P(44) = P(45) = 0 \\ C(41) = C(42) = C(43) = C(44) = C(45) = 0 \end{cases}$$

The solution to the above problem with sum-of-bits depends on the S-block being chosen and requires a different approach.

5. CONCLUSION

Modification of the GOST 28147-89 algorithm, that is, using the XOR operation instead of the mod232 operation, results of quadratic cryptanalysis method for the 5th round was used based on addition of bits using mod232 addition operation.

Due to this operation, the number of unknowns in the equation increases, since the value of each resulting bit depends on the values of the bits preceding it in order. For this reason, it is desirable to choose zero values of the corresponding bits of data entering the first round and exiting the fifth round in order to achieve an efficient result.

Since the second and fourth round input bits depend on the output values from the first and fifth round reflections, there is no option to select these bits. For this reason, it is necessary to consider these values as unknown.

The stages of using the quadratic cryptanalysis method for five rounds of GOST 28147-89 algorithm are created. In order to achieve an effective result in this method, it is shown that it is important to select the zero values of the corresponding bits of data entering the first round and exiting the fifth round.

REFERENCES

Akhmedov B.B. “Nonlinear cryptanalysis for modification of the XOR Encryption algorithm GOST 28147-89”, I Международная научно-практическая интернет-конференция «Актуальные вопросы физико-математических и технических наук: теоретические и прикладные исследования», г.Киев. 2021 г. 81-97 стр. www.openscilab.org.

Akhmedov B.B., Aloev R.D. Application of quadratic cryptanalysis for a five round XOR modification of the encryption algorithm GOST 28147-89 // International Journal of Science and Research (IJSR), https://www.ijsr.net/search_index_results_paperid.php?id=SR20818180335, Volume 9 Issue 8, August 2020, 1101 – 1109, ISSN: 2319-7064, India).

Carlet, C., & Gaborit, P. (2006). Hyper-bent functions and cyclic codes. *Journal of Combinatorial Theory, Series A*, *113*(3), 466-482.

Chee, S., Lee, S., & Kim, K. (1994, November). Semi-bent functions. In *International Conference on the Theory and Application of Cryptology* (pp. 105-118). Springer, Berlin, Heidelberg.

Dobbertin, H., & Leander, G. (2004, October). A survey of some recent results on bent functions. In *International Conference on Sequences and Their Applications* (pp. 1-29). Springer, Berlin, Heidelberg.

Dobbertin, H., & Leander, G. (2005). Cryptographer's Toolkit for Construction of $8 $-Bit Bent Functions. *Cryptology ePrint Archive*.

Kaliski, B. S., & Robshaw, M. J. (1994, August). Linear cryptanalysis using multiple approximations. In *Annual International Cryptology Conference* (pp. 26-39). Springer, Berlin, Heidelberg.

Knudsen, L. R., & Robshaw, M. J. (1996, May). Non-linear approximations in linear cryptanalysis. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 224-236). Springer, Berlin, Heidelberg.

Kuz'min, A. S., Markov, V. T., Nechaev, A. A., Shishkin, V. A., & Shishkov, A. B. (2008). Bent and hyper-bent functions over a field of 2ℓ elements. *Problems of Information Transmission*, *44*(1), 12-33.

Kuzmin, A. S., Markov, V. T., Nechaev, A. A., & Shishkov, A. B. (2006). Approximation of Boolean functions by monomial ones.

Logachev, O. A., Sal'nikov, A. A., & Yashchenko, V. V. (2004). Boolean functions in coding theory and cryptology. *MCCME, Moscow*.

Pfitzmann, B. (Ed.). (2003). *Advances in Cryptology–EUROCRYPT 2001: International Conference on the Theory and Application of Cryptographic Techniques Innsbruck, Austria, May 6–10, 2001, Proceedings* (Vol. 2045). Springer.

Qu, C., Seberry, J., & Pieprzyk, J. (2000). Homogeneous bent functions. *Discrete Applied Mathematics*, *102*(1-2), 133-139.

Quisquater, B. A. D. C. C. (2004). M Franklin M On multiple linear approximations. In *Advances in Cryptology–CRYPTO* (Vol. 2004).

Sakurai, K., & Furuya, S. (1997, January). Improving linear cryptanalysis of LOKI91 by probabilistic counting method. In *International Workshop on Fast Software Encryption* (pp. 114-133). Springer, Berlin, Heidelberg.

Vinokurov, A. Algorithm for cryptographic data transformation GOST 28147 89.

Youssef, A. M. (2007). Generalized hyper-bent functions over GF (p). *Discrete applied mathematics*, *155*(8), 1066-1070.

DOI: https://doi.org/10.34010/injiiscom.v3i2.8445
p-ISSN 2810-0670 e-ISSN 2775-5584

Kuryazov D.M., Sattarov A.B., Akhmedov B.B. Блокли симметрик шифрлаш алгоритмлари бардошлилигини замонавий криптотаҳлил усуллари билан баҳолаш. Ўқув қўлланма. Т.: «Aloqachi». 2017, 228 бет.