Application of Quadratic Cryptanalysis for a Five Round XOR Modification of the Encryption Algorithm Gost 28147-89

Rakhmatillo Djuraevich Aloev[1], **Bardosh Bobonazarovich Akhmedov**[2]

[1, 2]Department of Computational Mathematics and Information Systems, National University of Uzbekistan named after M. Ulugbek, Tashkent, Uzbekistan

Abstract: ***In the paper, we give analysis for the mathematical foundations of quadratic approximations; singularities of a binary operation $\langle\cdot,\cdot\rangle_k$ in the vector fieldZ_2^m, mathematical foundations of quadratic approximations of a special form (Boolean functions), and quadratic approximations of block ciphers. We also present the mathematical foundations of constructing correlation matrices using quadratic approximations for estimating nonlinear reflections of S-blocks in the block coding algorithm GOST 28147-89. Examples of four-bit permutations recommended for use in S-blocks of the algorithm GOST 28147-89 [6] are considered. It is shown that in almost all cases there are more probable (compared to linear) quadratic relations of a special form on the input and output bits of these permutations. Quadratic approximations are developed for round transformations of the algorithm GOST 28147-89. Also, quadratic relations of a special form are developed for input and output bits for a five round XOR modification of the encryption algorithm GOST 28147-89. The solutions of the problems of applying quadratic cryptanalysis to find some bits of round keys are given.***

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

1. Introduction

Currently, the possibilities of linear, differential, linear-differential, algebraic, and correlation cryptanalysis are being investigated to verify and evaluate the strength of encryption algorithms. Many works are devoted to improving applications of linear cryptanalysis. In particular, to increase the efficiency of the linear cryptanalysis method, it is proposed to consider several linear approximations simultaneously for one combination of key bits [9,10]. 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 [11].

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 [14], 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 28147-89 is resistant to these methods (with no less than five rounds of encryption in a linear cryptanalysis and seven rounds in a differential 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* [12-14] 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* [15], *partially bent functions* [16], Z$-$*bent functions* [17], *homogeneous bent functions* [18], *hyperbent functions* [19–22].

The main idea of using linear cryptanalysis of nonlinear approximations [23] 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 Quadratic cryptanalysis

N. Tokareva has investigated the possibilities of quadratic cryptanalysis of block ciphers, which are based on quadratic approximations of a special kind [1,4]. Namely, a binary operation$\langle\cdot,\cdot\rangle_k$wasdefined in [24] for each integer k, $1 \le k \le \frac{m}{2}$, on the set of vectorsZ_2^m, which, based on its properties, can be considered an analog of the scalar product of vectors over Z_2. The definition was given in the framework of the code-theoretic approach; in this case, it was essentially used the classification of Z_4-linear Hadamard-type codes obtained in the works by D. Krotov [3,4]. For a fixed vector $u \in Z_2^m$, the function $\langle u, v\rangle_k$of the variables$v_1, v_2, \dots, v_m$is linear or quadratic.

The work is of the theoretical character. Modifications of algorithms for the 1 and 2 linear Matsui crypt analyses [2] are proposed for the extended class of approximating functions. Formulas are given for calculating the absolute values of the dominance and reliability of the algorithms. It is shown that the use of *k-bent* functions as encryption functions allows us to reduce the maximum absolute value of prevalence to its minimum value and, therefore, to maximize the cipher's resistance to these quadratic approximations. Examples of four-bit substitutions recommended for use in the replacement nodes (S-blocks) of the algorithms GOST 28147-89, DES, s3DES are considered. Using a computer, it has been shown that for all these substitutions (except for one) there are more probable (compared to linear) quadratic relations of a special form for the input and output bits of these substitutions [1, 5].

In [8], the results of studies on the construction of correlation matrices based on the binary product $\langle u,v\rangle_k$ for six-digit transformations, as well as quadratic approximations and their combined use with linear correlation equations for determining key bits, are presented. This paper is a continuation of [8], and we consider the construction of correlation matrices based on the binary operation $\langle u,v\rangle_k$ for four-bit S-block transformations of the symmetric encryption algorithm GOST 28147-89, as well as the formation of quadratic approximations for round transformations. Also, for a five-round XOR modification of the symmetric encryption algorithm, GOST 28147-89 we consider the formation of the approximation equation for the input and output bits, the issues of finding round keys, and the use of quadratic cryptanalysis.

For the class of all Boolean functions of m variables$m \in Z$, let binary vectors $v = (v_1, v_2, \dots, v_m)$, $u = (u_1, u_2, \dots, u_m)$be defined, where$u_i, v_i \in Z_2$. For these binary vectors and any $k \in Z$, thebinaryoperation $\langle \cdot,\cdot \rangle_k$: $Z_2^m \times Z_2^m \to Z_2$, $1 \le k \le \frac{m}{2}$is defined in a following way[1]:$\langle u,v\rangle_k =$

$$\left(\oplus_{i=1}^{k} \oplus_{j=i}^{k} (u_{2i-1} \oplus u_{2i})(u_{2j-1} \oplus u_{2j})(v_{2i-1} \oplus v_{2i})(v_{2j-1} \oplus v_{2j})\right) \oplus \langle u,v\rangle, \quad (1)$$

here$\oplus_{i=1}^{k}$denotes the sum modulo 2 for$i = \overline{1,k}$, $\langle u,v\rangle$ is the usual scalar product of binary vectors overZ_2, i.e. $\langle u,v\rangle = u_1 v_1 \oplus u_2 v_2 \oplus \dots \oplus u_m v_m$. Note that coordinates of $v = (v_1, v_2, \dots, v_m)$, $u = (u_1, u_2, \dots, u_m)$ participate in the operation $\langle \cdot,\cdot \rangle_k$unequally. Namely, for the given k, exactly $2k$ first coordinates of each of the vectors $\boldsymbol{u}$, $\boldsymbol{v}$ are in both quadratic summands and linear ones; the others are only in linear ones. It follows from the definition that, for example, for$m = 4$:

$$\langle u,v\rangle_1 = \langle u,\hat{v}\rangle, \qquad (2)$$

here$\hat{v} = (v_2, v_1, v_3, v_4, \dots, v_m)$ is obtained from the vector $\boldsymbol{v}$ by a permutation of the coordinates v_1 and v_2.

As an example, we give an expression for the operation$\langle u,v\rangle_2$when$m = 4$:

$$\langle u,v\rangle_2 = (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1 \oplus v_2)(v_3 \oplus v_4) \oplus u_2 v_1 \oplus u_1 v_2 \oplus u_4 v_3 \oplus u_3 v_4 \qquad (3)$$

The main idea of the proposed approach is to expand the search for the most probable relationships for bits of plaintext, cipher text and key: from a variety of linear relationships to a variety of linear and quadratic relations of a special kind. The proved in [1] implies that for any even m, the power of the class of approximating functions is determined by the following equality:

$$|\Delta_m| = 2^m \left(1 + \sum_{k=2}^{m/2} \binom{m}{2k} \frac{(2k-1)!!}{2^k}\right).$$

The power of the class $\Delta_m$at$m = 4$ is equal to $\Delta_m = 28$, of which the number of linear functions is equal to$2^m = 16$, and nonlinear ones is equal to 12.

The application of nonlinear approximations in linear cryptanalysis using the Matsiu algorithm for block ciphers with r rounds of encryption is based on the following equation [1, 2]:

$$\langle \boldsymbol{a}, \pi(P)\rangle_i \oplus \langle \boldsymbol{b}, \sigma(C)\rangle_j = \langle \boldsymbol{d}, \tau(K)\rangle_k \qquad (4)$$

This equation holds with some probability $p = 1/2 + \varepsilon$with 0< $\varepsilon \le 1/2$, where theparameter $\varepsilon$is called the predominance of equality (4).

Here P is a plaintext, $P \in Z_2^m$, m_{key} is the key length, K is the encryption key,К $\in Z_2^{m_{key}}$,$\boldsymbol{a}, \boldsymbol{b} \in Z_2^m$, $\boldsymbol{d} \in Z_2^{m_{key}}$ are chosen vectors; $\pi, \sigma \in S_m, \tau \in S_{m_{key}}$ arefixed transformations; $1 \le i \le m/2$, $1 \le j \le m/2$, $1 \le k \le m_{key}/2$are integers.

For an unknown value of K, based on the collected statistics of pairs of plaintext and encrypted texts(P,C), where C=F(P,K),taking into account the parameter ε, it is decided that the relation $\langle \boldsymbol{d}, \tau(K)\rangle_k = \delta$ (for someδfromZ_2)is true. Using the obtained relation, a further analysis of the algorithm is carried out.

3. Research Method

3.1 Correlation matrices

In [1], formulas are given for calculating the absolute values of the predominance ε (associated with calculating Walsh-Hadamard coefficients k) and for calculating the reliability of algorithms. It is shown that the use of the bent function as encryption functions allows to reduce the maximum absolute value of prevalence to its minimum value and, therefore, to maximize the cipher's resistance to the considered quadratic approximations. The properties of approximating functions that can be used in quadratic cryptanalysis for matching nonlinear round approximations are given. The strength of the block cipher depends on the strength of the S-blocks used in it. To conduct quadratic cryptanalysis effectively, it is necessary to find more probable (compared to linear) quadratic relations, similar to (4), to the input and output bits of these permutations.
In the book by A.G. Rostovtsev and E.B. Makhovenko [25], a series of extreme four-digit permutations S$_1$, …, S$_{10}$ is given that are recommended for S-blocks of the standard GOST 28147-89. From each permutation by multiplying it by affine permutations, a whole class of external substitutions is obtained. All of them are selected so as to maximize the resistance of the cipher to methods of the linear and differential cryptanalysis.

The number of functions in the class Δ$_4$is equal to 28. 16 of them are linear functions, 12 are quadratic ones, which can be listed as follows [5]:

$\langle 0101, v_1v_2v_3v_4\rangle_2, \langle 0110, v_1v_2v_3v_4\rangle_2, \langle 1001, v_1v_2v_3v_4\rangle_2, \langle 1010, v_1v_2v_3v_4\rangle_2,$
$\langle 0101, v_1v_3v_2v_4\rangle_2, \langle 0110, v_1v_3v_2v_4\rangle_2, \langle 1001, v_1v_3v_2v_4\rangle_2, \langle 1010, v_1v_3v_2v_4\rangle_2,$
$\langle 0101, v_1v_4v_2v_3\rangle_2, \langle 0110, v_1v_4v_2v_3\rangle_2, \langle 1001, v_1v_4v_2v_3\rangle_2, \langle 1010, v_1v_4v_2v_3\rangle_2$

The binary vector $v = (v_1, v_2, v_3, v_4)$ in the binary operation $\langle\cdot,\cdot\rangle_2$is multiplied by integers from 0 to 15. Consider the relations

$$\langle \boldsymbol{a}, \pi(P)\rangle_i \oplus \langle \boldsymbol{b}, \sigma(C)\rangle_j = 0, \qquad (5)$$

Where for i = 1numbers from 0 to 15 and the identic permutation π correspond to the vector ***a*** (what corresponds to all linear combinations of bits of P); for$i$ = 2 the numbers 5, 6, 9, 10 and permutations π = id,(1324),(1342) correspond to the vector ***a*** (what corresponds to quadratic combinations of bits of P).

Similarly for$j$ = 1 and 2, we choose values for ***b***and σ. Under these conditions, the functions $\langle \boldsymbol{a}, \pi(P)\rangle_i, \langle \boldsymbol{b}, \sigma(C)\rangle_j$run through the whole set of functions $\Delta_4$without repetitions[5].

For example, S-block of the substitution S_1={4,10,9,2,13,8,0,14,6,11,1,12,7, 15,5,3} is selected for the standard algorithm GOST 28147-89.In accordance with formula (5), the correlation matrix for the binary operation $\langle\cdot,\cdot\rangle_2$is formulated. The correlation matrix of various linear and quadratic relations is presented in table 1.

Table 1: The correlation matrix of the selected S_1 -block

		j=1 id																	j=2 id					j=2 (1,3,2,4)					j=2 (1,4,2,3)			
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		5	6	9	10		5	6	9	10		5	6	9	10
i=1 id		16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8		8	8	8	8		8	8	8	8		8	8	8	8
		8	6	12	6	12	10	8	10	6	8	10	8	6	8	10	8		10	8	8	10		10	6	6	10		8	6	6	8
		8	8	6	10	6	10	8	8	6	10	8	8	4	4	10	6		8	10	8	10		6	8	6	12		6	6	8	12
		8	10	6	8	10	8	4	10	4	6	6	8	10	8	8	6		6	6	4	8		8	10	8	6		6	8	10	4
		8	12	10	6	6	10	8	12	10	10	8	8	8	8	6	6		8	10	8	10		10	8	6	8		10	6	8	8
		8	6	10	12	6	12	8	10	8	6	6	8	10	8	8	10		10	10	4	8		8	14	8	10		6	12	8	8
		8	8	12	8	8	4	8	8	8	8	4	8	8	4	8	8		4	8	8	4		4	8	8	4		8	8	8	8
		8	6	8	6	8	10	12	6	6	8	6	8	10	8	6	4		10	12	8	6		10	10	6	6		12	10	6	8
		8	10	8	6	8	10	8	6	10	4	6	4	6	8	10	8		10	8	4	6		8	8	4	8		6	8	4	6
		8	8	8	8	8	8	8	8	8	4	12	8	8	4	4	8		12	4	8	8		10	6	10	10		6	10	6	6
		8	10	6	8	10	8	12	10	8	6	6	12	6	8	8	10		10	10	8	4		6	8	6	8		8	10	4	10
		8	12	10	10	10	10	8	4	6	10	8	8	8	8	6	10		8	10	8	10		8	10	8	10		8	8	10	10
		8	6	6	8	10	8	8	10	8	10	6	4	6	8	4	10		6	10	8	8		6	8	6	8		8	6	8	10
		8	8	10	10	6	6	8	8	6	6	8	8	4	12	6	6		8	6	8	6		4	6	8	10		4	8	6	10
		8	10	8	10	8	6	12	10	6	8	10	4	10	8	10	8		10	8	12	6		8	8	12	8		10	12	8	10
		8	8	8	12	12	8	8	8	12	8	8	8	8	8	8	4		8	8	8	8		6	10	10	10		6	10	10	10
i=2 id	5	8	8	10	10	8	8	10	10	8	8	2	10	8	8	10	10		6	12	6	4		4	12	6	6		8	10	8	10
	6	8	6	12	10	6	8	6	8	8	6	8	6	10	4	6	8		8	6	6	8		8	10	10	8		6	10	10	6
	9	8	10	8	6	10	4	10	8	8	6	8	10	6	4	6	8		8	6	10	4		6	4	8	6		8	8	4	8
	10	8	8	6	10	8	12	10	10	8	4	10	10	8	8	6	10		14	8	6	8		10	10	8	12		6	12	6	8
i=2 (13,2,4)	5	8	6	8	10	8	10	12	10	10	8	6	8	6	8	6	12		10	12	8	6		6	10	6	10		8	10	6	12
	6	8	6	8	10	8	10	4	10	6	8	6	4	10	8	6	8		6	8	4	10		8	12	8	8		6	8	12	6
	9	8	10	4	6	12	6	8	10	6	8	6	8	6	8	6	8		6	8	8	6		6	6	6	6		8	6	6	8
	10	8	10	8	10	8	10	8	10	6	4	6	12	10	8	10	8		10	8	4	6		8	12	8	8		6	12	8	6
i=2 (1,4,2,3)	5	8	6	10	8	8	6	10	8	10	8	8	6	6	4	4	10		8	10	10	6		6	6	8	8		8	8	6	10
	6	8	8	8	8	10	6	6	10	6	10	2	6	8	8	8	8		2	10	6	6		4	10	6	4		8	6	10	8
	9	8	8	4	8	10	10	6	10	6	6	10	6	8	8	4	8		10	6	6	10		10	8	8	10		6	8	8	6
	10	8	10	10	8	8	6	6	8	6	4	8	10	10	4	8	6		8	4	6	6		8	8	10	6		6	10	8	4

3.2 Quadratic relations of a special form

In accordance with the correlation matrix of the selected S-block, the maximum deviation satisfies the equation $\langle \boldsymbol{a}, \pi(P)\rangle_i \oplus \langle \boldsymbol{b}, \sigma(C)\rangle_j = 0$with the probability p=7/8 in the following cases:

1) $i = 1, a = 5, \pi = id, j = 2, b = 6, \sigma = (1324)\langle(0101),(p_1,p_2,p_3,p_4)\rangle_1 \oplus \langle(0110),(c_1,c_3,c_2,c_4)\rangle_2 = 0$

$$p_1 \oplus p_4 = c_1c_2 \oplus c_2c_3 \oplus c_1c_4 \oplus c_3c_4 \oplus c_1 \oplus c_4$$

2) $i = 2, a = 10, \pi = id, j = 2, b = 5, \sigma = id\langle(1010),(p_1,p_2,p_3,p_4)\rangle_2 \oplus \langle(0101),(c_1,c_2,c_3,c_4)\rangle_2 = 0$

$$p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_2 \oplus p_4 = c_1c_3 \oplus c_1c_4 \oplus c_2c_3 \oplus c_2c_4 \oplus c_1 \oplus c_3$$

3) $i = 2, a = 5, \pi = id, j = 1, b = 10, \sigma = id\langle(0101),(p_1,p_2,p_3,p_4)\rangle_2 \oplus \langle(1010),(c_1,c_2,c_3,c_4)\rangle_1 = 1$

$$p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_1 \oplus p_3 = c_2 \oplus c_3 \oplus 1$$

4) $i = 2, a = 6, \pi = (1423), j = 1, b = 10, \sigma = id\langle(0110), (p_1, p_4, p_2, p_3)\rangle_2 \oplus \langle(1010), (c_1, c_2, c_3, c_4)\rangle_1 = 1$

$$p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_1 \oplus p_3 = c_2 \oplus c_4 \oplus 1$$

5) $i = 2, a = 6, \pi = (1423), j = 2, b = 5, \sigma = id\langle(0110), (p_1, p_4, p_2, p_3)\rangle_2 \oplus \langle(0101), (c_1, c_2, c_3, c_4)\rangle_2 = 1$

$$p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_1 \oplus p_3 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_1 \oplus c_3 \oplus 1$$

Also, for the remaining S-block permutations, various linear and quadratic relations were calculated, and the most probable approximation equations were revealed for them. The results are presented in table 2:

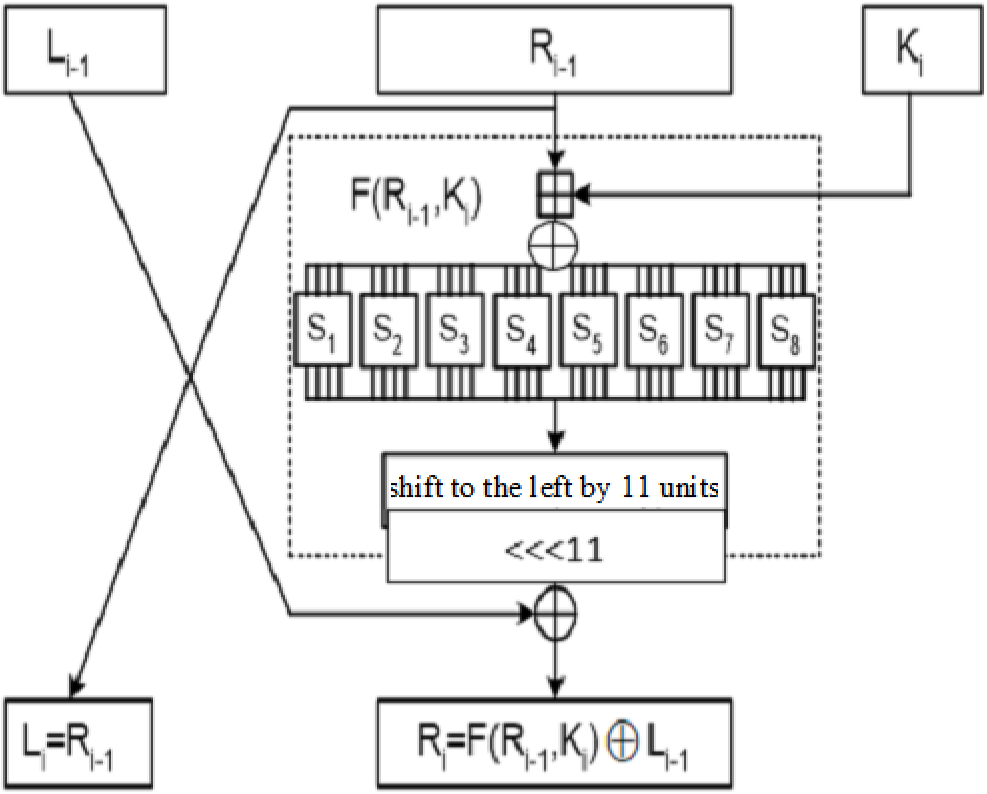
Table 2: The most probable equations for S-blocks of substitutions

S-block	The approximation equation	Probability value	Deviation value
1	$p_1 \oplus p_4 = c_1c_2 \oplus c_2c_3 \oplus c_1c_4 \oplus c_3c_4 \oplus c_1 \oplus c_4$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_2 \oplus p_4 = c_1c_3 \oplus c_1c_4 \oplus c_2c_3 \oplus c_2c_4 \oplus c_1 \oplus c_3$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_1 \oplus p_3 = c_2 \oplus c_3 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_1 \oplus p_3 = c_2 \oplus c_3 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_1 \oplus p_3 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_1 \oplus c_3 \oplus 1$	p = 1/8	Δ=3/4
2	$p_1 \oplus p_3 \oplus p_4 = c_1 \oplus c_4 \oplus 1$ $p_1 \oplus p_2 = c_1 \oplus c_2 \oplus c_4$ $p_1 \oplus p_2 \oplus p_3 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_2 \oplus c_3$ $p_1p_2 \oplus p_1p_4 \oplus p_2p_3 \oplus p_3p_4 \oplus p_2 \oplus p_3 = c_1 \oplus c_2 \oplus c_4$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_4 \oplus p_3 = c_3 \oplus c_4 \oplus 1$	p = 1/8	Δ=3/4
3	$p_1 \oplus p_4 = c_1 \oplus c_3$ $p_2 \oplus p_3 \oplus p_4 = c_1 \oplus c_3 \oplus c_4$ $p_2 \oplus p_3 = c_1 \oplus c_2 \oplus c_3 \oplus 1$ $p_1 \oplus p_3 = c_1c_2 \oplus c_2c_3 \oplus c_1c_4 \oplus c_3c_4 \oplus c_1 \oplus c_2 \oplus 1$ $p_4 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_2 \oplus c_4 \oplus 1$ $p_1 \oplus p_4 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_3 \oplus c_4$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_1 \oplus p_3 = c_1 \oplus c_2 \oplus 1$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_2 \oplus p_4 = c_1 \oplus c_3$ $p_1p_2 \oplus p_1p_4 \oplus p_2p_3 \oplus p_3p_4 \oplus p_1 \oplus p_4 = c_1 \oplus c_2 \oplus c_3$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_1 \oplus p_3 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_1 \oplus c_3 \oplus 1$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_1 \oplus p_3 = c_1c_2 \oplus c_1c_3 \oplus c_2c_4 \oplus c_3c_4 \oplus c_3 \oplus c_4$	p = 1/8	Δ=3/4
4	$p_3 = c_1 \oplus c_2 \oplus c_3 \oplus c_4 \oplus 1$ $p_1 \oplus p_3 \oplus p_4 = c_1$ $p_2 \oplus p_4 = c_3 \oplus 1$ $p_3 \oplus p_4 = c_1c_2 \oplus c_2c_3 \oplus c_1c_4 \oplus c_3c_4 \oplus c_2 \oplus c_3$ $p_3 \oplus p_4 = c_1c_2 \oplus c_1c_3 \oplus c_2c_4 \oplus c_3c_4 \oplus c_1 \oplus c_3$ $p_1 \oplus p_2 \oplus p_3 \oplus p_4 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_1 \oplus c_2 \oplus 1$ $p_1 \oplus p_2 \oplus p_4 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_3 \oplus c_4$ $p_1p_2 \oplus p_1p_4 \oplus p_2p_3 \oplus p_3p_4 \oplus p_2 \oplus p_3 = c_4 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_2 \oplus p_4 = c_3 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_1 \oplus p_2 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_1 \oplus c_3 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_1 \oplus p_2 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_1 \oplus c_3 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_3 \oplus p_4 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_2 \oplus c_4$	p = 1/8	Δ=3/4
5	$p_3 = c_1 \oplus c_2 \oplus c_3 \oplus c_4$ $p_1 \oplus p_2 \oplus p_3 \oplus p_4 = c_1c_2 \oplus c_2c_3 \oplus c_1c_4 \oplus c_3c_4 \oplus c_1 \oplus c_2$ $p_1p_2 \oplus p_1p_4 \oplus p_2p_3 \oplus p_3p_4 \oplus p_1 \oplus p_4 = c_1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_2 \oplus p_4 = c_1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_3 \oplus p_4 = c_1 \oplus c_2 \oplus c_3 \oplus 1$	p = 1/8	Δ=3/4
6	$p_3 \oplus p_4 = c_1 \oplus c_3 \oplus c_4$ $p_1 \oplus p_2 \oplus p_3 = c_3$ $p_3 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_2 \oplus c_3 \oplus 1$ $p_1 \oplus p_2 \oplus p_4 = c_1c_2 \oplus c_2c_3 \oplus c_1c_4 \oplus c_3c_4 \oplus c_2 \oplus c_3 \oplus 1$ $p_3 = c_1c_2 \oplus c_2c_4 \oplus c_1c_3 \oplus c_3c_4 \oplus c_1 \oplus c_2 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_2 \oplus p_4 = c_1 \oplus c_3 \oplus c_4$	p = 1/8	Δ=3/4
7	$p_1 = c_4 \oplus 1$ $p_2 \oplus p_3 \oplus p_4 = c_2 \oplus c_4$ $p_1 \oplus p_4 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_1 \oplus c_3 \oplus 1$ $p_3 \oplus p_4 = c_1c_2 \oplus c_1c_4 \oplus c_2c_3 \oplus c_3c_4 \oplus c_1 \oplus c_2 \oplus 1$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_1 \oplus p_3 = c_2 \oplus c_3 \oplus 1$ $p_1p_3 \oplus p_1p_4 \oplus p_2p_3 \oplus p_2p_4 \oplus p_2 \oplus p_4 = c_3$ $p_1p_2 \oplus p_2p_3 \oplus p_2p_3 \oplus p_3p_4 \oplus p_1 \oplus p_2 = c_2 \oplus c_3 \oplus 1$ $p_1p_2 \oplus p_1p_3 \oplus p_2p_4 \oplus p_3p_4 \oplus p_2 \oplus p_4 = c_3$ $p_1p_3 \oplus p_2p_3 \oplus p_1p_4 \oplus p_2p_4 \oplus p_1 \oplus p_3 = c_1c_3 \oplus c_2c_3 \oplus c_1c_4 \oplus c_2c_4 \oplus c_1 \oplus c_3 \oplus 1$	p = 1/8	Δ=3/4
8	$p_1 \oplus p_3 = c_1 \oplus c_4 \oplus 1$	p = 1/8	Δ=3/4

	$p_2 = c_1 \oplus c_2$ $p_2 \oplus p_3 = c_2 \oplus c_3 \oplus c_4 \oplus 1$ $p_1 \oplus p_2 \oplus p_4 = c_1 \oplus c_2 \oplus c_3 \oplus c_4 \oplus 1$ $p_1 \oplus p_3 = c_1 c_2 \oplus c_2 c_3 \oplus c_1 c_4 \oplus c_3 c_4 \oplus c_2 \oplus c_3$ $p_2 = c_1 c_2 \oplus c_1 c_4 \oplus c_2 c_3 \oplus c_3 c_4 \oplus c_1 \oplus c_2$ $p_1 \oplus p_4 = c_1 c_2 \oplus c_1 c_4 \oplus c_2 c_3 \oplus c_3 c_4 \oplus c_3 \oplus c_4$		

3.3. Quadratic cryptanalysis

Next, we consider the application of the found most probable linear and quadratic cryptanalysis relationships for a five round XOR modification of the encryption algorithm GOST 28147-89. Below is a functional diagram of the transformations of the i-round XOR modification of this algorithm:



Picture 1: i-round XOR modifications of the algorithm GOST 28147-89

To conduct quadratic cryptanalysis of the 5-round encryption algorithm GOST 28147-89, it is necessary to choose effective combinations of approximation equations.

Picture 2 shows a scheme of the construction of the approximation equation using, as an example, the 5-round algorithm GOST 28147-89 by the identified most probable relationships for pairs of S_1-and S_6-blocks.In accordance with this scheme, the key bits of the third round are not involved in the equation, and the equations of relations for the input bits of the first round and the output bits of the fifth round are developed. In the first and fifth rounds for the S_1-block, the following approximation equations are used:

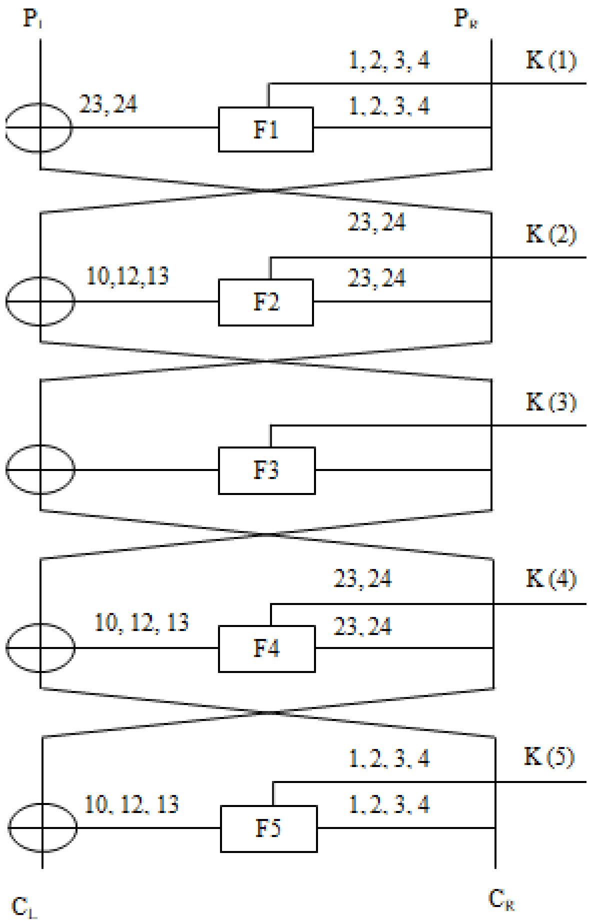
$$(p_1 \oplus p_2)(p_3 \oplus p_4) \oplus p_1 \oplus p_3 = \\ p1p3 \oplus p1p4 \oplus p2p3 \oplus p2p4 \oplus p1 \oplus p3 = c2 \oplus c3 \oplus 1. \quad (6)$$

The 4-bits of the input of block S_1 correspond to 1, 2, 3, 4-bits of the right block of theare added to the corresponding bits of the right side of the plaintext. The output 2 and 3-bits of block S_1, after a cyclic left shift of 11 bits, shifted by 23 and 24-bits of the right side, are added modulo 2 (XOR) to 23 and 24 bits of the left side of the plaintext block and these bits correspond to 3 and 4-input bits of block S_6.

In the second and fourth rounds for the S_6-block, the following approximation equations are used:

$$p_3 \oplus p_4 = c_1 \oplus c_3 \oplus c_4. \quad (7)$$

3 and 4- input bits of block S_6 correspond to 23 and 24-bits of the input text round and, respectively, 23 and 24-bits of the round key are added to 23 and 24-bits of the input text. Output 1, 3, and 4-bits of block S_6 are 21, 23, and 24-bits of a block of text, and after a cyclic left shift of 11 bits, shifted by 10, 12 and 13-bits of the right side, are added modulo 2 (XOR) to 10, 12 and 13-bits of the left side of the block of plaintext.



In the 1st round, in accordance with (6), we obtain $(P[33]\oplus P[34])*(P[35]\oplus P[36])\oplus P[33]\oplus P[35]\oplus(K_1[1]\oplus K_1[2])*(K_1[3]\oplus K_1[4])\oplus K_1[1]\oplus K_1[3]\oplus 1 = Y_1[23]\oplus Y_1[24]\oplus P[23]\oplus P[24]$ (8)

Here P[i] are bits of a plaintext, and they, in turn, consist of concatenation of the left and right parts of the input text, i.e. express 64-bit (1,2,...,31,32,33,...,64) $P=P_L\cup P_R=(P[1], P[2], \dots, P[32])\cup(P[33], P[34], \dots, P[64])$. The value $Y_r[i]$ denotes the *i*-bit after a cyclic shift to the left by 11 digits of the output value S of the block of the *r*-round. $K_r[i]$ denotes the *i*-bit of the round key, and $P_r[i]$ denotes the *i*-bit of the input text of the *r*-round.

23 and 24-bits of the output value of the first round are input values of the second round $Y_1[23]\oplus Y_1[24]\oplus P[23]\oplus P[24]=P_2[23]\oplus P_2[24]$ (9).

This relation is the connecting node of the first and second rounds.

When entering the round transform of the S block, a round key is added to them, i.e. $P_2[23]\oplus P_2[24]\oplus K_2[23]\oplus K_2[24]$, and they correspond to the third and fourth bits of block S_6, we obtain on the second round in accordance with (7) the following equations:

$P_2[23]\oplus P_2[24]\oplus K_2[23]\oplus K_2[24]= Y'_2[21]\oplus Y'_2[23]\oplus Y'_2[24]$;
after a cyclic shift to the left by 11 digits and adding the left side to the input text of the round, we get:
$P_2[23]\oplus P_2[24]\oplus K_2[23]\oplus K_2[24]=Y_2[10]\oplus Y_2[12]\oplus Y_2[13]\oplus P[42]\oplus P[44]\oplus P[45]$ (10)

In accordance with (9), equations (8) and (10), the relation takes the following form:
$(P[33]\oplus P[34])*(P[35]\oplus P[36])\oplus P[33]\oplus P[35]\oplus(K_1[1]\oplus K_1[2])*(K_1[3]\oplus K_1[4])\oplus K_1[1]\oplus K_1[3]\oplus 1= K_2[23]\oplus K_2[24]\oplus Y_2[10]\oplus Y_2[12]\oplus Y_2[13]\oplus P[42]\oplus P[44]\oplus P[45]$(11)

We obtain in accordance with (6) on the fifth round:
$(C[33]\oplus C[34])*(C[35]\oplus C[36])\oplus C[33]\oplus C[35]\oplus(K_5[1]\oplus K_5[2])*(K_5[3]\oplus K_5[4])\oplus K_5[1]\oplus K_5[3]\oplus 1= Y_5[23]\oplus Y_5[24]\oplus C[23]\oplus C[24]$ (12)

Here C [i] denotes the bits of the cipher text and, in turn, consists of concatenating the left and right parts of the output text, i.e. expresses the 64-bit (1,2,...,31,32,33,...,64) cipher text $C=C_L\cup C_R=(C[1], C[2], \dots, C[32])\cup(C[33], C[34], \dots, C[64])$.
23 and 24-bits of the output value of the fifth round correspond to 3 and 4-bits of block S_6, so we obtain on the fourth round and in accordance with (7) the following equations:

$P_4[23]\oplus P_4[24]\oplus K_4[23]\oplus K_4[24] = Y_4[10]\oplus Y_4[12]\oplus Y_4[13]\oplus C[42]\oplus C[44]\oplus C[45]$ (13)

Here, too, by the property of the Feistel network, the input values of the fifth round are respectively equal to the output values of the fourth round, i.e.

$P_4[23]\oplus P_4[24]=Y_5[23]\oplus Y_5[24]\oplus C[23]\oplus C[24]$.

Therefore, relations (12) and (13) will take the following form:
$(C[33]\oplus C[34])*(C[35]\oplus C[36])\oplus C[33]\oplus C[35]\oplus(K_5[1]\oplus K_5[2])*(K_5[3]\oplus K_5[4])\oplus K_5[1]\oplus K_5[3]\oplus 1= K_4[23]\oplus K_4[24]\oplus Y_4[10]\oplus Y_4[12]\oplus Y_4[13]\oplus C[42]\oplus C[44]\oplus C[45]$ (14)

Hence, we obtain the following equations from relations (11) and (14):
$Y_2[10]\oplus Y_2[12]\oplus Y_2[13]\oplus P[42]\oplus P[44]\oplus P[45]=(P[33]\oplus P[34])*(P[35]\oplus P[36])\oplus P[33]\oplus P[35]\oplus(K_1[1]\oplus K_1[2])*(K_1[3]\oplus K_1[4])\oplus K_1[1]\oplus K_1[3]\oplus K_2[23]\oplus K_2[24]\oplus 1$;
$Y_4[10]\oplus Y_4[12]\oplus Y_4[13]\oplus C[42]\oplus C[44]\oplus C[45]=(C[33]\oplus C[34])*(C[35]\oplus C[36])\oplus C[33]\oplus C[35]\oplus(K_5[1]\oplus K_5[2])*(K_5[3]\oplus K_5[4])\oplus K_5[1]\oplus K_5[3]\oplus K_4[23]\oplus K_4[24]\oplus 1$.

The output value of the second round is equal to the input value of the fourth round, i.e.
$Y_2[10]\oplus Y_2[12]\oplus Y_2[13]\oplus P[42]\oplus P[44]\oplus P[45]=Y_4[10]\oplus Y_4[12]\oplus Y_4[13]\oplus C[42]\oplus C[44]\oplus C[45]$,
and, therefore, we obtain the following relation:
$(K_1[1]\oplus K_1[2])*(K_1[3]\oplus K_1[4])\oplus K_1[1]\oplus K_1[3]\oplus K_2[23]\oplus K_2[24]\oplus K_4[23]\oplus K_4[24]\oplus (K_5[1]\oplus K_5[2])*(K_5[3]\oplus K_5[4])\oplus K_5[1]\oplus K_5[3]=(P[33]\oplus P[34])*(P[35]\oplus P[36])\oplus P[33]\oplus P[35]\oplus P[23]\oplus P[24]\oplus (C[33]\oplus C[34])*(C[35]\oplus C[36])\oplus C[33]\oplus C[35]\oplus C[23]\oplus C[24]$ (15)

The probability of fulfilling equation (15) depends on the fulfillment of relations of the first, second, fourth, and fifth rounds; therefore, the deviation values are calculated as follows:

$\Delta(S_{(1)} \oplus S_{(2)} \oplus S_{(4)} \oplus S_{(5)})=\Delta_{1*}\Delta_{2*}\Delta_{4*}\Delta_5$
$=(3/4)*(3/4)*(3/4)*(3/4)=0{,}3164$

Thus, the probability of fulfilling equation (15) in accordance with the lemma defining a static linear analog of nonlinear functions [7] $\Delta=|1-2p|$, is $p=(1+\Delta)/2=0{,}6582$.

Having analyzed several open and correspondingly encrypted texts for the cases T>N/2 and p>1/2, it is determined that the statistical value of equation (15) is zero [7].

$(K_1[1]\oplus K_1[2])*(K_1[3]\oplus K_1[4])\oplus K_1[1]\oplus K_1[3]\oplus K_2[23]\oplus K_2[24]\oplus K_4[23]\oplus K_4[24]\oplus$
$(K_5[1]\oplus K_5[2])*(K_5[3]\oplus K_5[4])\oplus K_5[1]\oplus K_5[3]=0.$

For the correlation matrix of linear and quadratic relations of input and output bits of S blocks of five round XOR modifications of the encryption algorithm GOST 28147-89, the following equations are obtained, which have a probability different from p=0,5:

Table 3: The approximation equation for the 5-round XOR modification of the cipher algorithm GOST 28147-89

No	Equation	Probability values
S_1:S_6block	$(K_1[1]\oplus K_1[2])*(K_1[3]\oplus K_1[4])\oplus K_1[1]\oplus K_1[3]\oplus K_2[23]\oplus K_2[24]\oplus K_4[23]\oplus K_4[24]\oplus (K_5[1]\oplus K_5[2])*(K_5[3]\oplus K_5[4])\oplus K_5[1]\oplus K_5[3]=0$	p=0,66
	$(K_1[1]\oplus K_1[4])*(K_1[2]\oplus K_1[3])\oplus K_1[1]\oplus K_1[3]\oplus K_2[23]\oplus K_2[24]\oplus K_4[23]\oplus K_4[24]\oplus (K_5[1]\oplus K_5[4])*(K_5[2]\oplus K_5[3])\oplus K_5[1]\oplus K_5[3]=0$	*p* = 0,66
	$K_1[2] \oplus K_1[3] \oplus K_1[4] \oplus K_2[25] \oplus K_4[25] \oplus K_5[2] \oplus K_5[3] \oplus K_5[4]=1$	*p*=0,43
	$K_1[4] \oplus K_5[4] \oplus K_2[24] \oplus K_4[24]=0$	*p* = 0,47
S_2:S_7block	$(K_1[5]\oplus K_1[8])*(K_1[6]\oplus K_1[7])\oplus K_1[5]\oplus K_1[6]\oplus K_1[7]\oplus K_1[8]\oplus K_2[26]\oplus K_2[27]\oplus K_2[28]\oplus(K_5[5]\oplus K_5[8])*(K_5[6]\oplus K_5[7])\oplus K_5[5]\oplus K_5[6]\oplus K_5[7]\oplus K_5[8]\oplus K_4[26]\oplus K_4[27]\oplus K_4[28]=1$	p=0,57
	$K_1[7] \oplus K_5[7] \oplus K_2[28] \oplus K_4[28]=0$	*p* = 0,47
	$K_1[7] \oplus K_1[8] \oplus K_5[7] \oplus K_5[8] \oplus K_2[29] \oplus K_4[29] = 0$	*p* = 0,47
S_3:S_8block	$(K_1[9]\oplus K_1[12)*(K_1[10]\oplus K_1[11])\oplus K_1[9]\oplus K_1[11]\oplus K_2[30]\oplus K_2[31]\oplus K_4[30]\oplus K_4[31]\oplus (K_5[9]\oplus K_5[12)*(K_5[10]\oplus K_5[11])\oplus K_5[9]\oplus K_5[11] = 0$	*p*=0,34
	$(K_1[9]\oplus K_1[11)*(K_1[10]\oplus K_1[12])\oplus K_1[9]\oplus K_1[12]\oplus K_2[30]\oplus K_2[31]\oplus K_2[32]\oplus K_4[30]\oplus K_4[31]\oplus K_4[32] \oplus(K_5[9]\oplus K_5[11)*(K_5[10]\oplus K_5[12])\oplus K_5[9]\oplus K_5[12]=0$	*p*=0,57
	$K_1[9]\oplus K_1[10] \oplus K_1[11]\oplus K_2[30]\oplus K_4[30]\oplus K_5[9] \oplus K_5[10] \oplus K_5[11] =0$	*p* = 0,47
	$K_1[9]\oplus K_1[10]\oplus K_1[12] \oplus K_2[30] \oplus K_4[30] \oplus K_5[9] \oplus K_5[10] \oplus K_5[12]=0$	*p*=0,43
S_4:S_2 and S_4:S_1 blocks	$(K_1[13]\oplus K_1[15)*(K_1[14]\oplus K_1[16])\oplus K_1[14]\oplus K_1[15]\oplus K_2[5]\oplus K_4[5]\oplus \oplus(K_5[13]\oplus K_5[15)*(K_5[14]\oplus K_5[16])\oplus K_5[14]\oplus K_5[15]=0$ (K.2.14) (*S_4:S_2)*	p=0,43
	$(K_1[13]\oplus K_1[16)*(K_1[14]\oplus K_1[15])\oplus K_1[14]\oplus K_1[16]\oplus K_2[4]\oplus K_4[4] \oplus \oplus(K_5[13]\oplus K_5[16)*(K_5[14]\oplus K_5[15])\oplus K_5[14]\oplus K_5[16]= 0$	*p* = 0,43
	$K_1[14]\oplus K_1[16]\oplus K_2[4]\oplus K_4[4] \oplus K_5[14]\oplus K_5[16]= 0$	*p*=0,47
S_5:S_2block	$(K_1[17]\oplus K_1[19)*(K_1[18]\oplus K_1[20])\oplus K_1[17]\oplus K_1[20]\oplus K_2[6]\oplus K_4[6] \oplus \oplus(K_5[17]\oplus K_5[19])*(K_5[18]\oplus K_5[20])\oplus K_5[17]\oplus K_5[20]=0$	*p* =0,43
	$(K_1[17]\oplus K_1[20])*(K_1[18]\oplus K_1[19])\oplus K_1[18]\oplus K_1[20]\oplus K_2[6]\oplus K_4[6] \oplus \oplus(K_5[17]\oplus K_5[20])*(K_5[18]\oplus K_5[19])\oplus K_5[18]\oplus K_5[20]= 0$	*p* = 0,43
	$(K_1[17]\oplus K_1[20])*(K_1[18]\oplus K_1[19])\oplus K_1[19]\oplus K_1[20]\oplus K_2[6]\oplus K_2[7]\oplus K_2[8]\oplus K_4[6]\oplus K_4[7]\oplus K_4[8]\oplus(K_5[17]\oplus K_5[20])*(K_5[18]\oplus K_5[19])\oplus K_5[19]\oplus K_5[20]=0$	*p* = 0,43
	$K_1[19]\oplus K_1[20]\oplus K_2[6]\oplus K_4[6]\oplus K_5[19]\oplus K_5[20]=0$	*p*=0,47
	$K_1[19]\oplus K_1[20]\oplus K_2[9]\oplus K_4[9]\oplus K_5[19]\oplus K_5[20]= 1$	*p*= 0,47
S_6:S_3block	$K_1[21]\oplus K_1[22]\oplus K_1[23]\oplus K_2[12]\oplus K_4[12]\oplus K_5[21]\oplus K_5[22]\oplus K_5[23]=0$	*p* =0,43
	$K_1[22]\oplus K_1[24]\oplus K_2[13]\oplus K_4[13]\oplus K_5[22]\oplus K_5[24]=1$	*p*=0,47
S_7:S_4block	$(K_1[25]\oplus K_1[28])*(K_1[26]\oplus K_1[27])\oplus K_1[25]\oplus K_1[26]\oplus K_2[15]\oplus K_2[16]\oplus K_4[15]\oplus K_4[16]\oplus(K_5[25]\oplus K_5 [28])*(K_5[26]\oplus K_5[27])\oplus K_5[25]\oplus K_5[26]=0$	*p* =0,66
	$(K_1[25]\oplus K_1[26])*(K_1[27]\oplus K_1[28])\oplus K_1[25]\oplus K_1[27]\oplus K_2[15]\oplus K_2[16]\oplus K_4[15]\oplus K_4[16]\oplus(K_5[25]\oplus K_5 [26])*(K_5[27]\oplus K_5[28])\oplus K_5[25]\oplus K_5[27]=0$	*p* = 0,66
	$K_1[25]\oplus K_2[17]\oplus K_4[17]\oplus K_5[25]=0$	*p*=0,43
	$K_1[19]\oplus K_1[20]\oplus K_2[6]\oplus K_4[6]\oplus K_5[19]\oplus K_5[20]=0$	*p*=0,47
S_8:S_7:S_5block	$K_1[29]\oplus K_1[30]\oplus K_1[25]\oplus K_2[17]\oplus K_2[18]\oplus K_2[19]\oplus K_2[20]\oplus K_4[17]\oplus K_4[18]\oplus K_4[19]\oplus K_4[20] \oplus K_5[29]\oplus K_5[30]\oplus K_5[25]=1$	*p* =0,57
	$K_1[30] \oplus K_1[32]\oplus K_2[21]\oplus K_4[21]\oplus K_5[30] \oplus K_5[32]=0$	*p*=0,47
	$K_1[30] \oplus K_1[31]\oplus K_1[32]\oplus K_2[19]\oplus K_4[19]\oplus K_5[30] \oplus K_5[31]\oplus K_5[32]=0$	*p*=0,43

Based on the equations of table 3, the key bits are found, they are listed in table 4.

Table 4: Found bits of the key

Number of key bits	1-round	2-round	4-round	5-round
14	$K_1[1]=0$, $K_1[2]=0$, $K_1[3]=1$, $K_1[4]=1$	$K_2[23]=1$, $K_2[24]=1$, $K_2[25]=0$	$K_4[23]=1$, $K_4[24]=1$, $K_4[25]=1$	$K_5[1]=0$, $K_5[2]=0$, $K_5[3]=1$, $K_5[4]=1$
16	$K_1[5]=1$, $K_1[6]=0$, $K_1[7]=1$, $K_1[8]=1$	$K_2[26]=0$, $K_2[27]=0$, $K_2[28]=0$ $K_2[29]=0$	$K_4[26]=1$,$K_4[27]=0$, $K_4[28]=0$, $K_4[29]=0$	$K_5[5]=1$, $K_5[6]=0$, $K_5[7]=1$, $K_5[8]=1$
14	$K_1[9]=1$, $K_1[10]=0$, $K_1[11]=0$, $K_1[12]=1$	$K_2[30]=0$, $K_2[31]=0$, $K_2[32]=0$	$K_4[30]=0$, $K_4[31]=0$, $K_4[32]=0$	$K_5[9]=1$, $K_5[10]=0$, $K_5[11]=0$, $K_5[12]=1$
12	$K_1[13]=1$, $K_1[14]=0$, $K_1[15]=1$, $K_1[16]=0$	$K_2[4]=0$, $K_2[5]=0$	$K_4[4]=0$, $K_4[5]=0$	$K_5[13]=0$, $K_5[14]=0$, $K_5[15]=0$, $K_5[16]=0$
16	$K_1[17]=1$, $K_1[18]=1$, $K_1[19]=0$, $K_1[20]=0$	$K_2[6]=0$, $K_2[7]=0$, $K_2[8]=1$, $K_2[9]=1$	$K_4[6]=0$, $K_4[7]=1$, $K_4[8]=0$, $K_4[9]=0$	$K_5[17]=1$, $K_5[18]=1$, $K_5[19]=0$, $K_5[20]=0$
12	$K_1[21]=1$, $K_1[22]=0$, $K_1[23]=1$, $K_1[24]=0$	$K_2[12]=1$, $K_2[13]=0$,	$K_4[12]=1$, $K_4[13]=1$,	$K_5[21]=1$, $K_5[22]=0$, $K_5[23]=1$, $K_5[24]=0$
14	$K_1[25]=0$, $K_1[26]=0$, $K_1[27]=0$, $K_1[28]=0$	$K_2[15]=0$, $K_2[16]=0$, $K_2[17]=1$	$K_4[15]=0$,$K_4[16]=0$, $K_4[17]=1$	$K_5[25]=0$, $K_5[26]=0$, $K_5[27]=0$, $K_5[28]=0$
20	$K_1[25]=0$, $K_1[29]=0$, $K_1[30]=0$, $K_1[31]=0$ $K_1[32]=0$	$K_2[17]=1$, $K_2[18]=0$, $K_2[19]=1$, $K_2[20]=0$, $K_2[21]=1$	$K_4[17]=1$,$K_4[18]=0$, $K_4[19]=0$,$K_4[20]=0$, $K_4[21]=0$	$K_5[25]=0$, $K_5[29]=0$, $K_5[30]=0$, $K_5[31]=0$, $K_5[32]=1$

4. Conclusion Remarks

In the paper, for any integer k, the role of the binary operation $\langle u, v\rangle_k$is analyzed in the construction of correlation matrices of S blocks and in the formation of quadratic approximations.

It is analyzed the use of quadratic approximations for estimating nonlinear S-block transformations of block encryption algorithms.

The process of generating high probability relationship equations between the input and output bits of nonlinear S-block transforms based on correlation matrices is studied, and the corresponding software is developed.

An algorithm for the application of quadratic cryptanalysis for five round XOR modifications of the standard encryption algorithm GOST 28147-89 has been developed. Based on this algorithm, an approximation equation is formed for the input values of the first round and the output values of the fifth round.

Quadratic equations of relations are constructed for the five round characteristics forS_1:$S_6$and S_7:S_4blocks with the probability p=0, 66 and forS_3:S_8 blocks with the probability p=0,34 (deviation 0,16).

It is shown that for five round XOR modifications of the standard encryption algorithm GOST 28147-89, these equations have a higher probability than the approximation equations of linear cryptanalysis.

To determine the statistical values of the obtained quadratic equations, experiments were performed with the selected open and corresponding encrypted software texts.

In the experiment, 13 quadratic and 15 linear equations of approximation are used. As a result, 28 equations with 32 bits of keys of the first and fifth rounds and 25 bits of keys of the second and fourth rounds are analyzed.

Using the above equations with the probability p = 0,66, the following bits of round keys were found:

- In the first and fifth rounds:k_1, k_2, k_3, k_4, k_9, k_{10}, k_{11}, k_{12}, k_{25}, k_{26}, k_{27}, k_{28};
- In the second and fourth rounds:k_{15}, k_{16}, k_{23}, k_{24} , k_{30}, k_{31}

It is shown that the probability of finding the remaining bits of the key participating in the equation of relations is not less than the probability of the linear cryptanalysis method.

References

[1] Tokareva N.N. On quadratic approximations in block ciphers // Problems Inform. Transmission, 44:3 (2008), 266–286.

[2] Matsui M. Linear Cryptanalysis Method for DES Cipher // Advances in Cryptology _ EUROCRYPT'93 (Proc. Workshop on the Theory and Application of Cryptographic Techniques. Lofthus, Norway. May 23–27, 1993). Lecture Notes in Comput. Sci. V. 765. Berlin: Springer, 1994. P. 386–397.

[3] Krotov, D.S., $\mathbb{Z}_4$-linear Perfect Codes, Diskretn. Anal. Issled. Oper., Ser. 1, 2000, vol. 7, no. 4, pp. 78–90.

[4] Krotov D.S. Z_4-linear Hadamard and extended perfect codes//WCC'2001 (Proc. International Workshop on Coding and Cryptography. Paris, January 8–12, 2001). P. 329–334.

[5] Tokareva N.N. "Quadratic approximations of the special type for the 4-bit Permutations in S-boxes». Journal «Mathematical Methods of Cryptography». № 1(1). UDK 003.26 519.7. 2008, pp.50-54.

[6] State standard of the USSR. Information processing systems. Cryptographic protection. The cryptographic conversion algorithm GOST 28147-89. IPK publishing house of standards Moscow, 1989.

[7] Babenko L.K., Ishukova E.A. Modern block cipher algorithms and methods for their analysis. Scientific publication – M., «Gelios ARV», 2006. – 376 pages.

[8] Akhmedov B.B. A correlation matrix using quadratic approximations of a special form for S-blocks of the DES encryption algorithm // "Information security in the field of communications and informatization. Problems and solutions" Collection of Abstracts and

Articles of the Republican Seminar. Tashkent, 2015, pp.9-13.

[9] Kaliski B., Robshaw M. Linear Cryptanalysis Using Multiple Approximations // Advances in Cryptology — CRYPTO'94 (Proc. 14th Annual International Cryptology Conference. Santa Barbara, California, USA. August 21–25, 1994). Lecture Notes in Comput. Sci. V. 839. Berlin:Springer, 1994. P. 26–39.

[10] Biryukov A., De Canniere C., Quisquater M. On Multiple Linear Approximations // Advances in Cryptology — CRYPTO 2004 (Proc. 24th Annual International Cryptology Conference. Santa Barbara, California, USA. August 15-19, 2004). Lecture Notes in Comput. Sci. V. 3152. Springer–Verlag, 2004. P. 1–22.

[11] Sakurai K., Furuya S. Improving Linear Cryptanalysis of LOKI91 by Probabilistic Counting Method // Fast Software Encryption — FSE'97 (Proc. 4th International Workshop, Haifa, Israel. January 20-22, 1997). Lecture Notes in Comput. Sci. V. 1267. Berlin: Springer, 1997. P. 114–133.

[12] Rothaus O. On bent functions//J.Combin. Theory. Ser.A. 1976. V. 20. N 3. P. 300–305.

[13] Logachev, O.A., Sal'nikov, A.A., and Yashchenko, V.V., Boolean Functions in Coding Theory and Cryptology, Moscow: Mos. Tsentr Nepreryvnogo Mat. Obrazovaniya (MCCME), 2004.

[14] Dobbertin H., Leander G. A Survey of Some Recent Results on Bent Functions // Sequences and their applications — SETA 2004 (Proc. Third International Conference. Seul, Korea. October 24–28, 2004). Lecture Notes in Comput. Sci. V. 3486. Berlin: Springer, 2005. P. 1–29.

[15] Chee S., Lee S., Kim K. Semi-bent Functions // Advances in Cryptology — ASIACRYPT '94 (Proc. 4th International Conference on the Theory and Applications of Cryptology. Wollongong, Australia. November 28 – December 1, 1994). Lecture Notes in Comput. Sci. V. 917. Berlin:Springer, 1995. P. 107–118.

[16] Dobbertin H., Leander G. Cryptographer's Toolkit for Construction of 8-Bit Bent Functions //Cryptology ePrint Archive, Report 2005/089, available at http://eprint.iacr.org/.

[17] Qu C., Seberry J., Pieprzyk J. Homogeneous Bent Functions // Discrete Applied Mathematics. 2000. V. 102. N 1–2. P. 133–139.

[18] Youssef A., Gong G. Hyper-bent functions // Advances in cryptology — EUROCRYPT'2001 (Proc. International Conference on the Theory and Application of Cryptographic Techniques. Innsbruk, Austria. May 6–10, 2001). Lecture Notes in Comput. Sci. V. 2045. Berlin: Springer, 2001. P. 406–419.

[19] Kuz'min, A.S., Markov, V.T., Nechaev, A.A., and Shishkov, A.B., Approximation of Boolean Functions by Monomial Ones, Diskret. Mat., 2006, vol. 18, no. 1, pp. 9–29.

[20] Carlet C., Gaborit P. Hyper-bent functions and cyclic codes // J. Combin. Theory. Ser. A.2006. V. 113. N 3. P. 466–482.

[21] Youssef A.M. Generalized hyper-bent functions over GF(p) // Discrete Applied Mathematics. 2007. V. 155. N 8. P. 1066–1070.

[22] Kuz'min, A.S., Markov, V.T., Nechaev, A.A., Shishkin, V.A., and Shishkov, A.B., Bent and Hyper-bent Functions over a Field of 2ℓ Elements, Probl. Peredachi Inf., 2008, vol. 44, no. 1, pp. 15–37.

[23] Knudsen L. R., Robshaw M. J. B. Non-linear Approximation in Linear Cryptanalysis // Advances in Cryptology — EUROCRYPT'96 (Proc. Workshop on the Theory and Application of Cryptographic Techniques. Saragossa, Spain. May 12–16, 1996). Lecture Notes in Comput. Sci. V. 1070. Springer-Verlag, 1996. P. 224–236.

[24] Tokareva, N.N., Bent Functions with Stronger Nonlinearity Properties: *k*-Bent Functions, Diskretn. Anal. Issled. Oper., Ser. 1, 2007, vol. 14, no. 4, pp. 76–102.

[25] Rostovtsev, A.G. and Makhovenko, E.B., Introduction to the Theory of Iterated Ciphers, St. Petersburg: Mir i Sem'ya, 2003.