Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 1 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

The Encryption Algorithms GOST-IDEA16-2 and GOST-RFWKIDEA16-2

By Gulom Tuychiev

National University of Uzbekistan, Uzbekistan

Abstract- In the paper created a block encryption algorithms GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16- 2 based on networks IDEA16-2 and RFWKIDEA16-2, with the use the round function of the encryption algorithm GOST 28147-89. The block length of created block encryption algorithm is 128 bits, the number of rounds is 8, 12 and 16.

Keywords: GOST 28147-89, Lai-Massey scheme, round function, round keys, output transformation.

GJCST-E Classification : G.4, E.3

Strictly as per the compliance and regulations of:

The Encryption Algorithms GOST-IDEA16-2 and GOST-RFWKIDEA16-2

Gulom Tuychiev

Abstract- In the paper created a block encryption algorithms GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2 based on networks IDEA16-2 and RFWKIDEA16-2, with the use the round function of the encryption algorithm GOST 28147-89. The block length of created block encryption algorithm is 128 bits, the number of rounds is 8, 12 and 16

Keywords: GOST 28147-89, Lai-Massey scheme, round function, round keys, output transformation.

I. Introduction

The encryption algorithm GOST 28147-89 is a standard encryption algorithm of the Russian Federation. It is based on a Feistel network. This encryption algorithm is suitable for hardware and software implementation, meets the necessary cryptographic requirements for resistance and, therefore, does not impose restrictions on the degree of secrecy of the information being protected. The algorithm implements the encryption of 64-bit blocks of data using the 256 bit key. In round functions used eight S-box of size 4x4 and operation of the cyclic shift by 11 bits. To date GOST 28147-89 is resistant to cryptographic attacks.

On the basis of encryption algorithm IDEA and scheme Lai-Massey developed the networks IDEA16-2 and RFWKIDEA16-2, consisting from two round function. In the networks IDEA16-2 and RFWKIDEA16-2, similarly as in the Feistel network, when it encryption and decryption using the same algorithm. In the networks used two round function having four input and output blocks and as the round function can use any transformation.

As the round function networks IDEA4-2 [1], RFWKIDEA4-2 [5], PES4-2 [6], RFWKPES4-2 [7], PES8-4 [2], RFWKPES8-4 [8] using the round function of the encryption algorithm GOST 28147-89 [4] created the encryption algorithm GOST28147-89-IDEA4-2 [9], GOST28147-89-RFWKIDEA4-2 [10], GOST28147-89-PES4-2 [11], GOST28147-89-RFWKPES4-2 [12], GOST28147-89-PES8-4 [13] and GOST28147-89-RFWKPES8-4 [13].

Author: Candidate technical science (Ph.d), the teacher of National University of Uzbekistan, Uzbekistan, Tashkent.
e- mail: blasterjon@gmail.com

In this paper, applying the round function of the encryption algorithm GOST 28147-89 as round functions of the networks IDEA16-2 [14] and RFWKIDEA16-2 [15], developed new encryption algorithms GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2.

In the encryption algorithms GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2 block length is 256 bits, the key length is changed from 256 bits to 1024 bits in increments of 128 bits and a number of rounds equal to 8, 12, 16, allowing the user depending on the degree of secrecy of information and speed of encryption to choose the number of rounds and key length. Below is the structure of the proposed encryption algorithm.

II. The Structure of the Encryption Algorithm GOST28147-89-IDEA16-2

In the encryption algorithm GOST28147-89-IDEA16-2 the length of subblocks X^0, X^1, X^2,..., X^{15}, length of round keys $K_{24(i-1)}$, $K_{24(i-1)+1}$, $K_{24(i-1)+2}$, ..., $K_{18(i-1)+15}$, $i=\overline{1...n+1}$, $K_{24(i-1)+16}$, $K_{24(i-1)+17}$, $K_{24(i-1)+18}$, ..., $K_{24(i-1)+23}$ $i=\overline{1...n}$, K_{24n+16}, K_{24n+17}, K_{24n+18}, ..., K_{24n+47} are equal to 8-bits. The length of the input and output blocks of round functions is 32 bits. This encryption algorithm round function GOST 28147-89 is applied twice and in each round function employed eight S-boxes, i.e. the total number of S-boxes is 16. The structure of the encryption algorithm GOST28147-89-PES16-2 is shown in Figure 1 and the S-boxes shown in Table 1.

Consider the round function block encryption algorithm GOST28147-89-IDEA16-2. First the 8-bit subblocks T^0, T^1, ..., T^7 combined from 32-bit subblocks, i.e. $T_0 = T^0 \| T^1 \| T^2 \| T^3$, T_1 = $T^4 \| T^5 \| T^6 \| T^7$. Subblocks T_0, T_1 are summed round keys $K_{24(i-1)+16} \| K_{24(i-1)+17} \| K_{24(i-1)+18} \|$ $K_{24(i-1)+19}$, $K_{24(i-1)+20} \| K_{24(i-1)+21} \| K_{24(i-1)+22} \| K_{24(i-1)+23}$ i.e.

$$S^0 = T_0 + (K_{24(i-1)+16} \| K_{24(i-1)+17} \| K_{24(i-1)+18} \| K_{24(i-1)+19}),$$

$$S^1 = T_1 + (K_{24(i-1)+20} \| K_{24(i-1)+21} \| K_{24(i-1)+22} \| K_{24(i-1)+23}).$$

Global Journal of Computer Science and Technology (E) Volume XVI Issue III Version I Year 2016

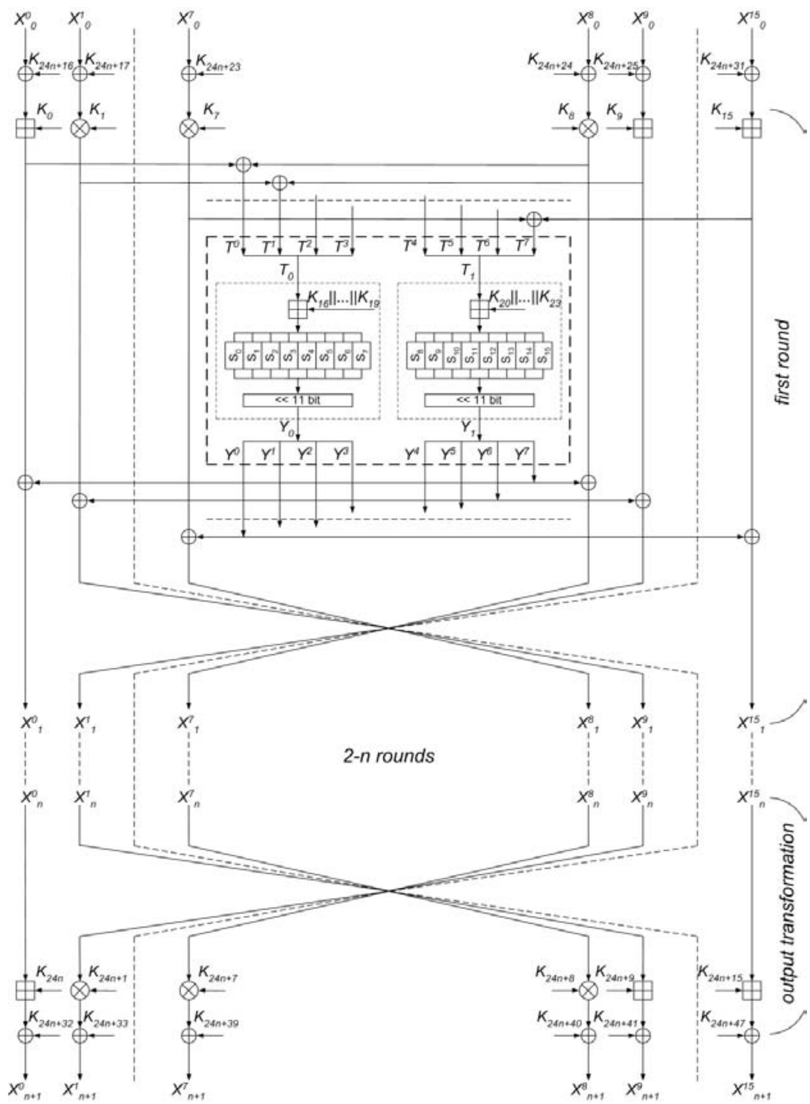

Figure 1 : The scheme n-rounded encryption algorithm GOST28147-89-IDEA16-2

Table 1 : The S-boxes of encryption algorithm GOST28147-89-RFWKPES4-2

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
S0	0x4	0x5	0xB	0x9	0xE	0x8	0xD	0x0	0x6	0xC	0xF	0x7	0x2	0x1	0x3	0xA
S1	0x5	0x4	0xA	0x8	0xF	0x9	0xC	0x1	0x7	0xD	0xE	0x6	0x3	0x0	0x2	0xB
S2	0xE	0xB	0x4	0x2	0xF	0x7	0xC	0x0	0x8	0x9	0xA	0xD	0x6	0x5	0x3	0x1
S3	0xF	0xA	0x5	0x3	0xE	0x6	0xD	0x1	0x9	0x8	0xB	0xC	0x7	0x4	0x2	0x0
S4	0xD	0xC	0xB	0x1	0x4	0x0	0xF	0x3	0x7	0xE	0x5	0x6	0x9	0x2	0x8	0xA
S5	0xA	0x3	0x4	0x6	0xB	0xF	0x0	0xC	0x8	0x9	0x2	0x1	0xE	0x5	0x7	0xD
S6	0xB	0x2	0x5	0x7	0xA	0xE	0x1	0xD	0x9	0x8	0x3	0x0	0xF	0x4	0x6	0xC
S7	0xC	0x5	0x2	0x0	0xD	0x9	0x6	0xA	0xE	0xF	0x4	0x7	0x8	0x3	0x1	0xB
S8	0xD	0x4	0x3	0x1	0xC	0x8	0x7	0xB	0xF	0xE	0x5	0x6	0x9	0x2	0x0	0xA
S9	0xE	0x7	0x0	0x2	0xF	0xB	0x4	0x8	0xC	0xD	0x6	0x5	0xA	0x1	0x3	0x9
S10	0xF	0x6	0x1	0x3	0xE	0xA	0x5	0x9	0xD	0xC	0x7	0x4	0xB	0x0	0x2	0x8
S11	0x1	0x0	0x7	0x5	0x8	0x4	0xB	0xF	0x3	0xA	0x9	0x2	0xD	0xE	0xC	0x6
S12	0x2	0x3	0x4	0x6	0xB	0x7	0x8	0xC	0x0	0x9	0xA	0x1	0xE	0xD	0xF	0x5
S13	0x3	0x2	0x5	0x7	0xA	0x6	0x9	0xD	0x1	0x8	0xB	0x0	0xF	0xC	0xE	0x4
S14	0x4	0x5	0x2	0x0	0xD	0x1	0xE	0xA	0x6	0xF	0xC	0x7	0x8	0xB	0x9	0x3
S15	0x5	0x4	0x3	0x1	0xC	0x0	0xF	0xB	0x7	0xE	0xD	0x6	0x9	0xA	0x8	0x2

32-bit subblocks S^0, S^1 divided into eight four bit subblocks $S^0 = s_0^0 \| s_1^0 \| s_2^0 \| s_3^0 \| s_4^0 \| s_5^0 \| s_6^0 \| s_7^0$, $S^1 = s_0^1 \| s_1^1 \| s_2^1 \| s_3^1 \| s_4^1 \| s_5^1 \| s_6^1 \| s_7^1$. Four bit subblocks s_i^0, s_i^1, $i = \overline{0...7}$ transformed into the S-boxes: $R^0 = S_0(s_0^0) \| S_1(s_1^0) \| S_2(s_2^0) \| S_3(s_3^0) \| S_4(s_4^0) \| S_5(s_5^0) \| S_6(s_6^0) \| S_7(s_7^0)$, $R^1 = S_8(s_0^1) \| S_9(s_1^1) \| S_{10}(s_2^1) \| S_{11}(s_3^1) \| S_{12}(s_4^1) \| S_{13}(s_5^1) \| S_{14}(s_6^1) \| S_{15}(s_7^1)$. The resulting 32-bit subblocks R^0, R^1 cyclically shifted left by 11 bits and we obtain subblocks Y_0, Y_1: $Y_0 = R^0 <<11$, $Y_1 = R^1 <<11$. Thereafter 32-bit subblocks Y_0, Y_1 divided into four 8-bit subblocks Y^0, Y^1, ..., Y^7 i.e., $Y_0 = Y^0 \| Y^1 \| Y^2 \| Y^3$, $Y_1 = Y^4 \| Y^5 \| Y^6 \| Y^7$.

Consider the encryption process of encryption algorithm GOST28147-89-IDEA16-2. Initially the 128-bit plaintext *X* partitioned into subblocks of 8-bits X_0^0, X_0^1, X_0^2, ..., X_0^{15}, and performs the following steps:

1. subblocks X_0^0, X_0^1, X_0^2, ..., X_0^{15} summed by XOR respectively with round key K_{24n+16}, K_{24n+17}, K_{24n+18}, ..., K_{24n+31}: $X_0^j = X_0^j \oplus K_{24n+16+j}$, $j = \overline{0...15}$.
2. subblocks X_0^0, X_0^1, X_0^2, ..., X_0^{15} multiplied and summed respectively with the round keys $K_{24(i-1)}$, $K_{24(i-1)+1}$, $K_{24(i-1)+2}$, ..., $K_{24(i-1)+15}$, $i = \overline{1...n+1}$ and calculated 8-bit subblocks T^0, T^1, T^2, ..., T^7. This step can be represented as follows:
$$T_0 = (X_{i-1}^0 + K_{24(i-1)}) \oplus (X_{i-1}^8 \cdot K_{24(i-1)+8}),$$
$$T_1 = (X_{i-1}^1 \cdot K_{24(i-1)+1}) \oplus (X_{i-1}^9 + K_{24(i-1)+9}),$$
$$T_2 = (X_{i-1}^2 + K_{24(i-1)+2}) \oplus (X_{i-1}^{10} \cdot K_{24(i-1)+10}),$$
$$T_3 = (X_{i-1}^3 \cdot K_{24(i-1)+3}) \oplus (X_{i-1}^{11} + K_{24(i-1)+11}),$$
$$T_4 = (X_{i-1}^4 + K_{24(i-1)+4}) \oplus (X_{i-1}^{12} \cdot K_{24(i-1)+12}),$$
$$T_5 = (X_{i-1}^5 \cdot K_{24(i-1)+5}) \oplus (X_{i-1}^{13} + K_{24(i-1)+13}),$$
$$T_6 = (X_{i-1}^6 + K_{24(i-1)+6}) \oplus (X_{i-1}^{14} \cdot K_{24(i-1)+14}),$$
$$T_7 = (X_{i-1}^7 \cdot K_{24(i-1)+7}) \oplus (X_{i-1}^{15} + K_{24(i-1)+15}),\ i = 1.$$
3. to 8-bit subblocks T^0, T^1, T^2, ..., T^7 applied round functions and get 8-bit subblocks Y^0, Y^1, Y^2, ..., Y^7.
4. subblocks Y^0, Y^1, Y^2, ..., Y^7 are summed to XOR with subblocks X_{i-1}^0, X_{i-1}^1, X_{i-1}^2, ..., X_{i-1}^{15}, i.e. $X_{i-1}^j = X_{i-1}^j \oplus Y^{7-j}$, $X_{i-1}^{j+8} = X_{i-1}^{j+8} \oplus Y^{7-j}$, $j = \overline{0...7}$, $i = 1$.
5. at the end of the round subblocks swapped, i.e., $X_i^j = X_{i-1}^{15-j}$, $j = \overline{1...14}$, $i = 1$
6. repeating steps 2-5 *n* times, i.e., $i = \overline{2...n}$ obtain subblocks X_n^0, X_n^1, X_n^2, ..., X_n^{15}.
7. in output transformation round keys K_{24n}, K_{24n+1}, K_{24n+2}, ..., K_{24n+15} are multiplied and summed into subblocks, i.e.
$$X_{n+1}^0 = X_n^0 + K_{24n},\quad X_{n+1}^1 = X_n^{14} \cdot K_{24n+1},$$
$$X_{n+1}^2 = X_n^{13} + K_{24n+2},\quad X_{n+1}^3 = X_n^{12} \cdot K_{24n+3},$$
$$X_{n+1}^4 = X_n^{11} + K_{24n+4},\quad X_{n+1}^5 = X_n^{10} \cdot K_{24n+5},$$
$$X_{n+1}^6 = X_n^9 + K_{24n+6},\quad X_{n+1}^7 = X_n^8 \cdot K_{24n+7},$$
$$X_{n+1}^8 = X_n^7 \cdot K_{24n+8},\quad X_{n+1}^9 = X_n^6 + K_{24n+9},$$
$$X_{n+1}^{10} = X_n^5 \cdot K_{24n+10},\quad X_{n+1}^{11} = X_n^4 + K_{24n+11},$$
$$X_{n+1}^{12} = X_n^3 \cdot K_{24n+12},\quad X_{n+1}^{13} = X_n^2 + K_{24n+13},$$
$$X_{n+1}^{14} = X_n^1 \cdot K_{24n+14},\quad X_{n+1}^{15} = X_n^{15} + K_{24n+15}$$
8. subblocks X_{n+1}^0, X_{n+1}^1, X_{n+1}^2, ..., X_{n+1}^{15} are summed to XOR with the round K_{24n+32}, K_{24n+33}, K_{24n+34}, .., K_{24n+47}: $X_{n+1}^j = X_{n+1}^j \oplus K_{24n+32+j}$, $j = \overline{0...7}$.

As ciphertext plaintext X receives the combined 8-bit subblocks $X_{n+1}^0 \| X_{n+1}^1 \| X_{n+1}^2 \| ... \| X_{n+1}^{15}$.

III. Key Generation of the Encryption Algorithm Gost28147-89-Idea16-2

In *n*-round encryption algorithm GOST28147-89-IDEA16-2 in each round used twenty four round keys of the 8-bit and output transformation sixteen round keys of the 8-bit. In addition, before the first round and after the output transformation we used sixteen round keys of 8-bits. Total number of 8-bit round keys is equal to 24*n*+48. In Figure 4 encryption used encryption round keys K_i^c instead of K_i^c, while decryption used decryption round keys K_i^d. If *n*=8 then need 240 to generate round keys, if *n*=12, you need to generate 336 round keys and if *n*=16 need 432 to generate round keys.

The key encryption algorithm *K* of length l ($256 \le l \le 1024$) bits is divided into 8-bit round keys K_0^c, K_1^c,..., $K_{Lenght-1}^c$, $Lenght = l/8$, here $K = \{k_0, k_1, ..., k_{l-1}\}$, $K_0^c = \{k_0, k_1, ..., k_7\}$, $K_1^c = \{k_8, k_9, ..., k_{15}\}$,..., $K_{Lenght-1}^c = \{k_{l-8}, k_{l-7}, ..., k_{l-1}\}$ and $K = K_0^c \| K_1^c \| ... \| K_{Lenght-1}^c$. Then we calculate $K_L = K_0^c \oplus K_1^c \oplus ... \oplus K_{Lenght-1}^c$. If $K_L = 0$ then K_L is chosen as 0xC5, i.e. K_L =0xC5. Round keys K_i^c, $i = \overline{Lenght...24n+47}$ are computed as follows

$K_i^c = Sbox0(K_{i-Lenght}^c) \oplus Sbox1(RotWord(K_{i-Lenght+1}^c))$ $\oplus K_L$. After each round key generation the value K_L is cyclic shift to the left by 1 bit. Here, RotWord8()-cyclic shift to the left of 1 bit of the 11-bit subblock, Sbox-transformation a 8-bit subblock in the S-boxes, $Sbox0(S) = S_0(t^0) \| S_1(t^1)$, $Sbox1(S) = S_8(t^0) \| S_9(t^1)$ and t^0, t^1-four bit subblock, $T = t^0 \| t^1$-eight bit subblock.

Decryption round keys K_i^d are computed on the basis of encryption round keys K_i^c and decryption round keys of the output transformation associate with of encryption round keys as follows:

$$(K_{24n}^d, K_{24n+1}^d, K_{24n+2}^d, K_{24n+3}^d, K_{24n+4}^d, K_{24n+5}^d, K_{24n+6}^d, K_{24n+7}^d, K_{24n+8}^d, K_{24n+9}^d, K_{24n+10}^d, K_{24n+11}^d, K_{24n+12}^d, K_{24n+13}^d, K_{24n+14}^d, K_{24n+15}^d) = (-K_0^c, (K_1^c)^{-1}, -K_2^c, (K_3^c)^{-1}, -K_4^c, (K_5^c)^{-1}, -K_6^c, (K_7^c)^{-1}, (K_8^c)^{-1}, -K_9^c, (K_{10}^c)^{-1}, -K_{11}^c, (K_{12}^c)^{-1}, -K_{13}^c, (K_{14}^c)^{-1}, -K_{15}^c).$$

Decryption round keys of the first round associate with of encryption round keys as follows:

$$(K_0^d, K_1^d, K_2^d, K_3^d, K_4^d, K_5^d, K_6^d, K_7^d, K_8^d, K_9^d, K_{10}^d, K_{11}^d, K_{12}^d, K_{13}^d, K_{14}^d, K_{15}^d, K_{16}^d, K_{17}^d, K_{18}^d, K_{19}^d, K_{20}^d, K_{21}^d, K_{22}^d, K_{23}^d) = (-K_{24n}^c, (K_{24n+1}^c)^{-1}, -K_{24n+2}^c, (K_{24n+3}^c)^{-1}, -K_{24n+4}^c, (K_{24n+5}^c)^{-1}, -K_{24n+6}^c, (K_{24n+7}^c)^{-1}, (K_{24n+8}^c)^{-1}, -K_{24n+9}^c, (K_{24n+10}^c)^{-1}, -K_{24n+11}^c, (K_{24n+12}^c)^{-1}, -K_{24n+13}^c, (K_{24n+14}^c)^{-1}, -K_{24n+15}^c, K_{24(n-1)+16}^c, K_{24(n-1)+17}^c, K_{24(n-1)+18}^c, K_{24(n-1)+19}^c, K_{24(n-1)+20}^c, K_{24(n-1)+21}^c, K_{24(n-1)+22}^c, K_{24(n-1)+23}^c).$$

Decryption round keys of the second, third and n-round associates with the encryption round keys as follows:

$$(K_{24(i-1)}^d, K_{24(i-1)+1}^d, K_{24(i-1)+2}^d, K_{24(i-1)+3}^d, K_{24(i-1)+4}^d, K_{24(i-1)+5}^d, K_{24(i-1)+6}^d, K_{24(i-1)+7}^d, K_{24(i-1)+8}^d, K_{24(i-1)+9}^d, K_{24(i-1)+10}^d, K_{24(i-1)+11}^d, K_{24(i-1)+12}^d, K_{24(i-1)+13}^d, K_{24(i-1)+14}^d, K_{24(i-1)+15}^d, K_{24(i-1)+16}^d, K_{24(i-1)+17}^d, K_{24(i-1)+18}^d, K_{24(i-1)+19}^d, K_{24(i-1)+20}^d, K_{24(i-1)+21}^d, K_{24(i-1)+22}^d, K_{24(i-1)+23}^d) = (-K_{24(n-i+1)}^c, (K_{24(n-i+1)+14}^c)^{-1}, -K_{24(n-i+1)+13}^c, (K_{24(n-i+1)+12}^c)^{-1}, -K_{24(n-i+1)+11}^c, (K_{24(n-i+1)+10}^c)^{-1}, -K_{24(n-i+1)+9}^c, (K_{24(n-i+1)+8}^c)^{-1}, (K_{24(n-i+1)+7}^c)^{-1}, -K_{24(n-i+1)+6}^c, (K_{24(n-i+1)+5}^c)^{-1}, -K_{24(n-i+1)+4}^c, (K_{24(n-i+1)+3}^c)^{-1}, -K_{24(n-i+1)+2}^c, (K_{24(n-i+1)+1}^c)^{-1}, -K_{24(n-i+1)+15}^c, K_{24(n-i)+16}^c, K_{24(n-i)+17}^c, K_{24(n-i)+18}^c, K_{24(n-i)+19}^c, K_{24(n-i)+20}^c, K_{24(n-i)+21}^c, K_{24(n-i)+22}^c, K_{24(n-i)+23}^c), i = \overline{2...n}.$$

Decryption round keys applied to the first round and after the output transformation associated with the encryption round keys as follows: $K_{24n+16+j}^d = K_{24n+32+j}^c$, $K_{24n+32+j}^d = K_{24n+16+j}^c$, $j = \overline{0...7}$.

IV. The Structure of the Encryption Algorithm GOST28147-89-RFWKIDEA16-2

In the encryption algorithm GOST28147-89-RFWKIDEA16-2 the length of subblocks X^0, X^1, X^2 ,..., X^{15}, length of round keys $K_{16(i-1)}$, $K_{16(i-1)+1}$, $K_{16(i-1)+2}$, ..., $K_{16(i-1)+15}$, $i = \overline{1...n+1}$, K_{16n+16}, K_{16n+17}, K_{16n+18}, ..., K_{16n+47} are equal to 8-bits. The length of the input and output blocks of round functions is 32 bits. This encryption algorithm round function GOST 28147-89 is applied twice and in each round function employed eight S-boxes, i.e. the total number of S-boxes is 16. The structure of the encryption algorithm GOST28147-89-PES16-2 is shown in Figure 2 and the S-boxes shown in Table 1.

Consider the round function block encryption algorithm GOST28147-89-RFWKIDEA16-2. First the 8-bit subblocks T^0, T^1, ..., T^7 combined from 32-bit subblocks, i.e. $T_0 = T^0 \| T^1 \| T^2 \| T^3$, $T_1 = T^4 \| T^5 \| T^6 \| T^7$. 32-bit subblocks T_0, T_1 divided into eight four bit subblocks $T_0 = t_0^0 \| t_1^0 \| t_2^0 \| t_3^0 \| t_4^0 \| t_5^0 \| t_6^0 \| t_7^0$, $T_1 = t_0^1 \| t_1^1 \| t_2^1 \| t_3^1 \| t_4^1 \| t_5^1 \| t_6^1 \| t_7^1$. Four bit subblocks t_i^0, t_i^1, $i = \overline{0...7}$ transformed into the S-boxes: $R^0 = S_0(t_0^0) \| S_1(t_1^0) \| S_2(t_2^0) \| S_3(t_3^0) \| S_4(t_4^0) \| S_5(t_5^0) \| S_6(t_6^0) \| S_7(t_7^0)$, $R^1 = S_8(t_0^1) \| S_9(t_1^1) \| S_{10}(t_2^1) \| S_{11}(t_3^1) \| S_{12}(t_4^1) \| S_{13}(t_5^1) \| S_{14}(t_6^1) \| S_{15}(t_7^1)$. The resulting 32-bit subblocks R^0, R^1 cyclically shifted left by 11 bits and we obtain subblocks Y_0, Y_1: $Y_0 = R^0 <<11$, $Y_1 = R^1 <<11$. Thereafter 32-bit subblocks Y_0, Y_1 divided into four 8-bit subblocks Y^0, Y^1, ..., Y^7 i.e., $Y_0 = Y^0 \| Y^1 \| Y^2 \| Y^3$, $Y_1 = Y^4 \| Y^5 \| Y^6 \| Y^7$.

Consider the encryption process of encryption algorithm GOST28147-89-IDEA16-2. Initially the 128-bit plaintext \$X\$ partitioned into subblocks of 8-bits X_0^0, X_0^1, X_0^2, ..., X_0^{15}, and performs the following steps:

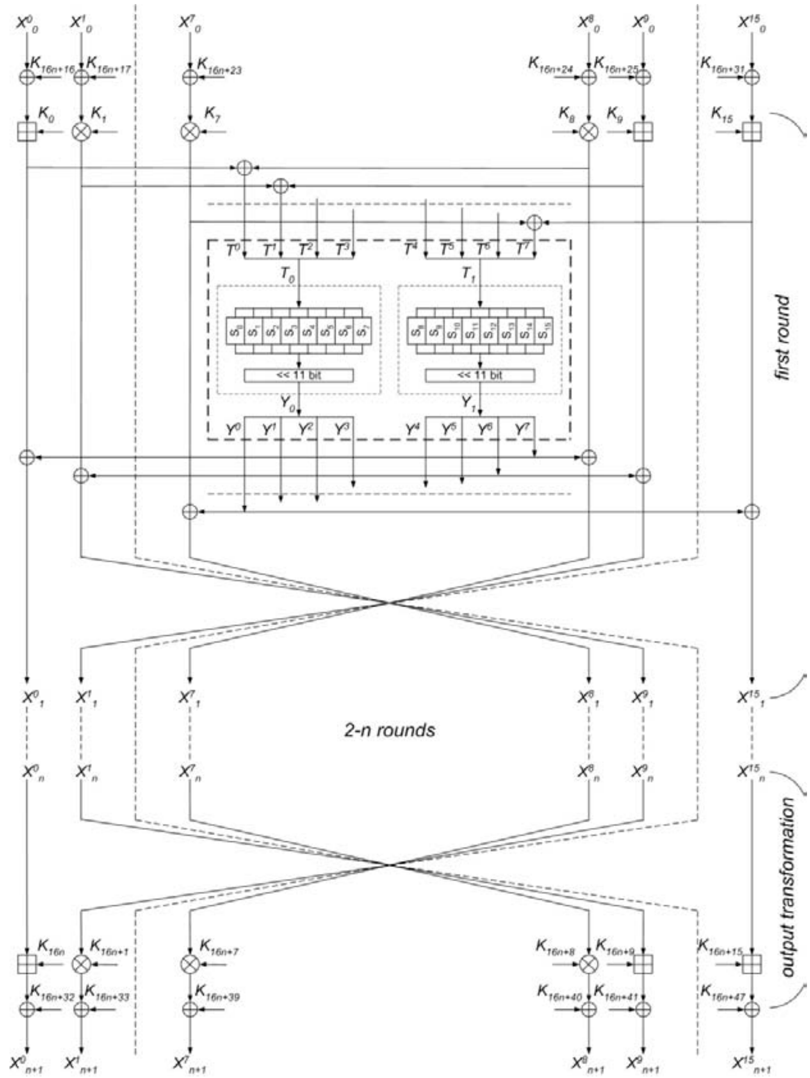

Figure 2 : The scheme n-rounded encryption algorithm GOST28147-89-RFWKIDEA16-2

1. subblocks X_0^0, X_0^1, X_0^2, ..., X_0^{15} summed by XOR respectively with round key K_{16n+16}, K_{16n+17}, K_{16n+18}, ..., K_{16n+31} i.e $X_0^j = X_0^j \oplus K_{16n+16+j}$, $j=\overline{0...7}$.
2. subblocks X_0^0, X_0^1, X_0^2, ..., X_0^{15} multiplied and summed respectively with the round keys $K_{16(i-1)}$, $K_{16(i-1)+1}$, $K_{16(i-1)+2}$, ..., $K_{16(i-1)+15}$ and calculated 8-bit subblocks T^0, T^1, T^2, ..., T^7. This step can be represented as follows:
$T_0 = (X_{i-1}^0 + K_{16(i-1)}) \oplus (X_{i-1}^8 \cdot K_{16(i-1)+8})$,
$T_1 = (X_{i-1}^1 \cdot K_{16(i-1)+1}) \oplus (X_{i-1}^9 + K_{16(i-1)+9})$,
$T_2 = (X_{i-1}^2 + K_{16(i-1)+2}) \oplus (X_{i-1}^{10} \cdot K_{16(i-1)+10})$,
$T_3 = (X_{i-1}^3 \cdot K_{16(i-1)+3}) \oplus (X_{i-1}^{11} + K_{16(i-1)+11})$,
$T_4 = (X_{i-1}^4 + K_{16(i-1)+4}) \oplus (X_{i-1}^{12} \cdot K_{16(i-1)+12})$,
$T_5 = (X_{i-1}^5 \cdot K_{16(i-1)+5}) \oplus (X_{i-1}^{13} + K_{16(i-1)+13})$,
$T_6 = (X_{i-1}^6 + K_{16(i-1)+6}) \oplus (X_{i-1}^{14} \cdot K_{16(i-1)+14})$,
$T_7 = (X_{i-1}^7 \cdot K_{16(i-1)+7}) \oplus (X_{i-1}^{15} + K_{16(i-1)+15})$, $i=1$.
3. to 8-bit subblocks T^0, T^1, T^2, ..., T^7 applied round functions and get 8-bit subblocks Y^0, Y^1, Y^2, ..., Y^7.
4. subblocks Y^0, Y^1, Y^2, ..., Y^7 are summed to XOR with subblocks X_{i-1}^0, X_{i-1}^1, X_{i-1}^2, ..., X_{i-1}^{15} i.e. $X_{i-1}^j = X_{i-1}^j \oplus Y^{7-j}$, $X_{i-1}^{j+8} = X_{i-1}^{j+8} \oplus Y^{7-j}$, $j=\overline{0...7}$, $i=1$.
5. at the end of the round subblocks swapped, i.e., $X_i^j = X_{i-1}^{15-j}$, $j=\overline{1...14}$, $i=1$.
6. repeating steps 2-5 n times, i.e., $i=\overline{2...n}$ obtain subblocks X_n^0, X_n^1, X_n^2, ..., X_n^{15}.

7. in output transformation round keys K_{16n}, K_{16n+1}, K_{16n+2}, ..., K_{16n+15} are multiplied and summed into subblocks X_n^0, X_n^1, X_n^2, ..., X_n^{15}, i.e. $X_{n+1}^0 = X_n^0 + K_{16n}$, $X_{n+1}^1 = X_n^{14} \cdot K_{16n+1}$, $X_{n+1}^2 = X_n^{13} + K_{16n+2}$, $X_{n+1}^3 = X_n^{12} \cdot K_{16n+3}$, $X_{n+1}^4 = X_n^{11} + K_{16n+4}$, $X_{n+1}^5 = X_n^{10} \cdot K_{16n+5}$, $X_{n+1}^6 = X_n^9 + K_{16n+6}$, $X_{n+1}^7 = X_n^8 \cdot K_{16n+7}$, $X_{n+1}^8 = X_n^7 \cdot K_{16n+8}$, $X_{n+1}^9 = X_n^6 + K_{16n+9}$, $X_{n+1}^{10} = X_n^5 \cdot K_{16n+10}$, $X_{n+1}^{11} = X_n^4 + K_{16n+11}$, $X_{n+1}^{12} = X_n^3 \cdot K_{16n+12}$, $X_{n+1}^{13} = X_n^2 + K_{16n+13}$, $X_{n+1}^{14} = X_n^1 \cdot K_{16n+14}$, $X_{n+1}^{15} = X_n^{15} + K_{16n+15}$.
8. subblocks X_{n+1}^0, X_{n+1}^1, X_{n+1}^2, ..., X_{n+1}^{15} are summed to XOR with the round key K_{16n+32}, K_{16n+33}, K_{16n+34}, .., K_{16n+47}: $X_{n+1}^j = X_{n+1}^j \oplus K_{16n+32+j}$, $j = \overline{0...7}$.

As ciphertext plaintext X receives the combined 8-bit subblocks $X_{n+1}^0 \| X_{n+1}^1 \| X_{n+1}^2 \| ... \| X_{n+1}^{15}$.

V. Key Generation of the Encryption Algorithm Gost28147-89-Rfwkidea16-2

In n-round encryption algorithm GOST28147-89-IDEA16-2 in each round used sixteen round keys of the 8-bit and output transformation sixteen round keys of the 8-bit. In addition, before the first round and after the output transformation we used sixteen round keys of 8-bits. Total number of 8-bit round keys is equal to 16n+48. In Figure 4 encryption used encryption round keys K_i^c instead of K_i, while decryption used decryption round keys K_i^d.

The key encryption algorithm K of length l ($256 \le l \le 1024$) bits is divided into 8-bit round keys K_0^c, K_1^c,..., $K_{Lenght-1}^c$, $Lenght = l/8$, here $K = \{k_0, k_1, ..., k_{l-1}\}$, $K_0^c = \{k_0, k_1, ..., k_7\}$, $K_1^c = \{k_8, k_9, ..., k_{15}\}$, ..., $K_{Lenght-1}^c = \{k_{l-8}, k_{l-7}, ..., k_{l-1}\}$ and $K = K_0^c \| K_1^c \| ... \| K_{Lenght-1}^c$.

Then we calculate $K_L = K_0^c \oplus K_1^c \oplus ... \oplus K_{Lenght-1}^c$.

If $K_L = 0$ then K_L is chosen as 0xC5, i.e. K_L =0xC5.

Round keys K_i^c, $i = \overline{Lenght...16n+47}$ are computed as follows $K_i^c = Sbox0(K_{i-Lenght}^c) \oplus Sbox1(RotWord(K_{i-Lenght+1}^c)) \oplus K_L$. After each round key generation the value K_L is cyclic shift to the left by 1 bit. Here, RotWord8()-cyclic shift to the left of 1 bit of the 11-bit subblock, Sbox-transformation a 8-bit subblock in the S-boxes, $Sbox0(T) = S_2(t^0) \| S_3(t^1)$, $Sbox1(T) = S_{10}(t^0) \| S_{11}(t^1)$, $T = t^0 \| t^1$ and t^0, t^1-four bit subblock, T -eight bit subblock.

Decryption round keys K_i^d are computed on the basis of encryption round keys K_i^c and decryption round keys of the output transformation associate with of encryption round keys as follows:

$$(K_{16n}^d, K_{16n+1}^d, K_{16n+2}^d, K_{16n+3}^d, K_{16n+4}^d, K_{16n+5}^d, K_{16n+6}^d, K_{16n+7}^d, K_{16n+8}^d, K_{16n+9}^d, K_{16n+10}^d, K_{16n+11}^d, K_{16n+12}^d, K_{16n+13}^d, K_{16n+14}^d, K_{16n+15}^d) = (-K_0^c, (K_1^c)^{-1}, -K_2^c, (K_3^c)^{-1}, -K_4^c, (K_5^c)^{-1}, -K_6^c, (K_7^c)^{-1}, (K_8^c)^{-1}, -K_9^c, (K_{10}^c)^{-1}, -K_{11}^c, (K_{12}^c)^{-1}, -K_{13}^c, (K_{14}^c)^{-1}, -K_{15}^c).$$

Decryption round keys of the first round associate with of encryption round keys as follows:

$$(K_0^d, K_1^d, K_2^d, K_3^d, K_4^d, K_5^d, K_6^d, K_7^d, K_8^d, K_9^d, K_{10}^d, K_{11}^d, K_{12}^d, K_{13}^d, K_{14}^d, K_{15}^d) = (-K_{16n}^c, (K_{16n+1}^c)^{-1}, -K_{16n+2}^c, (K_{16n+3}^c)^{-1}, -K_{16n+4}^c, (K_{16n+5}^c)^{-1}, -K_{16n+6}^c, (K_{16n+7}^c)^{-1}, (K_{16n+8}^c)^{-1}, -K_{16n+9}^c, (K_{16n+10}^c)^{-1}, -K_{16n+11}^c, (K_{16n+12}^c)^{-1}, -K_{16n+13}^c, (K_{16n+14}^c)^{-1}, -K_{16n+15}^c).$$

Decryption round keys of the second, third and n-round associates with the encryption round keys as follows:

$$(K_{16(i-1)}^d, K_{16(i-1)+1}^d, K_{16(i-1)+2}^d, K_{16(i-1)+3}^d, K_{16(i-1)+4}^d, K_{16(i-1)+5}^d, K_{16(i-1)+6}^d, K_{16(i-1)+7}^d, K_{16(i-1)+8}^d, K_{16(i-1)+9}^d, K_{16(i-1)+10}^d, K_{16(i-1)+11}^d, K_{16(i-1)+12}^d, K_{16(i-1)+13}^d, K_{16(i-1)+14}^d, K_{16(i-1)+15}^d) = (-K_{16(n-i+1)}^c, (K_{16(n-i+1)+14}^c)^{-1}, -K_{16(n-i+1)+13}^c, (K_{16(n-i+1)+12}^c)^{-1}, -K_{16(n-i+1)+11}^c, (K_{16(n-i+1)+10}^c)^{-1}, -K_{16(n-i+1)+9}^c, (K_{16(n-i+1)+8}^c)^{-1}, (K_{16(n-i+1)+7}^c)^{-1}, -K_{16(n-i+1)+6}^c, (K_{16(n-i+1)+5}^c)^{-1}, -K_{16(n-i+1)+4}^c, (K_{16(n-i+1)+3}^c)^{-1}, -K_{16(n-i+1)+2}^c, (K_{16(n-i+1)+1}^c)^{-1}, -K_{16(n-i+1)+15}^c), i = \overline{2...n}.$$

Decryption round keys applied to the first round and after the output transformation associated with the encryption round keys as follows: $K_{16n+16+j}^d = K_{16n+32+j}^c$, $K_{16n+32+j}^d = K_{16n+16+j}^c$, $j = \overline{0...7}$

VI. Results

As a result of this study built a new block encryption algorithms called GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2. This algorithm is based on a networks IDEA16-2 and RFWKIDEA16-2 using the round function of GOST 28147-89. Length of block encryption algorithm is 128 bits, the number of rounds and key lengths is variable. Wherein the user depending on the degree of secrecy of the information and speed of encryption can select the number of rounds and key length.

It is known, that the S-box encryption algorithm GOST 28147-89 are secret and used as a long-term key.

Global Journal of Computer Science and Technology (E) Volume XVI Issue III Version I Year 2016

following Table 2 summarizes options openly declared S-box such as: $\deg$ -degree of algebraic nonlinearity; NL -nonlinearity; λ -resistance to linear cryptanalysis; δ -resistance to differential cryptanalysis; SAC-strict avalanche criterion; BIC-bit independence criterion.To S-box was resistant to cryptanalysis it is necessary that the values $\deg$ and NL were large, and the values λ, δ, SAC and BIC small. In block cipher algorithms GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2 for all S-boxes, the following equation: $\deg = 3$, $NL = 4$, $\lambda = 0.5$, $\delta = 3/8$, SAC≤ 2, BIC≤ 4, i.e. resistance is not lower than the algorithm GOST 28147-89. These S-boxes are created based on Nyberg construction [3].

Table 2 : Parameters of the S-boxes encryption algorithm GOST 28147-89

№	Parameters	S1	S2	S3	S4	S5	S6	S7	S8
1	$\deg$	2	3	3	2	3	3	2	2
2	NL	4	2	2	2	2	2	2	2
3	λ	0.5	3/4	3/4	3/4	3/4	3/4	3/4	3/4
4	δ	3/8	3/8	3/8	3/8	1/4	3/8	0.5	0.5
5	SAC	2	2	2	4	2	4	2	2
6	BIC	4	2	4	4	4	4	2	4

IV. Conclusions

In this way, built a new block encryption algorithms called GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2 based on networks IDEA16-2 and RFWKIDEA16-2 using the round function of GOST 28147-89. Installed that the resistance offered by the author block cipher algorithm not lower than the resistance of the algorithm GOST 28147-89.

References Références Referencias

1. Aripov M.M. Tuychiev G.N. The network IDEA4–2, consists from two round functions // Infocommunications: Networks–Technologies–Solutions. –Tashkent, 2012, №4 (24), pp. 5559.
2. Aripov M.M. Tuychiev G.N. The network PES8–4, consists from four round functions // Materials of the international scientific conference конференции «Modern problems of applied mathematics and information technologies–Al–Khorezmiy 2012», Volume №I, –Tashkent, 2012, pp. 16–19.
3. Bakhtiyorov U., Tuychiev G. About Generation Resistance S Box And Boolean Function On The Basis Of Nyberg Construction // Materials scientific-technical conference «Applied mathematics and information security», Tashkent, 2014, 28–30 april, -pp. 317–324
4. GOST 28147–89. National Standard of the USSR. Information processing systems. Cryptographic protection. Algorithm cryptographic transformation.
5. Tuychiev G.N. The networks RFWKIDEA4–2, IDEA4–1 and RFWKIDEA4–1 // Acta of Turin polytechnic university in Tashkent, 2013, №3pp. 71-77
6. Tuychiev G.N. The network PES4–2, consists from two round functions // Uzbek journal of the problems of informatics and energetics. –Tashkent, 2013, №56, pp. 107–111
7. Tuychiev G.N. About networks PES4–1 and RFWKPES4–2, RFWKPES4–1 developed on the basis of network PES4–2 // Uzbek journal of the problems of informatics and energetics. –Tashkent, 2015, №12, pp. 100-105.
8. Tuychiev G.N. About networks RFWKPES8–4, RFWKPES8–2, RFWKPES8–1, developed on the basis of network PES8–4 // Transactions of the international scientific conference «Modern problems of applied mathematics and information technologies–Al–Khorezmiy 2012», Volume№ 2, –Samarkand, 2014, pp. 32–36
9. Tuychiev G. Creating a data encryption algorithm based on network IDEA4-2, with the use the round function of the encryption algorithm GOST 28147-89 // Infocommunications: Networks–Technologies–Solutions. –Tashkent, 2014, №4 (32), pp. 4954
10. Tuychiev G. Creating a encryption algorithm based on network RFWKIDEA4–2 with the use the round function of the GOST 28147-89 // International Conference on Emerging Trends in Technology, Science and Upcoming Research in Computer Science (ICDAVIM-2015), //printed in International Journal of Advanced Technology in Engineering and Science, 2015, vol. 3, №1pp. 427-432
11. Tuychiev G. Creating a encryption algorithm based on network PES4-2 with the use the round function of the GOST 28147-89 // TUIT Bulleten, -Tashkent, 2015, №2(34)pp. 132-136
12. Tuychiev G. Creating a encryption algorithm based on network RFWKPES4–2 with the use the round function of the GOST 28147–89 // International Journal of Multidisciplinary in Cryptology and Information Security, 2015, vol.4., №2, pp. 14-17
13. Tuychiev G. The encryption algorithms GOST28147–89–PES8–4 and GOST28147–89–RFWKPES8–4 // «Information Security in the light of the Strategy Kazakhstan-2050»: proceedings III International scientific-practical conference (15-16 October 2015, Astana). - Astana, 2015. pp. 355-371
14. Tuychiev G.N. About networks IDEA16–4, IDEA16–2, IDEA16–1, created on the basis of network IDEA16–8 // Compilation of theses and reports republican seminar «Information security in the sphere communication and information. Problems and their solutions» –Tashkent, 2014

15. Tuychiev G.N. About networks RFWKIDEA16–8, RFWKIDEA16–4, RFWKIDEA16–2, RFWKIDEA16–1, created on the basis network IDEA16–8 // Ukrainian Scientific Journal of Information Security, –Kyev, 2014, vol. 20, issue 3, pp. 259–263

Global Journals Inc. (US) Guidelines Handbook 2016

www.GlobalJournals.org