Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

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

Tuychiev Gulom[1]

[1] National University of Uzbekistan

Received: 10 December 2015 Accepted: 1 January 2016 Published: 15 January 2016

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.

Index terms— GOST 28147-89, Lai-Massey scheme, round function, round keys, output transformation

1 I. Introduction

he 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].

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.

2 II.

The Structure of the Encryption Algorithm Gost28147-89-Idea16-2

In the encryption algorithm GOST28147-89-IDEA16-2 the length of subblocks 0 X , 1 X , 2 X ,..., 15 X , length of round keys **??** and the S-boxes shown in Table **??**.

Consider the round function block encryption algorithm GOST28147-89-IDEA16-2. First the 8-bit subblocks 0 T , 1 T , ...,

3 7

T combined from 32-bit subblocks, i.e. = 0 T 3 2 1 0 || || || T T T T , = 1 T 7 6 5 4 || || || T T T T . Subblocks 0 T , 1 T are summed round keys || || || 18) 1 (24 17) 1 (24 16) 1 (24 + ? + ? + ? i i i K K K 19) 1 (24 + ? i K , 23) 1 (24 22) 1 (24 21) 1 (24 20) 1 (24 || || || + ? + ? + ? + ? i i i i K K K K i.e.+ ? + ? + ? + ? + = i i i i K K K K T S ,) || || || (23) 1 (24 22) 1 (24 21) 1 (24 20) 1 (24 1 1 + ? + ? + ? + ? + = i i i i K K K K T S .

T Figure **??** : The scheme n-rounded encryption algorithm GOST28147-89-IDEA16-2 The S-boxes of encryption algorithm GOST28147-89-RFWKPES4-2 0x0 0x1 0x2 0x3 0x4 0x5 0x6 0x7 0x8 0x9 0xA 0xB 0x? 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 K : j n j j K X X + + ? = 16 24 0 0 , 15 ... 0 = j . 2. subblocks 0 0 X , 1 0 X , 2 0 X , ..., 15 0

X multiplied and summed respectively with the round keys) 1 (24 ? i K , 1) 1 (24 + ? i K , 2) 1 (24 + ? i K , ?,) ( ) (8) 1 (24 8 1) 1 (24 0 1 0 + ? ? ? ? ? ? + = i i i i K X K X T ,) ( ) (9) 1 (24 9 1 1) 1 (24 1 1 1 + ? ? + ? ? + ? ? = i i i i K X K X T ,) ( ) (10) 1 (24 10 1 2) 1 (24 2 1 2 + ? ? + ? ? ? ? + = i i i i K X K X T ,) ( ) (11) 1 (24 11 1 3) 1 (24 3 1 3 + ? ? + ? ? + ? ? = i i i i K X K X T ,) ( ) (12) 1 (24 12 1 4) 1 (24 4 1 4 + ? ? + ? ? ? ? + = i i i i K X K X T ,) ( ) (13) 1 (24 13 1 5) 1 (24 5 1 5 + ? ? + ? ? + ? ? = i i i i K X K X T ,) ( ) (14) 1 (24 14 1 6) 1 (24 6 1 6 + ? ? + ? ? ? ? + = i i i i K X K X T ,) ( ) (15) 1 (24 15 1 7) 1 (24 7 1 7 + ? ? + ? ? + ? ? = i i i i K X K X T , 1 = i . 3. to 8-bit subblocks 0 T , 1 T , 2 T , ..., 7

T applied round functions and get 8-bit subblocks0 Y , 1 Y , 2 Y , ..., 7 Y . 4. subblocks 0 Y , 1 Y , 2 Y , ..., 7 Y are summed to XOR with subblocks 0 1 ? i X , 1 1 ? i X , 2 1 ? i X , ..., 15 1 ? i X , i. ?. j j i j i Y X X ? ? ? ? = 7 1 1 , j j i j i Y X X ? + ? + ? ? = 7 8 1 8 1 , 7 ... 0 = j , 1 = i . 5

. at the end of the round subblocks swapped, i.

?., j i j i X X ? ? = 15 1 , 14 ... 1 = j , 1 = i 6. repeating steps 2-5 n times, i.e., n i ... 2 = obtain subblocks 0 n X , 1 n X , 2 n X , ...,+ = + , 1 24 14 1 1 + + ? = n n n K X X , 2 24 13 2 1 + + + = n n n K X X , 3 24 12 3 1 + + ? = n n n K X X , 4 24 11 4 1 + + + = n n n K X X , 5 24 10 5 1 + + ? = n n n K X X , 6**24**9 6 1 + + + = n n n K X X , 7 24 8 7 1 + + ? = n n n K X X , 8 24 7 8 1 + + ? = n n n K X X , 9 24 6 9 1 + + + = n n n K X X , 10**24**5 10 1 + + ? = n n n K X X , 11**24**4 11 1 + + + = n n n K X X , 12 24 3 12 1 + + ? = n n n K X X , 13 24 2 13 1 + + + = n n n K X X , 14**24**1 14 1 + + ? = n n n K X X , 15**24**15 15 1 + + + = n n n K X X 8. subblocks 0 1 + n X , 1 1 + n X , 2 1 + n X , ...,K : j n j n j n K X X + + + + ? = 32 24 1 1 , 7 ... 0 = j .

As ciphertext plaintext X receives the combined 8-bit subblocks + + + + n n n n X X X X . III.

4 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 24n+48. In Figure **??** The key encryption algorithm K of length l (1024 256 ? ? l) bits is divided into 8-bit round keys c K 0 , c K 1 ,..., c Lenght K 1 ? , 8 / l Lenght = , here } ,..., , { 1 1 0 ? = l k k k K , } ,..., , { 7 1 0 0 k k k K c = , } ,..., , { 15 9 8 1 k k k K c = ,..., } ,..., , { 1 7 8 1 ? ? ? ? = l l l c Lenght k k k K and c Lenght c c K K K K 1 1 0 || ... || || ? = .

Then we calculatec Lenght c c L K K K K 1 1 0 ... ? ? ? ? = . If 0 = L K then L K is chosen as 0xC5, i.e. L K =0xC5. Round keys c i K , 47 24 ... + = n Lenght i are computed as follows)) ((1) (0 1 c Lenght i c Lenght i c i K RotWord Sbox K Sbox K + ? ? ? = L K ? .

After each round key generation the value L K is cyclic shift to the left by 1 bit. Here, RotWord8()-cyclic shift to the left of 1 bit of the 11-bit subblock, Sboxtransformation a 8-bit subblock in the S-boxes,) (||) ( ) (0 1 1 0 0 t S t S S Sbox = ,) (||) ( ) (). ,) (, ,) (, ,) (, ,)**(,) (, ,) (, ,) (, ,) (, ( ) , , , , , , , , , , , , , , , , (15 1**K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K ? ? ? ? ? ? ? ? = ? ? ? ? ? ? ? ? + + + + + + + + + + + + + + + +

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

). , , , , , ... 2), , , K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K

K K K K K K K K K K K K K + ? + ? + ? + ? + ? +n i K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K c i

5 THE STRUCTURE OF THE ENCRYPTION ALGORITHM GOST28147-89-RFWKIDEA16-2

In the encryption algorithm GOST28147-89-RFWKIDEA16-2 the length of subblocks0 X , 1 X , 2 X ,..., 15 X , length of round keys) 1 (16 ? i K , 1) 1 (16 + ? i K , 2) 1 (16 + ? i K , ?,11 0 0 « = R Y , 11 1 1 « = R Y . Thereafter 32-bit subblocks 0 Y , 1 Y divided into four 8-bit subblocks 0 Y , 1 Y , ..., 7 Y i.e., = 0 Y 3 2 1 0 || || || Y Y Y Y , = 1 Y 7 6 5 4 || || || Y Y Y Y .

Consider the encryption process of encryption algorithm GOST28147-89-IDEA16-2. Initially the 128-bit plaintext X partitioned into subblocks of 8-bits 0 0 X , 1 0 X , 2 0 X , ...) 1 (16 ? i K , 1) 1 (16 + ? i K , 2) 1 (16 + ? i K , ..., 15) 1 (16 + ? i K and calculated 8-bit subblocks 0 T , 1 T , 2 T , ?, 7 T . This step can be represented as follows:) ( ) (8) 1 (16 8 1) 1 (16 0 1 0 + ? ? ? ? ? ? ? + = i i i i K X K X T ,) ( ) (9) 1 (16 9 1 1) 1 (16 1 1 1 + ? ? + ? ? + ? ? = i i i i K X K X T ,) ( ) (10) 1 (16 10 1 2) 1 (16 2 1 2 + ? ? + ? ? ? ? + = i i i i K X K X T ,) ( ) (11) 1 (16 11 1 3) 1 (16 3 1 3 + ? ? + ? ? + ? ? = i i i i K X K X T ,) ( ) (12) 1 (16 12 1 4) 1 (16 4 1 4 + ? ? + ? ? ? ? + = i i i i K X K X T ,) ( ) (13) 1 (16 13 1 5) 1 (16 5 1 5 + ? ? + ? ? + ? ? = i i i i K X K X T ,) ( ) (14) 1 (16 14 1 6) 1 (16 6 1 6 + ? ? + ? ? ? ? + = i i i i K X K X T ,) ( ) (15) 1 (16 15 1 7) 1 (16 7 1 7 + ? ? + ? ? + ? ? = i i i i K X K X T , 1 = i . 3. to 8-bit subblocks 0 T , 1 T , 2 T , ..., 7 T applied round functions and get 8-bit subblocks 0 Y , 1 Y , 2 Y , ..., 7 Y . 4. subblocks 0 Y , 1 Y , 2 Y , ..., 7 Y are summed to XOR with subblocks 0 1 ? i X , 1 1 ? i X , 2 1 ? i X , ?, 15 1 ? i X i.?. j j i j i Y X X ? ? ? ? = 7 1 1 , j j i j i Y X X ? + ? + ? ? =+ + + + n n n n X X X X . V.

6 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 8bits. Total number of 8-bit round keys is equal to 16n+48. In Figure **??**) bits is divided into 8-bit round keysc K 0 , c K 1 ,..., c Lenght K 1 ? , 8 / l Lenght = , here } ,..., , { 1 1 0 ? = l k k k K , } ,..., , { 7 1 0 0 k k k K c = , } ,..., , { 15 9 8 1 k k k K c = , ..., } ,..., , { 1 7 8 1 ? ? ? ? = l l l c Lenght k k k K and c Lenght c c K K K K 1 1 0 || ... || || ? = . Then we calculate c Lenght c c L K K K K 1 1 0 ... ? ? ? ? = . If 0 = L K then L K is chosen as 0xC5, i.e. L K =0xC5. Round keys c i K , 47 16 ... + = n Lenght i are computed as follows ? = ?) (0 c Lenght i c i K Sbox K L c Lenght i K K RotWord Sbox ? + ?)) ((**1 1**

. After each round key generation the value L K is cyclic shift to the left by 1 bit.

Here, RotWord8()-cyclic shift to the left of 1 bit of the 11bit subblock, Sbox-transformation a 8-bit subblock in the S-boxes,) (||) ( ) (0 1 3 0 2 t S t S T Sbox = ,) (||) ( ) (1K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K ? ? ? ? ? ? ? ? ? = ? ? ? ? ? ? ? ? ? + + + + + + + + + + + + + + + +

Decryption round keys of the first round associate with of encryption round keys as follows:). ,) (, ,)**(, ,) (, ,) (,) (, ,) (, ,) (, ,) (, ( ) , , , , , , , , , , , , , , , , (15 16**K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K Kn i K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K K

7 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. [1] [2] [3] [4]

[2]Year 2016 ( ) E

[3]c n d d d d d d d d d d d d d d d d d d d d d d d d

[4]T combined from 32-bit


OPEN
ASSOCIATION
OF RESEARCH
SOCIETY, USA
RESEARCH | DIVERSITY | ETHICS

Figure 1:

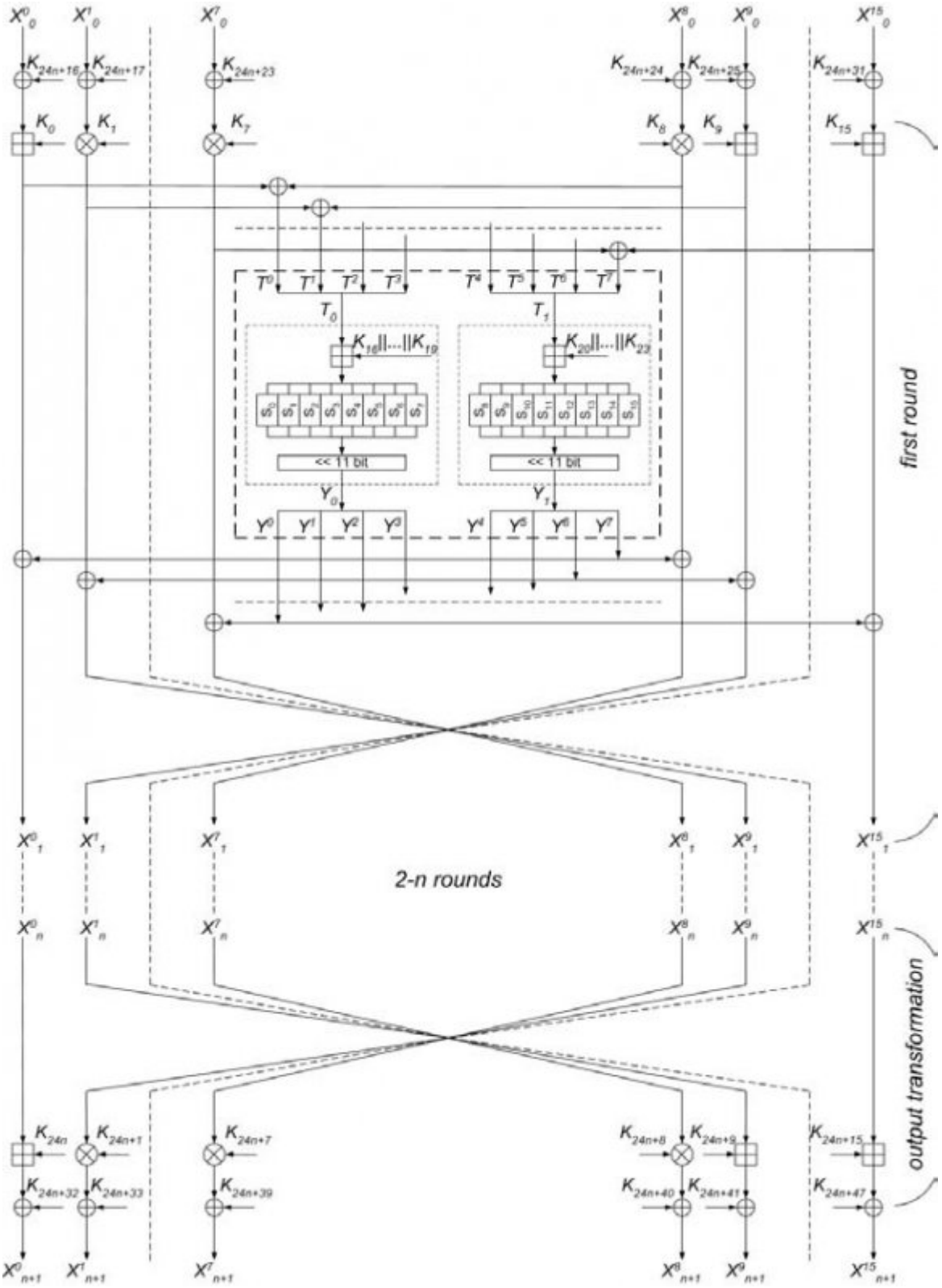

Figure 2: =

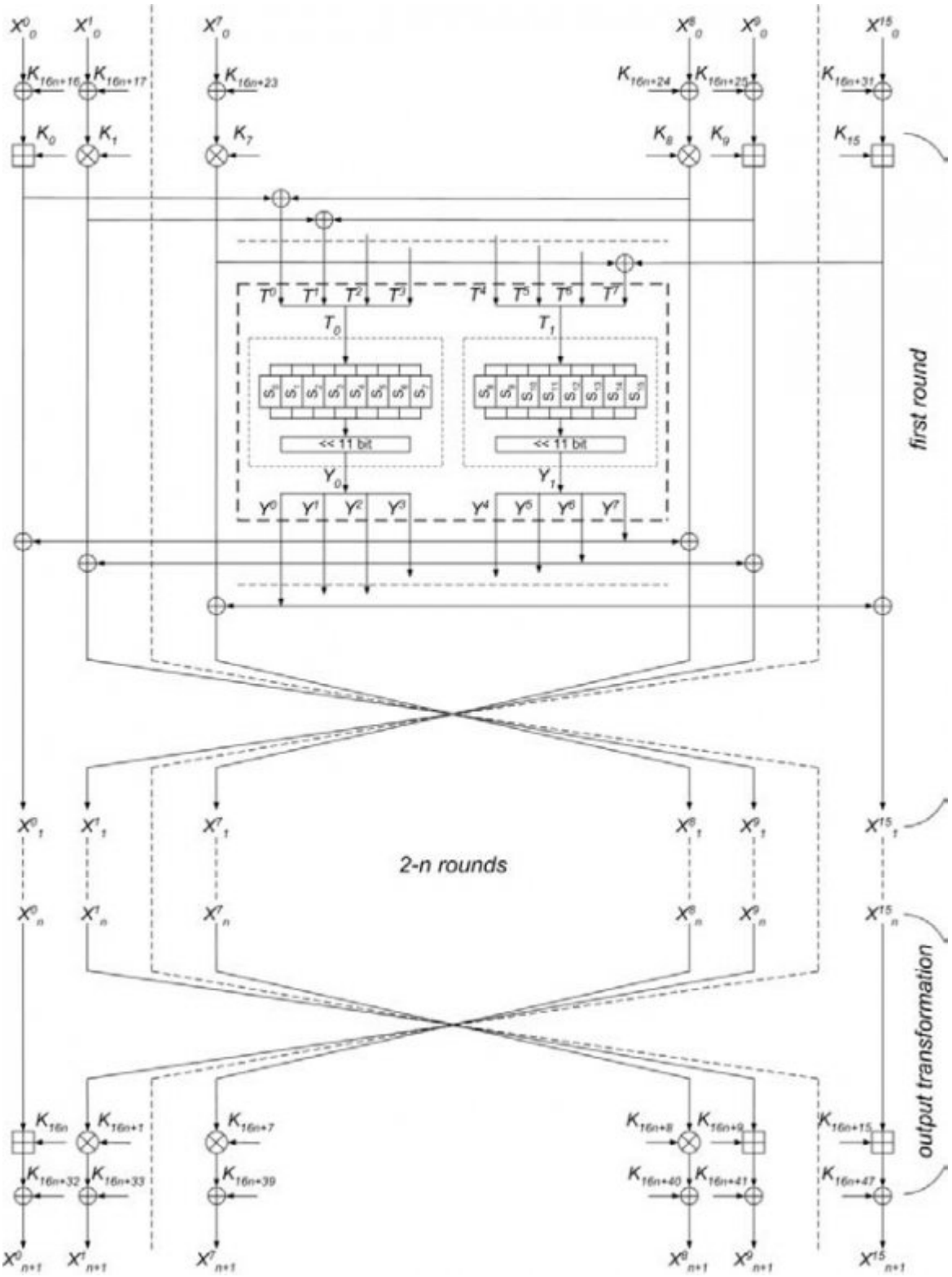

Figure 3:

Figure 4: Table

7. in output transformation round keys

K 16 + n 2 , ..., K 16 + n 15

subblocks 0 n X ,

X n 0 + 1 = X n + K 16 n
0
X 2 + 1 n = X 13 n + K 16
X 4 + 1 n = X 11 n + K 16 n
X 6 + 1 n = X 9 + K 16 n
n
X 8 + 1 n = X 7 ? K 16 n +
n
X 10 + n 1 = X 5 ? K 16 n + 10
n
X 12 + 1 n = X 3 ? K 16 n 12 +
n
X 14 + 1 = X 1 ? K 16 n 14 +
n

8. subblocks 0 + 1 n X , 1 n X , 2 1 + + 1 n X , ..., 15 + 1 n X are to XOR with the round key

K 16 + n 47 : X j n + 1 = X

As ciphertext plaintext X receives the combined
8-bit subblocks 0 1 || i subblo 0 n X , 1 n X , 2 n X , ..., 15 n X .

148). ,) (
149 following Table **??** summarizes options openly declared S-box such as: deg -degree of algebraic nonlinearity;
150 NL -nonlinearity; ? -resistance to linear cryptanalysis; ? -resistance to differential cryptanalysis; SAC-strict
151 avalanche criterion; BIC-bit independence criterion.To Sbox was resistant to cryptanalysis it is necessary that
152 the values deg and NL were large, and the values ? , ? , SAC and BIC small. In block cipher algorithms
153 GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2 for all S-boxes, the following equation:
154 i.e. resistance is not lower than the algorithm GOST 28147-89. These S-boxes are created based on Nyberg
155 construction [3]. IV.

156 .1 CONCLUSIONS

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

161 [Bakhtiyorov and Tuychiev ()] *About Generation Resistance S Box And Boolean Function On The Basis Of
162 Nyberg Construction // Materials scientifictechnical conference «Applied mathematics and information
163 security*, U Bakhtiyorov , G Tuychiev . 2014, 28-30 april. Tashkent. p. .

164 [Tuychiev ()] *About networks IDEA16-4, IDEA16-2, IDEA16-1, created on the basis of network IDEA16-8 //
165 Compilation of theses and reports republican seminar «Information security in the sphere communication and
166 information. Problems and their solutions*, G N Tuychiev . 2014. Tashkent.

167 [Tuychiev ()] *About networks PES4-1 and RFWKPES4-2, RFWKPES4-1 developed on the basis of network
168 PES4-2 // Uzbek journal of the problems of informatics and energetics*, G N Tuychiev . 2015. Tashkent. p. .

169 [Tuychiev ()] 'About networks RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2, RFWKIDEA16-1, cre-
170 ated on the basis network IDEA16-8 // Ukrainian Scientific Journal of Information Security'. G N Tuychiev
171 . *Kyev* 2014. 20 (3) p. .

172 [Tuychiev ()] *About networks RFWKPES8-4, RFWKPES8-2, RFWKPES8-1, developed on the basis of network
173 PES8-4 // Transactions of the international scientific conference «Modern problems of applied mathematics
174 and information technologies-Al-Khorezmiy*, G N Tuychiev . 2012. 2014. p. .

175 [Tuychiev] *Creating a data encryption algorithm based on network IDEA4-2, with the use the round function of
176 the encryption algorithm*, G Tuychiev . GOST 28147-89.

177 [Tuychiev ()] *Creating a encryption algorithm based on network PES4-2 with the use the round function of the
178 GOST 28147-89 // TUIT Bulleten, -Tashkent*, G Tuychiev . 2015. 2 p. .

179 [Tuychiev ()] 'Creating a encryption algorithm based on network RFWKIDEA4-2 with the use the round function
180 of the GOST 28147-89 // International Conference on Emerging Trends in Technology'. G Tuychiev .
181 *International Journal of Advanced Technology in Engineering and Science* 2015. 3 p. . (Science and Upcoming
182 Research in Computer Science)

183 [Tuychiev (2015)] 'Creating a encryption algorithm based on network RFWKPES4-2 with the use the round
184 function of the GOST 28147-89 // International Journal of Multidisciplinary in Cryptology and Information
185 Security'. G Tuychiev . *The encryption algorithms GOST28147-89-PES8-4 and GOST28147-89-RFWKPES8-
186 4 // «Information Security in the light of the Strategy Kazakhstan-2050»: proceedings III International
187 scientific-practical conference*, (Astana; Astana) 2015. October 2015. 2015. 4 p. .

188 [National Standard of the USSR. Information processing systems. Cryptographic protection. Algorithm cryptographic transforma
189 *National Standard of the USSR. Information processing systems. Cryptographic protection. Algorithm
190 cryptographic transformation*, GOST 28147-89.

191 [References Références Referencias Table 2 : Parameters of the S-boxes encryption algorithm GOST]
192 *References Références Referencias Table 2 : Parameters of the S-boxes encryption algorithm GOST*,
193 p. .

194 [Aripov and Tuychiev ()] *The network IDEA4-2, consists from two round functions // Infocommunications:
195 Networks-Technologies-Solutions*, M M Aripov , G N Tuychiev . 2012. Tashkent. 4 p. .

196 [Tuychiev ()] *The network PES4-2, consists from two round functions // Uzbek journal of the problems of
197 informatics and energetics*, G N Tuychiev . 2013. Tashkent. p. .

198 [Aripov and Tuychiev ()] *The network PES8-4, consists from four round functions // Materials of the inter-
199 national scientific conference ? ?????????? «Modern problems of applied mathematics and information
200 technologies-Al-Khorezmiy*, M M Aripov , G N Tuychiev . 2012. 2012. Tashkent. II p. .

201 [Tuychiev ()] *The networks RFWKIDEA4-2, IDEA4-1 and RFWKIDEA4-1 // Acta of Turin polytechnic
202 university in Tashkent*, G N Tuychiev . 2013. 3 p. .

203 [US) Guidelines Handbook Global Journals Inc ()] 'US) Guidelines Handbook'. www.GlobalJournals.org
204 *Global Journals Inc* 2016.