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 GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4

Gulom Tuychiev[1]

[1] National University of Uzbekistan.

Received: 10 December 2015 Accepted: 2 January 2016 Published: 15 January 2016

Abstract

In the paper created a new encryption algorithms GOST28147â??”89â??”IDEA8â??”4 and GOST28147â??”89â??”RFWKIDEA8â??” 4 based on networks IDEA8â??”4 and RFWKIDEA8â??”4, with the use the round function of the encryption algorithm GOST 28147â??”89. The block length of created block encryption algorithm is 256 bits, the number of rounds is 8, 12 and 16.

Index terms— feystel network, laiâ??”massey scheme, round function, round keys, output transformation, multiplication, addition, sâ??”box.

1 I. Introduction

he encryption algorithm GOST 28147-89 [4] 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 Lai-Massey scheme developed the networks IDEA8-4 [6] and RFWKIDEA8-4 [7], consisting from four round function. In the networks IDEA8-4 and RFWKIDEA8-4, similarly as in the Feistel network, in encryption and decryption using the same algorithm. In the networks used four round function having one 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 [8], RFWKPES4-2 [8], PES8-4 [2], RFWKPES8-4 [10], IDEA16-2 [11], RFWKIDEA16-2 [12] encryption algorithm GOST 28147-89 created the encryption algorithm GOST28147-89-IDEA4-2 [13],

GOST28147-89-RFWKIDEA4-2 [14], GOST28147-89-PES4-2 [15], GOST28147-89-RFWKPES4-2 [16], GOST28147-89-PES8-4, GOST28147-89-RFWKPES8-4

[17], GOST28147-89-IDEA16-2, GOST28147-89-RFWKIDEA16-2 [18].

In this paper, applying the round function of the encryption algorithm GOST 28147-89 as round functions of the networks IDEA8-4 and RFWKIDEA8-4, developed new encryption algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKI DEA8-4. In the encryption algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4 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 Encryption Algorithm

Gost28147-89-idea8-4

The structure of the encryption algorithm GOST28147-89-IDEA8-4. In the encryption algorithm GOST28147-89-IDEA8-4 length of the subblocks 0 X , 1 X , ?, 7 X , length of the round keys to 32-bits. In this encryption

algorithm the round function GOST 28147-89 is applied four time and in each round function used eight S-boxes, i.e. the total number of S-boxes is 32. The structure of the encryption algorithm GOST28147-89-IDEA8-4 is shown in Figure **??** and the S-boxes shown in Table 1.) 1 (12 ? i K , 1) 1 (12 + ? i K , ?, 7) 1 (12 + ? i K , 1 ... 1 + = n i , 8) 1 (12 + ? i K , 9) 1 (12 + ? i K , 10) 1 (12 + ? i K ,

3 C

Consider the round function of a encryption algorithm GOST28147-89-IDEA8-4. The 32-bit subblocks 0 T , 1 T , 2 T , 3 T are summed round keys8) 1 (12 + ? i K , 9) 1 (12 + ? i K , 10) 1 (12 + ? i K , 11) 1 (12 + ? i K , n i ... 1 = , i.e. 8) 1 (**12**0 0 + ? + = i K T S , 9) 1 (**12**1 1 + ? + = i K T S , 10) 1 (**12**2 2 + ? + = i K T S , 11) 1 (**12**3 3 + ? + = i K T S

. 32-bit subblocks 0 S , Y , 1 Y , 2 Y , 3 Y : 11 0 0 « = R Y , 11 1 1 « = R Y , 11 2 2 « = R Y , 11 3 3 « = R Y .+ ? ? ? ? + ? ? = i i i i K X K X T ,) ( ) (5) 1 (**12**5 1 1) 1 (12 1 1 1 + ? ? + ? ? + ? ? = i i i i K X K X T ,) ( ) (6) 1 (**12**6 1 2) 1 (12 2 1 2 + ? ? + ? ? + ? ? = i i i i K X K X T ,) ( ) (7) 1 (**12**7 1 3) 1 (12 3 1 3 + ? ? + ? ? + ? ? = i i i i K X K X T , 1 = i 3. to sublocks 0 T , 1 T , 2 T , 3 T applying the round function and get the 32-bit subblocks 0 Y , 1 Y , 2 Y , 3 Y . 4. subblocks 0 Y , 1 Y , 2 Y , 3 Y are summed to XOR with subblocks 0 1 ? i X , 1 1 ? i X , ?, 7 1 ? i X , i.?. 3 0 1 0 1 Y X X i i ? = ? ? , 2 1 1 1 1 Y X X i i ? = ? ? , 1 2 1 2 1 Y X X i i ? = ? ? , 0 3 1 3 1 Y X X i i ? = ? ? , 3 4 1 4 1 Y X X i i ? = ? ? , 2 5 1 5 1 Y X X i i ? = ? ? , 1 6 1 6 1 Y X X i i ? = ? ? , 0 7 1 7 1 Y X X i i ? = ? ? , 1 = i . 5.

At the end of the round subblocks swapped, i.e,0 1 0 ? = i i X X ,**6 1 1 ?**= i i X X ,**5 1 2 ?**= i i X X ,**4 1 3 ?**= i i X X , 3 1 4 ? = i i X X , 2 1 5 ? = i i X X , 1 1 6 ? = i i X X , 7 1 7 ? = i i X X , 1 = i .

The Encryption Algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4 0x0 0x1 0x2 0x3 0x4 0x5 0x6 0x7 0x8 0x9 0xA 0xB 0x? 0xD 0xE 0xF S0 0x4 0x5 0xA 0x8 0xD 0x9 0xE 0x2 0x6 0xF 0xC 0x7 0x0 0x3 0x1 0xB S1 0x5 0x4 0xB 0x9 0xC 0x8 0xF 0x3 0x7 0xE 0xD 0x6 0x1 0x2 0x0 0xA S2 0x6 0x7 0x8 0xA 0xF 0xB 0xC 0x0 0x4 0xD 0xE 0x5 0x2 0x1 0x3 0x9 S3 0x7 0x6 0x9 0xB 0xE 0xA 0xD 0x1 0x5 0xC 0xF 0x4 0x3 0x0 0x2 0x8 S4 0x8 0x9 0x6 0x4 0x1 0x5 0x2 0xE 0xA 0x3 0x0 0xB 0xC 0xF 0xD 0x7 S5 0x9 0x8 0x7 0x5 0x0 0x4 0x3 0xF 0xB 0x2 0x1 0xA 0xD 0xE 0xC 0x6 S6 0xA 0xB 0x4 0x6 0x3 0x7 0x0 0xC 0x8 0x1 0x2 0x9 0xE 0xD 0xF 0x5 S7 0xB 0xA 0x5 0x7 0x2 0x6 0x1 0xD 0x9 0x0 0x3 0x8 0xF 0xC 0xE 0x4 S8 0xC 0xD 0x2 0x0 0x5 0x1 0x6 0xA 0xE 0x7 0x4 0xF 0x8 0xB 0x9 0x3 S9 0xE 0xF 0x0 0x2 0x7 0x3 0x4 0x8 0xC 0x5 0x6 0xD 0xA 0x9 0xB 0x1 S10 0xF 0xE 0x1 0x3 0x6 0x2 0x5 0x9 0xD 0x4 0x7 0xC 0xB 0x8 0xA 0x0 S11 0x1 0x8 0x7 0xD 0x0 0x4 0x3 0xF 0xB 0xA 0x9 0x2 0x5 0x6 0xC 0xE S12 0x2 0xB 0x4 0xE 0x3 0x7 0x0 0xC 0x8 0x9 0xA 0x1 0x6 0x5 0xF 0xD S13 0x3 0xA 0x5 0xF 0x2 0x6 0x1 0xD 0x9 0x8 0xB 0x0 0x7 0x4 0xE 0xC S14 0x4 0x5 0xA 0x0 0xD 0x1 0x6 0x2 0xE 0x7 0xC 0xF 0x8 0x3 0x9 0xB S15 0x5 0x4 0xB 0x1 0xC 0x0 0x7 0x3 0xF 0x6 0xD 0xE 0x9 0x2 0x8 0xA S16 0x6 0x7 0x8 0x2 0xF 0x3 0x4 0x0 0xC 0x5 0xE 0xD 0xA 0x1 0xB 0x9 S17 0x7 0x6 0x9 0x3 0xE 0x2 0x5 0x1 0xD 0x4 0xF 0xC 0xB 0x0 0xA 0x8 S18 0x8 0x9 0x6 0xC 0x1 0xD 0xA 0xE 0x2 0xB 0x0 0x3 0x4 0xF 0x5 0x7 S19 0x9 0x8 0x7 0xD 0x0 0xC 0xB 0xF 0x3 0xA 0x1 0x2 0x5 0xE 0x4 0x6 S20 0xA 0xB 0x4 0xE 0x3 0xF 0x8 0xC 0x0 0x9 0x2 0x1 0x6 0xD 0x7 0x5 S21 0xB 0xA 0x5 0xF 0x2 0xE 0x9 0xD 0x1 0x8 0x3 0x0 0x7 0xC 0x6 0x4 S22 0xC 0xD 0x2 0x8 0x5 0x9 0xE 0xA 0x6 0xF 0x4 0x7 0x0 0xB 0x1 0x3 S23 0xD 0xC 0x3 0x9 0x4 0x8 0xF 0xB 0x7 0xE 0x5 0x6 0x1 0xA 0x0 0x2 S24 0x1 0x8 0x7 0x5 0x0 0xC 0xB 0xF 0x3 0x2 0x9 0xA 0xD 0x6 0x4 0xE S25 0x2 0xB 0x4 0x6 0x3 0xF 0x8 0xC 0x0 0x1 0xA 0x9 0xE 0x5 0x7 0xD S26 0x3 0xA 0x5 0x7 0x2 0xE 0x9 0xD 0x1 0x0 0xB 0x8 0xF 0x4 0x6 0xC S27 0xF 0xE 0x1 0xB 0x6 0xA 0xD 0x9 0x5 0xC 0x7 0x4 0x3 0x8 0x2 0x0 S28 0xE 0xF 0x0 0xA 0x7 0xB 0xC 0x8 0x4 0xD 0x6 0x5 0x2 0x9 0x3 0x1 S29 0xA 0xB 0xC 0xE 0x3 0xF 0x0 0x4 0x8 0x1 0x2 0x9 0x6 0x5 0x7 0xD S30 0xB 0xA 0xD 0xF 0x2 0xE 0x1 0x5 0x9 0x0 0x3 0x8 0x7 0x4 0x6 0xC S31 0xC 0xD 0xA 0x8 0x5 0x9 0x6 0x2 0xE 0x7 0x4 0xF 0x0 0x3 0x1 0xB 0 n X , 1 n X , ?, 7 n X , i.e. n n n K X X 12 0 0 1 ? = + , 1**12**6 1 1 + + + = n n n K X X , 2 12 5 2 1 + + ? = n n n K X X , 3**12**4 3 1 + + + = n n n K X X , 4**12**3 4 1 + + + = n n n K X X , 5 12 2 5 1 + + ? = n n n K X X , 6**12**1 6 1 + + + = n n n K X X , 7 12 7 7 1 + + ? = n n n K X X . 8. subblocks 0 1 + n X , 1 1 + n X , ...,j n j n j n K X X + + + + ? = 16 12 1 1 , 7 ... 0 = j .

As ciphertext receives the combined 32-bit subblocks7 1 2 1 1 1 0 1 || ... || || || + + + + n n n n X X X X

. In the encryption algorithm GOST28147-89-IDEA8-4 when encryption and decryption using the same algorithm, only when decryption calculates the inverse of round keys depending on operations and are applied in reverse order. One important goal of encryption is key generation.

Key generation of the encryption algorithm GOST28147-89-IDEA8-4. In the n-round encryption algorithm GOST28147-89-IDEA8-4 used in each round 12 round keys of 32 bits and the output transformation of 8 round keys of 32 bits. In addition, prior to the first round and after the output transformation is applied 8 round keys on 32 bits. The total number of 32-bit round keys is equal to 12n+24. Hence, if n=8 then necessary 120, if n=12 then 168 and if n=16 then 216 to generate round keys.

The key of the encryption algorithm length of l (1024 256 ? ? l) bits is divided into 32-bit round keys c K 0 , c K 1 , ..., c Lenght K 1 ? , 32 / l Lenght = , here } ,..., , { 1 1 0 ? = l k k k K , } ,..., , { 31 1 0 0 k k k K c = , } ,..., , { 63 33 32 1 k k k K c = , ..., } ,..., , { 1 31 32 1 ? ? ? ? = l l l c Lenght k k k K . Then calculated c Lenght c c L K K K K 1 1 0 ... ? ? ? ? = . If 0 = L K then as L K selected 0xC5C31537, i.e. 0xC5C31537 = L K . Round keys c i K , 23 12 ... + = n Lenght i

calculated as follows: ? = ?) (0 c Lenght i c i K SBox K)) (32 (1 1 c Lenght i K RotWord SBox + ? L K

? .? ? ? ? + + + + + + + ? ? ? ? = c c c c c c c c c d n d n d n d n d n d n d n d n K K K K K K K K K K K K K K K K

Decryption round keys of the second, third and n-round associates with the encryption round keys as follows: . ... 2), , ,, ,) (, ,) (, , ,) (, ,) (( ) , , , , , , , , , , , , (**11**)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 c i n c i n c i n c i n c i n c i n c i n c i n c i n c i n d i d i d i d i d i d i d i d i d i d i d i d i = ? ? ? ? = + ? + ? + ? + ? ? + + ? + + ? ? + + ? + + ? + + ? ? + + ? + + ? ? + ? + ? + ? + ? + ? + ? + ? + ? + ? + ? + ? + ?

4 C

). , , , c n c n c n c n c n c n c n c n c n d d d 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 + ? + ? + ? + ? ? + + ? + + + ? +

5 III.

The Encryption Algorithm Gost28147-89-rfwkidea8-4.

The structure of the encryption algorithm GOST28147-89-RFWKIDEA8-4. In the encryption algorithm GOST28147-89-RFWKIDEA8-4 length of the subblocks 0 X , 1 X , ?, 7 X , length of the round keys) 1 (8 ? i K , 1) 1 (8 + ? i K , ?, 7) 1 (8 + ? i K , 1 ... 1 + = n i , 8 8 + n K , 5 8 + n K , ..., 23 8 + n K

are equal to 32-bits. In this encryption algorithm the round function GOST 28147-89 is applied four time and in each round function used eight S-boxes, i.e. the total number of S-boxes is 32. The structure of the encryption algorithm GOST28147-89-IDEA8-4 is shown in Figure 2 and the S-boxes shown in Table 1. Y , 1 Y , 2 Y , 3 Y : 11 0 0 « = R Y ,**11**1 1 « = R Y , 11 2 2 « = R Y , 11 3 3 « = R Y

. Consider the encryption process of encryption algorithm GOST28147-89-RFWKIDEA8-4. Initially the 256-bit plaintext X partitioned into subblocks of 32-bits 0 0 X , 1 0 X , ?, 7 0 X and performs the following steps: 1. sublocks X summed by XOR with the round keys0 0 X , 1 0 X , ?,8 8 + n K , 9 8 + n K , ..., 15 8 + n K : j n j j K X X + + ? = 8 8 0 0 , 7 ... 0 = j . 2. sublocks 0 0 X , 1 0 X , ?,**7 0**

X are multiplied and summed to the round keys) 1 (8 ? i K , 1) 1 (8 + ? i K , ..., 7) 1 (8 + ? i K

and calculates a 32-bit subblocks 0 T , 1 T ,2 T , 3 T as follows:) ( ) (4) 1 (8 4 1) 1 (8 0 1 0 + ? ? ? ? + ? ? = i i i i K X K X T ,**) ( ) (5) 1 (8 5 1 1) 1 (8 1 1 1**+ ? ? + ? ? + ? ? = i i i i K X K X T ,) ( ) (6) 1 (8 6 1 2) 1 (8 2 1 2 + ? ? + ? ? + ? ? = i i i i K X K X T ,**) ( ) (7) 1 (8 7 1 3) 1 (8 3 1 3**+ ? ? + ? ? + ? ? = i i i i K X K X T , 1 = i . 3. to sublocks 0 T , 1 T , 2 T , 3

T applying the round function and get the 32-bit subblocks0 Y , 1 Y , 2 Y 3 Y . 4. subblocks 0 Y , 1 Y , 2 Y , 3 Y are summed to XOR with subblocks 0 1 Y X X i i ? = ? ? 0 7 1 7 1 Y X X i i ? = ? ? , 1 = i . 5.

At the end of the round subblocks swapped, i.e,0 1 0 ? = i i X X ,**6 1 1 ?**= i i X X ,**5 1 2 ?**= i i X X ,**4 1 3 ?**= i i X X 3 1 4 ? = i i X X ,**2 1 5 ?**= i i X X

, As ciphertext receives the combined 32-bit subblocks 1 1 6 ? = i i X X ,**7 1 7 ?**= i i X X , 1 = i . 7.X , 1 n X , ?, 7 n X , i.e. n n n K X X 8 0 0 1 ? = + , 1 8 6 1 1 + + + = n n n K X X ,**2 8 5 2 1 +**+ ? = n n n K X X ,**3 8 4 3 1 +**+ + = n n n K X X ,**4 8 3 4 1 +**+ + = n n n K X X , 5 8 2 5 1 + + ? = n n n K X X ,**6 8 1 6 1 +**+ + = n n n K X X ,**7 8 7 7 1 +**+ ? = n n n K X X . 8. subblocks 0 1 + n X , 1 1 + n X ,+ + + + n n n n X X X X

. In the encryption algorithm GOST28147-89-RFWKIDEA8-4 when encryption and decryption using the same algorithm, only when decryption calculates the inverse of round keys depending on operations and are applied in reverse order. One important goal of encryption is key generation.

Key generation of the encryption algorithm GOST28147-89-RFWKIDEA8-4.

In the n-round encryption algorithm GOST28147-89-RFWKIDEA8-4 used in each round 8 round keys of 32 bits and the output transformation of 8 round keys of 32 bits. In addition, prior to the first round and after the output transformation is applied 8 round keys on 32 bits. The total number of 32-bit round keys is equal to 8n+24.

The key length of the encryption algorithm l (1024 256 ? ? l

) bits is divided into 32-bit round keys c K 0, c K 1 , ..., c Lenght K 1 ? , 32 / l Lenght = , here } ,..., , { 1 1 0 ? = l k k k K , } ,..., , { 31 1 0 0 k k k K c = , } ,..., , { 63 33 32 1 k k k K c = , ..., } ,..., , { 1 31 32 1 ? ? ? ? = l l l c Lenght k k k K . Then calculated c Lenght c c L K K K K 1 1 0 ... ? ? ? ? = . If 0 = L K then as L K selected 0xC5C31537, i.e. 0xC5C31537 = L K . Round keys c i K , 23 8 ... + = n Lenght i

calculated as follows:

)) (32 (1) (0 1 c Lenght i c Lenght i c i K RotWord SBox K SBox K + ? ? ? = L K ? .

After each generation of round keys value L K cyclically shifted left by 1 bit.

Decryption round keys are computed on the basis of encryption round keys and decryption round keys of the first round associate with of encryption round keys as follows:). , ,)(, , ,) (, ,) (( ) , , , , , , , (**7 8**K K K K K K K K K K K K K K K K + + ? + + + ? + + ? ? ? ? ? ? =

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

6. repeating the steps 2-5 n time, i.e. n i ... 2 = , obtained the subblocks 0 n X , 1 n X , ?, 7 n X . ... 2),) (, ,)(, , ,) (, ,) (( ) , , , , , , , (**1 7**n i K K K K K K K K K K K K K K K K K K K K K c i n c i n c i n c i n c i n c i

n c i n c i n d i d i d i d i d i d i d i d i d i = ? ? ? ? = ? + + ? + + ? ? + + ? + + ? + + ? ? + + ? + + ? ? + ? + ? + ? + ? + ? + ? + ? + ? + ? ? ? ?

6 Decryption

keys output transformation associated with the encryption keys as follows:).) (, ,)(, , ,) (, ,) (( ) , , , , , , , (**1 7 6**+ + + + + + ? ? ? ? = c c c c c c c c c d n d n d n d n d n d n d n K K K K K K K K K K K K K K K K

Decryption round keys applied to the first round and after the conversion of the output associated with encryption keys as follows:

7 IV. Results

As a result of this study built a new block encryption algorithms called GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4. 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 256 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 S-box of the block encryption algorithm GOST 28147-89 are confidential and are used as long-term keys. In Table 2 below describes the options openly declared S-box such as: deg-degree of the algebraic nonlinearity; NL -nonlinearity; ? -relative resistance to the linear cryptanalysis; ? -relative resistance to differential cryptanalysis; SAC -criterion strict avalanche effect; the BIC criterion of independence of output bits. For S-box was resistant to crypt attack it is necessary that the values deg and NL were large, and the values ? , ? , SAC and BIC small. To S-Box was resistant to cryptanalysis it is necessary that the values deg and NL were large, and the values ? , ? , SAC and BIC small. In block cipher algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4 for all S-boxes, the following equation:3 deg = , 4 = NL

, = ? 0.5, = ? 3/8, SAC=4, BIC=4. i.e. resistance is not lower than the algorithm GOST28147-89. These S-boxes are created based on Nyberg construction [3]. [1] [2] [3]

Figure 1: ?

[1] c n c n d d d d d d d d d

[2] The Encryption Algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4

[3] © 2016 Global Journals Inc. (US)

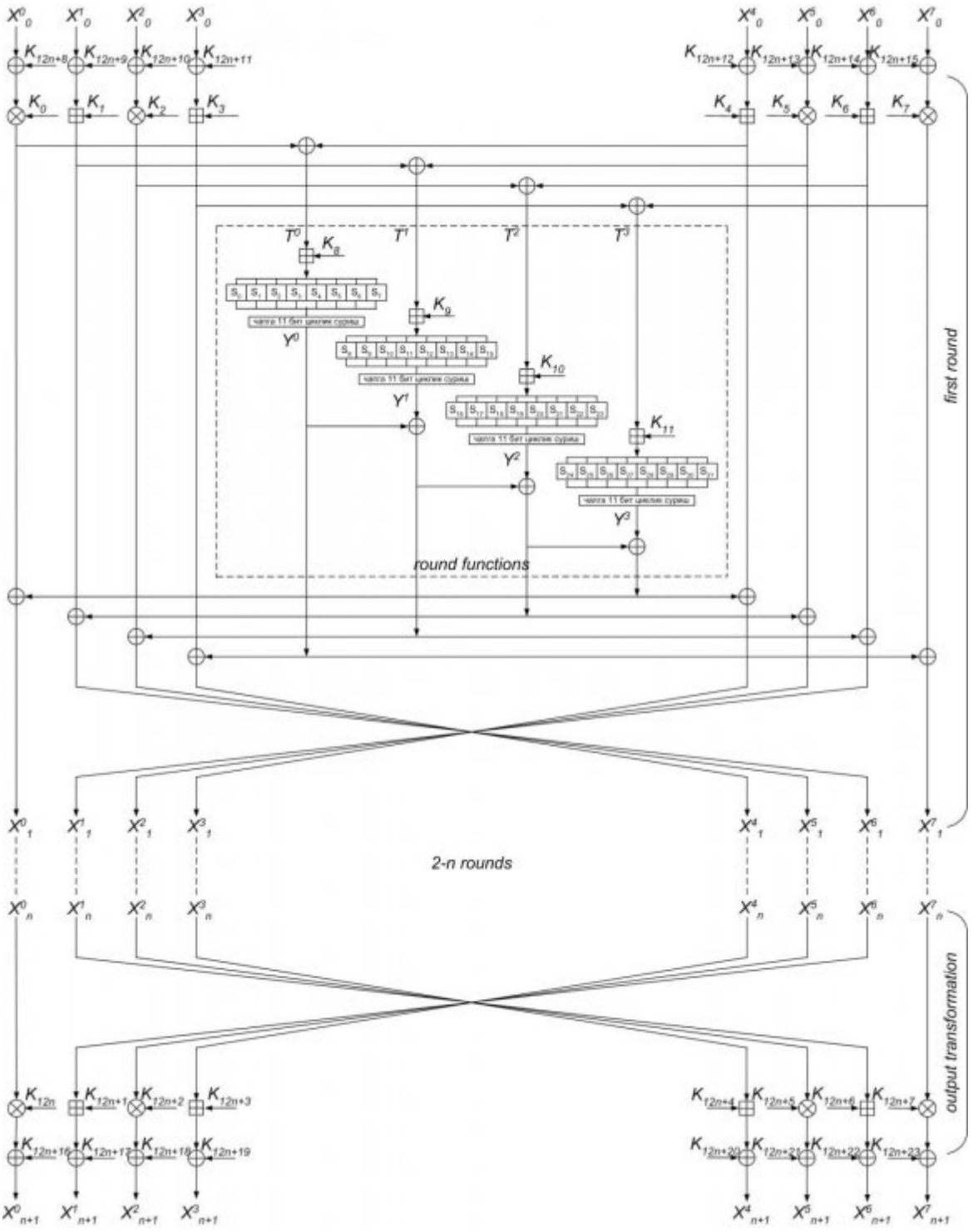
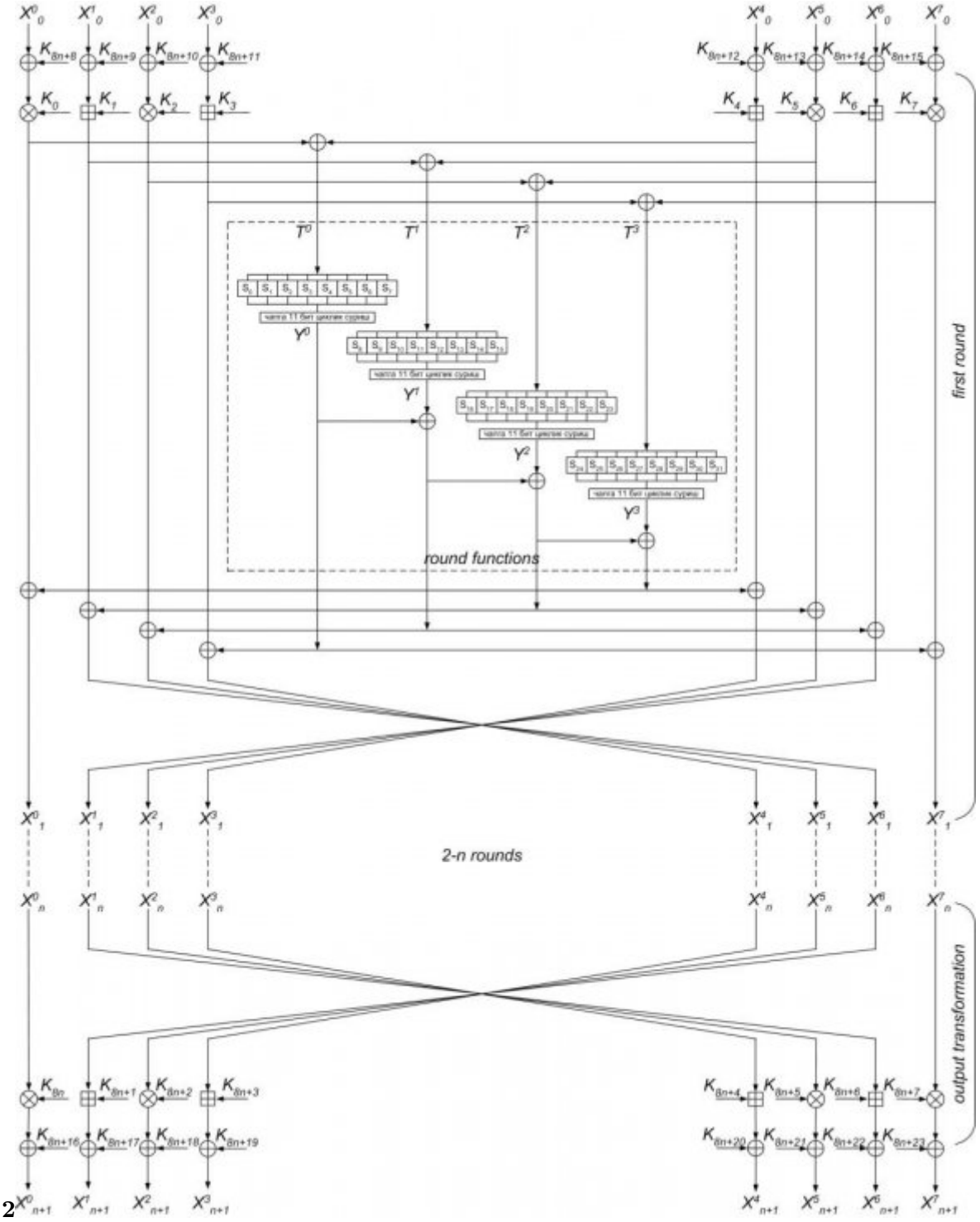

first round
round functions
2-n rounds
output transformation

Figure 2: =



2

Figure 3: Figure 2 :

1

Year 2016
31
Volume XVI Issue V Version I
)
(C
Global Journal of Computer Science and Technology

Figure 4: Table 1 :

i = 2

obtained the subblocks 0 n X , 1 n X , ?, 7 n X .
7. in output transformation round keys n K K 1 12 , 12 , + n ..., K 12 7 are multiplied and summed into subblocks + n

Figure 5:

n K 8 , 1 8 + n K , ...,
7 K are multiplied and summed into subblocks 0 8 + n n

Figure 6:

2

?	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	?	0.5	3/4 3/4		3/4 3/4		3/4	3/4	3/4
4	?	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

Figure 7: Table 2 :

[Infocommunications ()] , // Infocommunications . 2014. Tashkent. 4 p. . (Networks-Technologies-Solutions)

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

[Tuychiev ()] *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*, G N Tuychiev . 2014. Tashkent.

[Tuychiev ()] *About networks IDEA8-2, IDEA8-1 and RFWKIDEA8-4, RFWKIDEA8-2, RFWKIDEA8-1 developed on the basis of network IDEA8-4 // Uzbek mathematical journal*, G N Tuychiev . 2014. Tashkent. 3 p. .

[Tuychiev ()] *About networks PES4-1 and RFWKP-ES4-2, RFWKPES4-1 developed on the basis of network PES4-2 // Uzbek journal of the problems of informatics and energetics*, G Tuychiev . 2015. Tashkent. p. .

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

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

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

[Tuychiev ()] *Creating a encryption algorithm based on network PES4-2 with the use the round function of the GOST 28147-89 // TUIT Bulleten*, G Tuychiev . 2015. Tashkent. 4 p. .

[Tuychiev ()] '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'. G Tuychiev . *International Journal of Advanced Technology in Engineering and Science* 2015. 3 p. . (Science and Upcoming Research in Computer Science)

[Tuychiev ()] 'Creating a encryption algorithm based on network RFWKPES4-2 with the use the round function of the GOST 28147-89'. G Tuychiev . *The encryption algorithms GOST28147-89-PES8-4 and GOST28147-89*, 2015. 2 p. .

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

[RFWKPES8-4 // «Information Security in the light of the Strategy Kazakhstan-2050»: proceedings III International scientific-p *RFWKPES8-4 // «Information Security in the light of the Strategy Kazakhstan-2050»: proceedings III International scientific-practical conference*, (Astana; Astana) October 2015. 2015. p. .

[Tuychiev] 'The Encryption Algorithms GOST-IDEA16-2 and GOST-RFWKIDEA16-2 // Global journal of Computer science and technology: E Network'. G Tuychiev . *Web & security* 16 (1) p. .

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

[Tuychiev ()] *The network IDEA8-4, consists from four round functions // Infocommunications: Networks*, G N Tuychiev . 2013. 2 p. . (Technologies-Solutions. -Tashkent)

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

[Aripov and Tuychiev ()] *The network PES8-4, consists from four round functions // Materials of the international scientific conference ??????????? «Modern problems of applied mathematics and information technologies-Al-Khorezmiy*, M Aripov , G Tuychiev . 2012. 2012. Tashkent. 2 p. .

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