TO THE NETWORKS RFWKIDEA32–16, 32–8, 32–4, 32–2 AND RFWKIDEA32–1, BASED ON THE NETWORK IDEA32–16

Tuychiev G.N.

ABSTRACT

In this article, based on a network IDEA32-16 we have developed 5 new networks: RFWKIDEA32-16, RFWKIDEA32-8, RFWKIDEA32-4, RFWKIDEA32-2, RFWKIDEA32, that do not use round keys in round functions. It shows that in offered networks such Feistel network, encryption and decryption using the same algorithm as a round function can be used any transformation.

KEYWORDS

Feystel network, Lai–Massey scheme, encryption, decryption, encryption algorithm, round function, round keys, output transformation, block, subblock, multiplication, addition, multiplicative inverse, additive inverse

1.INTRODUCTION

H. Lai. and J. Massey replace the DES algorithm developed a new block encryption algorithm PES [2]. However, after the publication of works by E. Biham and A. Shamir on the application of the method of differential cryptanalysis to the algorithm PES, it was modified by increasing its resistance and called IPES. A year later it was renamed IDEA [3]. These algorithms are based on schema Lai-Massey and the basis for the design of these algorithms is the "mixing operations different algebraic groups".

Encryption PES and IDEA, similarly as in DES, the block length is 64 bits. 64 bit block is divided into four 16-bit sub-blocks and operations are carried out on these 16-bit sub-blocks. In the process of encryption PES and IDEA to pairs of 16-bit sub-blocks used three different group operations:

In algorithms PES and IDEA, similarly as in DES, the block length is 64 bits. 64–bit block is divided into four 16–bit subblocks, and operations are performed on 16–bit subblocks. In the process ofencryptionPESand IDEAto pairsof 16–bitsubblocksapplies threedifferent groupoperations

– bitwise exclusive–OR (XOR), denoted as $\oplus$ (xor);

– addition of integers modulo 2^{16}, when the subblock is considered as a typical representation of an integer on the basis of two. Operation is denoted as $\boxplus$ (add);

– multiplication of integers modulo $2^{16}+1$, when the subblock is considered as a typical representation of an integer in base two, except that the subblock of all zeros is assumed to be 2^{16} . Operation is denoted as ⊗ (mul).

In encryption algorithms PES and IDEA round keys are multiplied by modulo $2^{16}+1$ and added by modulo 2^{16} with the corresponding subblocks. In MA the transformation is limited to the operation of multiplication by modulo $2^{16}+1$ and addition by modulo 2^{16}, i.e. not used operations such as shift, substitution with S–box, etc. In the work [1, 4–6] by the authors based on the structure of the encryption algorithm IDEA developed networks IDEA4–2, IDEA8–4, IDEA16–8, IDEA32–16 consisting of two, four, eight and sixteen round functions. In developed networks encrypted and decrypting, similarly as Feystel network, use the same algorithm. And as round functions, it is possible to use any transformation.

In network IDEA32–16 in each round are applied 48 round keys, and 16 round keys are applied in round functions, 32 round keys are multiplied and summed with the subblocks. Through the use of 32 round key subblocks, round functions the network IDEA32–16 can be used without a key. In addition, the network IDEA32–16 round functions have one input and output subblock. As round functions you can use functions in which there are two input and output subblocks, four input and output subblocks, eight input and output subblocks and sixteen input and output subblocks. Scheme of n–rounded network IDEA32–16 shown in Figure 1.

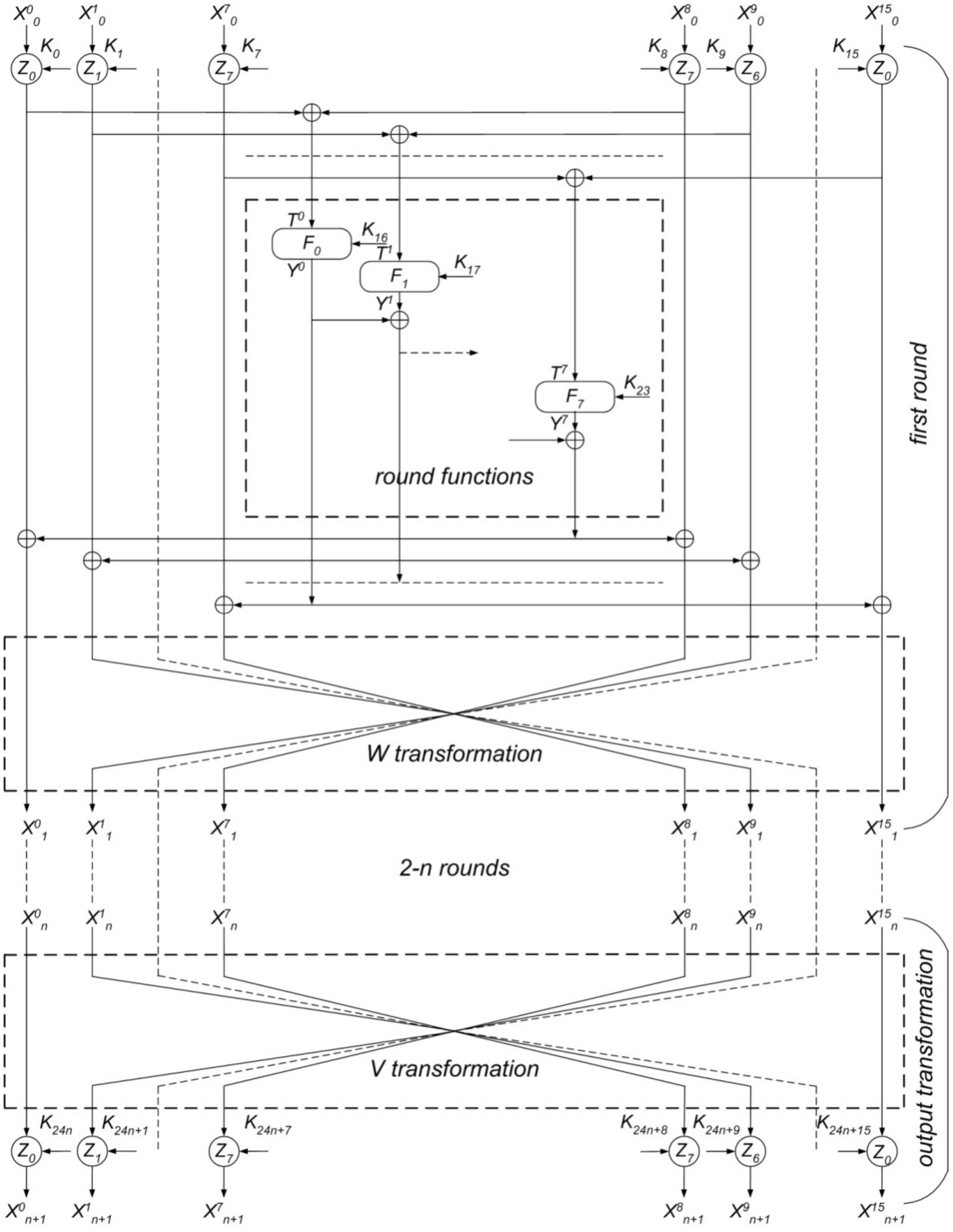

Fig. 1. Scheme of n–rounded network IDEA32–16

In Fig. 1 $z_i$operation ⊗ (mul), ⊞ (add) or⊕ (xor). Here ⊞– addition of integers modulo 2^{32} (2^{16}, 2^{8}), ⊗–multiplication of integers modulo $2^{32}+1$ ($2^{16}+1$, $2^{8}+1$).

In this paper on base of the network IDEA32–16 is developed:

– a network RFWKIDEA32–16 (round function without key IDEA32–16), consisting of sixteen round functions,

– a network RFWKIDEA32–8 (round function without key IDEA32–8), consisting of eight round functions,

– a network RFWKIDEA32–4 (round function without key IDEA32–4), consisting of four round functions,

– a network (RFWKIDEA32–2 round function without key IDEA32–2), consisting of two round functions,

– a network RFWKIDEA32–1 (round function without key IDEA32–1), consisting of one round functions.

2.STRUCTURE OF THE NETWORK RFWKIDEA32–16

In the network RFWKIDEA32–16 length of the subblocks X^0, X^1, ..., X^{31}, length of the round keys $X_{32(i-1)}$, $X_{32(i-1)+1}$, ..., $X_{32(i-1)+31}$, $i=\overline{1...n+1}$, as well as the length of the input and output subblocks round functions F_0, F_1, ..., F_{15} equal to 32 (16, 8) bits. Scheme of n–rounded network RFWKIDEA32–16 shown in Fig. 2, and the encryption process is given in the following formula.

$$\left\{\begin{array}{l}
X_i^0=(X_{i-1}^0(z_0)K_{32(i-1)})\oplus Y^0\oplus Y^1\oplus Y^2\oplus...\oplus Y^{15}\\
X_i^1=(X_{i-1}^{30}(z_1)K_{32(i-1)+30})\oplus Y^0\oplus Y^1\\
X_i^2=(X_{i-1}^{29}(z_2)K_{32(i-1)+29})\oplus Y^0\oplus Y^1\oplus Y^2\\
\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
X_i^{15}=(X_{i-1}^{16}(z_{15})K_{32(i-1)+16})\oplus Y^0\oplus Y^1\oplus Y^2\oplus...\oplus Y^{15}\\
X_i^{16}=(X_{i-1}^{15}(z_{15})K_{32(i-1)+15})\oplus Y^0\\
X_i^{17}=(X_{i-1}^{14}(z_{14})K_{32(i-1)+14})\oplus Y^0\oplus Y^1\\
X_i^{18}=(X_{i-1}^{13}(z_{13})K_{32(i-1)+13})\oplus Y^0\oplus Y^1\oplus Y^2\\
\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
X_i^{31}=(X_{i-1}^{31}(z_0)K_{32(i-1)+31})\oplus Y^0
\end{array}\right., \quad i=\overline{1...n} \qquad (1)$$

$$\left\{\begin{array}{l}
X_{n+1}^{0} = (X_{n}^{0}(z_{0})K_{32n}) \\
X_{n+1}^{1} = (X_{n}^{30}(z_{1})K_{32n+1}) \\
X_{n+1}^{2} = (X_{n}^{29}(z_{2})K_{32n+2}) \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_{n+1}^{15} = (X_{n}^{16}(z_{15})K_{32n+15}) \\
X_{n+1}^{16} = (X_{n}^{15}(z_{15})K_{32n+16}) \\
X_{n+1}^{17} = (X_{n}^{14}(z_{14})K_{32n+17}) \\
X_{n+1}^{18} = (X_{n}^{13}(z_{13})K_{32n+18}) \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_{n+1}^{31} = (X_{n}^{31}(z_{0})K_{32n+31})
\end{array}\right. , \textit{ in output transformation}$$

Round function can be represented as $Y^{0} = F_{0}(T_{i}^{0})$, $Y^{1} = F_{1}(T^{1})$, $Y^{2} = F_{2}(T^{3})$,..., $Y^{15} = F_{15}(T^{15})$. Here $T^{j} = (X_{i-1}^{j}(z_{j})K_{32(i-1)+j}) \oplus (X_{i-1}^{16+j}(z_{15-j})K_{32(i-1)+16+j})$, $j = \overline{0...15}$ – input subblocks of round functions and Y^{0}, Y^{1}, …, Y^{15} – output subblocks of round functions

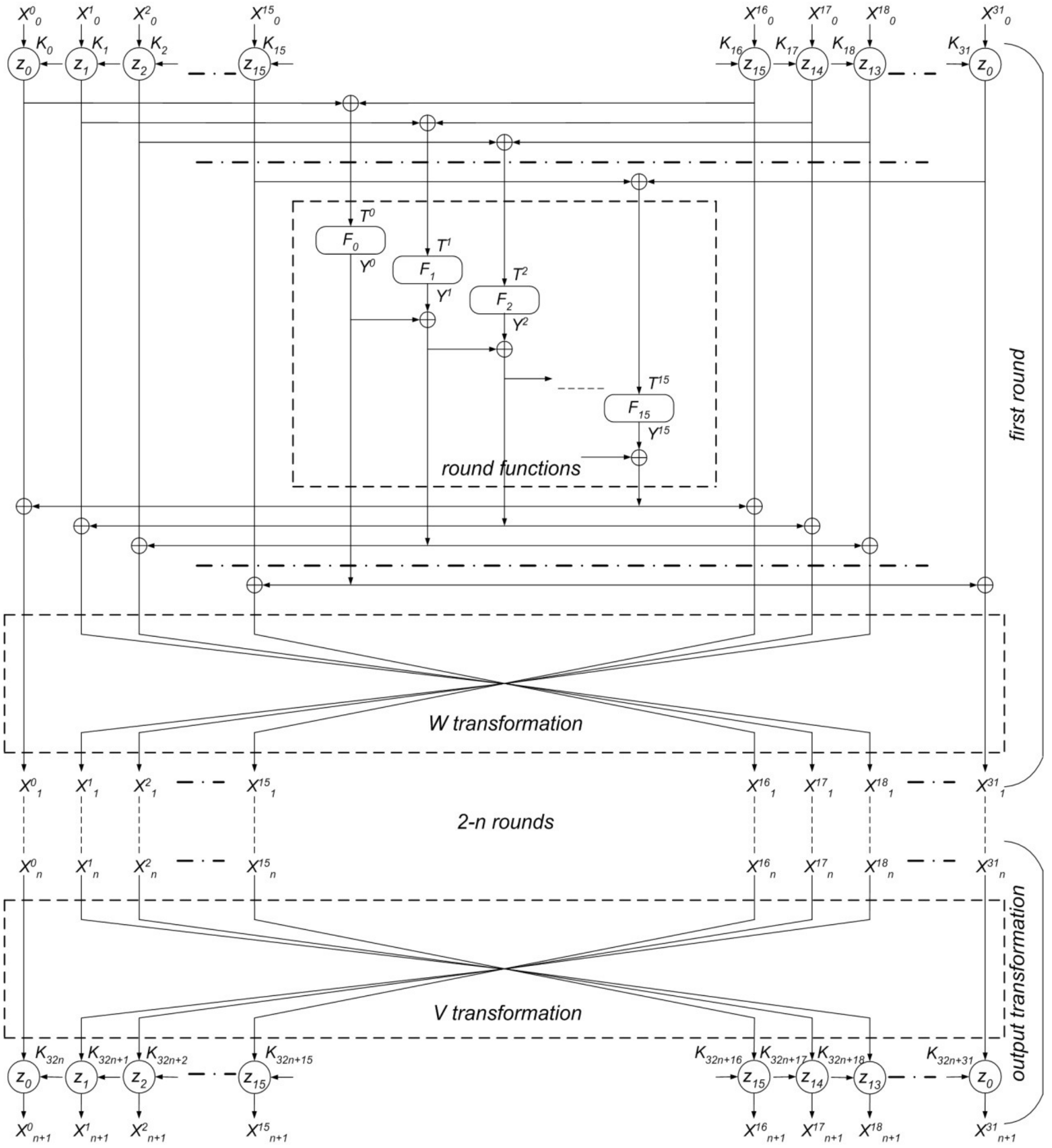

Fig. 2. Scheme of n–rounded network RFWKIDEA32–16

3.THE STRUCTURE OF THE NETWORK RFWKIDEA32–8, RFWKIDEA32–4, RFWKIDEA32–2, RFWKIDEA32–1.

In the network RFWKIDEA32–16 round functions has one input and output subblock.In addition, in block ciphers are used round function with two input and output subblocks. On the basis network RFWKIDEA32–16 it is possible to build a network in which the round function has four input and output subblock, eight input and output subblock and the sixteen input and output subblocks. Network for which the round functions have two input and output subblocks, and applies the eight round functions, called RFWKIDEA32–

8. Similarly, the network to which the round function has four input and output subblocks, and applies four round distance functions is called RFWKIDEA32–4, etc. In the same way the network RFWKIDEA32–2 and RFWKIDEA32–1.Scheme of the round functions of the networks RFWKIDEA32–8, RFWKIDEA32–4, RFWKIDEA32–2, RFWKIDEA32–1 shown in Fig. 3, 4, 5, 6.

In the network RFWKIDEA32–8 round functions F_0, F_1, $F_2,\dots,F_7$ have two input and output subblocks, the length of subblocks is equal to 32 (16, 8) bits. If as the input subblock is put $T0=[T^0,T^1]$, $T1=[T^2,T^3]$, $T2=[T^4,T^5]$, ..., $T7=[T^{14},T^{15}]$, and as the output subblock of the round functions take $Y0=[Y^0,Y^1]$, $Y1=[Y^2,Y^3]$, $Y2_i=[Y^4,Y^5]$, ..., $Y7=[Y^{14},Y^{15}]$, the round functions can be represented as $Y0=F_0(T0)$, $Y1=F_1(T1)$, $Y2=F_2(T2)$, ..., $Y7=F_7(T7)$. For the correctness of the encryption process round function $Y0=F_0(T0)$ can be written as $Y^0=F_0^0(T^0,T^1)$, $Y^1=F_0^1(T^0,T^1)$, and round function $Y1=F_1(T1)$ can be written as $Y^2=F_1^0(T^2,T^3)$, $Y^3=F_1^1(T^2,T^3)$ and so on, round function $Y7=F_7(T7)$ can be written as $Y^{14}=F_7^0(T^{14},T^{15})$, $Y^{15}=F_7^1(T^{14},T^{15})$.

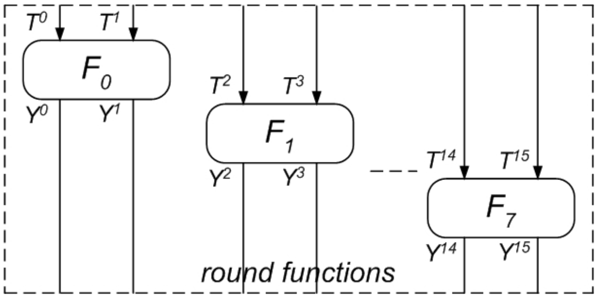

Fig.3. Scheme of the round function of the network RFWKIDEA32–8

In the network RFWKIDEA32–4 round function F_0, F_1, F_2, F_3 have four input and output subblocks of 32 (16, 8) bits. If $T0=[T^0,T^1,T^2,T^3]$, $T1=[T^4,T^5,T^6,T^7]$, $T2=[T^8,T^9,T^{10},T^{11}]$, $T3=[T^{12},T^{13},T^{14},T^{15}]$–input subblock, $Y0=[Y^0,Y^1,Y^2,Y^3]$, $Y1=[Y^4,Y^5,Y^6,Y^7]$, $Y2=[Y^8,Y^9,Y^{10},Y^{11}]$, $Y3=[Y^{12},Y^{13},Y^{14},Y^{15}]$–output subblock of round function, the round function can be represented as $Y0=F_0(T0)$, $Y1=F_1(T1)$, $Y2=F_2(T2)$, $Y3=F_3(T3)$. For the correctness of the encryption process round function $Y0=F_0(T0)$ can be written as $Y^0=F_0^0(T^0,T^1,T^2,T^3)$, $Y^1=F_0^1(T^0,T^1,T^2,T^3)$, …, $Y^3=F_0^3(T^0,T^1,T^2,T^3)$, $Y1=F_1(T1)$ rounder function can be written as $Y^4=F_1^0(T^4,T^5,T^6,T^7)$, $Y^5=F_1^1(T^4,T^5,T^6,T^7)$,…, $Y^7=F_1^3(T^4,T^5,T^6,T^7)$ and so on, rounder function $Y3 = F_3(T3, K)$ can be written as $Y^{12} = F_3^0(T^{12}, T^{13}, T^{14}, T^{15})$, $Y^{13} = F_3^1(T^{12}, T^{13}, T^{14}, T^{15})$, …, $Y^{15} = F_3^3(T^{12}, T^{13}, T^{14}, T^{15})$.

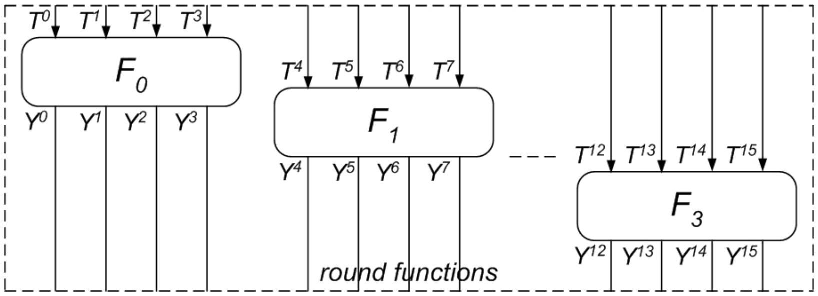

Fig.4. Scheme of the round function of the network RFWKIDEA32–4

Similarly, in the network RFWKIDEA32–2 round functions F_0, F_1 have eight input and output subblocks of 32 (16, 8) bits. If $T0 = [T^0, T^1, ..., T^7]$, $T1 = [T^8, T^9, ..., T_i^{15}]$–input subblock and $Y0 = [Y^0, Y^1, ..., Y^7]$, $Y1 = [Y^8, Y^9, ..., Y^{15}]$–output subblock of round function, the round function can be represented as $Y0 = F_0(T0)$, $Y1 = F_1(T1)$. For the correctness of the encryption process round function $Y0 = F_0(T0)$ can be written as $Y^0 = F_0^0(T^0, T^1, ..., T_i^7)$, $Y^1 = F_0^1(T^0, T^1, ..., T^7)$, …..,$Y^7 = F_0^7(T^0, T^1, ..., T^7)$,round function $Y1 = F_1(T1)$ can be written as $Y^8 = F_1^0(T^8, T^9, ..., T^{15})$,$Y^9 = F_1^1(T^8, T^9, ..., T^{15})$,……., $Y^{15} = F_1^7(T^8, T^9, ..., T^{15})$.

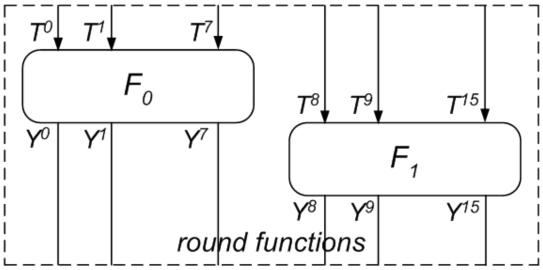

Fig.5. Scheme of the rounder function of the RFWKIDEA32 network

As the network RFWKIDEA32–2, if in the network RFWKIDEA32–1, as the input subblock take $T = [T^0, T^1, ..., T^{15}]$ and as output subblock round function taking $Y = [Y^0, Y^1, ..., Y^{15}]$, the round function can be represented as $Y = F(T)$. For the correctness of the encryption process round function $Y = F(T)$ can be written as $Y^0 = F^0(T^0, T^1, ..., T^{15})$, $Y^1 = F^1(T^0, T^1, ..., T^{15})$, ..., $Y^{15} = F^{15}(T^0, T^1, ..., T^{15})$.

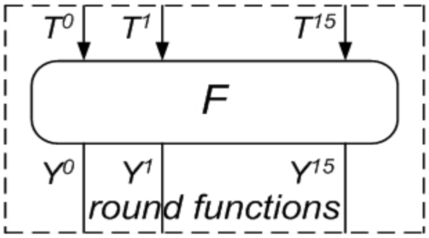

Fig.6. Scheme of the round function of the network RFWKIDEA32–1

In networks RFWKIDEA32–8, RFWKIDEA32–4, RFWKIDEA32–2, RFWKIDEA32–1 F_i^j – is output $j+1$ subblock of round functions F_i.

Encryption process networks RFWKIDEA32–8, RFWKIDEA32–4, RFWKIDEA32–2, RFWKIDEA32–1 similar on (1) formula, but instead $Y^0 \oplus Y^1$ put Y^1, instead $Y^0 \oplus Y^1 \oplus Y^2$ put Y^2 and so on, instead $Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{15}$ put Y^{15}.

4.ROUND KEYS GENERATION OF THE NETWORKS RFWKIDEA32–16, RFWKIDEA32–8, RFWKIDEA32–4, RFWKIDEA32–2 AND RFWKIDEA32–1.

In $n-$roundednetworks RFWKIDEA32–16, RFWKIDEA32–8, RFWKIDEA32–4, RFWKIDEA32–2 and RFWKIDEA32–1 in each round apply 32 round keys in the output transformation 32 round keys, i.e. the number of all round keys equal to $32n+32$. When encryption in Figure 1 is used instead of K_i encryption round keys K_i^c, while decryption round decryption key K_i^d.

In networks RFWKIDEA32–16, RFWKIDEA32–8, RFWKIDEA32–4, RFWKIDEA32–2, RFWKIDEA32–1 decryption round keys the first round associated with the encryption round keys by the formula (2).

$$\begin{aligned}
&(K_0^d, K_1^d, K_2^d, K_3^d, K_4^d K_5^d, K_6^d, K_7^d, K_8^d, K_9^d, K_{10}^d, K_{11}^d, K_{12}^d, K_{13}^d, K_{14}^d, K_{15}^d, K_{16}^d, K_{17}^d,\\
&K_{18}^d, K_{19}^d, K_{20}^d, K_{21}^d, K_{22}^d, K_{23}^d, K_{24}^d, K_{25}^d, K_{26}^d, K_{27}^d, K_{28}^d, K_{29}^d, K_{30}^d, K_{31}^d) = ((K_{32n}^c)^{z_0},\\
&(K_{32n+1}^c)^{z_1}, (K_{32n+2}^c)^{z_2}, (K_{32n+3}^c)^{z_3}, (K_{32n+4}^c)^{z_4}, (K_{32n+5}^c)^{z_5}, (K_{32n+6}^c)^{z_6}, (K_{32n+7}^c)^{z_7},\\
&(K_{32n+8}^c)^{z_8}, (K_{32n+9}^c)^{z_9}, (K_{32n+10}^c)^{z_{10}}, (K_{32n+11}^c)^{z_{11}}, (K_{32n+12}^c)^{z_{12}}, (K_{32n+13}^c)^{z_{13}}, (K_{32n+14}^c)^{z_{14}}, \qquad (2)\\
&(K_{32n+15}^c)^{z_{15}}, (K_{32n+16}^c)^{z_{15}}, (K_{32n+17}^c)^{z_{14}}, (K_{32n+18}^c)^{z_{13}}, (K_{32n+19}^c)^{z_{12}}, (K_{32n+20}^c)^{z_{11}}, (K_{32n+21}^c)^{z_{10}},\\
&(K_{32n+22}^c)^{z_9}, (K_{32n+23}^c)^{z_8}, (K_{32n+24}^c)^{z_7}, (K_{32n+25}^c)^{z_6}, (K_{32n+26}^c)^{z_5}, (K_{32n+27}^c)^{z_4}, (K_{32n+28}^c)^{z_3},\\
&(K_{32n+29}^c)^{z_2}, (K_{32n+30}^c)^{z_1}, (K_{32n+31}^c)^{z_0})
\end{aligned}$$

If as operation z$_i$, $i=\overline{0...15}$ applies the operation mul, then $K=K^{-1}$, applies the operation mul add, then $K=-K$ and applies the operation xor, then $K=K$, here K^{-1} – multiplicative inversion K by modulo $2^{32}+1$ ($2^{16}+1, 2^{8}+1$), $-K$ – additive inverse K by modulo 2^{32} ($2^{16}, 2^{8}$).For 32, 16 and 8 bit numbers calculated $K \otimes K^{-1} = 1 \bmod (2^{32}+1)$, $K \otimes K^{-1} = 1 \bmod (2^{16}+1)$, $K \otimes K^{-1} = 1 \bmod (2^{8}+1)$ and $-K \boxplus K$ =0, $K \oplus K = 1$.

Decryption round keys output transformation associated with the encryption round key as follows:

$$\begin{aligned}
&(K^{d}_{32n}, K^{d}_{32n+1}, K^{d}_{32n+2}, K^{d}_{32n+3}, K^{d}_{32n+4}, K^{d}_{32n+5}, K^{d}_{32n+6}, K^{d}_{32n+7}, K^{d}_{32n+8}, K^{d}_{32n+9}, K^{d}_{32n+10},\\
&K^{d}_{32n+11}, K^{d}_{32n+12}, K^{d}_{32n+13}, K^{d}_{32n+14}, K^{d}_{32n+15}, K^{d}_{32n+16}, K^{d}_{32n+17}, K^{d}_{32n+18}, K^{d}_{32n+19}, K^{d}_{32n+20},\\
&K^{d}_{32n+21}, K^{d}_{32n+22}, K^{d}_{32n+23}, K^{d}_{32n+24}, K^{d}_{32n+25}, K^{d}_{32n+26}, K^{d}_{32n+27}, K^{d}_{32n+28}, K^{d}_{32n+29}, K^{d}_{32n+30},\\
&K^{d}_{32n+31}) = ((K^{c}_{0})^{z_0}, (K^{c}_{1})^{z_1}, (K^{c}_{2})^{z_2}, (K^{c}_{3})^{z_3}, (K^{c}_{4})^{z_4}, (K^{c}_{5})^{z_5}, (K^{c}_{6})^{z_6}, (K^{c}_{7})^{z_7}, (K^{c}_{8})^{z_8}, \qquad (3)\\
&(K^{c}_{9})^{z_9}, (K^{c}_{10})^{z_{10}}, (K^{c}_{11})^{z_{11}}, (K^{c}_{12})^{z_{12}}, (K^{c}_{13})^{z_{13}}, (K^{c}_{14})^{z_{14}}, (K^{c}_{15})^{z_{15}}, (K^{c}_{16})^{z_{15}}, (K^{c}_{17})^{z_{14}}, (K^{c}_{18})^{z_{13}},\\
&(K^{c}_{19})^{z_{12}}, (K^{c}_{20})^{z_{11}}, (K^{c}_{21})^{z_{10}}, (K^{c}_{22})^{z_9}, (K^{c}_{23})^{z_8}, (K^{c}_{24})^{z_7}, (K^{c}_{25})^{z_6}, (K^{c}_{26})^{z_5}, (K^{c}_{27})^{z_4}, (K^{c}_{28})^{z_3},\\
&(K^{c}_{29})^{z_2}, (K^{c}_{30})^{z_1}, (K^{c}_{31})^{z_0})
\end{aligned}$$

Similarly, the decryption round keys of the second, third, and n–round associated with encryption round keys by the formula (3).

$$\begin{aligned}
&(K^{d}_{32(i-1)}, K^{d}_{32(i-1)+1}, K^{d}_{32(i-1)+2}, K^{d}_{32(i-1)+3}, K^{d}_{32(i-1)+4}, K^{d}_{32(i-1)+5}, K^{d}_{32(i-1)+6}, K^{d}_{32(i-1)+7},\\
&K^{d}_{32(i-1)+8}, K^{d}_{32(i-1)+9}, K^{d}_{32(i-1)+10}, K^{d}_{32(i-1)+11}, K^{d}_{32(i-1)+12}, K^{d}_{32(i-1)+13}, K^{d}_{32(i-1)+14},\\
&K^{d}_{32(i-1)+15}, K^{d}_{32(i-1)+16}, K^{d}_{32(i-1)+17}, K^{d}_{32(i-1)+18}, K^{d}_{32(i-1)+19}, K^{d}_{32(i-1)+20}, K^{d}_{32(i-1)+21},\\
&K^{d}_{32(i-1)+22}, K^{d}_{32(i-1)+23}, K^{d}_{32(i-1)+24}, K^{d}_{32(i-1)+25}, K^{d}_{32(i-1)+26}, K^{d}_{32(i-1)+27}, K^{d}_{32(i-1)+28},\\
&K^{d}_{32(i-1)+29}, K^{d}_{32(i-1)+30}, K^{d}_{32(i-1)+31}) = ((K^{c}_{32(n-i+1)})^{z_0}, (K^{c}_{32(n-i+1)+30})^{z_1}, (K^{c}_{32(n-i+1)+29})^{z_2},\\
&(K^{c}_{32(n-i+1)+28})^{z_3}, (K^{c}_{32(n-i+1)+27})^{z_4}, (K^{c}_{32(n-i+1)+26})^{z_5}, (K^{c}_{32(n-i+1)+25})^{z_6}, (K^{c}_{32(n-i+1)+24})^{z_7}, \quad (4)\\
&(K^{c}_{32(n-i+1)+23})^{z_8}, (K^{c}_{32(n-i+1)+22})^{z_9}, (K^{c}_{32(n-i+1)+21})^{z_{10}}, (K^{c}_{32(n-i+1)+20})^{z_{11}}, (K^{c}_{32(n-i+1)+19})^{z_{12}},\\
&(K^{c}_{32(n-i+1)+18})^{z_{13}}, (K^{c}_{32(n-i+1)+17})^{z_{14}}, (K^{c}_{32(n-i+1)+16})^{z_{15}}, (K^{c}_{32(n-i+1)+15})^{z_{15}}, (K^{c}_{32(n-i+1)+14})^{z_{14}},\\
&(K^{c}_{32(n-i+1)+13})^{z_{13}}, (K^{c}_{32(n-i+1)+12})^{z_{12}}, (K^{c}_{32(n-i+1)+11})^{z_{11}}, (K^{c}_{32(n-i+1)+10})^{z_{10}}, (K^{c}_{32(n-i+1)+9})^{z_9},\\
&(K^{c}_{32(n-i+1)+8})^{z_8}, (K^{c}_{32(n-i+1)+7})^{z_7}, (K^{c}_{32(n-i+1)+6})^{z_6}, (K^{c}_{32(n-i+1)+5})^{z_5}, (K^{c}_{32(n-i+1)+4})^{z_4},\\
&(K^{c}_{32(n-i+1)+3})^{z_3}, (K^{c}_{32(n-i+1)+2})^{z_2}, (K^{c}_{32(n-i+1)+1})^{z_1}, (K^{c}_{32(n-i+1)+31})^{z_0}), \; i = \overline{2...n}
\end{aligned}$$

As can be seen from equation (3) for decryption keys of encryption used in the reverse order, only requires the computation of the inversion in accordance operation z$_i$, $i=\overline{0...15}$.When encryption in the first round encryption keys K^{c}_{0}, K^{c}_{1}, …, K^{c}_{15} into subblocks are used in a operation z$_i$, then decryption the output transformation requires the computation of inversion operation, ie., $K^d_{32n} = (K^c_0)^{z_0}$, $K^d_{32n+1} = (K^c_1)^{z_1}$, ..., $K^d_{32n+15} = (K^c_{15})^{z_{15}}$. If z_0= z_3= z_6= z_9= z_{12}= z_{15}=mul, z_1= z_4= z_7= z_{10}= z_{13}= add, z_2= z_5=z_8= z_{11}= z_{14}=xor, then (3) the formula is as follows:

$$\begin{aligned}
&(K^d_{32n}, K^d_{32n+1}, K^d_{32n+2}, K^d_{32n+3}, K^d_{32n+4}, K^d_{32n+5}, K^d_{32n+6}, K^d_{32n+7}, K^d_{32n+8}, K^d_{32n+9},\\
&K^d_{32n+10}, K^d_{32n+11}, K^d_{32n+12}, K^d_{32n+13}, K^d_{32n+14}, K^d_{32n+15}, K^d_{32n+16}, K^d_{32n+17}, K^d_{32n+18},\\
&K^d_{32n+19}, K^d_{32n+20}, K^d_{32n+21}, K^d_{32n+22}, K^d_{32n+23}, K^d_{32n+24}, K^d_{32n+25}, K^d_{32n+26}, K^d_{32n+27},\\
&K^d_{32n+28}, K^d_{32n+29}, K^d_{32n+30}, K^d_{32n+31}) = ((K^c_0)^{-1}, -K^c_1, K^c_2, (K^c_3)^{-1}, -K^c_4, K^c_5,\\
&(K^c_6)^{-1}, -K^c_7, K^c_8, (K^c_9)^{-1}, -K^c_{10}, K^c_{11}, (K^c_{12})^{-1}, -K^c_{13}, K^c_{14}, (K^c_{15})^{-1}, (K^c_{16})^{-1},\\
&K^c_{17}, -K^c_{18}, (K^c_{19})^{-1}, K^c_{20}, -K^c_{21}, (K^c_{22})^{-1}, K^c_{23}, -K^c_{24}, (K^c_{25})^{-1}, K^c_{26}, -K^c_{27}, (K^c_{28})^{-1},\\
&K^c_{29}, -K^c_{30}, (K^c_{31})^{-1})
\end{aligned}$$

5.CONCLUSION

In paper on the basis of the network IDEA32–16 developed networks RFWKIDEA32–16, RFWKIDEA32–8, RFWKIDEA32–4, RFWKIDEA32–2 and RFWKIDEA32–1. In developed networks, as round functions you can choose any transformation, including one–way functions. Because when decrypting no need to calculate inverse functions so to round functions, ie,

Based on these networks, when the length of the subblocks is equal to 32 bits, you can construct the encryption algorithm is the block length of 1024 bits, while the length of the subblocks is equal to 16 bits, you can construct the encryption algorithm is the block length of 512 bits and the length of the subblocks is equal to 8 bits, we can construct the encryption algorithm is the block length of 256 bits. If you choose as operations z_i, $i = \overline{0...15}$ operation mul, add and xor, all possible variants of this choice is equal to 3^{16}.

The advantage of the developed networks is that the encryption and decryption using the same algorithm. It gives comfort for creating hardware and software–hardware tools.

In addition, as the round function using the round function of the existing encryption algorithms for example, encryption algorithms based on Feistel network, you can developed these algorithms on the basis of the above networks.

REFERENCES

[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. 55–59.

[2] Lai X., Massey J.L. A proposal for a new block encryption standard //Advances in Cryptology – Proc. Eurocrypt'90, LNCS 473, Springer–Verlag, 1991, pp. 389–404

[3] Lai X., Massey J.L. On the design and security of block cipher //ETH series in information processing, v.1, Konstanz: Hartung–GorreVerlag, 1992.

[4] Tuychiev G.N. The network IDEA8–4, consists from four round functions // Infocommunications: Networks–Technologies –Solutions. –Tashkent, 2013. №2 (26), pp. 55–59.

[5] Tuychiev G.N. The network IDEA16–8, consists from eight round functions // Bulletin TSTU. – Tashkent, 2014, №1, pp. 183–187.

[6] Tuychiev G.N. The network IDEA16–8, consists from sixteen round functions // Bulletin NUUz. – Tashkent, 2013, №4/1, pp. 57–61.

Authors

TuychievGulomNumonovich – teacher of National university of Uzbekistan, Ph.D. in technics, Republic of Uzbekistan, Tashkent, e-mail: blasterjon@mail.com