INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS

ISSN(print): 2643-9840, ISSN(online): 2643-9875

Volume 05 Issue 05 May 2022

DOI: 10.47191/ijmra/v5-i5-14, Impact Factor: 6.261

Page No. 975-982

The Network EPES8–2

Abdumannon Kodirjonovich Jumakulov

Lecturer, Kokand branch of Tashkent state technical university

ABSTRACT: The article presents the EPES8–2 network with two round functions using the same algorithm for encryption and decryption.

KEYWORDS: Feystel network, Lai-Massey scheme, encryption, decryption, round keys, round functions.

INTRODUCTION

Currently, block encryption algorithms based on the Feystel network are widely used. Block encryption algorithms based on the Feystel network include encryption algorithms such as DES, GOST 28147-89, as well as block encryption algorithms such as CAST-256, DFC, E2, LOKI97, which participated in the competition announced by NIST. The advantage of this network is that a single algorithm is used for encryption and decryption, only the encryption round keys are used in reverse order for decryption. Encryption and decryption processes of the Feistel network can be expressed by the following formulas:

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \end{cases}, i = \overline{1...n} \quad (1)$$

$$\begin{cases} R_{i-1} = L_i \\ L_{i-1} = R_i \oplus F(L_i, K_i) \end{cases}, i = \overline{n...1} \quad (2)$$

The PES [7] block encryption algorithm was developed in 1990 and is based on the Lai-Massey scheme. In 1991, the authors modified this block encryption algorithm and named it IDEA [8]. In these block encryption algorithms, round keys $2^{16}+1$ are multiplied by the module on the part blocks, 2^{16} added by the module, and in MA transformation, $2^{16}+1$ modular multiplication, 2^{16} module addition operations are used, i.e. not used operations such as shift, substitution with S-box, etc. However, a single algorithm is used in encryption and decryption, as well as encryption round keys are used in reverse order in decryption, just like the Feistel network. The IDEA NXT block encryption algorithm is based on the extended Lai-Massey scheme developed by P. Junod, S. Vaudenay. Later, the IDEA NXT algorithm came to be known as FOX [9]. Using the structure of the PES block encryption algorithm, networks with round function PES4–2, PES8–4, PES32–16 and PES2m–m were created [1-6].

In this article based on the structure encryption algorithm PES the EPES8–2 (extended PES) network was developed, which consists of eight subblocks and two round functions.

NETWORK STRUCTURE

In the proposed EPES8-2 network, the operations $\otimes$ (mul), $\boxplus$ (add) ва $\oplus$ (xor) can be used as operations z0, z_1, z_2, z_3. Here $\otimes$ – multiplication of 32 (16, 8) bit blocks by module $2^{32}+1$ ($2^{16}+1, 2^8+1$), $\boxplus$– addition of 32 (16, 8) bit blocks by module 2^{32} ($2^{16}, 2^8$) and $\oplus$ – addition of 32 (16, 8) bit blocks by XOR. It is possible to create block encryption algorithms with a block length of 256 bits when the length of the subblocks of the network is 32 bits, 128 bits with a block length of 16 bits, and 64 bits with a block length of 8 bits. The network encryption formula (3) and the functional scheme are shown in Figure 1.

The Network EPES8–2

$$\begin{cases} X_i^0 = (X_{i-1}^2(z_1)K_{10(i-1)+2}) \oplus T_i^0 \oplus T_i^1 \\ X_i^1 = (X_{i-1}^3(z_1)K_{10(i-1)+3}) \oplus T_i^0 \\ X_i^2 = (X_{i-1}^0(z_0)K_{10(i-1)}) \oplus T_i^0 \oplus T_i^1 \\ X_i^3 = (X_{i-1}^1(z_0)K_{10(i-1)+1}) \oplus T_i^0 \\ X_i^4 = (X_{i-1}^6(z_3)K_{10(i-1)+6}) \oplus T_i^0 \oplus T_i^1 \\ X_i^5 = (X_{i-1}^7(z_3)K_{10(i-1)+7}) \oplus T_i^0 \\ X_i^6 = (X_{i-1}^4(z_2)K_{10(i-1)+4}) \oplus T_i^0 \oplus T_i^1 \\ X_i^7 = (X_{i-1}^5(z_2)K_{10(i-1)+5}) \oplus T_i^0 \end{cases}, \; i = \overline{1...n} \qquad (3)$$

$$\begin{cases} X_{n+1}^0 = (X_n^0(z_0)K_{10n}) \\ X_{n+1}^1 = (X_n^1(z_0)K_{10n+1}) \\ X_{n+1}^2 = (X_n^2(z_1)K_{10n+2}) \\ X_{n+1}^3 = (X_n^3(z_1)K_{10n+3}) \\ X_{n+1}^4 = (X_n^4(z_2)K_{10n+4}) \\ X_{n+1}^5 = (X_n^5(z_2)K_{10n+5}) \\ X_{n+1}^6 = (X_n^6(z_3)K_{10n+6}) \\ X_{n+1}^7 = (X_n^7(z_3)K_{10n+7}) \end{cases}, \textit{ in the output transformation}$$

where T_i^0, T_i^1 round functions are described in the following formulas:

$T_i^0 = F_0(((X_{i-1}^0(z_0)K_{10(i-1)}) \oplus (X_{i-1}^2(z_1)K_{10(i-1)+2})) \oplus ((X_{i-1}^4(z_2)K_{10(i-1)+4}) \oplus (X_{i-1}^6(z_3)K_{10(i-1)+6})), K_{10(i-1)+8})$,

$T_i^1 = F_1(((X_{i-1}^1(z_0)K_{10(i-1)+1}) \oplus (X_{i-1}^3(z_1)K_{10(i-1)+3})) \oplus ((X_{i-1}^5(z_2)K_{10(i-1)+5}) \oplus (X_{i-1}^7(z_3)K_{10(i-1)+7})), K_{10(i-1)+9})$

In the network EPES8–2 the length of round keys $K_{10(i-1)}$, $K_{10(i-1)+1}$,..., $K_{10(i-1)+7}$, $i = \overline{1...n+1}$, the input and output bits of round functions F_0, F_1 is equal (16, 8) bits. The length of round keys $K_{10(i-1)+8}$, $K_{10(i-1)+9}$, $i = \overline{1...n}$ optional to 32 (16, 8) bits.

The Network EPES8–2

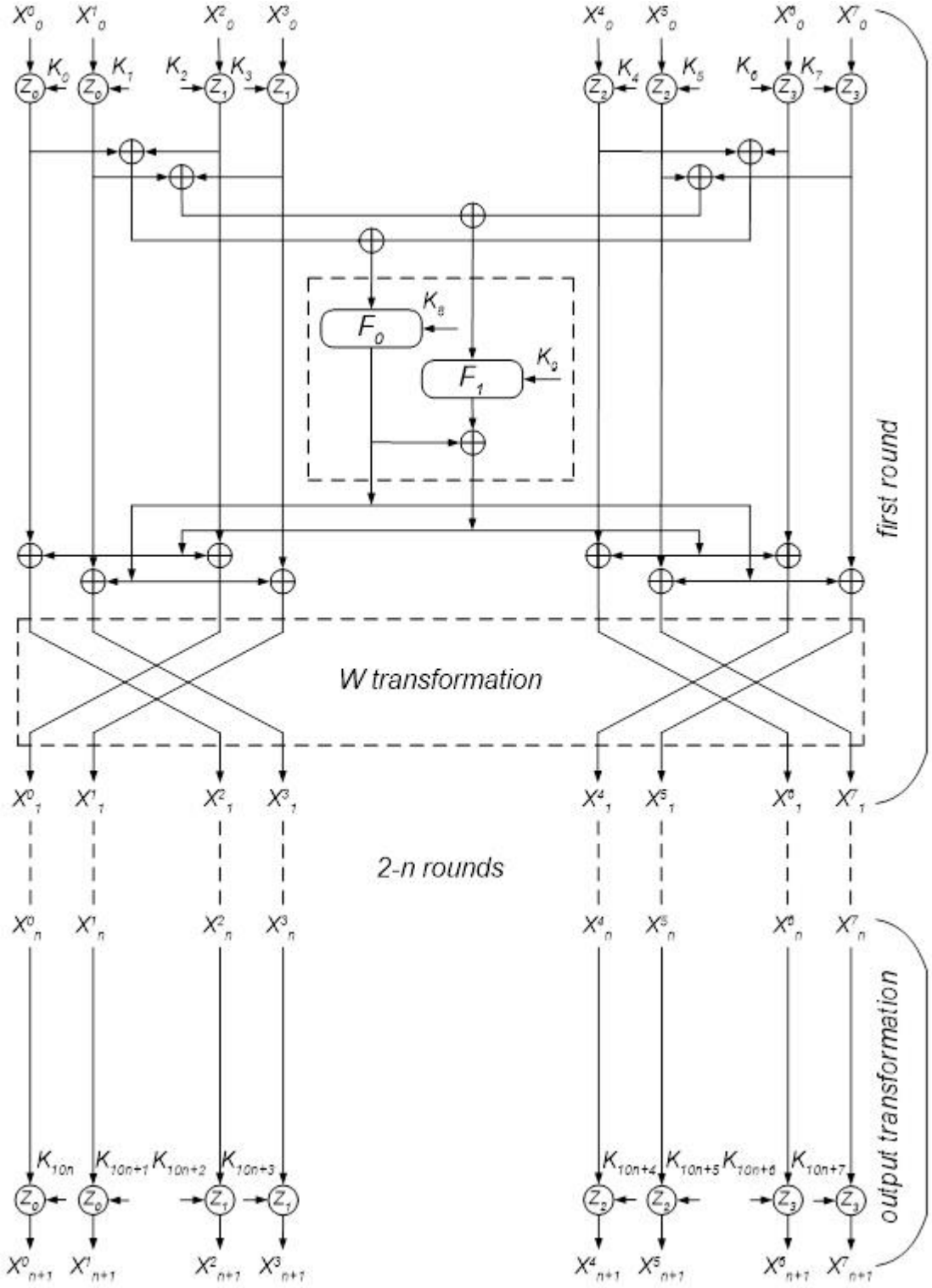

Figure 1. The scheme of EPES8–2 network

In W transformation in each round the subblocks X_{i-1}^{0} and X_{i-1}^{2}, X_{i-1}^{1} and X_{i-1}^{3}, X_{i-1}^{4} and X_{i-1}^{6}, X_{i-1}^{5} and X_{i-1}^{7} will replaced between themselves. Based on the replacement of subblocks, each variants of networks EPES8–2 can be build. The networks represented in fig.1 accept as first variants,

–only subblocks X_{i-1}^{0} ва X_{i-1}^{2}, X_{i-1}^{4} ва X_{i-1}^{6}, $i=\overline{1...n}$ replaced, as second variant

–subblocks not replaced, as third variant,

– only subblocks X_{i-1}^{1} ва X_{i-1}^{3}, X_{i-1}^{5} ва X_{i-1}^{7}, $i=\overline{1...n}$ replaced, as fourth variant can be accepted as a network.

The Network EPES8–2

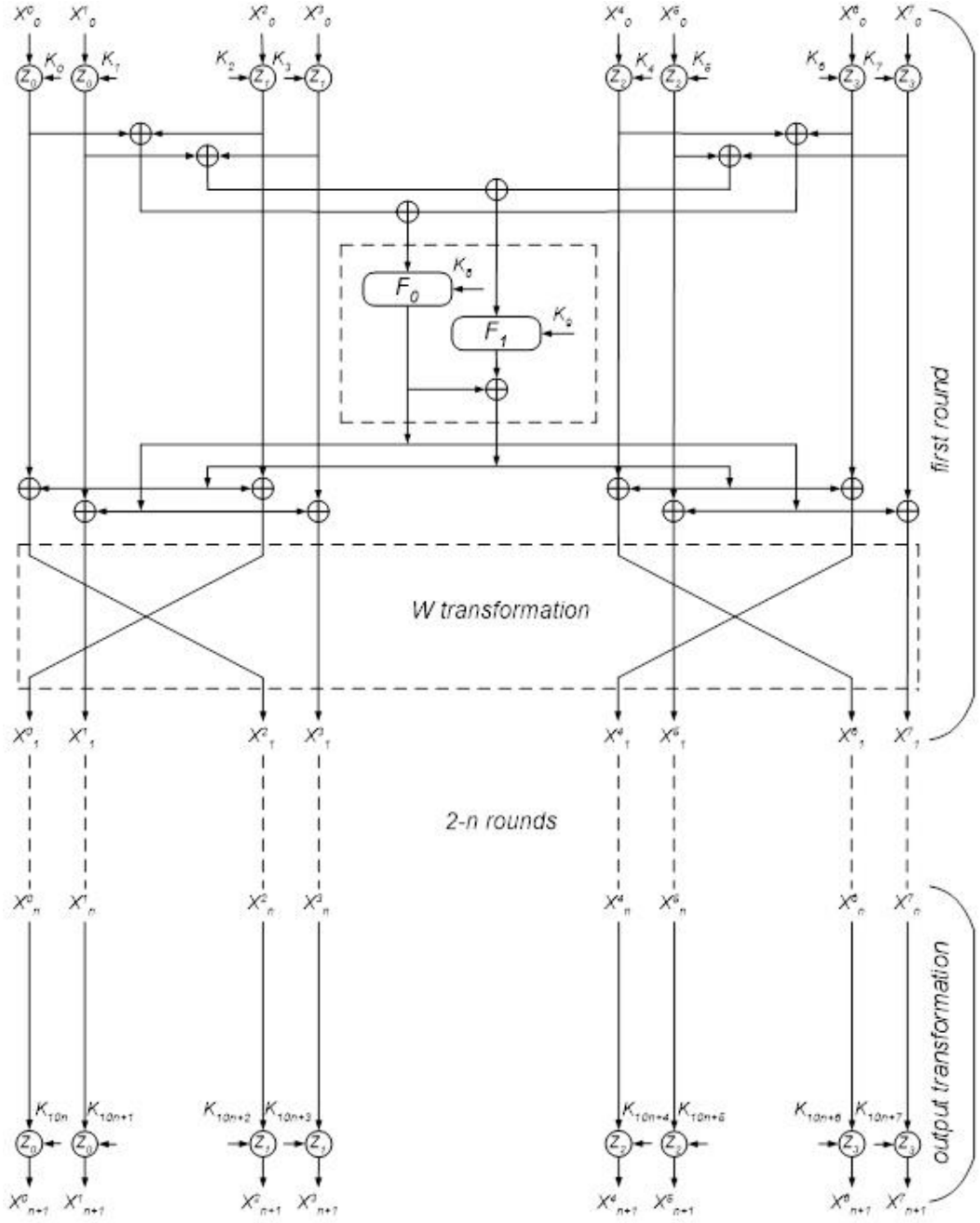

Figure 2. The scheme of second variant EPES8–2 network

The Network EPES8–2

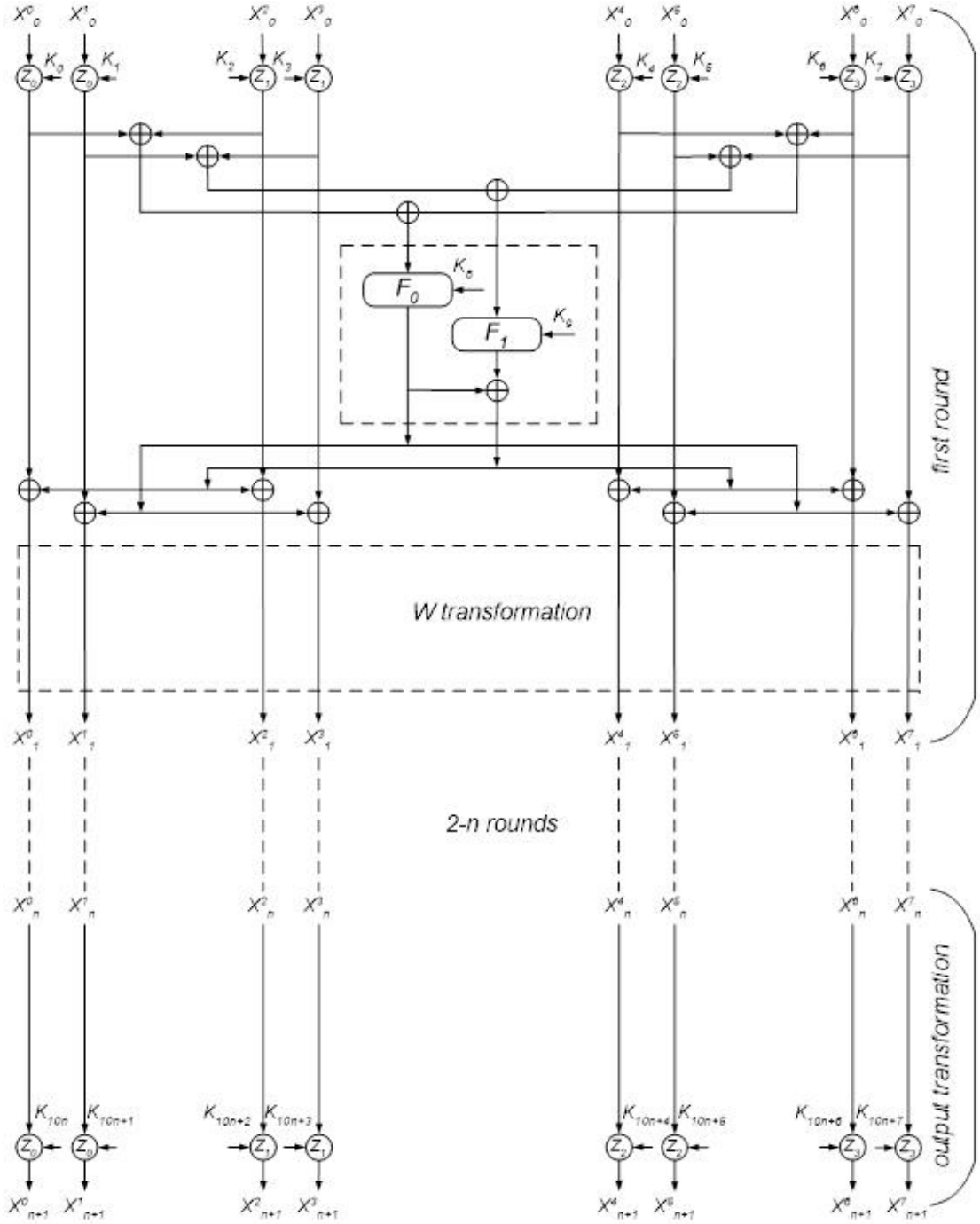

Figure 3. The scheme of third variant EPES8–2 network

The Network EPES8–2

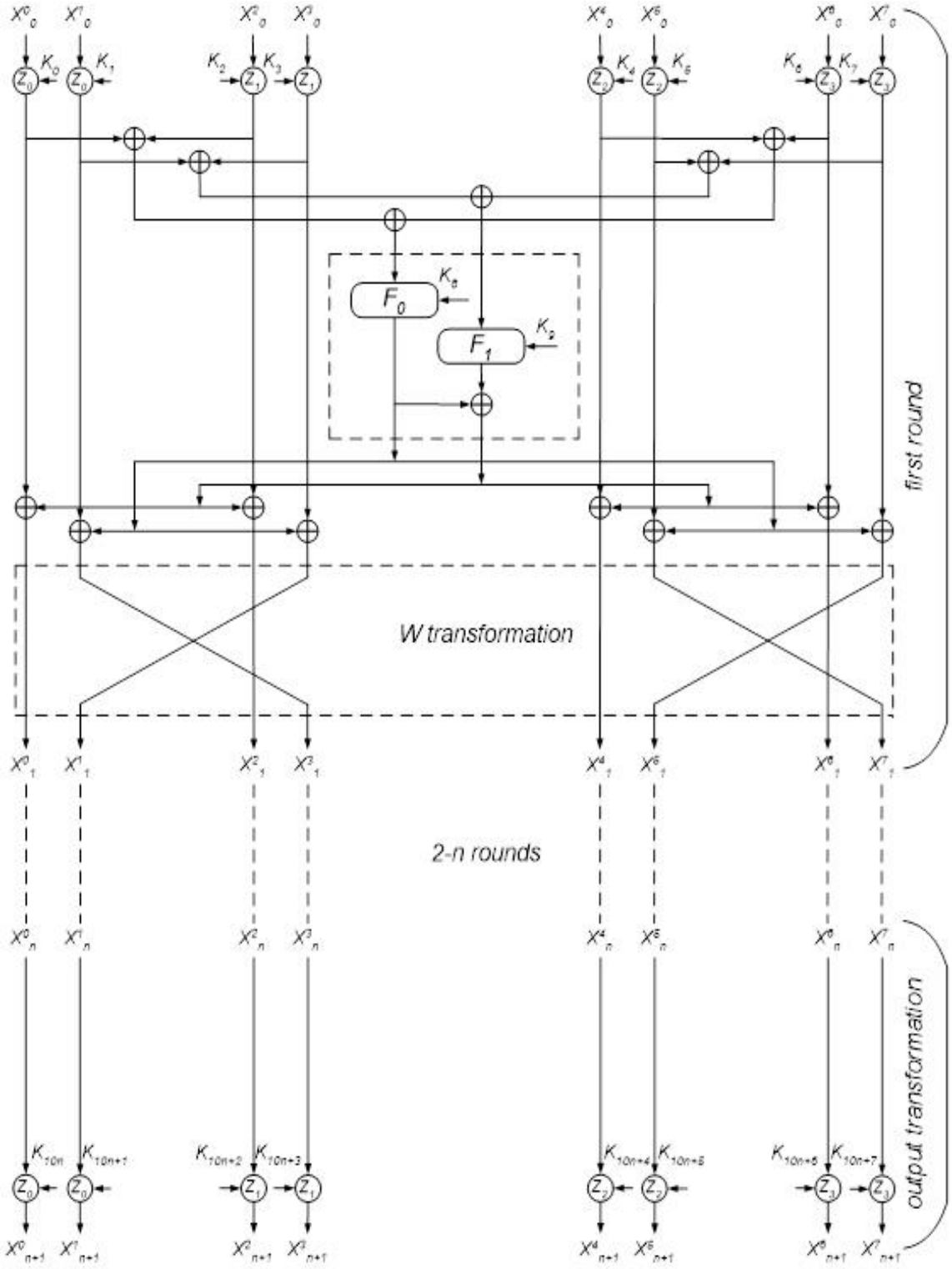

Figure 4. The scheme of fourth variant EPES8–2 network

KEYS GENERATION

n $n-$ rounded EPES8–2 network, in each round applied 10 round keys and in the output transformation applied 8 round keys, i.e. the total number of round keys is $10n+8$. In encryption, the basis of key K generating encryption round keys K_i^c. Decryption round keys K_i^d are created based on encryption round keys K_i^c. In encryption process in Figure 1 and formula (3), uses an encryption round key K_i^c instead of K_i and decryption process uses a decryption round key K_i^d, i.e. a single algorithm is used for encryption and decryption, only the order of the round keys. The *n*-round EPES8–2 network in all variants The first, second and n-round decryption round keys are associated to the encryption round keys as follows:

The Network EPES8–2

$$(K^d_{10(i-1)}, K^d_{10(i-1)+1}, K^d_{10(i-1)+2}, K^d_{10(i-1)+3}, K^d_{10(i-1)+4}, K^d_{10(i-1)+5}, K^d_{10(i-1)+6}, K^d_{10(i-1)+7}, K^d_{10(i-1)+8}, K^d_{10(i-1)+9}) =$$
$$((K^c_{10(n-i+1)})^{z_0}, (K^c_{10(n-i+1)+1})^{z_0}, (K^c_{10(n-i+1)+2})^{z_1}, (K^c_{10(n-i+1)+3})^{z_1}, (K^c_{10(n-i+1)+4})^{z_2}, (K^c_{10(n-i+1)+5})^{z_2}, \quad (4)$$
$$(K^c_{10(n-i+1)+6})^{z_3}, (K^c_{10(n-i+1)+7})^{z_3}, K^c_{10(n-i)+8}, K^c_{10(n-i)+9}), i = \overline{1...n.}$$

If z_0, z_1, z_2, z_3 applied as $\otimes$ operations, then $K = K^{-1}$, $\boxplus$ operations are applied, then $K = -K$ and $\oplus$ are applied, then $K = K$, here K^{-1} – multiplication inversion K by modulo $2^{32}+1$ ($2^{16}+1, 2^8+1$), $-K$ - additive inversion K by modulo 2^{32} ($2^{16}, 2^8$). For 32 bit numbers $K \otimes K^{-1} = 1 \bmod(2^{32}+1)$, 16 bit numbers $K \otimes K^{-1} = 1 \bmod(2^{16}+1)$, 8 bit numbers $K \otimes K^{-1} = 1 \bmod(2^8+1)$ and $-K \boxplus K = 0$, $K \oplus K = 0$.

The decryption round keys of the output transformation are associated with encryption round keys as follows:

$$(K^d_{10n}, K^d_{10n+1}, K^d_{10n+2}, K^d_{10n+3}, K^d_{10n+4}, K^d_{10n+5}, K^d_{10n+6}, K^d_{10n+7}) = ((K^c_0)^{z_0}, (K^c_1)^{z_0}, (K^c_2)^{z_1},$$
$$(K^c_3)^{z_1}, (K^c_4)^{z_2}, (K^c_5)^{z_2}, (K^c_6)^{z_3}, (K^c_7)^{z_3}). \quad (5)$$

RESULTS

In article on the basis of the encryption algorithm PES developed EPES8–2 network. In developed network as round function can choose any transformation, including one-way functions. Because when decryption no need to calculate inverse round functions. 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 networks, you can develop these algorithms on the basis of the above networks.

REFERENCES:

1) Aripov M.M., Tuychiev G.N. PES8–4 network consisting of four rounds of functions // Proceedings of the International Scientific Conference "Actual Problems of Applied Mathematics and Information Technology - Al-Khwarizmi 2012", collection № II. - Tashkent. 2012, 16–19 p.
2) Tuychiev G.N. PES4–2 network consisting of two rounds of functions // Journal of Informatics and Energy Problems journal of Uzbekistan, –Tashkent, 2013. №5–6, 107–111 p. (05.00.00, №5).
3) Tuychiev G.N. About PES4–1, RFWKPES4–2, PES4–1 networks created on the basis of PES4–2 network // Informatics and Energy Problems jounal of Uzbekistan. – Tashkent, 2015. №1–2, 100–105 p. (05.00.00, №5).
4) Tuychiev G.N. About RFWKPES8–4, RFWKPES8–2, RFWKPES8–1 networks created on the basis of PES8–4 network // Collection of reports of the international conference “Actual problems of applied mathematics and information technologies – Al-Khwarizmi 2014”, collection № 2, –Samarkand. 2014, 32–36 p.
5) Tuychiev G.N. About RFWKPES32–16, RFWKPES32–8, RFWKPES32–4, RFWKPES32–2 and RFWKPES32–1 networks created on the basis of PES32–16 network // “Information security in the field of communication and information. Problems and ways to solve them”, Republican seminar collection of reports and abstracts. – Tashkent, 2014.
6) Tuychiev G.N. On the PES2m–m network consisting of m round functions and its modification // Security of Information. –Kyiv, 2015. Volume 21. No. 1. 52–63 p.
7) Lai X., Massey J.L. A proposal for a new block encryption standard. Advances in Cryptology - Proc. Eurocrypt’90, LNCS 473, Springer – Verlag, 1991, 389–404 p.
8) Lai X., Massey J.L. On the design and security of block cipher. ETH series in information processing, v.1, Konstanz: Hartung–Gorre Verlag, 1992.
9) Junod, P., Vaudenay, S.. FOX: a new family of block ciphers. In 11th Selected Areas in Cryptography (SAC) Workshop, LNCS 3357, pages 114–129. Springer–Verlag.
10) Akbarov D.E., Umarov Sh.A. Working out the new algorithm enciphered the data with a symmetric key. //Siberian Federal University. Engineering & Technologies. 2016, 9(2), 214-224 p, DOI: 10.17516/1999-494x-2016-9-2-214-224.
11) Akbarov D., Umarov Sh. Mathematical characteristics of application of mathematical characteristics of logical operations and table substitution in cryptographic transformations. //Scientific-technical journal: 2021, V.4, №2 pp 6-14.

12) Abdurakhmonova, M. M., ugli Mirzayev, M. A., Karimov, U. U., & Karimova, G. Y. (2021). Information Culture And Ethical Education In The Globalization Century. *The American Journal of Social Science and Education Innovations*, *3*(03), 384-388.
13) Akbarov D. E. Umarov Sh. A.(2020). Applying Logical Operations and table replacements in modeling basic transformations of Symmetric block encryption algorithms //International Journal of Mechanical and Production Engineering Research and Development. – Т. 10. – №. 3. – С. 15041-15046.