GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 10, Issue 12, Dec. (2022)

THE NETWORK SREPES8–2

Gulom Tuychiyev
National University of Uzbekistan

Abdumannon Jumakulov
Lecturer Kokand University

Xurshidjon Jumakulov
Kokan State Pedagogical Institute

ABSTRACT

The article presents a network of SREXPES8–2 with two round functions, which uses a single algorithm for encryption and decryption of sequential blocks of parts.

Keywords. Lai-Massey scheme, encryption, decryption, round keys, round functions.

INTRODUCTION

The PES block encryption algorithm was developed in 1990 year and is based on the Lai-Massey scheme. In 1991, the authors modified this encryption algorithm and named it IDEA. In these encryption algorithms, round keys are multiplied by the module on the part blocks $2^{16}+1$, added by the module 2^{16}, and in the 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, 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. Using the structure of the PES block encryption algorithm, created networks PES4–2 [6], PES8–4 [1], PES32–16 [8] and PES2m–m [9], EPES8–2 [2] consisting from round function

Currently, block ciphers are widely used, which use the same encryption and decryption algorithm. Examples of such block cipher algorithms are block cipher algorithms, based on the Feistel network. In the Feistel network, the permutation and substitution operations are reflected in the round functions, and the round function does not depend on the structure of the network. In addition, it is possible to use round functions as one-way function. One of the actual tasks is the development of a network based on the structure of the encryption algorithm PES and the extended Lai-Massey scheme, using the same algorithm for encryption and decryption, by using round functions instead of MA transformation. Based on the above, this article presents the network SREPES8-2 (subblocks successively replaced extended PES) developed based on the structure of the encryption algorithm PES and the extended Ley-Massey scheme, consisting of eight subblocks and two round functions.

Network structure. In the proposed network SREPES8–2, the operations $\otimes$ (mul), $\boxplus$ (add) ва $\oplus$ (xor) can be used as operations z_0, 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.

In the network SREPES8–2 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 32 (16, 8) bits. The length of round keys $K_{10(i-1)+8}$, $K_{10(i-1)+9}$, $i=\overline{1...n}$ not equal to 32 (16, 8) bits. The encryption formula of the network is given in formula (1), and the functional scheme is shown in Figure 1, and the round functions described in the formula

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

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

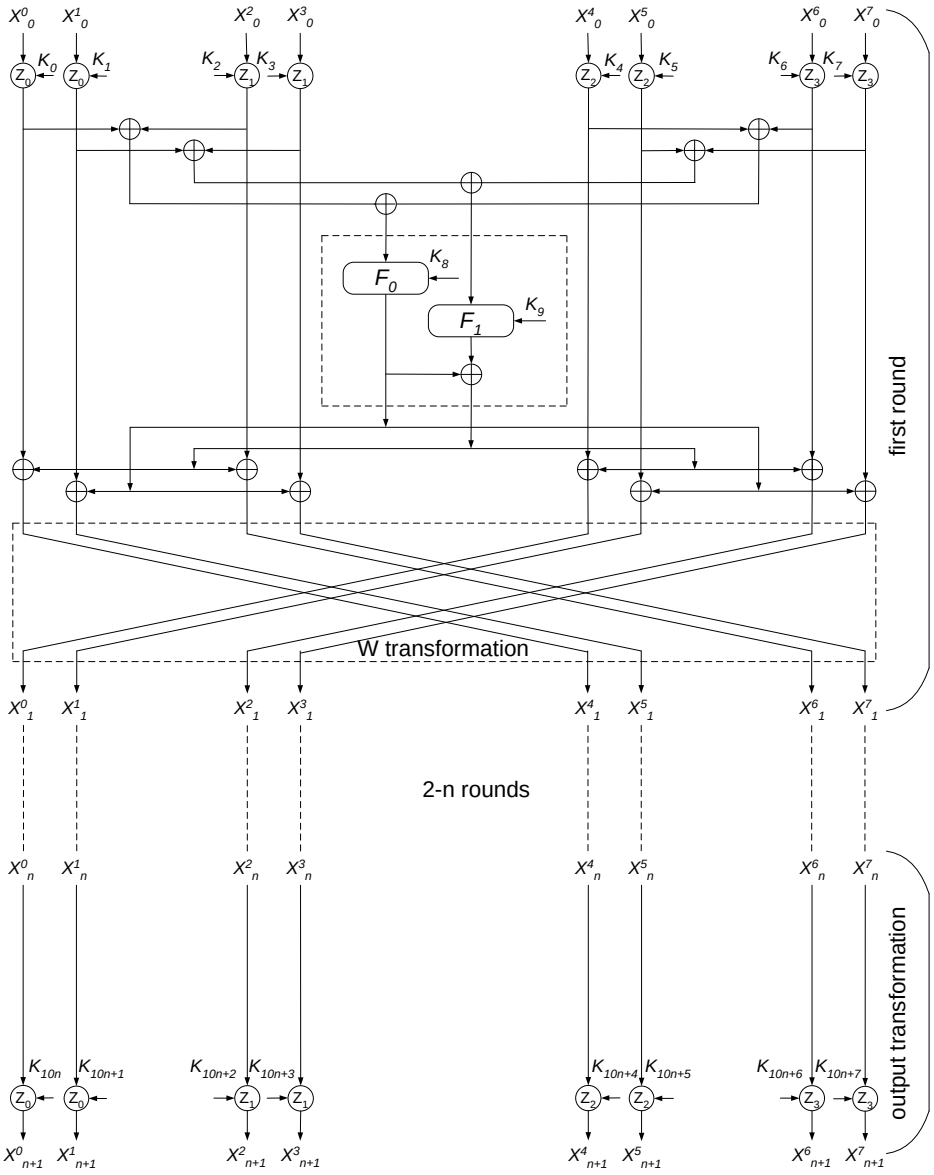

Fig 1. Functional scheme of network SREPES8–2

In W transformation in each round the subblocks X_{i-1}^0 and X_{i-1}^4, X_{i-1}^1 and X_{i-1}^5, X_{i-1}^2 and X_{i-1}^6, X_{i-1}^3 and X_{i-1}^7 will replaced between themselves. Based on the replacement of subblocks, each

variants of networks SREPES8–2 can be build. The networks represented in fig.1 accept as first variants,

- only subblocks X_{i-1}^0 and X_{i-1}^4, X_{i-1}^1 and X_{i-1}^5, X_{i-1}^2 and X_{i-1}^6, $i=\overline{1...n}$ replaced, as second variant (Fig. 2),
- only subblocks X_{i-1}^0 and X_{i-1}^4, X_{i-1}^1 and X_{i-1}^5, $i=\overline{1...n}$ replaced, as third variant (Fig. 3),
- only subblocks X_{i-1}^0 and X_{i-1}^4, $i=\overline{1...n}$ replaced, as fourth variant (Fig. 4),
- subblocks is not replaced, as fifth variant (Fig. 5),
- only subblocks X_{i-1}^1 and X_{i-1}^5, X_{i-1}^2 and X_{i-1}^6, X_{i-1}^3 and X_{i-1}^7, $i=\overline{1...n}$ replaced, as sixth variant (Fig. 6),
- only subblocks X_{i-1}^2 and X_{i-1}^6, X_{i-1}^3 and X_{i-1}^7, $i=\overline{1...n}$ replaced, as seventh variant (Fig. 7),
- only subblocks X_{i-1}^3 and X_{i-1}^7, $i=\overline{1...n}$ replaced, as eighth variant (Fig. 8).

$$\begin{cases} X_i^0 = (X_{i-1}^4(z_2)K_{10i-6}) \oplus T_i^0 \oplus T_i^1 \\ X_i^1 = (X_{i-1}^5(z_2)K_{10i-5}) \oplus T_i^0 \\ X_i^2 = (X_{i-1}^6(z_3)K_{10i-4}) \oplus T_i^0 \oplus T_i^1 \\ X_i^3 = (X_{i-1}^7(z_3)K_{10i-3}) \oplus T_i^0 \\ X_i^4 = (X_{i-1}^0(z_0)K_{10i-10}) \oplus T_i^0 \oplus T_i^1 \\ X_i^5 = (X_{i-1}^1(z_0)K_{10i-9}) \oplus T_i^0 \\ X_i^6 = (X_{i-1}^2(z_1)K_{10i-8}) \oplus T_i^0 \oplus T_i^1 \\ X_i^7 = (X_{i-1}^3(z_1)K_{10i-7}) \oplus T_i^0 \end{cases}, \quad i=\overline{1...n} \tag{1}$$

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

The encryption process in variants 2–8 are similar to (1), only

- in the second variant, X_i^3 and X_i^7 values,
- in the third variant, X_i^2 and X_i^6, X_i^3 and X_i^7 values,
- in the fourth variant, X_i^1 and X_i^5, X_i^2 and X_i^6, X_i^3 and X_i^7 values,
- in the fifth variant, X_i^0 and X_i^4, X_i^1 and X_i^5, X_i^2 and X_i^6, X_i^3 and X_i^7 values,
- in the sixth variant, X_i^0 and X_i^4 values,
- in the seventh variant, X_i^0 and X_i^4, X_i^1 and X_i^5 values,
- in the eighth variant, X_i^0 and X_i^4, X_i^1 and X_i^5, X_i^2 and X_i^6 values are replaced

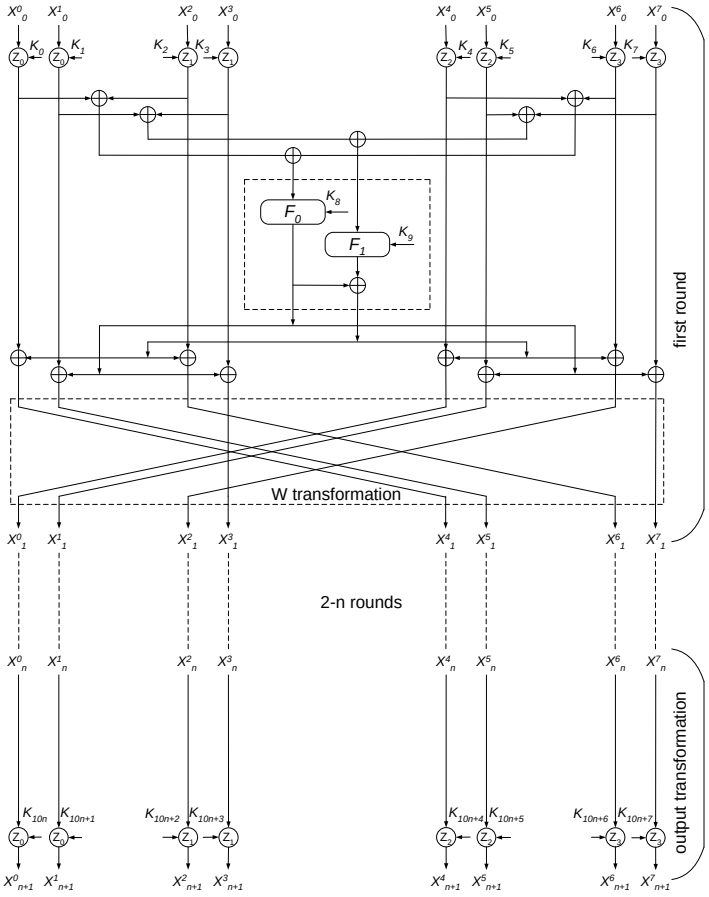

Fig.2. Second variant of network SREPES8–2

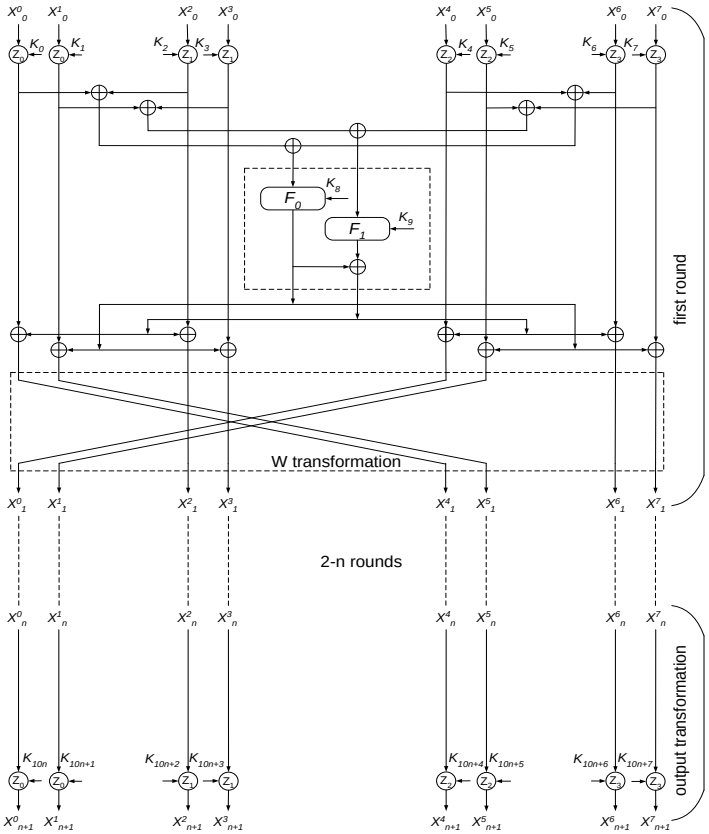

Fig.3. Third variant of network SREPES8–2

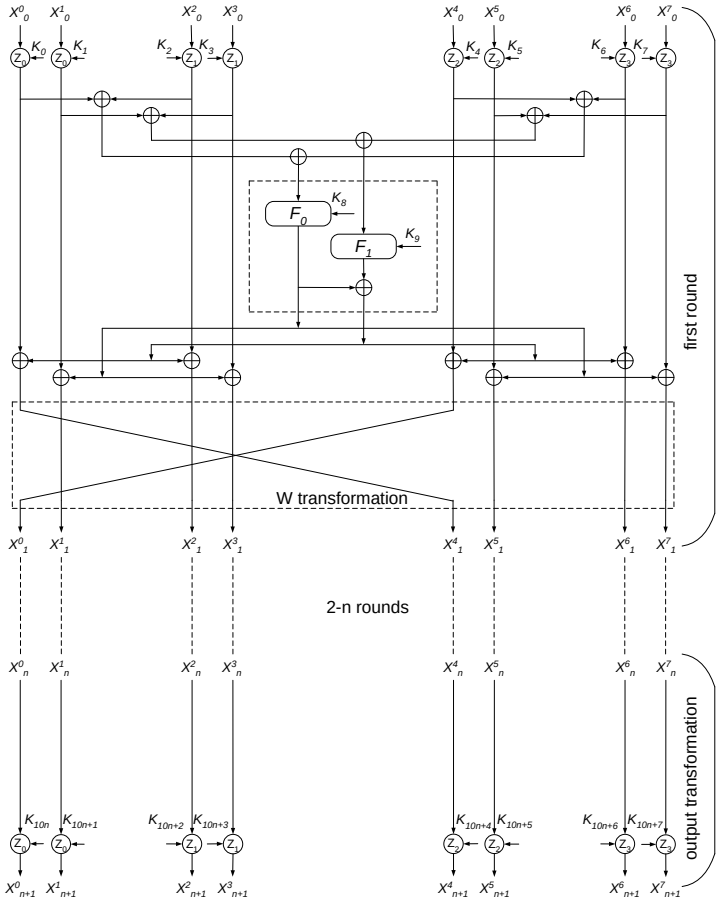

Fig.4. Fourth variant of network SREPES8–2

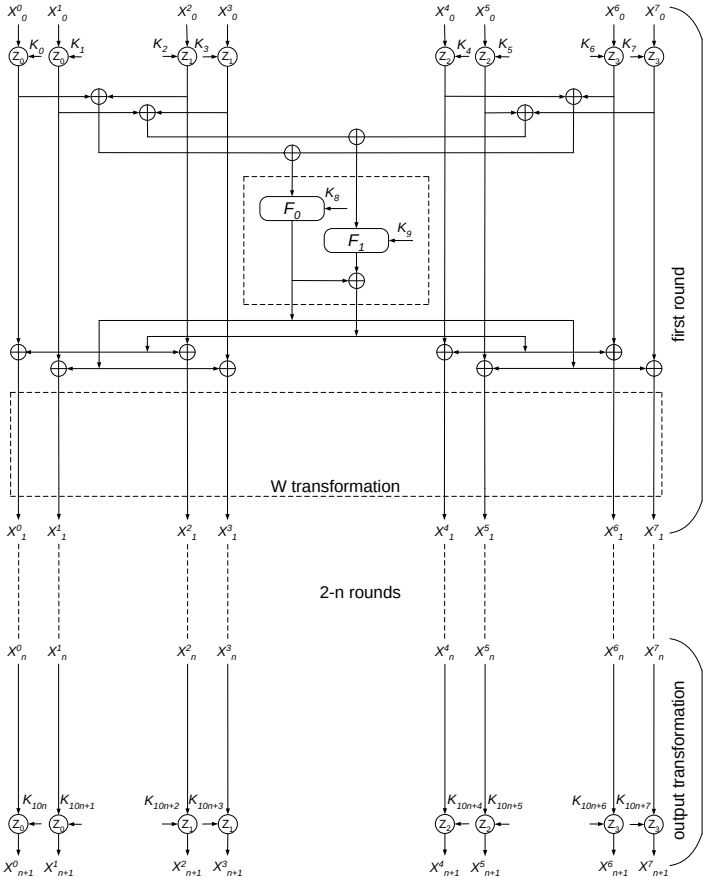

Fig.5. Fifth variant of network SREPES8–2

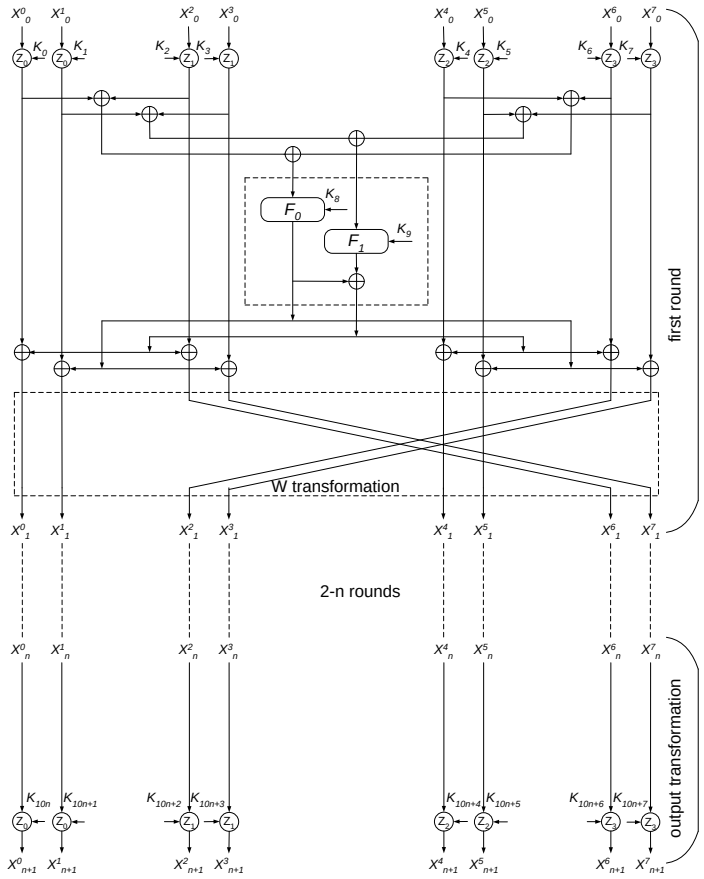

Fig.6. Sixth variant of network SREPES8–2

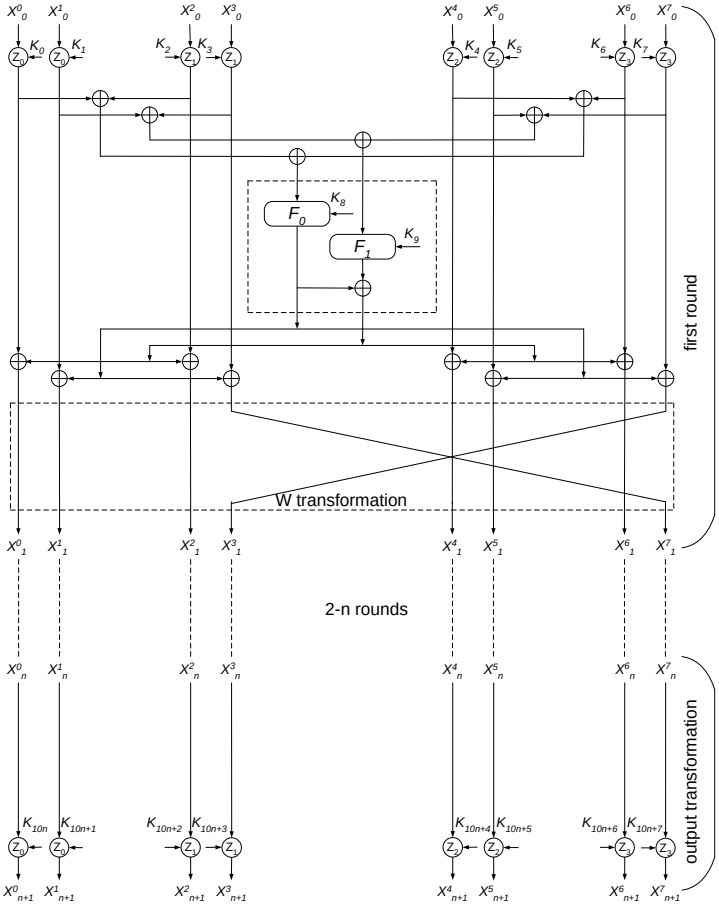

Fig.7. Seventh variant of network SREPES8–2

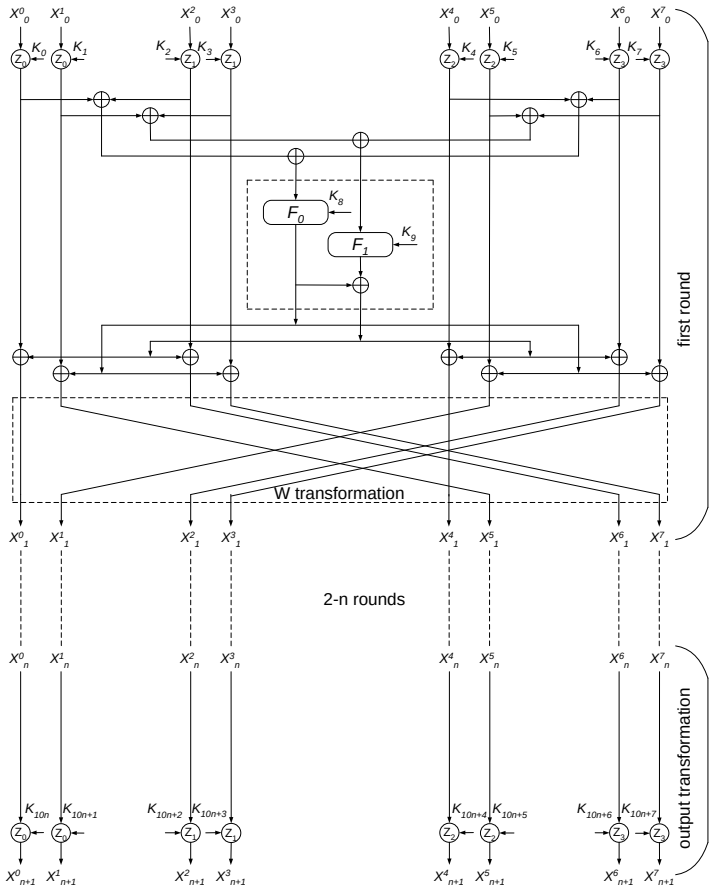

Fig.8. Eighth variant of network SREPES8–2

Keys generation. In $n-$rounded SREPES8–2 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:

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

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:

$$(K_{10n}^d, K_{10n+1}^d, K_{10n+2}^d, K_{10n+3}^d, K_{10n+4}^d, K_{10n+5}^d, K_{10n+6}^d, K_{10n+7}^d) = ((K_0^c)^{z_0}, (K_1^c)^{z_0}, (K_2^c)^{z_1}, (K_3^c)^{z_1}, (K_4^c)^{z_2}, (K_5^c)^{z_2}, (K_6^c)^{z_3}, (K_7^c)^{z_3}). \quad (3)$$

RESULTS

In article on the basis of the encryption algorithm PES and the extended Lai-Massey scheme developed network SREPES8–2. 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. Jumakulov A.K. The Network EPES8–2 // International journal of multidisciplinary research and analysis, 2022 vol. 5 issue 5, p. 975-982
3. Junod, P., Vaudenay, S.. FOX: a new family of block ciphers. In 11th Selected Areas in Cryptography (SAC) Workshop, LNCS 3357, p. 114–129. Springer–Verlag.
4. 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.
5. 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.
6. 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).
7. Tuychiev G.N.On the network PES16–8, consisting of eight round functions // Information security. –Kyiv. 2014. Volume 16. No.4. –p. 318–322.
8. Tuychiev G.N On the network PES32–16, consisting of sixteen round functions // Security of Information. –Kyiv. 2014. Volume 20. No.1. –p. 43–47.
9. Tuychiev G.N. On the network PES2m–m, consisting of m round functions and its modification // Security of Information. –Kyiv, 2015. Volume 21. No. 1. 52–63 p.