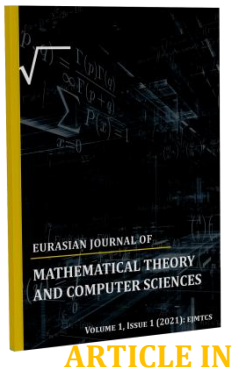
EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.916 www.in-academy.uz



THE NETWORK EPES16–4

Gulom Tuychiyev[1]
Abdumannon Jumakulov[2]
[1]National University of Uzbekistan, Tashkent, 100179, Olmazor, Uzbekistan.
[2]Kokand University, Kokand, 150700, Fergana, Uzbekistan
*Corresponding Author: jumakulov19862106@gmail.com
https://www.doi.org/10.5281/zenodo.7890861

ARTICLE INFO

Received: 26th April 2023
Accepted: 02nd May 2023
Online: 03rd May 2023

KEY WORDS

Lai-Massey scheme, algorithm, network, encryption, decryption, round keys, round functions.

ABSTRACT

The article presents the EPES16–4 network with four round functions using the same algorithm for encryption and decryption.

Introduction. The Proposed Encryption Standard (PES) is an iterated block cipher designed by Lai and Massey in 1990 [5], and this algorithm is based on the Lay–Messi scheme. PES is a 64-bit block cipher, using a 128-bit key. PES iterates 8 similar rounds plus an output transformation (that is treated as a half round). The International Data Encryption Algorithm (IDEA) is a 64-bit block cipher, using a 128-bit key, designed by Lai, Massey and Murphy in 1991 (see [6]). It is an evolution of PES. IDEA is a candidate block cipher [8] to the NESSIE Project [9]. NESSIE is a project within the Information Societies Technology (IST) Program of the European Commission. The block ciphers IDEA and PES use three group operations: addition modulo 2^{16}, represented by $\boxplus$, bitwise exclusive-or, denoted $\oplus$, and multiplication modulo $2^{16}+1$, denoted $\otimes$, with the exception that 2^{16} is interpreted as 0.

Main body. 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, created networks with round function PES4–2, PES8–4, PES32–16 and PES2m–m [1-6].

In this article based on the structure encryption algorithm PES developed network EPES16–4 (extended PES) was developed, which consists of sixteen subblocks and four round functions.

Network structure. In the proposed network EPES16–4, 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 512 bits when the length of the subblocks of the network is 32 bits, 256 bits with a block length of 16 bits, and 128 bits with a block length of 8 bits.

EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.916 www.in-academy.uz

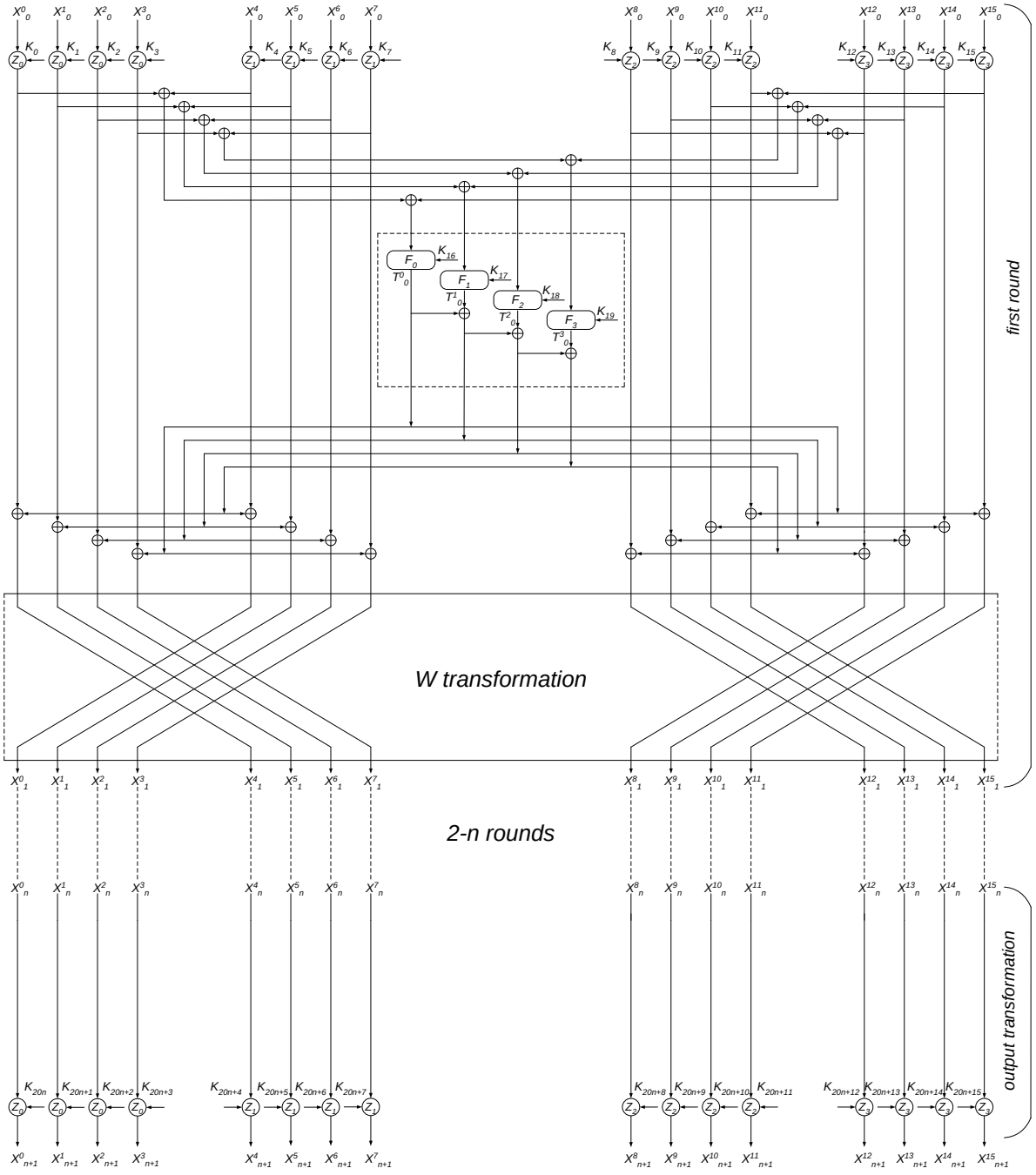
In the network EPES16–4 the length of round keys $K_{20(i-1)}$, $K_{20(i-1)+1}$,..., $K_{20(i-1)+15}$, $i=\overline{1...n+1}$ is equal 32 (16, 8) bits. The length of round keys $K_{20(i-1)+16}$, $K_{20(i-1)+17}$, ..., $K_{20(i-1)+19}$, $i=\overline{1...n}$ is not requested to be equal to 32 (16, 8) bits. 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

$$T_i^0 = F_0(((X_{i-1}^0(z_0)K_{20(i-1)}) \oplus (X_{i-1}^4(z_1)K_{20(i-1)+4})) \oplus ((X_{i-1}^8(z_2)K_{20(i-1)+8}) \oplus (X_{i-1}^{12}(z_3)K_{20(i-1)+12})), K_{20(i-1)+16})$$

$$T_i^1 = F_1(((X_{i-1}^1(z_0)K_{20(i-1)+1}) \oplus (X_{i-1}^5(z_1)K_{20(i-1)+5})) \oplus ((X_{i-1}^9(z_2)K_{20(i-1)+9}) \oplus (X_{i-1}^{13}(z_3)K_{20(i-1)+13})), K_{20(i-1)+17})$$

$$T_i^2 = F_2(((X_{i-1}^2(z_0)K_{20(i-1)+2}) \oplus (X_{i-1}^6(z_1)K_{20(i-1)+6})) \oplus ((X_{i-1}^{10}(z_2)K_{20(i-1)+10}) \oplus (X_{i-1}^{14}(z_3)K_{20(i-1)+14})), K_{20(i-1)+18})$$

$$T_i^3 = F_3(((X_{i-1}^3(z_0)K_{20(i-1)+3}) \oplus (X_{i-1}^7(z_1)K_{20(i-1)+7})) \oplus ((X_{i-1}^{11}(z_2)K_{20(i-1)+11}) \oplus (X_{i-1}^{15}(z_3)K_{20(i-1)+15})), K_{20(i-1)+19})$$



EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.916 www.in-academy.uz

Figure 1. The scheme of network EPES16–4

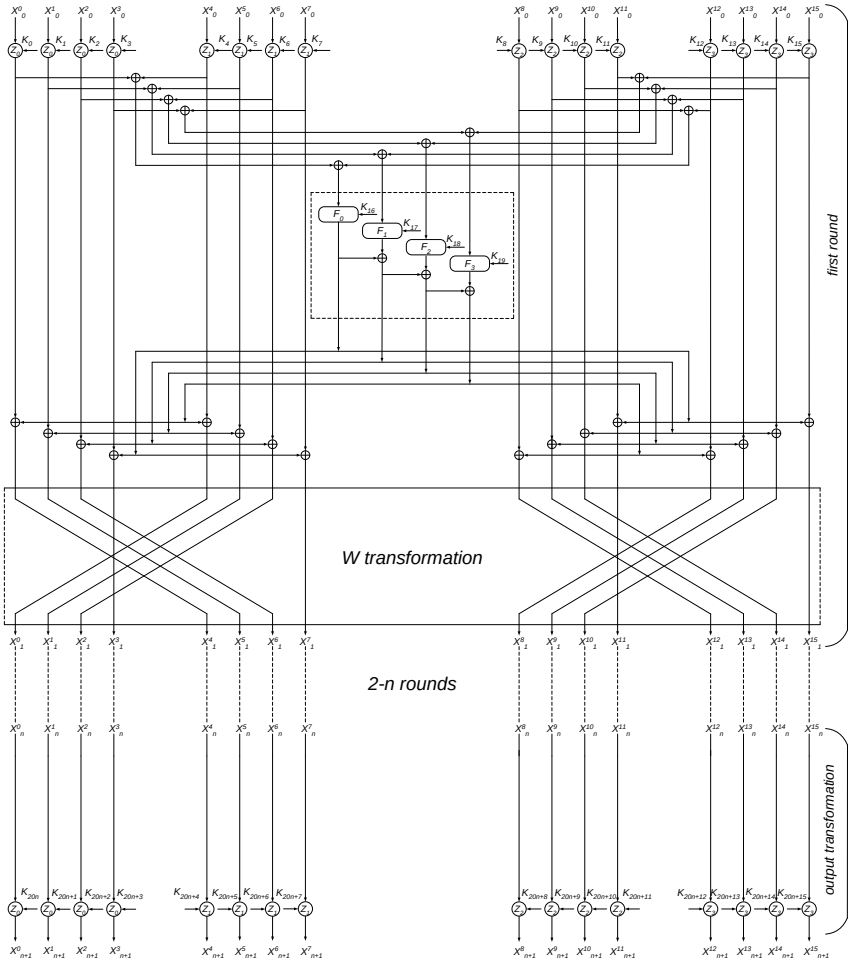
$$\begin{cases} X_i^0 = (X_{i-1}^4(z_1)K_{20(i-1)+4}) \oplus T_i^0 \oplus T_i^1 \oplus T_i^2 \oplus T_i^3 \\ X_i^1 = (X_{i-1}^5(z_1)K_{20(i-1)+5}) \oplus T_i^0 \oplus T_i^1 \oplus T_i^2 \\ X_i^2 = (X_{i-1}^6(z_1)K_{20(i-1)+6}) \oplus T_i^0 \oplus T_i^1 \\ X_i^3 = (X_{i-1}^7(z_1)K_{20(i-1)+7}) \oplus T_i^0 \\ X_i^4 = (X_{i-1}^0(z_0)K_{20(i-1)}) \oplus T_i^0 \oplus T_i^1 \oplus T_i^2 \oplus T_i^3 \\ X_i^5 = (X_{i-1}^1(z_0)K_{20(i-1)+1}) \oplus T_i^0 \oplus T_i^1 \oplus T_i^2 \\ X_i^6 = (X_{i-1}^2(z_0)K_{20(i-1)+2}) \oplus T_i^0 \oplus T_i^1 \\ X_i^7 = (X_{i-1}^3(z_0)K_{20(i-1)+3}) \oplus T_i^0 \\ X_i^8 = (X_{i-1}^{12}(z_3)K_{20(i-1)+12}) \oplus T_i^0 \oplus T_i^1 \oplus T_i^2 \oplus T_i^3 \\ X_i^9 = (X_{i-1}^{13}(z_3)K_{20(i-1)+13}) \oplus T_i^0 \oplus T_i^1 \oplus T_i^2 \\ X_i^{10} = (X_{i-1}^{14}(z_3)K_{20(i-1)+14}) \oplus T_i^0 \oplus T_i^1 \\ X_i^{11} = (X_{i-1}^{15}(z_3)K_{20(i-1)+15}) \oplus T_i^0 \\ X_i^{12} = (X_{i-1}^8(z_2)K_{20(i-1)+8}) \oplus T_i^0 \oplus T_i^1 \oplus T_i^2 \oplus T_i^3 \\ X_i^{13} = (X_{i-1}^9(z_2)K_{20(i-1)+9}) \oplus T_i^0 \oplus T_i^1 \oplus T_i^2 \\ X_i^{14} = (X_{i-1}^{10}(z_2)K_{20(i-1)+10}) \oplus T_i^0 \oplus T_i^1 \\ X_i^{15} = (X_{i-1}^{11}(z_2)K_{20(i-1)+11}) \oplus T_i^0 \end{cases}, \quad i = \overline{1...n} \qquad 1)$$

$$\begin{cases} X_{n+1}^0 = (X_n^0(z_0)K_{20n}) \\ X_{n+1}^1 = (X_n^1(z_0)K_{20n+1}) \\ X_{n+1}^2 = (X_n^2(z_0)K_{20n+2}) \\ X_{n+1}^3 = (X_n^3(z_0)K_{20n+3}) \\ X_{n+1}^4 = (X_n^4(z_1)K_{20n+4}) \\ X_{n+1}^5 = (X_n^5(z_1)K_{20n+5}) \\ X_{n+1}^6 = (X_n^6(z_1)K_{20n+6}) \\ X_{n+1}^7 = (X_n^7(z_1)K_{20n+7}) \\ X_{n+1}^8 = (X_n^8(z_2)K_{20n+8}) \\ X_{n+1}^9 = (X_n^9(z_2)K_{20n+9}) \\ X_{n+1}^{10} = (X_n^{10}(z_2)K_{20n+10}) \\ X_{n+1}^{11} = (X_n^{11}(z_2)K_{20n+11}) \\ X_{n+1}^{12} = (X_n^{12}(z_3)K_{20n+12}) \\ X_{n+1}^{13} = (X_n^{13}(z_3)K_{20n+13}) \\ X_{n+1}^{14} = (X_n^{14}(z_3)K_{20n+14}) \\ X_{n+1}^{15} = (X_n^{15}(z_3)K_{20n+15}) \end{cases}$$, in the output transformation

EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.916 www.in-academy.uz

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, X_{i-1}^8 and X_{i-1}^{12}, X_{i-1}^9 and X_{i-1}^{13}, X_{i-1}^{10} and X_{i-1}^{14}, X_{i-1}^{11} and X_{i-1}^{15} will be switched. Based on the replacement of subblocks, each variants of networks EPES16–4 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, X_{i-1}^8 and X_{i-1}^{12}, X_{i-1}^9 and X_{i-1}^{13}, X_{i-1}^{10} and X_{i-1}^{14}, $i=\overline{1...n}$ 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, X_{i-1}^8 and X_{i-1}^{12}, X_{i-1}^9 and X_{i-1}^{13} $i=\overline{1...n}$ replaced, as third variant (Fig. 3),
- only subblocks X_{i-1}^0 and X_{i-1}^4, X_{i-1}^8 and X_{i-1}^{12}, $i=\overline{1...n}$ 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, X_{i-1}^9 and X_{i-1}^{13}, X_{i-1}^{10} and X_{i-1}^{14}, X_{i-1}^{11} and X_{i-1}^{15}, $i=\overline{1...n}$ 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, X_{i-1}^{10} and X_{i-1}^{14}, X_{i-1}^{11} and X_{i-1}^{15}, $i=\overline{1...n}$ replaced, as seventh variant (Fig. 7),
- only subblocks X_{i-1}^3 and X_{i-1}^7, X_{i-1}^{11} and X_{i-1}^{15}, $i=\overline{1...n}$ replaced, as eighth variant (Fig. 8).



EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.916 www.in-academy.uz

Fig.2. Second variant of network EPES16–4

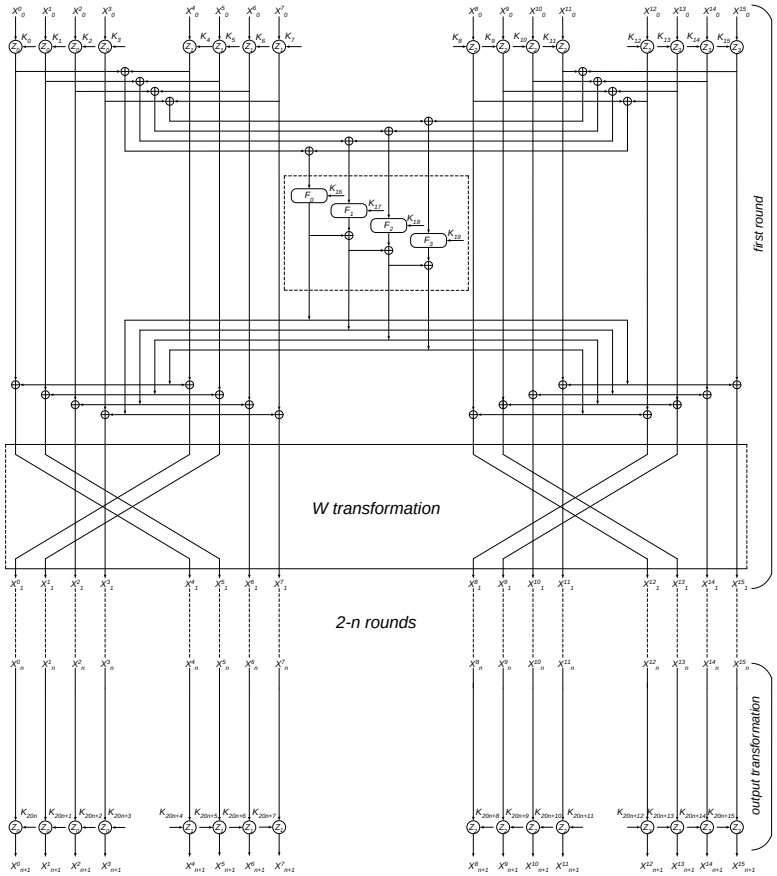
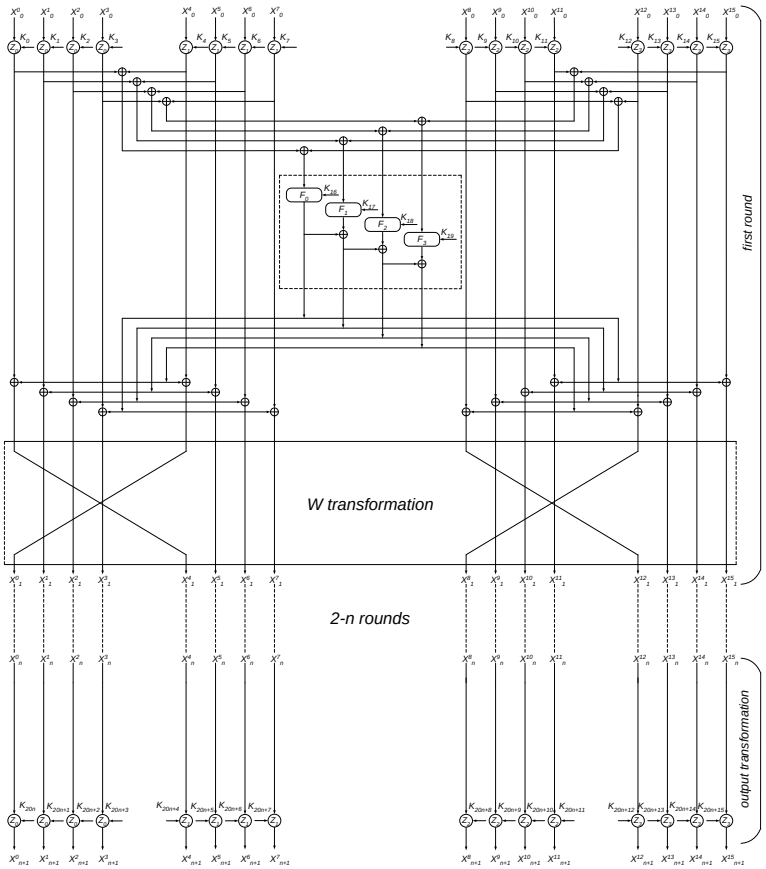


Fig.3. Third variant of network EPES16–4



EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.916 www.in-academy.uz

Fig.4. Fourth variant of network EPES16–4

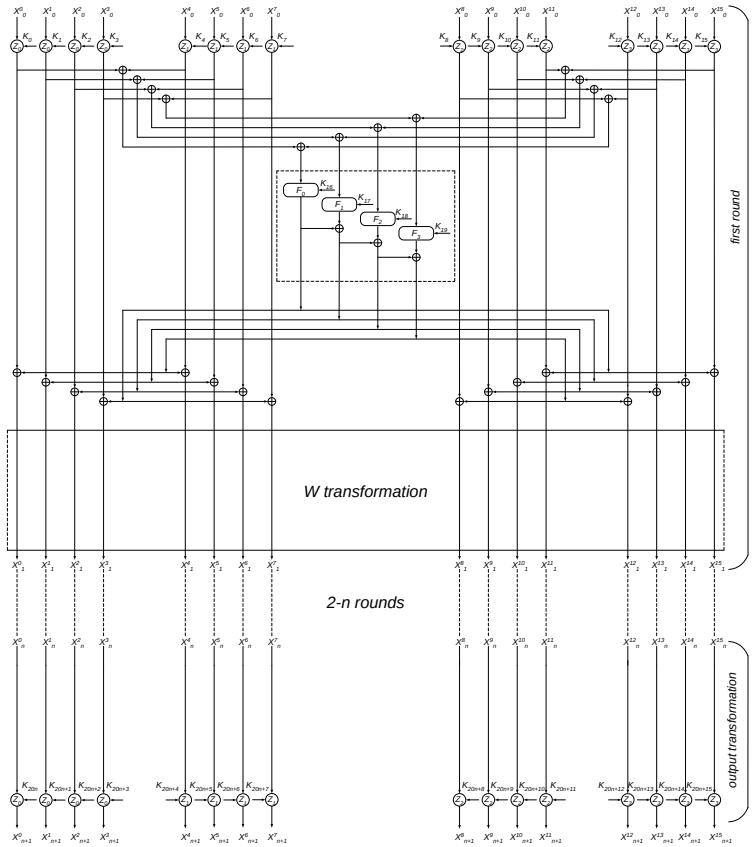
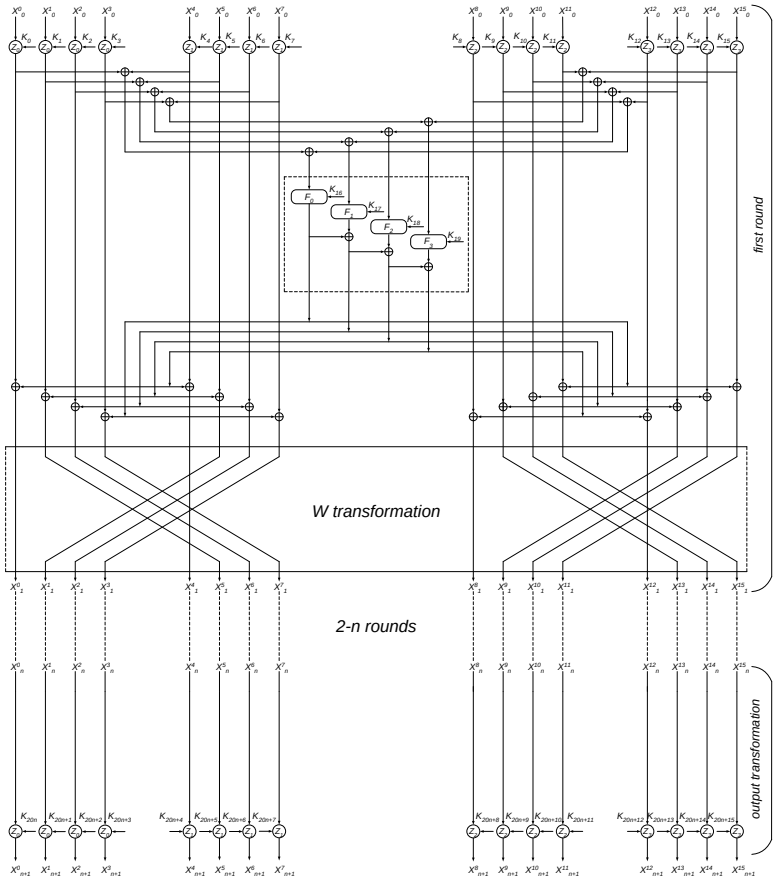


Fig.5. Fifth variant of network EPES16–4



EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.916 www.in-academy.uz

Fig.6. Sixth variant of network EPES16–4

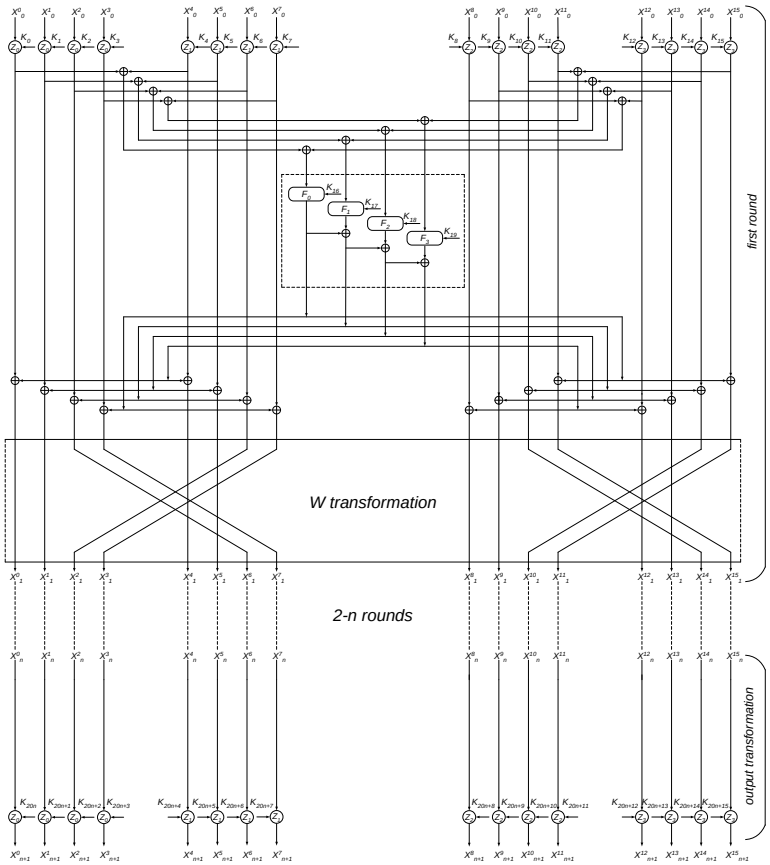
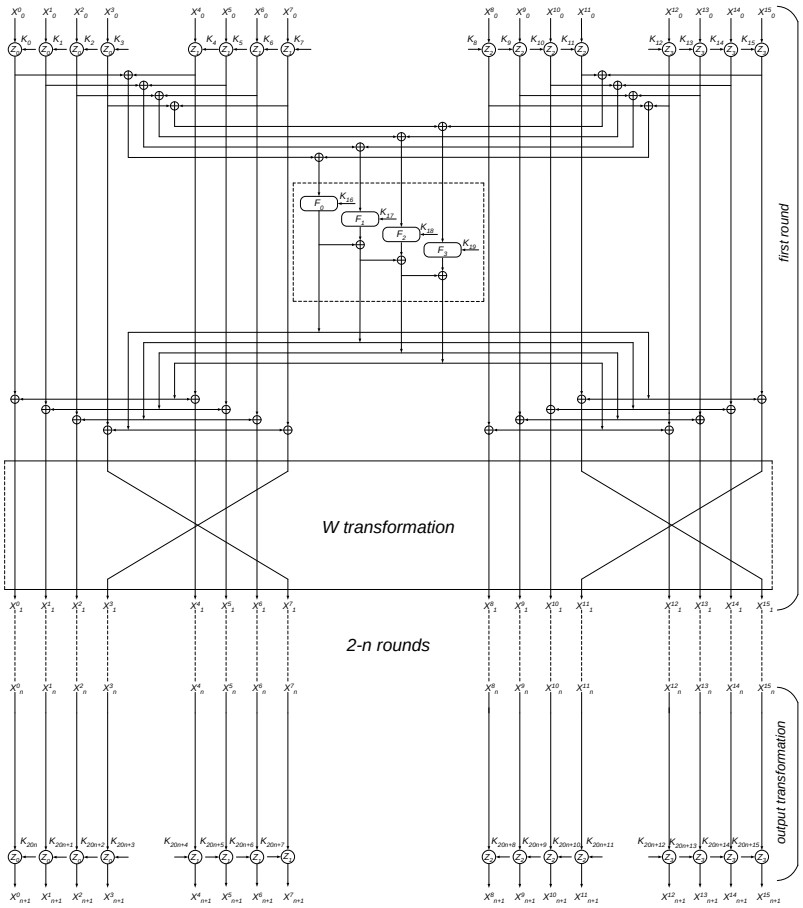


Fig.7. Seventh variant of network EPES16–4



EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.916 www.in-academy.uz

Fig.8. Eighth variant of network EPES16–4

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

- in the second variant, X_i^3 and X_i^7, X_i^{11} and X_i^{15} values,
- in the third variant, X_i^2 and X_i^6, X_i^3 and X_i^7, X_i^{10} and X_i^{14}, X_i^{11} and X_i^{15} 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, X_i^9 and X_i^{13}, X_i^{10} and X_i^{14}, X_i^{11} and X_i^{15} 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, X_i^8 and X_i^{12}, X_i^9 and X_i^{13}, X_i^{10} and X_i^{14}, X_i^{11} and X_i^{15} values,
- in the sixth variant, X_i^0 and X_i^4, X_i^8 and X_i^{12} values,
- in the seventh variant, X_i^0 and X_i^4, X_i^1 and X_i^5, X_i^8 and X_i^{12}, X_i^9 and X_i^{13} 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, X_i^8 and X_i^{12}, X_i^9 and X_i^{13}, X_i^{10} and X_i^{14} values are switched.

Keys generation. In $n-$rounded EPES16–4 network, in each round applied 20 round keys and in the output transformation applied 16 round keys, i.e. the total number of round keys is $20n+16$. 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 EPES16–4 network in all variants The first, second and n-round decryption round keys are associated to the encryption round keys as follows:

$$(K_{20(i-1)}^d, K_{20(i-1)+1}^d, K_{20(i-1)+2}^d, K_{20(i-1)+3}^d, K_{20(i-1)+4}^d, K_{20(i-1)+5}^d, K_{20(i-1)+6}^d, K_{20(i-1)+7}^d, K_{20(i-1)+8}^d, K_{20(i-1)+9}^d,$$
$$K_{20(i-1)+10}^d, K_{20(i-1)+11}^d, K_{20(i-1)+12}^d, K_{20(i-1)+13}^d, K_{20(i-1)+14}^d, K_{20(i-1)+15}^d, K_{20(i-1)+16}^d, K_{20(i-1)+17}^d, K_{20(i-1)+18}^d,$$
$$K_{20(i-1)+19}^d) = ((K_{20(n-i+1)}^c)^{z_0}, (K_{20(n-i+1)+1}^c)^{z_0}, (K_{20(n-i+1)+2}^c)^{z_0}, (K_{20(n-i+1)+3}^c)^{z_0}, (K_{20(n-i+1)+4}^c)^{z_1},$$
$$(K_{20(n-i+1)+5}^c)^{z_1}, (K_{20(n-i+1)+6}^c)^{z_1}, (K_{20(n-i+1)+7}^c)^{z_1}, (K_{20(n-i+1)+8}^c)^{z_2}, (K_{20(n-i+1)+9}^c)^{z_2}, (K_{20(n-i+1)+10}^c)^{z_2},$$
$$(K_{20(n-i+1)+11}^c)^{z_2}, (K_{20(n-i+1)+12}^c)^{z_3}, (K_{20(n-i+1)+13}^c)^{z_3}, (K_{20(n-i+1)+14}^c)^{z_3}, (K_{20(n-i+1)+15}^c)^{z_3}, K_{20(n-i)+16}^c,$$
$$K_{20(n-i)+17}^c, K_{20(n-i)+18}^c, K_{20(n-i)+19}^c), i = \overline{1...n}. \quad (2)$$

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:

$$(K^d_{20n}, K^d_{20n+1}, K^d_{20n+2}, K^d_{20n+3}, K^d_{20n+4}, K^d_{20n+5}, K^d_{20n+6}, K^d_{20n+7}, K^d_{20n+8}, K^d_{20n+9}, K^d_{20n+10}, K^d_{20n+11}, K^d_{20n+12},$$
$$K^d_{20n+13}, K^d_{20n+14}, K^d_{20n+15}) = ((K^c_0)^{z_0}, (K^c_1)^{z_0}, (K^c_2)^{z_0}, (K^c_3)^{z_0}, (K^c_4)^{z_1}, (K^c_5)^{z_1}, (K^c_6)^{z_1}, (K^c_7)^{z_1}, (K^c_8)^{z_2},$$
$$(K^c_9)^{z_2}, (K^c_{10})^{z_2}, (K^c_{11})^{z_2}, (K^c_{12})^{z_3}, (K^c_{13})^{z_3}, (K^c_{14})^{z_3}, (K^c_{15})^{z_3}). \quad (2)$$

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.