УДК 004.056.55

О СЕТИ PES16–8, СОСТОЯЩЕЙ ИЗ ВОСЬМИ РАУНДОВЫХ ФУНКЦИЙ

Гулом Туйчиев

В статье разработана сеть PES16–8, состоящая из восьми раундовых функций. Данная сеть создана с использованием структуры алгоритма блочного шифрования PES. В сети PES16–8, аналогично сети Фейстеля, при зашифровании и расшифровании используется один алгоритм и в качестве раундовых функций можно использовать любые преобразования. В сети PES16–8 длина подблоков равна 8, 16 и 32 битам и на основе этой сети можно создать алгоритм шифрования длиной блока 128, 256 и 512 битам. В сети PES16–8 алгебраические операции являются переменными, в качестве этих операции можно использовать операции сложения и умножения по модулю и XOR.

Ключевые слова: *сеть Фейстеля, схема Лай-Мэсси, алгоритм блочного шифрования, раунд, раундовая функция, раундовые ключи, выходное преобразование, блок, подблок, умножения по модулю, сложения по модулю, мультипликативная инверсия, аддитивная инверсия.*

Введение. Алгоритмы блочного шифрования как ГОСТ 28147–89, DES, Blowfish, E2 разработаны на основе сети Фейстеля. Преимуществом сети Фейстеля является, то, что при зашифровании и расшифровании исполь-зуется один алгоритм. Процесс зашифрования и расшифрования можно представить в виде формулы (1), (2).

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

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

Для сети Фейстеля выполняется равенство $L_{i-1} = R_i \oplus F(L_i, K_i) = L_{i-1} \oplus F(R_{i-1}, K_i) \oplus F(L_i, K_i) = L_{i-1}$. Это равенство означает, что при расшифровании нет необходимости вычисления обратной функции F^{-1}, т.е., в качестве раундовой функции F можно выбрать любые преобразования [2].

В 1990 году Х. Лай и Дж. Мэсси взамен алгоритма DES разработали новый алгоритм блочного шифрования PES [3]. Однако после публикации работ Э. Бихама и А. Шамира по дифференциальному криптоанализу алгоритм блочного шифрования PES был модифицирован усилением его криптостойкости и назван IPES [4]. Через год его переименовали в IDEA [5]. Эти алгоритмы основаны на схемы Лай-Мэсси и в конструкции алгоритмов лежит «смешение операций различных алгебраических групп».

В алгоритме шифрования PES первые два раундовых ключа умножаются по модулю $2^{16}+1$ на первые два подблока и следующие два раундовых ключа суммируются по модулю 2^{16} на соответствующие подблоки. В МА преобразовании ограничиваются использованием операции умножения по модулю $2^{16}+1$ и суммированием по модулю 2^{16} (т.е не используются такие операции как сдвиг, подстановка с помощью S-блоков и т.д.). В алгоритме шифрования PES при зашифровании и расшифровании, аналогично как у алгоритмов блочного шифрования основанных на сети Фейстеля, используется один и тот же алгоритм. В работе [1] на основе структуры алгоритма шифрования PES разра-ботана сеть под названием PES8–4, содержащая восемь подблоков и четыре раундовых функций. В сети PES8–4 при зашифровании и расшифровании, аналогично как у сети Фейстеля, используется один и тот же алгоритм. А в качестве раундовых функций можно использовать любые преобразования.

В данной статье на основе модификации сети PES8–4 разработана новая сеть под названием PES16–8, состоящая из шестнадцати подблоков и восьми раундовых функций. Сеть PES16–8 состоит из шестнадцати подблоков и восьми раундовых функций и в качестве раундовых функций можно использовать любые преобразования.

Целью статьи является создание сети наподобие сети Фейстеля, использующие один и тот же алгоритм при зашифровании и расшифровании.

Структура сети. В сети PES16–8 длина подблоков X^0, X^1, …, X^{15}, длина раундовых ключей $K_{24(i-1)}$, $K_{24(i-1)+1}$, …, $K_{24(i-1)+15}$, $i = \overline{1...n+1}$, а также длина входных и выходных блоков функций F_0, F_1, …, F_7 равна 32 (16, 8) бит. Длина раундовых ключей $K_{24(i-1)+16}$, $K_{24(i-1)+17}$, …, $K_{24(i-11)+23}$, $i = \overline{1...n}$, необязательно должна быть равной 32 (16, 8) битам. Схема *n*–раундовой сети PES16–8 приведена на Рис. 1, а процесс зашифрования приведен в (3).

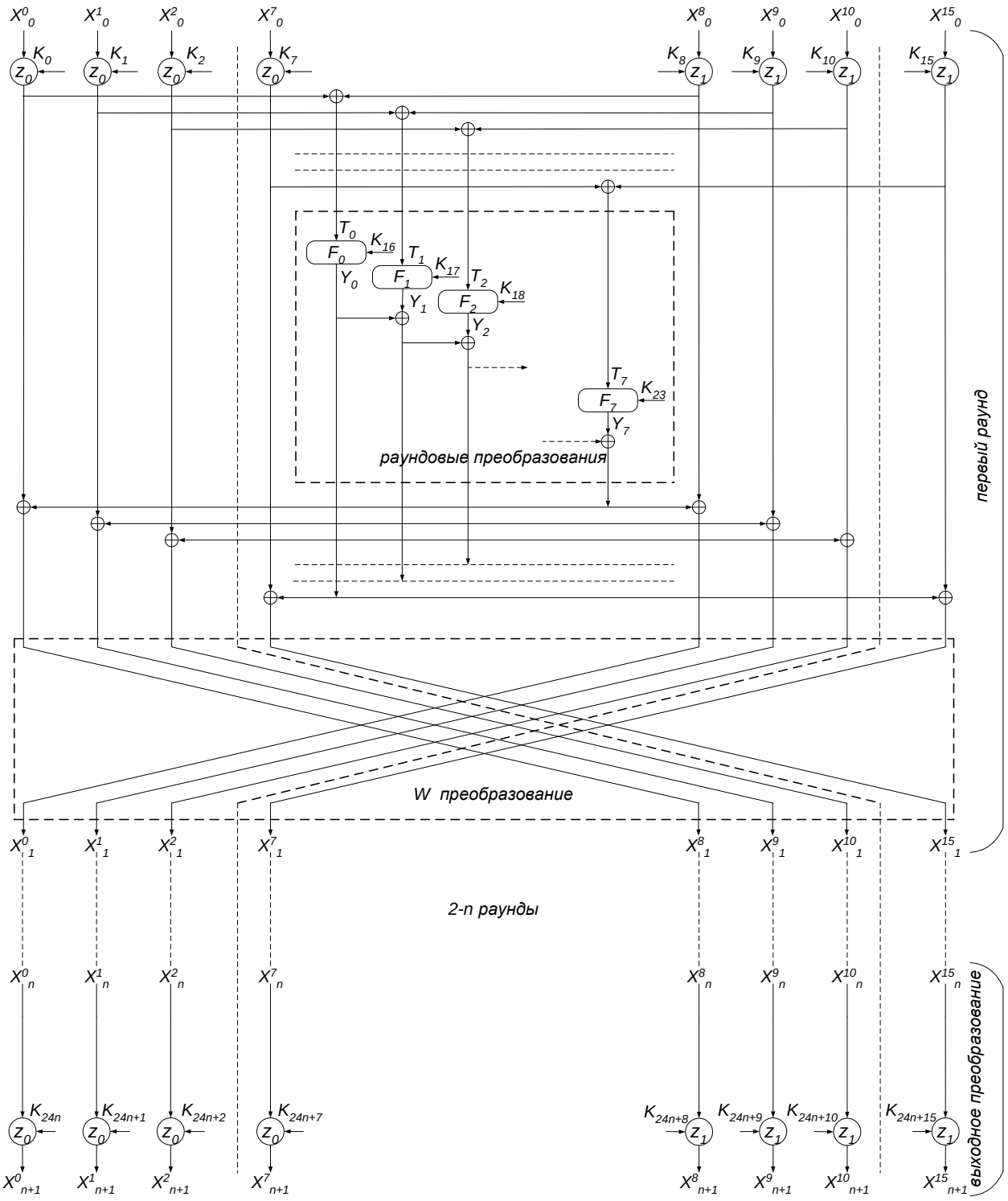

Рис. 1. Схема *n*–раундовой сети PES16–8

В качестве операции z_0, z_1 можно выбрать операции $\otimes$ (mul), $\boxplus$ (add) и $\oplus$ (xor). Здесь $\otimes$– операция умножения целых чисел по модулю $2^{32}+1$ $(2^{16}+1, 2^8+1)$, когда 32 (16, 8)-битный подблок рассматривается в качестве обычного представления целого числа по основанию два за исключением того, что подблок из всех нулей полагается равным 2^{32} $(2^{16}, 2^8)$, $\boxplus$– операция сложения целых чисел по модулю 2^{32} $(2^{16}, 2^8)$, когда 32 (16, 8)-битный рассматривается в качестве обычного представления целого числа по основанию два и $\oplus$– операция суммирования по XOR двух 32 (16, 8) битных подблоков. На основе этой сети можно построить алгоритм блочного шифрования длиной блока 512 бит при длине подблока равной 32 битам, длиной блока 256 бит при длине подблока равной 16 битам и длиной блока 128 бит при длине подблока равной 8 битам.

$$\begin{cases} X_i^0 = (X_{i-1}^8(z_1)K_{24(i-1)+8}) \oplus Y_0 \oplus Y_1 \oplus Y_2 \oplus ... \oplus Y_7 \\ X_i^1 = (X_{i-1}^9(z_1)K_{24(i-1)+9}) \oplus Y_0 \oplus Y_1 \oplus Y_2 \oplus ... \oplus Y_6 \\ X_i^2 = (X_{i-1}^{10}(z_1)K_{24(i-1)+10}) \oplus Y_0 \oplus Y_1 \oplus Y_2 \oplus ... \oplus Y_5 \\ ..... \\ X_i^7 = (X_{i-1}^{15}(z_1)K_{24(i-1)+15}) \oplus Y_0 \\ X_i^8 = (X_{i-1}^0(z_0)K_{24(i-1)}) \oplus Y_0 \oplus Y_1 \oplus Y_2 \oplus ... \oplus Y_7 \\ X_i^9 = (X_{i-1}^1(z_0)K_{24(i-1)+1}) \oplus Y_0 \oplus Y_1 \oplus Y_2 \oplus ... \oplus Y_6 \\ X_i^{10} = (X_{i-1}^2(z_0)K_{24(i-1)+2}) \oplus Y_0 \oplus Y_1 \oplus Y_2 \oplus ... \oplus Y_5 \\ ..... \\ X_i^{15} = (X_{i-1}^7(z_0)K_{24(i-1)+7}) \oplus Y_0 \end{cases}, \ i = \overline{1...n}. \quad (3)$$

$$\begin{cases} X_{n+1}^0 = (X_n^0(z_0)K_{24n}) \\ X_{n+1}^1 = (X_n^1(z_0)K_{24n+1}) \\ X_{n+1}^2 = (X_n^2(z_0)K_{24n+2}) \\ ..... \\ X_{n+1}^7 = (X_n^7(z_0)K_{24n+7}) \\ X_{n+1}^8 = (X_n^8(z_1)K_{24n+8}) \\ X_{n+1}^9 = (X_n^9(z_1)K_{24n+9}) \\ X_{n+1}^{10} = (X_n^{10}(z_1)K_{24n+10}) \\ ..... \\ X_{n+1}^{15} = (X_n^{15}(z_0)K_{24n+15}) \end{cases}, \textit{ в выходном преобразовании.}$$

$T_j = (X_{i-1}^j(z_0)K_{24(i-1)+j}) \oplus (X_{i-1}^{j+8}(z_1)K_{24(i-1)+8+j})$ и $Y_j = F_j(T_j, K_{24(i-1)+16+j})$, $j = \overline{0...7}$.

Как видно из рис. 1, в W преобразовании подблоки X^0 и X^8, X^1 и X^9, X^2 и X^{10}, X^3 и X^{11}, X^4 и X^{12}, X^5 и X^{13}, X^6 и X^{14}, X^7 и X^{15} поменяется между собой. В качестве первого варианта сети берём схему сети, приведенной на рис. 1, тогда:

– если заменить между собой только подблоки X^i и X^{i+8}, $i = \overline{0...6}$, то полученную сеть можно выбрать в качестве 2–варианта,

– если заменить между собой только подблоки X^i и X^{i+8}, $i = \overline{0...5}$, то полученную сеть можно выбрать в качестве 3–варианта,

– …..

– если заменить между собой только подблоки X^i и X^{i+8}, $i = \overline{0...1}$, то полученную сеть можно выбрать в качестве 7–варианта,

– если заменить между собой только подблоки X^0 и X^8, то полученную сеть можно выбрать в качестве 8–варианта,

– если в сети не менять места подблоков, то её можно выбрать в качестве 9–варианта,

– если заменить между собой только подблоки X^i и X^{i+8}, $i = \overline{1...7}$, то полученную сеть можно выбрать в качестве 10–варианта,

– если заменить между собой только подблоки X^i и X^{i+8}, $i = \overline{2...7}$, то полученную сеть можно выбрать в качестве 11–варианта,

– …,

– если заменить между собой только подблоки X^i и X^{i+8}, $i = \overline{6...7}$, то полученную сеть можно выбрать в качестве 15–варианта,

– если заменить между собой только подблоки X^7 и X^{15}, то полученную сеть можно выбрать в качестве 16–варианта.

Генерация ключей. В $n-$раундовой сети PES16–8 в каждом раунде применяются 24 раундовых ключей и в выходном преобразовании 16 раундовых ключей, т.е., число всех ключей равно $24n+16$. При зашифровании из ключа K генерируются $24n+16$ раундовых ключа зашифрования K_i^c. А раундовые ключи расшифрования K_i^d вычисляются на основе K_i^c. При зашифровании на рис. 1 и (3) вместо раундовых ключей K_i применяются раундовые ключи за-

шифрования K_i^c, а при расшифровании раундовые ключи дешифрования K_i^d, т.е., при зашифровании и расшифровании используется один и тот же алгоритм, меняются только раундовые ключи.

В $n-$раундовой сети PES16–8 раундовые ключи расшифрования связаны с ключами зашифрования по формуле (4).

$$
\begin{aligned}
&(K^d_{24(i-1)}, K^d_{24(i-1)+1}, K^d_{24(i-1)+2}, K^d_{24(i-1)+3},\\
&K^d_{24(i-1)+4}, K^d_{24(i-1)+5}, K^d_{24(i-1)+6}, K^d_{24(i-1)+7},\\
&K^d_{24(i-1)+8}, K^d_{24(i-1)+9}, K^d_{24(i-1)+10}, K^d_{24(i-1)+11},\\
&K^d_{24(i-1)+12}, K^d_{24(i-1)+13}, K^d_{24(i-1)+14}, K^d_{24(i-1)+15},\\
&K^d_{24(i-1)+16}, K^d_{24(i-1)+17}, K^d_{24(i-1)+18}, K^d_{24(i-1)+19},\\
&K^d_{24(i-1)+20}, K^d_{24(i-1)+21}, K^d_{24(i-1)+22}, K^d_{24(i-1)+23}) =\\
&((K^c_{24(n-i+1)})^{z_0}, (K^c_{24(n-i+1)+1})^{z_0}, (K^c_{24(n-i+1)+2})^{z_0},\\
&(K^c_{24(n-i+1)+3})^{z_0}, (K^c_{24(n-i+1)+4})^{z_0}, (K^c_{24(n-i+1)+5})^{z_0},\\
&(K^c_{24(n-i+1)+6})^{z_0}, (K^c_{24(n-i+1)+7})^{z_0}, (K^c_{24(n-i+1)+8})^{z_1},\\
&(K^c_{24(n-i+1)+9})^{z_1}, (K^c_{24(n-i+1)+10})^{z_1}, (K^c_{24(n-i+1)+11})^{z_1},\\
&(K^c_{24(n-i+1)+12})^{z_1}, (K^c_{24(n-i+1)+13})^{z_1}, (K^c_{24(n-i+1)+14})^{z_1},\\
&(K^c_{24(n-i+1)+15})^{z_1}, K^c_{24(n-i)+16}, K^c_{24(n-i)+17},\\
&K^c_{24(n-i)+18}, K^c_{24(n-i)+19}, K^c_{24(n-i)+20},\\
&K^c_{24(n-i)+21}, K^c_{24(n-i)+22}, K^c_{24(n-i)+23}),\ i=\overline{1...n}.
\end{aligned}
\tag{4}
$$

Если в качестве операции z_0, z_1 применяется операция mul, тогда $K=(K)^{-1}$, если применяется операция add, тогда $K=-K$ и если применяется операция xor, тогда $K=K$. Здесь K^{-1} – мультипликативная инверсия K по модулю $2^{32}+1$ $(2^{16}+1, 2^8+1)$, $-K$ – аддитивная инверсия K по модулю 2^{32} $(2^{16}, 2^8)$. Для 32, 16 и 8 битных чисел выполняются $K\otimes K^{-1}=1\bmod(2^{32}+1)$, $K\otimes K^{-1}=1\bmod(2^{16}+1)$, $K\otimes K^{-1}=1\bmod(2^8+1)$ и $-K\boxplus K=0$, $K\oplus K=0$.

Ключи расшифрования выходного преобразования связаны с ключами зашифрования по формуле (5).

$$
\begin{aligned}
&(K^d_{24n}, K^d_{24n+1}, K^d_{24n+2}, K^d_{24n+3}, K^d_{24n+4}, K^d_{24n+5}, K^d_{24n+6},\\
&K^d_{24n+7}, K^d_{24n+8}, K^d_{24n+9}, K^d_{24n+10}, K^d_{24n+11}, K^d_{24n+12},\\
&K^d_{24n+13}, K^d_{24n+14}, K^d_{24n+15}) = ((K^c_0)^{z_0}, (K^c_1)^{z_0}, (K^c_2)^{z_0},\\
&(K^c_3)^{z_0}, (K^c_4)^{z_0}, (K^c_5)^{z_0}, (K^c_6)^{z_0}, (K^c_7)^{z_0}, (K^c_8)^{z_1}, (K^c_9)^{z_1},\\
&(K^c_{10})^{z_1}, (K^c_{11})^{z_1}, (K^c_{12})^{z_1}, (K^c_{13})^{z_1}, (K^c_{14})^{z_1}, (K^c_{15})^{z_1}).
\end{aligned}
\tag{5}
$$

Например, если в качестве операции z_0, z_1 взята операции mul и add, то (5) формула будет выглядеть следующим образом:

$$
\begin{aligned}
&(K^d_{24n}, K^d_{24n+1}, K^d_{24n+2}, K^d_{24n+3}, K^d_{24n+4}, K^d_{24n+5},\\
&K^d_{24n+6}, K^d_{24n+7}, K^d_{24n+8}, K^d_{24n+9}, K^d_{24n+10},\\
&K^d_{24n+11}, K^d_{24n+12}, K^d_{24n+13}, K^d_{24n+14}, K^d_{24n+15}) =\\
&((K^c_0)^{-1}, (K^c_1)^{-1}, (K^c_2)^{-1}, (K^c_3)^{-1},\\
&(K^c_4)^{-1}, (K^c_5)^{-1}, (K^c_6)^{-1}, (K^c_7)^{-1}, -K^c_8,\\
&-K^c_9, -K^c_{10}, -K^c_{11}, -K^c_{12}, -K^c_{13}, -K^c_{14}, -K^c_{15}).
\end{aligned}
$$

Полученные результаты. На основе структуры алгоритма шифрования PES разработана новая сеть под названием PES16–8, состоящая из восьми раундовых функции и шестнадцати подблоков. Аналогично как у сети Фейстеля, в сети PES16–8 при зашифровании и расшифровании используется один и тот же алгоритм и в качестве раундовых функции можно выбрать любые преобразования, потому что при расшифровании нет необходимости вычисления обратных раундовых функций: F_0^{-1}, F_1^{-2}, ..., F_7^{-1}. В качестве операций z_0, z_1 можно выбрать операции mul, add и xor.

Заключение. Если выбрать в качестве операций z_0, z_1 операции mul, add и xor, всевозможные варианты данного выбора равны $3^2=9$. Кроме этого, в сети PES16–8 имеются шестнадцать вариантов. Если раундовые функции F_0, F_1, ..., F_7 постоянные, т.е. конкретные функции, на основе выбора операции и вариантов, можно построить 144 алгоритма блочного шифрования, основанных на сети PES16–8. Если учитывать то, что в алгоритмах блочного шифрования, основанных на сети PES16–8, в зашифровании и расшифровании используется один и тот же алгоритм, тогда это дает нам удобства при создании аппаратного или программно–аппаратного средства. Потому что, при зашифровании и расшифровании используется одно и то же аппаратное или программно–аппаратное средство. Кроме этого, в качестве раундовых функции F_0, F_1, …, F_7 используя раундовые функции существующих алгоритмов шифрования, например алгоритмы шифрования основанных на сети Фейстеля, можно перевести этих алгоритмы шифрования на основе сети PES16–8.

ЛИТЕРАТУРА

[1]. Арипов М.М., Туйчиев Г.Н. Сеть PES8–4, состоящая из четырех раундовых функций // Материалы международной научной конференции «Актуальные проблемы прикладной математики и информационных технологий – Аль–Хорезми 2002», – Ташкент, 2012, 16–19 с.

[2]. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты. М.: ТРИУМФ, 2003. –816 с.

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

[4]. Lai X., Massey J. Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology, EUROCRYP'91, LNCS 547, Springer- Verlag, 1991, pp 17–38,.

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

REFERENCES

[1]. Aripov M.M., Tuychiev G.N. The network PES8-4, consisting of four round function // Materials of the international scientific conference «Modern problems of applied mathematics and information technologies-Al-khorezmiy 2012», –Tashkent, 19-22 december, 2012, pp. 16–19.

[2]. Shneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc. New York, NY, p. 784

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

[4]. Lai X., Massey J. Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology, EUROCRYP'91, LNCS 547, Springer- Verlag, 1991, pp 17–38,.

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

ПРО МЕРЕЖУ PES16–8, ЯКА СКЛАДАЄТЬСЯ З ВОСЬМИ РАУНДОВИХ ФУНКЦІЙ

У статті розроблена мережа PES 16-8, що складається з восьми раундових функцій. Дана мережа створена з використанням структури алгоритму блочного шифрування PES. У мережі PES16-8, аналогічно мережі Фейстеля, при заши-фрованіі і расшифровании використовується один алгоритм і в якості раундових функцій можна використовувати будь-які перетворення. У мережі PES16-8 довжина подблоков дорівнює 8, 16 і 32 бітам і на основі цієї мережі можна створити алгоритм шифрування довжиною блоку 128, 256 і 512 бітам. У мережі PES16-8 алгебраїчні операції є змінними, в якості цих операції можна використовувати операції додавання і множення по модулю і XOR.

Ключові слова: мережа Фейстеля, схема Лай-Мессі, алгоритм блочного шифрування, раунд, раундова функція, раундові ключі, вихідns перетворення, блок, підблок, множення по модулю, додавання за модулем, мультиплікативна інверсія, аддитивная інверсія.

ABOUT THE NETWORK PES 16-8, CONSISTING OF EIGHT ROUND FUNCTION

In the paper develop network PES16-8, consisting of eight round functions. This network is created using the structure of block cipher algorithm PES. In the network PES16-8, similar Feistel network with encryption and decryption uses one algorithm and as the round functions can use any transformation. In the network PES16-8 length of subblock is 8, 16 and 32 bits and basis on the network can create the encryption algorithm a length of subblock 128, 256 and 512 bits. In a network PES16-8 algebraic operations are variable, as these operations can use the operations of addition and multiplication modulo and XOR.

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

Туйчиев Гулом Нумонович, кандидат технических наук, преподаватель Национального университета Узбекистана.

E-mail: blasterjon@gmail.com

Туйчієв Гулом Нумович, кандидат технічних наук, викладач Національного університета Узбекистана.

Tuychiev Gulom, PhD, Assossiate Professor, National university of Uzbekistan.