© Tuychiev G. About networks PES32-8, PES32-4, PES32-2 and PES32-1, created on the basis of network PES32-16 // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 164-168.

О СЕТЯХ PES32–8, PES32–4, PES32–2 И PES32–1, СОЗДАННЫХ НА ОСНОВЕ СЕТИ PES32–16

Гулом Туйчиев

Национальный университет Узбекистана им. Мирзо Улугбека, Республика Узбекистан

ТУЙЧИЕВ Гулом Нумонович, к.т.н.

Год и место рождения: 1981 год, г. Самарканд, Республика Узбекистан.
Образование: Националный университет Узбекистана им. Мирзо Улугбека, 2002.
Должность: преподаватель кафедры информатики и прикладного программирования.
Научные интересы: информационная безопасность.
Публикации: более 15 научных публикаций.
E-mail: blasterjon@gmail.com

Аннотация. *В статье на основе сети PES32–16 разработаны сети PES32–8, PES32–4, PES32–2 и PES32–1 состоящие из восьми, четырех, двух и одной раундовых функций. Раундовая функция сети PES32–8 имеет по два входных и выходных блока, раундовая функция сети PES32–4 имеет по четыре входных и выходных блока, раундовая функция сети PES32–2 имеет по восемь входных и выходных блоков и раундовая функция сети PES32–1 имеет по шестнадцать входных и выходных блоков. Основное преимущество предложенных сетей в том, что при зашифровании и расшифровании используется один и тот же алгоритм, а также в качестве раундовых функций можно использовать любые преобразования.*

Ключевые слова: *сеть Фейстеля, схема Лай-Мэсси, раундовая функция, зашифрование, расшифрование, мультипликативная инверсия, аддитивная инверсия*

Введение

Известно, что преимуществом сети Фейстеля является то, что при зашифрования и расшифровании используется один алгоритм и в качестве раундовой функции можно использовать любые преобразования. В алгоритмах шифрования PES [8], IDEA [9] при зашифрования и расшифровании используется один и тот же алгоритм, но раундовая функция не используется, вместо него применены МА преобразования. В работах [1-7] авторами на основе структуры алгоритма шифрования PES, IDEA разработаны сети под названием PES4-2, IDEA4–2, IDEA8–4, IDEA16–8, IDEA32–16, PES32-16, состоящие из двух, четырех, восьми и шестнадцати раундовых функций. В разработанных сетях при зашифрования и расшифровании используется один алгоритм и в качестве раундовой функции можно использовать любые преобразования.

В статье [3] была приведена сеть PES32-16, состоящая из тридцати двух подблоков и шестнадцати раундовых функций. Аналогично сети Фейстеля, в сети PES32–16 при зашифровании и расшифровании используется один и тот же алгоритм и в качестве раундовых функции можно выбрать любые преобразования.

В сети PES32–16 раундовые функции имеют по одному входному и выходному блоку. Кроме этого, в блочных шифрах применяются раундовые функции, имеющие по два входных и выходных блоков, по четыре входных и выходных блоков, и т.п.

В этой статье на основе сети PES32–16 разработаны:

– сеть PES32–8, состоящая из восьми раундовых функции,

– сеть PES32–4, состоящая из четырех раундовых функции,

– сеть PES32–2, состоящая из двух раундовых функции,

– сеть PES32–1, состоящая из одной раундовой функции.

Структура сети PES32-8

В сети PES32-8 длина подблоков X^0, X^1,..., X^{31}, длина раундовых ключей $K_{40(i-1)}$, $K_{40(i-1)+1}$,..., $K_{40(i-1)+31}$, $i=\overline{1...n+1}$, равна 32 (16, 8) бит. Длина раундовых ключей $K_{40(i-1)+32}$, $K_{40(i-1)+33}$,..., $K_{40(i-1)+39}$, $i=\overline{1...n}$, необязательно должна быть равной 32 (16, 8) битам. Раундовые функции F_0, F_1, …, F_7 имеют по два входных и выходных блоков, длина которых равны 32 (16, 8) битам. Схема n–раундовой сети PES32-8 приведена на Рис.1, а процесс зашифрования приведен в (1) формуле.

Если в качестве входного блока положим $T0=[T^0,T^1]$, $T1=[T^2,T^3]$, ..., $T7=[T^{14},T^{15}]$, и в качестве выходного блока раундовой функции берём $Y0=[Y^0,Y^1]$, $Y1=[Y^2,Y^3]$, $Y2=[Y^4,Y^5]$, …, $Y7=[Y^{14},Y^{15}]$, то раундовую функцию можно представить в виде $Y0=F_0(T0,K_{40(i-1)+32})$,

$Y1 = F_1(T1, K_{40(i-1)+33})$, …, $Y7 = F_7(T7_i, K_{40(i-1)+39})$. Здесь $T^j = (X_{i-1}^j(z_0)K_{40(i-1)+j}) \oplus (X_{i-1}^{16+j}(z_1)K_{40(i-1)+16+j})$, $i = \overline{0...15}$. Для корректности процесса зашифрования раундовую функцию $Y0 = F_0(T0, K_{40(i-1)+32})$ представим в виде $Y^0 = F_0^0(T^0, T^1, K_{40(i-1)+32})$, $Y^1 = F_0^1(T^0, T^1, K_{40(i-1)+32})$, а раундовую функцию $Y1 = F_1(T1, K_{40(i-1)+33})$ представим в виде $Y^2 = F_1^0(T^2, T^3, K_{40(i-1)+33})$, $Y^3 = F_1^1(T^2, T^3, K_{40(i-1)+33})$ и так далее, раундовую функцию $Y7 = F_7(T7_i, K_{40(i-1)+39})$ представим в виде $Y^{14} = F_7^0(T^{14}, T^{15}, K_{40(i-1)+39})$, $Y^{15} = F_7^1(T^{14}, T^{15}, K_{40(i-1)+39})$.

$$
\begin{cases}
X_i^0 = (X_{i-1}^{16}(z_0)K_{40(i-1)}) \oplus Y^{15} \\
X_i^1 = (X_{i-1}^{17}(z_0)K_{40(i-1)+30}) \oplus Y^{14} \\
X_i^2 = (X_{i-1}^{18}(z_0)K_{40(i-1)+29}) \oplus Y^{13} \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_i^{15} = (X_{i-1}^{31}(z_0)K_{40(i-1)+16}) \oplus Y^0 \ , \ i = \overline{1...n} \\
X_i^{16} = (X_{i-1}^{0}(z_1)K_{40(i-1)+15}) \oplus Y^{15} \\
X_i^{17} = (X_{i-1}^{1}(z_1)K_{40(i-1)+14}) \oplus Y^{14} \\
X_i^{18} = (X_{i-1}^{2}(z_1)K_{40(i-1)+13}) \oplus Y^{13} \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_i^{31} = (X_{i-1}^{15}(z_1)K_{40(i-1)+31}) \oplus Y^0
\end{cases}
\qquad (1)
$$

$$
\begin{cases}
X_{n+1}^0 = (X_n^0(z_0)K_{40n}) \\
X_{n+1}^1 = (X_n^1(z_0)K_{40n+1}) \\
X_{n+1}^2 = (X_n^2(z_0)K_{40n+2}) \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_{n+1}^{15} = (X_n^{15}(z_0)K_{40n+15}) \quad , \\
X_{n+1}^{16} = (X_n^{16}(z_1)K_{40n+16}) \quad \textit{в выходном} \\
X_{n+1}^{17} = (X_n^{17}(z_1)K_{40n+17}) \quad \textit{преобразовании} \\
X_{n+1}^{18} = (X_n^{18}(z_1)K_{40n+18}) \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_{n+1}^{31} = (X_n^{31}(z_1)K_{40n+31})
\end{cases}
$$

Как у сети PES32-8, в сети PES32-8 в качестве операции z_0, z_1 можно выбрать операции ⊗ (mul), ⊞ (add) и ⊕ (xor). Здесь ⊗–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} ($2^{16}, 2^8$), ⊞–операция сложение 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 ⊕– операция суммирования по XOR 32 (16, 8) битных подблоков.

Как у сети PES32-16, в сети PES32-8 на основе замены подблоков в W преобразовании, можно построит 32 вариантов сети PES32-8.

Генерация ключей сети PES32-8.

В n – раундовой сети PES32–8 в каждом раунде применяются 40 раундовых ключа и в последнем преобразовании 32 раундовых ключей, т.е., число всех ключей равно $40n+32$. При зашифровании из ключа K генерируются $40n+32$ раундовые ключи зашифрования K_i^c. А раундовые ключи расшифрования K_i^d вычисляются на основе K_i^c. При зашифровании в рис. 1 и (1) вместо раундовых ключей K_i применяются раундовые ключи K_i^c, а при расшифровании раундовые ключи K_i^d, т.е., при зашифровании и расшифровании используется один и тот же алгоритм, меняются только раундовые ключи.

В сети PES16–8 раундовые ключи расшифрования выходного преобразования связаны с ключами зашифрования по формуле (3).

$$
\begin{aligned}
&(K_{40n}^d, K_{40n+1}^d, K_{40n+2}^d, K_{40n+3}^d, K_{40n+4}^d, K_{40n+5}^d, K_{40n+6}^d, K_{40n+7}^d, K_{40n+8}^d, K_{40n+9}^d, K_{40n+10}^d, K_{40n+11}^d, \\
&K_{40n+12}^d, K_{40n+13}^d, K_{40n+14}^d, K_{40n+15}^d, K_{40n+16}^d, K_{40n+17}^d, K_{40n+18}^d, K_{40n+19}^d, K_{40n+20}^d, K_{40n+21}^d, K_{40n+22}^d, \\
&K_{40n+23}^d, K_{40n+24}^d, K_{40n+25}^d, K_{40n+26}^d, K_{40n+27}^d, K_{40n+28}^d, K_{40n+29}^d, K_{40n+30}^d, K_{40n+31}^d) = ((K_0^c)^{z_0}, \\
&(K_1^c)^{z_0}, (K_2^c)^{z_0}, (K_3^c)^{z_0}, (K_4^c)^{z_0}, (K_5^c)^{z_0}, (K_6^c)^{z_0}, (K_7^c)^{z_0}, (K_8^c)^{z_0}, (K_9^c)^{z_0}, (K_{10}^c)^{z_0}, (K_{11}^c)^{z_0}, \\
&(K_{12}^c)^{z_0}, (K_{13}^c)^{z_0}, (K_{14}^c)^{z_0}, (K_{15}^c)^{z_0}, (K_{16}^c)^{z_1}, (K_{17}^c)^{z_1}, (K_{18}^c)^{z_1}, (K_{19}^c)^{z_1}, (K_{20}^c)^{z_1}, (K_{21}^c)^{z_1}, \\
&(K_{22}^c)^{z_1}, (K_{23}^c)^{z_1}, (K_{24}^c)^{z_1}, (K_{25}^c)^{z_1}, (K_{26}^c)^{z_1}, (K_{27}^c)^{z_1}, (K_{28}^c)^{z_1}, (K_{29}^c)^{z_1}, (K_{30}^c)^{z_1}, (K_{31}^c)^{z_1}).
\end{aligned}
\qquad (3)
$$

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 $-K \boxplus K = 0$, $K \oplus K = 0$.

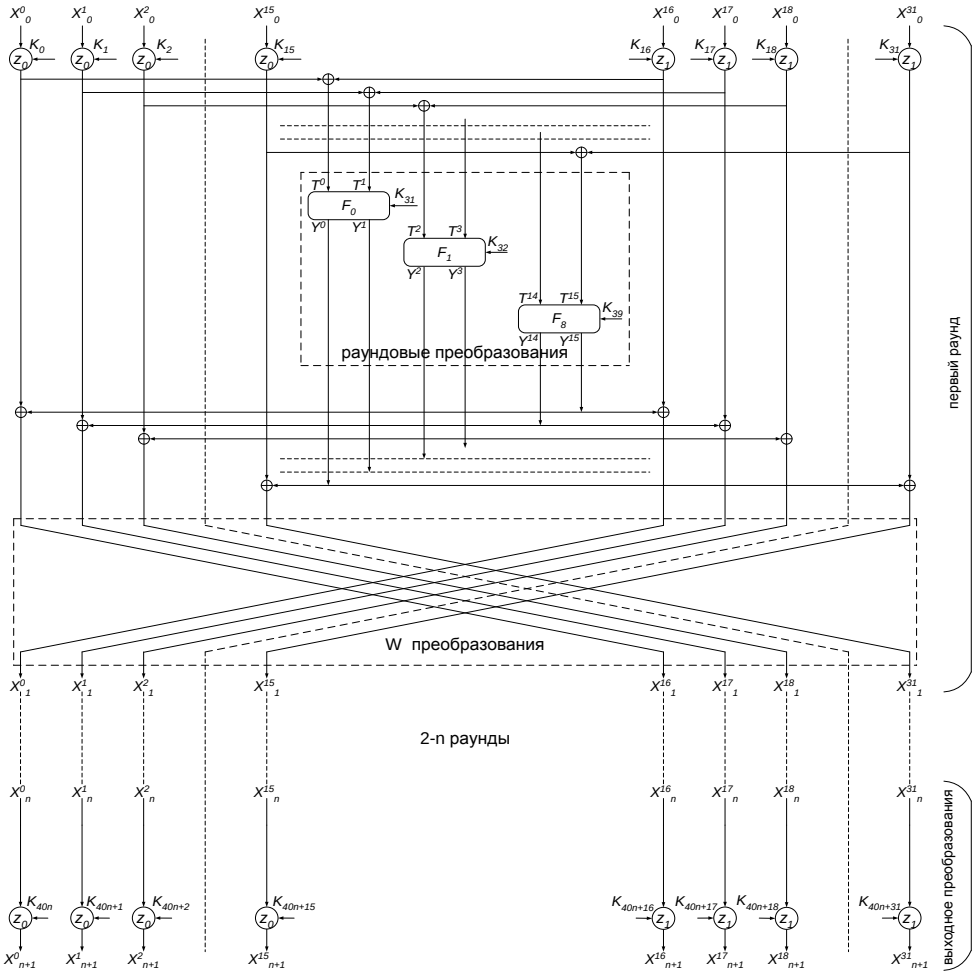

Рис. 1. Схема *n*–раундовой сети PES32–8

Как видно из формулы (3) при расшифровании ключи зашифрования применяются в обратном порядке, только требуется вычисление инверсии в соответствии операции z_0, z_1. При зашифровании в первом раунде ключи зашифрования K_0^c, K_1^c, ..., K_{31}^c на подблоки применяются по операции z_0, z_1, то расшифровании в выходном преобразовании требуется вычисление инверсии по операции z_0, z_1, т.е. $K_{40n}^d = (K_0^c)^{z_0}$, $K_{40n+1}^d = (K_1^c)^{z_0}$, ..., $K_{40n+31}^d = (K_1^c)^{z_1}$.

Таким же образом, ключи расшифрования первого, второго, и $n-$раунда связаны с ключами зашифрования по формуле (4).

$$
\begin{aligned}
&(K_{40(i-1)}^d, K_{40(i-1)+1}^d, K_{40(i-1)+2}^d, K_{40(i-1)+3}^d, K_{40(i-1)+4}^d, K_{40(i-1)+5}^d, K_{40(i-1)+6}^d, K_{40(i-1)+7}^d, K_{40(i-1)+8}^d,\\
&K_{40(i-1)+9}^d, K_{40(i-1)+10}^d, K_{40(i-1)+11}^d, K_{40(i-1)+12}^d, K_{40(i-1)+13}^d, K_{40(i-1)+14}^d, K_{40(i-1)+15}^d, K_{40(i-1)+16}^d,\\
&K_{40(i-1)+17}^d, K_{40(i-1)+18}^d, K_{40(i-1)+19}^d, K_{40(i-1)+20}^d, K_{40(i-1)+21}^d, K_{40(i-1)+22}^d, K_{40(i-1)+23}^d, K_{40(i-1)+24}^d,\\
&K_{40(i-1)+25}^d, K_{40(i-1)+26}^d, K_{40(i-1)+27}^d, K_{40(i-1)+28}^d, K_{40(i-1)+29}^d, K_{40(i-1)+30}^d, K_{40(i-1)+31}^d, K_{40(i-1)+32}^d,\\
&K_{40(i-1)+33}^d, K_{40(i-1)+34}^d, K_{40(i-1)+35}^d, K_{40(i-1)+36}^d, K_{40(i-1)+37}^d, K_{40(i-1)+38}^d, K_{40(i-1)+39}^d) = ((K_{40(n-i+1)}^c)^{z_0},\\
&(K_{40(n-i+1)+1}^c)^{z_0}, (K_{40(n-i+1)+2}^c)^{z_0}, (K_{40(n-i+1)+3}^c)^{z_0}, (K_{40(n-i+1)+4}^c)^{z_0}, (K_{40(n-i+1)+5}^c)^{z_0},\\
&(K_{40(n-i+1)+6}^c)^{z_0}, (K_{40(n-i+1)+7}^c)^{z_0}, (K_{40(n-i+1)+8}^c)^{z_0}, (K_{40(n-i+1)+9}^c)^{z_0}, (K_{40(n-i+1)+10}^c)^{z_0},\\
&(K_{40(n-i+1)+11}^c)^{z_0}, (K_{40(n-i+1)+12}^c)^{z_0}, (K_{40(n-i+1)+13}^c)^{z_0}, (K_{40(n-i+1)+14}^c)^{z_0}, (K_{40(n-i+1)+15}^c)^{z_0},\\
&(K_{40(n-i+1)+16}^c)^{z_1}, (K_{40(n-i+1)+17}^c)^{z_1}, (K_{40(n-i+1)+18}^c)^{z_1}, (K_{40(n-i+1)+19}^c)^{z_1}, (K_{40(n-i+1)+20}^c)^{z_1},\\
&(K_{40(n-i+1)+21}^c)^{z_1}, (K_{40(n-i+1)+22}^c)^{z_1}, (K_{40(n-i+1)+23}^c)^{z_1}, (K_{40(n-i+1)+24}^c)^{z_1}, (K_{40(n-i+1)+25}^c)^{z_1},\\
&(K_{40(n-i+1)+26}^c)^{z_1}, (K_{40(n-i+1)+27}^c)^{z_1}, (K_{40(n-i+1)+28}^c)^{z_1}, (K_{40(n-i+1)+29}^c)^{z_1}, (K_{40(n-i+1)+30}^c)^{z_1},\\
&(K_{40(n-i+1)+31}^c)^{z_1}, K_{40(n-i)+32}^c, K_{40(n-i)+33}^c, K_{40(n-i)+34}^c, K_{40(n-i)+35}^c, K_{40(n-i)+36}^c, K_{40(n-i)+37}^c,\\
&K_{40(n-i)+38}^c, K_{40(n-i)+39}^c), i = \overline{1...n.}
\end{aligned}
\tag{4}
$$

Структура сети PES32-4, PES32-2 и PES32-1

В вышеприведенной сети PES32-8 раундовые функции имеют два входа и два выхода. Таким же образом, на основе сети PES32-16 можно построить сети, в которых раундовые функции имеют по четыре входных и выходных блока, по восемь входных и выходных блока и по шестнадцать

входных и выходных блоков. Сеть, для которой раундовые функции имеют по четыре входных и выходных блоков, а также применяется четыре раундовых функций, называется PES32-4. Аналогично, сеть, для которой раундовые функции имеют по восемь входных и выходных блоков, а также применяется двух раундовые функции, называется PES32-2 и т.д. Таким же образом определяются сеть PES32–1. Схемы раундовых функций сети PES32–4, PES32–2, PES32–1 приведены на рис. 2, 3, 4.

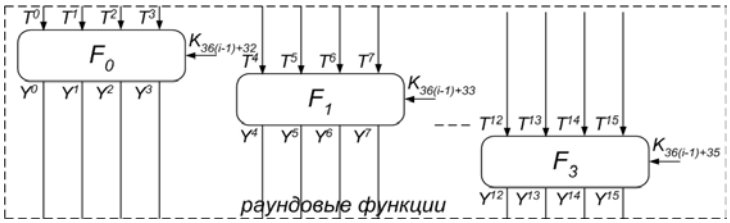

Рис. 2. Схема раундовой функции сети PES32–4

Процесс зашифрования сетей PES32-4, PES32-2 и PES32-1 аналогично как у сети PES32-8, только значение T^j и индекс раундовых ключей отличается. В сети PES32-4 раундовые функции F_0, F_1, F_2, F_3 имеют четыре входных и выходных блоков по 32 (16, 8) битам.

Если $T0=[T^0,T^1,T^2,T^3]$, $T1=[T^4,T^5,T^6,T^7]$, $T2=[T^8,T^9,T^{10},T^{11}]$, $T3=[T^{12},T^{13},T^{14},T^{15}]$ –входной блок, $Y0=[Y^0,Y^1,Y^2,Y^3]$, $Y1=[Y^4,Y^5,Y^6,Y^7]$, $Y2=[Y^8,Y^9,Y^{10},Y^{11}]$, $Y3=[Y^{12},Y^{13},Y^{14},Y^{15}]$ – выходной блок раундовых функции, то раундовую функцию можно представить в виде $Y0=F_0(T0,K_{36(i-1)+32})$, $Y1=F_1(T1,K_{36(i-1)+33})$, $Y2=F_2(T2,K_{36(i-1)+34})$, $Y3=F_3(T3,K_{36(i-1)+35})$. Здесь $T^j=(X^j_{i-1}(z_0)K_{36(i-1)+j})\oplus(X^{16+j}_{i-1}(z_1)K_{36(i-1)+16+j})$, $i=\overline{0...15}$. Для корректности процесса зашифрования раундовую функцию $Y0=F_0(T0,K_{36(i-1)+32})$ представим в виде $Y^0=F^0_0(T^0,T^1,T^2,T^3,K_{36(i-1)+32})$, $Y^1=F^1_0(T^0,T^1,T^2,T^3,K_{36(i-1)+32})$, …, $Y^3=F^3_0(T^0,T^1,T^2,T^3,K_{36(i-1)+32})$, раундовую функцию $Y1=F_1(T1,K_{36(i-1)+33})$ представим в виде $Y^4=F^0_1(T^4,T^5,T^6,T^7,K_{36(i-1)+33})$, $Y^5=F^1_1(T^4,T^5,T^6,T^7,K_{36(i-1)+33})$, …, $Y^7=F^3_1(T^4,T^5,T^6,T^7,K_{36(i-1)+33})$ и так далее, раундовую функцию $Y3=F_3(T3,K_{36(i-1)+35})$ представим в виде $Y^{12}=F^0_3(T^{12},T^{13},T^{14},T^{15},K_{36(i-1)+35})$, $Y^{13}=F^1_3(T^{12},T^{13},T^{14},T^{15},K_{36(i-1)+35})$, …, $Y^{15}=F^3_3(T^{12},T^{13},T^{14},T^{15},K_{36(i-1)+35})$.

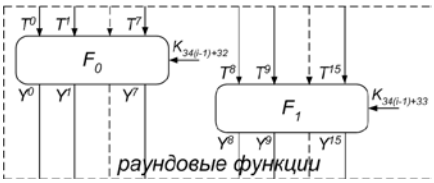

Рис. 3. Схема раундовой функции сети PES32–2

Таким же образом, в сети PES32-2 раундовые функции F_0, F_1 имеют восемь входных и выходных блоков по 32 (16, 8) битам. Если $T0=[T^0,T^1,...,T^7]$, $T1=[T^8,T^9,...,T^{15}_i]$ - входной блок и $Y0=[Y^0,Y^1,...,Y^7]$, $Y1=[Y^8,Y^9,...,Y^{15}]$ - выходной блок раундовой функции, то раундовую функцию можно представить в виде $Y0=F_0(T0,K_{34(i-1)+32})$, $Y1=F_1(T1,K_{34(i-1)+33})$. Здесь $T^j=(X^j_{i-1}(z_0)K_{34(i-1)+j})\oplus(X^{16+j}_{i-1}(z_1)K_{34(i-1)+16+j})$, $i=\overline{0...15}$. Для корректности процесса зашифрования, раундовую функцию $Y0=F_0(T0,K_{34(i-1)+32})$ представим в виде $Y^0=F^0_0(T^0,T^1,...,T^7,K_{34(i-1)+32})$, $Y^1=F^1_0(T^0,T^1,...,T^7,K_{34(i-1)+32})$, ….., $Y^7=F^7_0(T^0,T^1,...,T^7,K_{34(i-1)+32})$, раундовую функцию $Y1=F_1(T1,K_{34(i-1)+33})$ представим в виде $Y^8=F^0_1(T^8,T^9,...,T^{15},K_{34(i-1)+33})$, $Y^9=F^1_1(T^8,T^9,...,T^{15},K_{34(i-1)+33})$, ……., $Y^{15}=F^7_1(T^8,T^9,...,T^{15},K_{34(i-1)+33})$.

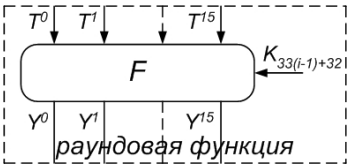

Рис. 4. Схема раундовой функции сети PES32–1

Как у сети PES32–2, если в сети PES32–1 в качестве входного блока берем $T=[T^0,T^1,...,T^{15}]$ и в качестве выходного блока раундовой функции берем $Y=[Y^0,Y^1,...,Y^{15}]$, то раундовую функцию можно представить в виде $Y=F(T,K_{33(i-1)+32})$. Здесь $T^j=(X^j_{i-1}(z_0)K_{33(i-1)+j})\oplus(X^{16+j}_{i-1}(z_1)K_{33(i-1)+16+j})$, $i=\overline{0...15}$. Для корректности процесса зашифрования, раундовую функцию $Y=F(T,K_{33(i-1)+32})$ представим в виде $Y^0=F^0(T^0,T^1,...,T^{15},K_{33(i-1)+32})$, $Y^1=F^1(T^0,T^1,...,T^{15},K_{33(i-1)+32})$, ..., $Y^{15}=F^{15}(T^0,T^1,...,T^{15},K_{33(i-1)+32})$. В сетях PES32–4, PES32–2, PES32–1 F^j_i – выходной $j+1$ блок раундовой функции F_i.

Генерация ключей сети PES32-4, PES32-2 и PES32-1

В сети PES32–4 в каждом раунде применяются 36 раундовые ключи, в сети PES32–2 34 раундовые ключи, в сети PES32–1 33 раундовые ключи и в последнем преобразовании 32 раундовых ключей,

т.е., число всех ключей для сети PES32–4 равно $36n+32$, для сети PES32–2 равно $34n+32$, для сети PES32–1 равно $33n+32$. Ключи расшифрования сетей вычисляются аналогично сети PES32–8, только в сети PES32–4 вместо индекса ключа 40 ставится 36, в сети PES32–2 ставится 34, в сети PES32–1 ставится 33.

Например, ключи расшифрования первого, второго, и $n-$раунда сети PES32–1 связаны с ключами зашифрования по формуле (5).

$$\begin{aligned}&(K^d_{33n},K^d_{33n+1},K^d_{33n+2},K^d_{33n+3},K^d_{33n+4},K^d_{33n+5},K^d_{33n+6},K^d_{33n+7},K^d_{33n+8},K^d_{33n+9},K^d_{33n+10},K^d_{33n+11},\\&K^d_{33n+12},K^d_{33n+13},K^d_{33n+14},K^d_{33n+15},K^d_{33n+16},K^d_{33n+17},K^d_{33n+18},K^d_{33n+19},K^d_{33n+20},K^d_{33n+21},K^d_{33n+22},\\&K^d_{33n+23},K^d_{33n+24},K^d_{33n+25},K^d_{33n+26},K^d_{33n+27},K^d_{33n+28},K^d_{33n+29},K^d_{33n+30},K^d_{33n+31})=((K^c_0)^{z_0},\\&(K^c_1)^{z_0},(K^c_2)^{z_0},(K^c_3)^{z_0},(K^c_4)^{z_0},(K^c_5)^{z_0},(K^c_6)^{z_0},(K^c_7)^{z_0},(K^c_8)^{z_0},(K^c_9)^{z_0},(K^c_{10})^{z_0},(K^c_{11})^{z_0},\\&(K^c_{12})^{z_0},(K^c_{13})^{z_0},(K^c_{14})^{z_0},(K^c_{15})^{z_0},(K^c_{16})^{z_1},(K^c_{17})^{z_1},(K^c_{18})^{z_1},(K^c_{19})^{z_1},(K^c_{20})^{z_1},(K^c_{21})^{z_1},\\&(K^c_{22})^{z_1},(K^c_{23})^{z_1},(K^c_{24})^{z_1},(K^c_{25})^{z_1},(K^c_{26})^{z_1},(K^c_{27})^{z_1},(K^c_{28})^{z_1},(K^c_{29})^{z_1},(K^c_{30})^{z_1},(K^c_{31})^{z_1}).\end{aligned} \tag{5}$$

Полученные результаты

На основе структуры сети PES32–16 разработаны сети PES32-8, PES32-4, PES32-2 и PES32-1, состоящие из восьми, четырех, двух и одно раундовых функций соответственно. Аналогично сети Фейстеля, в сетях PES32-8, PES32-4, PES32-2 и PES32-1 при зашифровании и расшифровании используется один и тот же алгоритм и в качестве раундовых функций можно выбрать любые преобразования, потому что при расшифровании нет необходимости вычисления обратных раундовых функций. Кроме этого, в разработанных сетях в качестве раундовых функциях можно выбрать функции с двумя, четырьмя, восьми и шестнадцати входных и выходных блоков.

Литература

[1] Туйчиев Г.Н. Сеть PES4–2, состоящая из двух раундовых функции // Проблемы информатики и энергетики. — Ташкент. — 2013. — №5-6. — С. 17-111.

[2] Арипов М.М., Туйчиев Г.Н. Сеть PES8–4, состоящая из четырех раундовых функции // Материалы международной научной конференции «Актуальные проблемы прикладной математики и информационных технологий Аль-Хоразми 2012», Том № II, — Ташкент. — 2012. — С. 16–19.

[3] Туйчиев Г.Н. Сеть PES32–16, состоящая из шестнадцати раундовых функции / Г.Н. Туйчиев // Безпека інформації. — Том 20, №1. — 2014. — С. 43–47.

[4] Арипов М.М., Туйчиев Г.Н. Сеть IDEA4–2, состоящая из двух раундовых функции // Инфокоммуникации: Сети–Технологии–Решения. – Ташкент. — 2012. — №4. — С. 55–59.

[5] Туйчиев Г.Н. Сеть IDEA8–4, состоящая из четырех раундовых функции // Инфо-коммуникации: Сети–Технологии–Решения. – Тошкент. —2013. — №2. — С. 55–59.

[6] Туйчиев Г.Н. Сеть IDEA16–8, состоящая из восьми раундовых функции //Вестник ТашГТУ. – Тошкент. — 2014. — №1. — С. 183–187.

[7] Туйчиев Г.Н. Сеть IDEA32–16, состоящая из шестнадцати раундовых функции // Вестник НУУз. – Тошкент. — 2013. — №4. — С. 57–61.

[8] 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

[9] 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.

УДК 003.056.55 (045)

Туйчиєв Г.Н. Про мережі PES32-8, PES32-4, PES32-2 і PES32-1, створені на основі мережі PES32-16

Анотація. *У статті на основі мережі PES32-16 розроблені мережі PES32-8, PES32-4, PES32-2 і PES32-1, що складаються з восьми, чотирьох, двох і однієї раундових функцій відповідно. Раундова функція мережі PES32-8 має по два вхідних і вихідних блоки, раундова функція мережі PES32-4 має по чотири вхідних і вихідних блоки, раундова функція мережі PES32-2 має по вісім вхідних і вихідних блоків і раундова функція мережі PES32-1 має по шістнадцять вхідних і вихідних блоків. Основна перевага запропонованих мереж в тому, що при зашифруванні і розшифруванні використовується один і той же алгоритм, а також в якості раундових функцій можна використовувати будь-які перетворення.*
Ключові слова: *мережа Фейстеля, схема Лай-Мессі, раундова функція, зашифрування, розшифрування, мультиплікативна інверсія, адитивна інверсія.*

Tuychiev G. About networks PES32-8, PES32-4, PES32-2 and PES32-1, created on the basis of network PES32-16

Abstract. *In the paper on the basis of the network PES32-16 networks PES32-8, PES32-4, PES32-2 and PES32-1 were developed – these consisting of eight, four, two, and one round function. Round function of network PES32-8 has two input and output blocks, the round function PES32-4 network has four input and output blocks, the round function PES32-2 network has eight input and output blocks and the round function network PES32-1 has sixteen input and output blocks. The main advantage of the proposed network is that encryption and decryption can use the same algorithm and as well as a round function can be any transformation.*
Key words: *Feistel network, Lai-Massey scheme, round function, encryption, decryption, multiplicative inverse, additive inverse.*

Отримано *15 травня 2014 року*, затверджено редколегією *10 червня 2014 року*