© Tuichiyev G. PES32-16 network consisting of sixteen round functions // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 1, p. 43-47.

СЕТЬ PES32-16, СОСТОЯЩАЯ ИЗ ШЕСТНАДЦАТИ РАУНДОВЫХ ФУНКЦИИ

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: Национальный 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. *Использование криптографических методов является одним из наиболее эффективных способов обеспечения конфиденциальности информации. В силу стремительного развития современной вычислительной техники, разработка новых и усовершенствование существующих криптографических алгоритмов (в частности блочных симметрических алгоритмов) является актуальной научной задачей. В статье разработана сеть PES32–16, состоящая из шестнадцати раундовых функций, в которой использована структура алгоритма блочного шифрования PES. Основное преимущество предложенной сети в том, что при зашифровании и расшифровании используется один и тот же алгоритм, а также то, что в качестве раундовых функций можно использовать любые преобразования.*

Ключевые слова: *сеть Фейстеля, схема Лай-Мэсси, раундовая функция, зашифрование, расшифрование, 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 используется один и тот же алгоритм. Процесс зашифрования и расшифрования можно представить в виде формулы (1), (2).

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

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

Для сети Фейстеля выполняется равенство $L_{i-1} = R_i \oplus F(L_i, K_i) = L_{i-1} \oplus F(R_{i-1}, K_i) \oplus \oplus F(L_i, K_i) = L_{i-1}$. Это равенство означает, что при расшифровании нет необходимости вычисления обратной функции F^{-1}, т.е., в качестве раундовой функции F можно выбрать любые преобразования [5].

В 1990 году Х. Лай и Дж. Мэсси взамен алгоритма DES разработали новый алгоритм блочного шифрования PES [6]. Однако после публикации работ Э. Бихама и А. Шамира по дифференциальному криптоанализу PES был модифицирован усилением его криптостойкости и назван IPES [7]. Через год его переименовали в IDEA [8]. Эти алгоритмы основаны на схемы Лай-Мэсси и в конструкции алгоритмов лежит «смешение операций различных алгебраических групп».

В алгоритме шифрования PES и IDEA, аналогично как у DES, длина блока равно 64 битам. 64 битный блок делится на четыре 16 битных подблока и операции производятся над 16 битным подблоками. На основе модификации IDEA разработан алгоритм шифрования IDEA-128 [9], в котором операции выполняются над 32-х битными подблоками и длина блока равна 128 битам. Кроме этого, на основе схемы Лай-Мэсси разработаны алгоритмы шифрования MESH-64, MESH-96, MESH-128 [10, 11] в которых длина блока равна 64, 96 и 128 битам соответственно.

В алгоритме шифрования PES первые два раундовые ключи умножаются по модулю $2^{16}+1$ на первые два подблока и следующие два раундовые ключи 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 [1-4] авторами на основе структуры алгоритма шифрования PES и IDEA разработана сеть под названием PES8–4, состоящая из четырех раундовых функций и сеть под названием IDEA4–2, IDEA8–4, IDEA32–16, состоящие из двух, четырех и шестнадцати раундовых функций. В разработанных сетях при зашифровании и расшифровании, аналогично как у сети Фейстеля, используется один и тот же алгоритм. А в качестве раундовых функций можно использовать любые преобразования. Данная статья является продолжением статьи [1-4] и в ней разработана новая сеть под названием PES32-16, состоящая из тридцати двух подблоков и шестнадцати раундовых функций.

Структура сети

В сети PES32-16 длина подблоков X^0, X^1,..., X^{31}, длина раундовых ключей $K_{48(i-1)}$, $K_{48(i-1)+1}$,..., $K_{48(i-1)+31}$, $i=\overline{1...n+1}$, а также длина входных и выходных блоков функций F_0, F_1,..., F_{15} равна 32 (16, 8) бит. Длина раундовых ключей $K_{48(i-1)+32}$, $K_{48(i-1)+33}$,..., $K_{48(i-1)+47}$, $i=\overline{1...n}$, необязательно должна быть равной 32 (16, 8) битам.

Схема n–раундовой сети PES16–8 приведена на рис. 1. и процесс зашифрования можно представить в виде следующих последовательностей:

1) при $i=1$ вычисляется значение $A_j=(X_{i-1}^j(z_0)K_{48(i-1)+j})\oplus(X_{i-1}^{j+16}(z_1)K_{48(i-1)+16+j})$, $j=\overline{0...15}$.

2) при $i=1$ вычисляется значение $B_0=F_0(A_0,K_{48(i-1)+32})$, $B_j=F_j(A_j,K_{48(i-1)+32+j})\oplus B_{j-1}$, $j=\overline{1...15}$

3) при $i=1$ подблоки X_{i-1}^j и X_{i-1}^{j+16} суммируются со значением B_{15-j} по XOR, $j=\overline{0...15}$.

4) при $i=1$ подблоки X_{i-1}^j и X_{i-1}^{j+16}, $j=\overline{0...15}$ заменяются.

5) при $i=1$ выполняются $X_i^j=X_{i-1}^j$, $j=\overline{0...31}$.

6) для $i=\overline{2...n}$ выполняются пункты 1–5.

7) в выходном преобразовании вычисляются $X_{n+1}^j=X_n^j(z_0)K_{48n+j}$, $X_{n+1}^j=X_n^j(z_1)K_{48n+16+j}$, $j=\overline{0...15}$.

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 32 (16, 8) битных подблоков. На основе этой сети можно построить алгоритм блочного шифрования длиной блока 1024 бит при длине подблока равной 32 битам, длиной блока 512 бит при длине подблока равной 16 битам и длиной блока 256 бит при длине подблока равной 8 битам.

Как видно из рис.1, в W преобразовании подблоки X_{i-1}^0 и X_{i-1}^{16}, X_{i-1}^1 и X_{i-1}^{17}, ..., X_{i-1}^{15} и X_{i-1}^{31} поменяется между собой. В качестве первого варианта сети PES32–16 берём схему, приведенную на рис. 1, тогда:

– если заменить между собой только подблоки X_{i-1} и X_{i-1}^{16}, X_{i-1}^1 и X_{i-1}^{17}, ..., X_{i-1}^{14} и X_{i-1}^{30}, $i=\overline{1...n}$, то полученную сеть можно выбрать в качестве 2–варианта,

– если заменить между собой только подблоки X_{i-1}^0 и X_{i-1}^{16}, X_{i-1}^1 и X_{i-1}^{17}, ..., X_{i-1}^{13} и X_{i-1}^{29}, $i=\overline{1...n}$, то полученную сеть можно выбрать в качестве 3–варианта,

– …..

– если заменить между собой только подблоки X_{i-1}^0 и X_{i-1}^{16}, X_{i-1}^1 и X_{i-1}^{17}, $i=\overline{1...n}$, то полученную сеть можно выбрать в качестве 15–варианта,

– если заменить между собой только подблоки X_{i-1}^0 и X_{i-1}^{16}, $i=\overline{1...n}$, то полученную сеть можно выбрать в качестве 16–варианта,

– если в сети не менять места подблоков, то её можно выбрать в качестве 17–варианта,

– если заменить между собой только подблоки X_{i-1}^1 и X_{i-1}^{17}, X_{i-1}^2 и X_{i-1}^{18}, ..., X_{i-1}^{15} и X_{i-1}^{31}, $i=\overline{1...n}$, то полученную сеть можно выбрать в качестве 18–варианта,

– если заменить между собой только подблоки X_{i-1}^2 и X_{i-1}^{18}, X_{i-1}^3 и X_{i-1}^{19}, ..., X_{i-1}^{15} и X_{i-1}^{31}, $i=\overline{1...n}$, то полученную сеть можно выбрать в качестве 19–варианта,

–…..

– если заменить между собой только подблоки X_{i-1}^{14} и X_{i-1}^{30}, X_{i-1}^{15} и X_{i-1}^{31}, $i=\overline{1...n}$, то полученную сеть можно выбрать в качестве 31–варианта,

– если заменить между собой только подблоки X_{i-1}^{15} и X_{i-1}^{31}, $i=\overline{1...n}$, то полученную сеть можно выбрать в качестве 32–варианта.

Генерация ключей

В $n-$раундовой сети PES32–16 в каждом раунде применяются 48 раундовых ключа и в последнем преобразовании 32 раундовых ключей, т.е., число всех ключей равно $48n+32$. При

зашифровании из ключа K генерируются $48n+32$ раундовые ключи зашифрования K_i^c. А раундовые ключи расшифрования K_i^d вычисляются на основе K_i^c. При зашифровании 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.

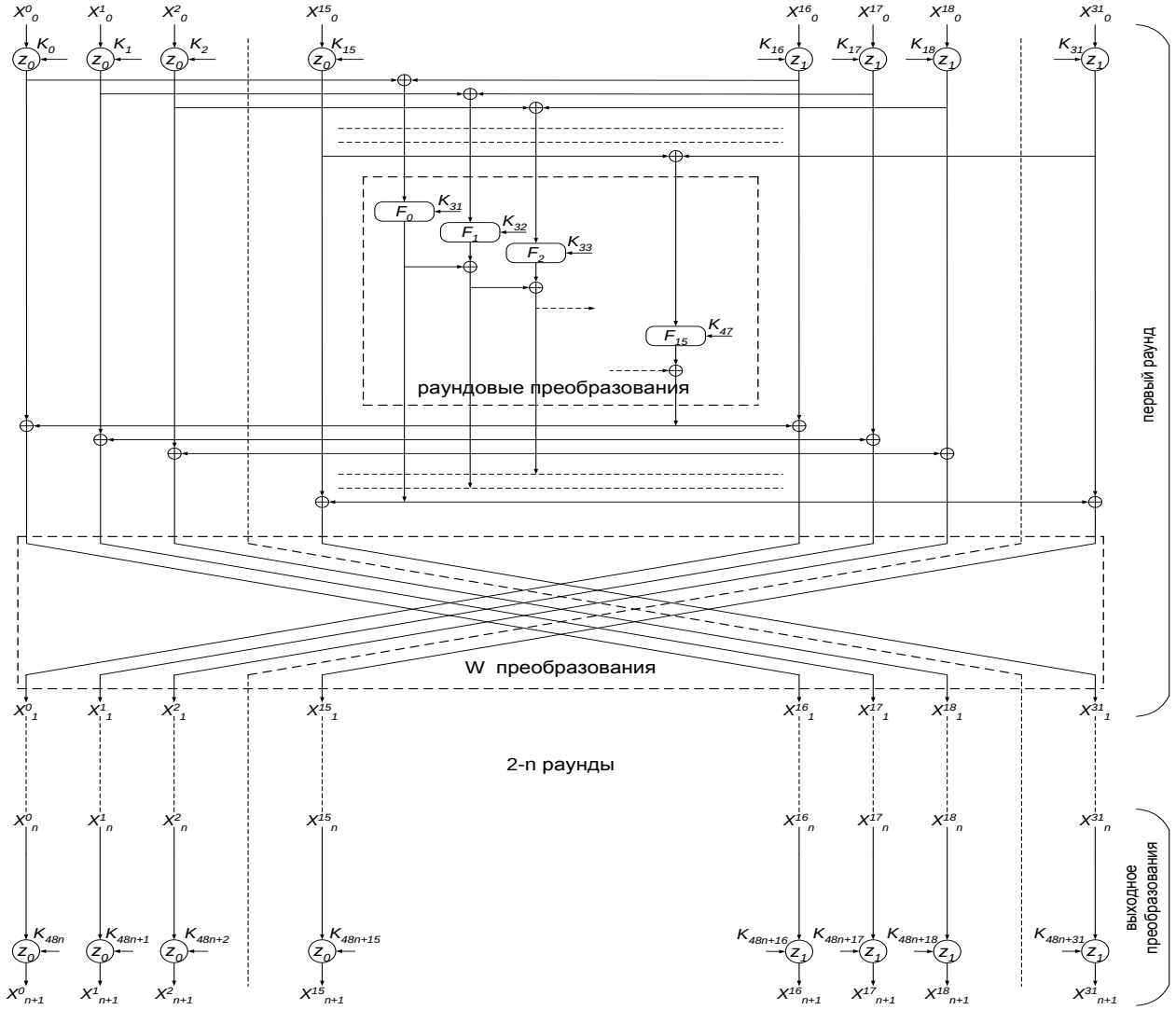

Рис. 1. Схема *n*–раундовой сети PES32–16

В $n-$раундовой сети PES16–8, независимо от её вариантов, раундовые ключи расшифрования связаны с ключами зашифрования по формуле (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 $-K \boxplus K=0$, $K\oplus K=0$.

$$
\begin{aligned}
&(K_{48n}^d,K_{48n+1}^d,K_{48n+2}^d,K_{48n+3}^d,K_{48n+4}^d,K_{48n+5}^d,K_{48n+6}^d,K_{48n+7}^d,K_{48n+8}^d,K_{48n+9}^d,K_{48n+10}^d,K_{48n+11}^d,K_{48n+12}^d,\\
&K_{48n+13}^d,K_{48n+14}^d,K_{48n+15}^d,K_{48n+16}^d,K_{48n+17}^d,K_{48n+18}^d,K_{48n+19}^d,K_{48n+20}^d,K_{48n+21}^d,K_{48n+22}^d,K_{48n+23}^d,K_{48n+24}^d,\\
&K_{48n+25}^d,K_{48n+26}^d,K_{48n+27}^d,K_{48n+28}^d,K_{48n+29}^d,K_{48n+30}^d,K_{48n+31}^d)=((K_0^c)^{z}0,(K_1^c)^{z}0,(K_2^c)^{z}0,(K_3^c)^{z}0,(K_4^c)^{z}0,\\
&(K_5^c)^{z}0,(K_6^c)^{z}0,(K_7^c)^{z}0,(K_8^c)^{z}0,(K_9^c)^{z}0,(K_{10}^c)^{z}0,(K_{11}^c)^{z}0,(K_{12}^c)^{z}0,(K_{13}^c)^{z}0,(K_{14}^c)^{z}0,(K_{15}^c)^{z}0,(K_{16}^c)^{z}1,(K_{17}^c)^{z}1,\\
&(K_{18}^c)^{z}1,(K_{19}^c)^{z}1,(K_{20}^c)^{z}1,(K_{21}^c)^{z}1,(K_{22}^c)^{z}1,(K_{23}^c)^{z}0,(K_{24}^c)^{z}0,(K_{25}^c)^{z}0,(K_{26}^c)^{z}1,(K_{27}^c)^{z}1,(K_{28}^c)^{z}1,(K_{29}^c)^{z}1,(K_{30}^c)^{z}1,(K_{31}^c)^{z}1).
\end{aligned}
\tag{3}
$$

Как видно из формулы (3) при расшифровании ключи зашифрования применяются в обратном порядке, только требуется вычисления инверсии в соответствии операциям z_0, z_1. При зашифровании в первом раунде ключи зашифрования K_0^c, K_1^c, ..., K_{32}^c на подблоки применяется по операциям z_0, z_1, то расшифрование в выходном преобразовании требует вычисления инверсии по операциям z_0, z_1, т.е. $K_{48n}^d = (K_0^c)^{z_0}$, $K_{48n+1}^d = (K_1^c)^{z_0}$, ..., $K_{48n+31}^d = (K_{31}^c)^{z_1}$.

Таким же образом, ключи расшифрования выходного преобразования связаны с ключами зашифрования по формуле (4):

$$
\begin{aligned}
&(K_{48(i-1)}^d, K_{48(i-1)+1}^d, K_{48(i-1)+2}^d, K_{48(i-1)+3}^d, K_{48(i-1)+4}^d, K_{48(i-1)+5}^d, K_{48(i-1)+6}^d, K_{48(i-1)+7}^d, K_{48(i-1)+8}^d, K_{48(i-1)+9}^d,\\
&K_{48(i-1)+10}^d, K_{48(i-1)+11}^d, K_{48(i-1)+12}^d, K_{48(i-1)+13}^d, K_{48(i-1)+14}^d, K_{48(i-1)+15}^d, K_{48(i-1)+16}^d, K_{48(i-1)+17}^d, K_{48(i-1)+18}^d,\\
&K_{48(i-1)+19}^d, K_{48(i-1)+20}^d, K_{48(i-1)+21}^d, K_{48(i-1)+22}^d, K_{48(i-1)+23}^d, K_{48(i-1)+24}^d, K_{48(i-1)+25}^d, K_{48(i-1)+26}^d, K_{48(i-1)+27}^d,\\
&K_{48(i-1)+28}^d, K_{48(i-1)+29}^d, K_{48(i-1)+30}^d, K_{48(i-1)+31}^d, K_{48(i-1)+32}^d, K_{48(i-1)+33}^d, K_{48(i-1)+34}^d, K_{48(i-1)+35}^d, K_{48(i-1)+36}^d,\\
&K_{48(i-1)+37}^d, K_{48(i-1)+38}^d, K_{48(i-1)+39}^d, K_{48(i-1)+40}^d, K_{48(i-1)+41}^d, K_{48(i-1)+42}^d, K_{48(i-1)+43}^d, K_{48(i-1)+44}^d, K_{48(i-1)+45}^d,\\
&K_{48(i-1)+46}^d, K_{48(i-1)+47}^d) = ((K_{48(n-i+1)}^c)^{z_0}, (K_{48(n-i+1)+1}^c)^{z_0}, (K_{48(n-i+1)+2}^c)^{z_0}, (K_{48(n-i+1)+3}^c)^{z_0}, (K_{48(n-i+1)+4}^c)^{z_0},\\
&(K_{48(n-i+1)+5}^c)^{z_0}, (K_{48(n-i+1)+6}^c)^{z_0}, (K_{48(n-i+1)+7}^c)^{z_0}, (K_{48(n-i+1)+8}^c)^{z_0}, (K_{48(n-i+1)+9}^c)^{z_0}, (K_{48(n-i+1)+10}^c)^{z_0},\\
&(K_{48(n-i+1)+11}^c)^{z_0}, (K_{48(n-i+1)+12}^c)^{z_0}, (K_{48(n-i+1)+13}^c)^{z_0}, (K_{48(n-i+1)+14}^c)^{z_0}, (K_{48(n-i+1)+15}^c)^{z_0}, (K_{48(n-i+1)+16}^c)^{z_1},\\
&(K_{48(n-i+1)+17}^c)^{z_1}, (K_{48(n-i+1)+18}^c)^{z_1}, (K_{48(n-i+1)+19}^c)^{z_1}, (K_{48(n-i+1)+20}^c)^{z_1}, (K_{48(n-i+1)+21}^c)^{z_1}, (K_{48(n-i+1)+22}^c)^{z_1},\\
&(K_{48(n-i+1)+23}^c)^{z_1}, (K_{48(n-i+1)+24}^c)^{z_1}, (K_{48(n-i+1)+25}^c)^{z_1}, (K_{48(n-i+1)+26}^c)^{z_1}, (K_{48(n-i+1)+27}^c)^{z_1}, (K_{48(n-i+1)+28}^c)^{z_1},\\
&(K_{48(n-i+1)+29}^c)^{z_1}, (K_{48(n-i+1)+30}^c)^{z_1}, (K_{48(n-i+1)+31}^c)^{z_1}, K_{84(n-i)+32}^c, K_{48(n-i)+33}^c, K_{48(n-i)+34}^c, K_{48(n-i)+35}^c,\\
&K_{48(n-i)+36}^c, K_{48(n-i)+37}^c, K_{48(n-i)+38}^c, K_{48(n-i)+39}^c, K_{48(n-i)+40}^c, K_{48(n-i)+41}^c, K_{48(n-i)+42}^c, K_{48(n-i)+43}^c, K_{48(n-i)+44}^c\\
&K_{48(n-i)+45}^c, K_{48(n-i)+46}^c, K_{48(n-i)+47}^c), \; i = \overline{1...n}.
\end{aligned}
\tag{4}
$$

Полученные результаты

На основе структуры алгоритма шифрования PES разработана новая сеть под названием PES32–16, состоящая из тридцати двух раундовых функций и шестнадцати подблоков. 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, потому что при расшифровании нет необходимости вычисления обратных раундовых функций: F_0^{-1}, F_1^{-1},..., F_{15}^{-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, то всевозможные варианты данного выбора равны $3^2 = 9$. Кроме этого, в сети PES32–16 имеются тридцать два варианта. Если раундовые функции F_0, F_1,..., F_{15} постоянные, т.е. конкретные функции, тогда на основе выбора операции и вариантов можно построить 288 алгоритмов блочного шифрования, основанных на сети PES32–16. Если учитывать то, что в алгоритмах блочного шифрования, основанных на сети PES32–16, в зашифровании и расшифровании используется один и тот же алгоритм, тогда это дает удобства при создании аппаратного или программно–аппаратного средства. Это объясняется тем, что при зашифровании и расшифровании используется одно и то же аппаратное или программно–аппаратное средство.

Литература

[1] Арипов М.М., Туйчиев Г.Н. Сеть PES8–4, состоящая из четырех раундовых функции //Матер. междунар. науч. конф. «Актуальные проблемы прикладной математики и информационных технологий Аль–Хорезми 2012», Том II, Ташкент, 2012. — С. 16-19 .

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

[3] Туйчиев Г.Н. Сеть IDEA8–4, состоящая из четырех раундовых функции // Инфокоммуникации: Сети–Технологии–Решения, Ташкент, 2013, №2. — С. 55–59.

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

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

[6] Lai X., Massey J.L. A proposal for a new block encryption standard. Advances in Cryptology – Advances in Cryptology-EUROCRYPT'90, LNCS 473, Springer-Verlag, Berlin, 1991, pp. 389-404.

[7] Lai X., Massey J.L. Markov ciphers and differential cryptanalysis. Advances in Cryptology, Proceeding EUROCRYPT'91, LNCS 547, Springer-Verlag, 1991, pp. 17-38.

[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] Nakahara J. On the Design of IDEA-128. http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2005/002.pdf

[10] Nakahara J., Rijmen V., Preneel B., Vandewalle J. The MESH Block Ciphers. The 4th International Workshop on Info. Security Applications, WISA 2003, Springer–Verlag, LNCS 2908, 2003, pp. 458–473

[11] Nakahara J. Faster Variants MESH Block Ciphers. The 5th International Conference on Cryptology in India, INDOCRYPT 2004, Springer–Verlag, LNCS 3348, 2004, pp. 162–174

УДК 003.056.55 (045)

Туйчієв Г.Н. Мережа PES32-16, що складається із шістнадцяти раундових функцій

Анотація. *Використання криптографічних методів є одним із найбільш ефективних способів забезпечення конфіденційності інформації. З огляду на розвиток сучасної обчислювальної техніки, розробка нових і удосконалення існуючих криптографічних алгоритмів (зокрема блокових симетричних алгоритмів) є актуальною науковою задачею. У статті розроблена мережа PES32-16, що складається з шістнадцяти раундових функцій, у якій використана структура алгоритму блокового шифрування PES. Основна перевага запропонованої мережі полягає у тому, що при зашифровуванні та розшифровуванні використовується один і той же алгоритм, а також те, що у якості раундових функцій можна використовувати будь-які перетворення.*

Ключові слова: *мережа Фейстеля, схема Лай-Массі, раундова функція, зашифрування, розшифрування, мультиплікативна інверсія, адитивна інверсія.*

Tuichiyev G. PES32-16 network consisting of sixteen round functions

Abstract. *Using the cryptographic methods is one of most effective way to provide information confidentiality. From the viewpoint of modern computation technologies cryptographic algorithms developing and improving (such as block symmetric algorithms) are actual scientific problem. In this paper we develop network PES32-16, consisting of sixteen round functions, which uses the structure of the block cipher algorithm PES. The main advantages of the proposed network are using the same algorithm for encryption and decryption and also ability for using any transformation as a round function.*

Key words: *Feistel network, Lai–Massey scheme, round function, encryption, decryption, multiplicative inverse, additive inverse.*

Отримано *16 січня 2014 року*, затверджено редколегією *05 лютого 2014 року*