УДК 004.056.55

О СЕТЯХ RFWKPES16–8, RFWKPES16–4, RFWKPES16–2 И RFWKPES16–1, СОЗДАННЫХ НА ОСНОВЕ СЕТИ PES16–8

Гулом Туйчиев

В статье на основе сети PES16–8 разработаны сети RFWKPES16–8, RFWKPES16–4, RFWKPES16–2 и RFWKPES16–1 состоящие из восьми, четырех, двух и одной раундовых функций. 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. В разработанных сетях длина подблоков равна 8, 16 и 32 битам и на основе этой сети можно создать алгоритм шифрования длиной блока 128, 256 и 512 битам. Кроме этого, 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, раундовая функция, зашифрование, расшифрование, мультипликативная инверсия, аддитивная инверсия.*

ВВЕДЕНИЕ. В 1990 году Х. Лай и Дж. Мэсси взамен алгоритма DES разработали новый алгоритм блочного шифрования PES [12]. Однако после публикации работ Э. Бихама и А. Шамира по дифференциальному криптоанализу PES был модифицирован усилением его криптостойкости и назван IPES. Через год его переименовали в IDEA [13]. Эти алгоритмы основаны на схеме Лай–Мэсси и в основе конструкции алгоритмов лежит «смешение операций различных алгебраических групп».

В алгоритмах шифрования PES и IDEA, аналогично как у DES, длина блока равна 64 битам. 64 битный блок делится на четыре 16 битных подблоков и операции производятся над 16 битными подблоками. В процессе шифрования PES и IDEA к парам 16–битных подблоков применяются три различных групповых операции:

– побитовое исключающее – ИЛИ (XOR), обозначаемое как $\oplus$ (xor);

– сложение целых чисел по модулю 2^{16}, когда подблок рассматривается в качестве обычного представления целого числа по основанию два. Операция обозначена как $\boxplus$ (add);

– перемножение целых чисел по модулю $2^{16}+1$, когда подблок рассматривается в качестве обычного представления целого числа по основанию два за исключением того, что подблок из всех нулей полагается равным 2^{16}. Операция обозначена как $\otimes$ (mul).

В алгоритмах шифрования PES, IDEA раундовые ключи умножаются по модулю $2^{16}+1$ и суммируются по модулю 2^{16} с соответствующимы подблоками. В МА преобразовании ограничиваются использова-нием 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 работе [1–8] авторами на основе структуры алгоритма шифрования PES, IDEA разработаны сети под названием PES4–2, IDEA4–2, PES8–4, IDEA8–4, PES16–8, IDEA16–8, IDEA32–16, PES32–16, состоящие из двух, четырех, восьми 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.

В сетях [1–8] раундовые функции имеют по одному входному и выходному блоку и в каждом раунде применены раундовые ключи. Кроме этого, раундовые ключи умножаются и суммируются с подблоками. За счет умножения и суммирования раундовых ключей к подблокам, раундовые функции указанных сетях можно применять без ключа. Кроме этого, функции, имеющие один входной и выходной блок, дают ограничения в разработке блочных алгоритмов шифрования. Потому что, сейчас в блочных шифрах применяются раундовые функции, имеющие несколько входных и выходных блоков.

На основе сети IDEA8–4 разработаны

– сеть RFWKIDEA8–4 (round function without key IDEA8–4), т.е., раундовые функции примененные без ключа сеть IDEA8–4, состоящая из четырех раундовых функции, в которой раундовые функции имеют по одному входному и выходному блоку,

– сеть RFWKIDEA8–2, состоящая из двух раундовых функции, в которой раундовые функции имеют по два входных и выходных блоков,

– сеть RFWKIDEA8–1, состоящая из одной раундовой функции, в которой

раундовые функции имеют по четыре входных и выходных блоков [9].

Таким же образом, на основе сети PES8–4 разработаны сети RFWKPES8–4, RFWKPES8–2, RFWKPES8–1 и на основе сети PES32–16 разработаны сети RFWKPES32–16, RFWKPES32–8, RFWKPES32–4, RFWKPES32–2 и RFWKPES32–1 [10–11].

В этой статье на основе сети PES16–8 разработаны:

– сеть RFWKPES16–8 (round function without key PES16–8), состоящая из восьми раундовых функций,

– сеть RFWKPES16–4 (round function without key PES16–4), состоящая из четырех раундовых функций,

– сеть RFWKPES16–2 (round function without key PES16–2), состоящая из двух раундовых функций,

– сеть RFWKPES16–1 (round function without key PES16–1), состоящая из одной раундовой функции.

Структура сети RFWKPES16–8. В сети RFWKPES16–8 длина подблоков X^0, X^1, …, X^{15}, длина раундовых ключей $K_{16(i-1)}$, $K_{16(i-1)+1}$, …, $K_{16(i-1)+15}$, $i=\overline{1...n+1}$, а также длина входных и выходных блоков функций F_0, F_1, …, F_7 равна 32 (16, 8) битам. Схема *n*–раундовой сети RFWKIDEA16–8 приведена на Рис. 1, а процесс зашифрования приведен в следующей формуле.

$$\begin{cases} X_i^0=(X_{i-1}^8(z_1)K_{16(i-1)+8})\oplus Y_0\ \oplus Y_1\ \oplus Y_2\ \oplus...\oplus Y_7\ ;\\ X_i^1=(X_{i-1}^9(z_1)K_{16(i-1)+9})\oplus Y_0\ \oplus Y_1\ \oplus Y_2\ \oplus...\oplus Y_6\ ;\\ X_i^2=(X_{i-1}^{10}(z_1)K_{16(i-1)+10})\oplus Y_0\ \oplus Y_1\ \oplus Y_2\ \oplus...\oplus Y_5\ ;\\ .....\\ X_i^7=(X_{i-1}^{15}(z_1)K_{16(i-1)+15})\oplus Y_0\ ;\\ X_i^8=(X_{i-1}^0(z_0)K_{16(i-1)})\oplus Y_0\ \oplus Y_1\ \oplus Y_2\ \oplus...\oplus Y_7\ ;\\ X_i^9=(X_{i-1}^1(z_0)K_{16(i-1)+1})\oplus Y_0\ \oplus Y_1\ \oplus Y_2\ \oplus...\oplus Y_6\ ;\\ X_i^{10}=(X_{i-1}^2(z_0)K_{16(i-1)+2})\oplus Y_0\ \oplus Y_1\ \oplus Y_2\ \oplus...\oplus Y_5\ ;\\ .....\\ X_i^{15}=(X_{i-1}^7(z_0)K_{16(i-1)+7})\oplus Y_0\ ; \end{cases} \quad i=\overline{1...n}. \tag{1}$$

$$\begin{cases} X_{n+1}^0=(X_n^0(z_0)K_{16n});\\ X_{n+1}^1=(X_n^1(z_0)K_{16n+1});\\ X_{n+1}^2=(X_n^2(z_0)K_{16n+2});\\ .....\\ X_{n+1}^7=(X_n^7(z_0)K_{16n+7});\\ X_{n+1}^8=(X_n^8(z_1)K_{16n+8});\\ X_{n+1}^9=(X_n^9(z_1)K_{16n+9});\\ X_{n+1}^{10}=(X_n^{10}(z_1)K_{16n+10});\\ .....\\ X_{n+1}^{15}=(X_n^{15}(z_0)K_{16n+15}), \end{cases} \quad \textit{в выходном преобразовании.}$$

Раундовые функции сети RFWKPES16–8 можно представит в виде $Y^0=F_0(T_i^0)$, $Y^1=F_1(T^1)$, $Y^2=F_2(T^3),\ldots$, $Y^7=F_7(T^7)$, здесь $T^j=(X_{i-1}^j(z_j)K_{16(i-1)+j})\oplus\ (X_{i-1}^{8+j}(z_{15-j})K_{16(i-1)+8+j})$, $j=\overline{0...7}$ – входные блоки раундовых функций и Y^j, $j=\overline{0...7}$ – выходные блоки раундовых функций.

В сети RFWKPES16–8 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 $2^{32}+1$

$(2^{16}+1, 2^8+1)$, $\boxplus$–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.

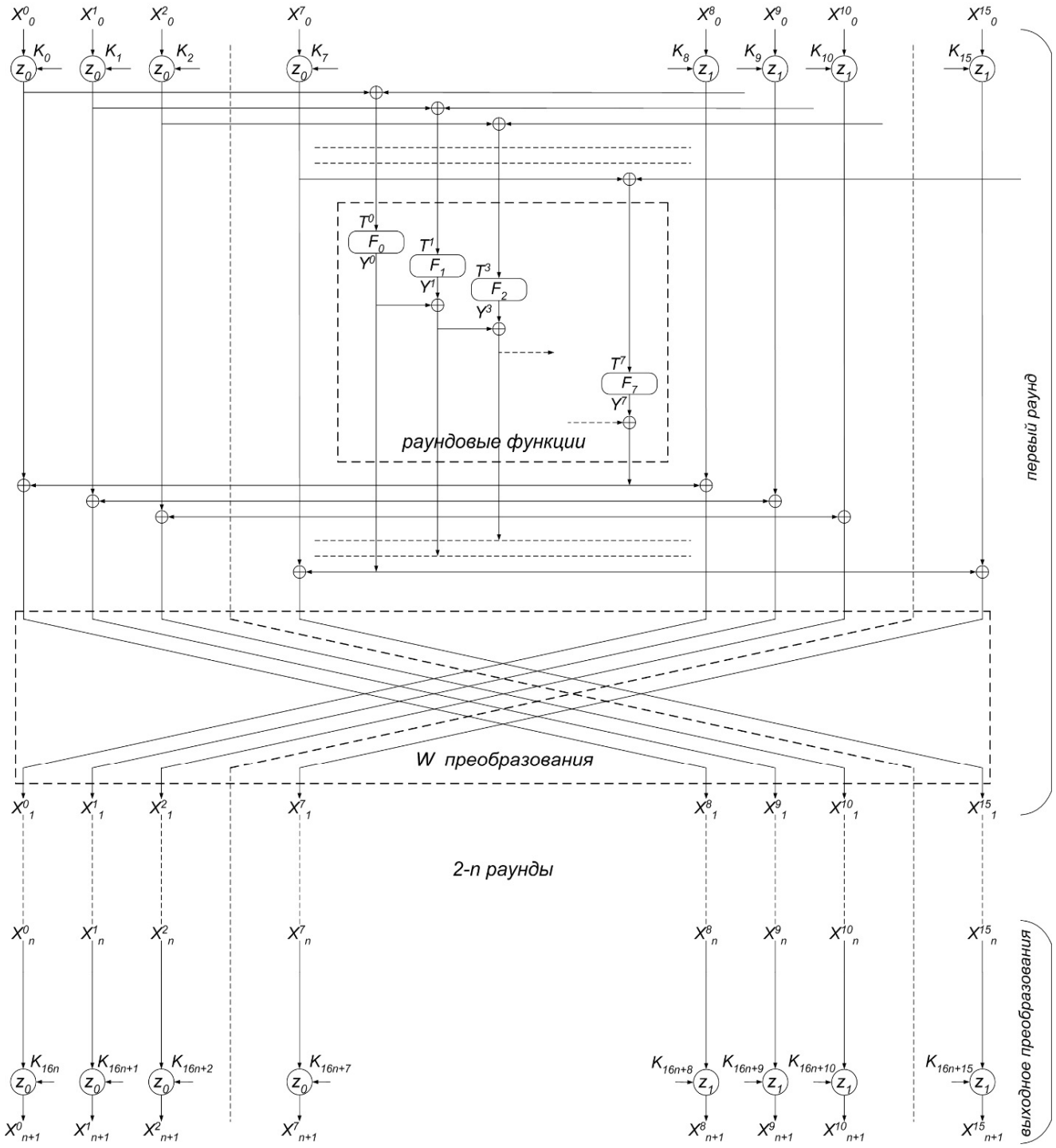

Рис. 1. Схема *n*–раундовой сети RFWKPES16–8

В сети RFWKPES16–8 раундовые функции имеют один входной и один выходной блок. Кроме этого, в блочных шифрах применяются раундовые функции, имеющие несколько входных и выходных блоков. Сеть, состоящая из четырех раундовых функций, в которых раундовые функции имеют по два входных и выходных блоков называется RFWKPES16–4. Аналогично, сеть, состоящая из двух раундовых функций, в которых раундовые функции имеют по четыре входных и выходных блоков называется RFWKPES16–2. Таким же образом, раундовые функции имеющие по восемь входных и выходных блоков и состоящие из однойраундовой функции называются RFWKPES16–1.

Структура сети RFWKPES16–4. В сети RFWKPES16–4 раундовые функции F_0, F_1, F_2, F_3 имеют по два входных и выходных блоков, длина которых равна 32 (16, 8) битам. Если в качестве входного блока положим $T0=[T^0,T^1]$, $T1=[T^2,T^3]$, $T2=[T^4,T^5]$, $T3=[T^6,T^7]$, и в качестве выходного блока раундовой функции берём $Y0=[Y^0,Y^1]$, $Y1=[Y^2,Y^3]$, $Y2=[Y^4,Y^5]$, $Y3=[Y^6,Y^7]$, то раундовую функцию можно представить в виде $Y0=F_0(T0)$, $Y1=F_1(T1)$, $Y2=F_2(T2)$, $Y3=F_3(T3)$. Для корректности процесса зашифрования раундовую функцию $Y0=F_0(T0)$ представим в виде $Y^0=F_0^0(T^0,T^1)$, $Y^1=F_0^1(T^0,T^1)$, а раундовую функцию $Y1=F_1(T1)$ представим в виде $Y^2=F_1^0(T^2,T^3)$, $Y^3=F_1^1(T^2,T^3)$ и так далее, раундовую функцию $Y3=F_3(T3)$ представим в виде $Y^6=F_3^0(T^6,T^7)$, $Y^7=F_3^1(T^6,T^7)$. Схема раундовые функции $i-$раунда сети RFWKPES16–4 приведена на Рис. 2.

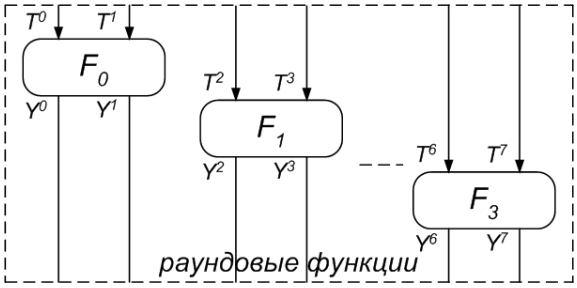

Рис. 2. Схема раундовых функций $i-$раунда сети RFWKPES16–4

Структура сети RFWKPES16–2. В сети RFWKPES16–2 раундовые функции F_0, F_1 имеют четыре входных и выходных блоков по 32 (16, 8) бит. Если $T0=[T^0,T^1,T^2,T^3]$, $T1=[T^4,T^5,T^6,T^7]$ – входной блок, $Y0=[Y^0,Y^1,Y^2,Y^3]$, $Y1=[Y^4,Y^5,Y^6,Y^7]$ – выходной блок раундовых функций, то раундовую функцию можно представить в виде $Y0=F_0(T0)$, $Y1=F_1(T1)$, $Y0=F_0(T0)$, $Y1=F_1(T1)$. Для корректности процесса зашифрования раундовую функцию $Y0=F_0(T0)$ представим в виде $Y^0=F_0^0(T^0,T^1,T^2,T^3)$, $Y^1=F_0^1(T^0,T^1,T^2,T^3)$, …, $Y^3=F_0^3(T^0,T^1,T^2,T^3)$, раундовую функцию $Y1=F_1(T1)$ представим в виде $Y^4=F_1^0(T^4,T^5,T^6,T^7)$, $Y^5=F_1^1(T^4,T^5,T^6,T^7)$, …, $Y^7=F_1^3(T^4,T^5,T^6,T^7)$. Схема раундовой функции i-раунда сети RFWKPES16–2, приведена на Рис. 3.

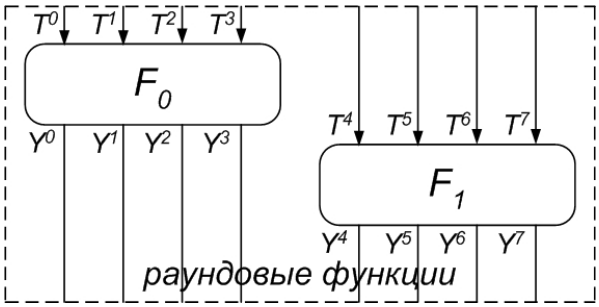

Рис. 3. Схема раундовых функций $i-$раунда сети RFWKPES16–2

В сетях RFWKPES16–8, RFWKPES16–4, RFWKPES16–2, RFWKPES16–1 в качестве F_i^j выбран выходной $j+1$ блок раундовой функции F_i.

Процесс зашифрования сетей RFWKPES16–8, RFWKPES16–4, RFWKPES16–2, RFWKPES16–1 похож на (1), только вместо $Y^0\oplus Y^1$ ставится Y^1, вместо $Y^0\oplus Y^1\oplus Y^2$ ставится Y^2 и так далее вместо $Y^0\oplus Y^1\oplus Y^2\oplus\ldots\oplus Y^{15}$ ставится Y^{15}.

Генерация ключей сети RFWKPES16–8, RFWKPES16–4, RFWKPES16–2, RFWKPES16–1. В $n-$раундовой сети RFWKPES16–8, RFWKPES16–4, RFWKPES16–2, RFWKPES16–1 в каждом раунде применяются 16 раундовые ключи и в последнем преобразовании 16 раундовых ключей, т.е., число всех ключей равно $16n+16$. При зашифровании на Рис. 1 и (1) формуле 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. Раундовые ключи расшифрования первого, второго, третьего и $n-$раунда вышеприведенных сетей связаны с раундовыми ключами зашифрования по формуле (2).

$$(K^d_{16(i-1)}, K^d_{16(i-1)+1}, K^d_{16(i-1)+2}, K^d_{16(i-1)+3}, K^d_{16(i-1)+4}, K^d_{16(i-1)+5}, K^d_{16(i-1)+6}, K^d_{16(i-1)+7}, K^d_{16(i-1)+8},$$
$$K^d_{16(i-1)+9}, K^d_{16(i-1)+10}, K^d_{16(i-1)+11}, K^d_{16(i-1)+12}, K^d_{16(i-1)+13}, K^d_{16(i-1)+14}, K^d_{16(i-1)+15}) = ((K^c_{16(n-i+1)})^{z_0},$$
$$(K^c_{16(n-i+1)+1})^{z_0}, (K^c_{16(n-i+1)+2})^{z_0}, (K^c_{16(n-i+1)+3})^{z_0}, (K^c_{16(n-i+1)+4})^{z_0}, (K^c_{16(n-i+1)+5})^{z_0}, \quad (2)$$
$$(K^c_{16(n-i+1)+6})^{z_0}, (K^c_{16(n-i+1)+7})^{z_0}, (K^c_{16(n-i+1)+8})^{z_1}, (K^c_{16(n-i+1)+9})^{z_1}, (K^c_{16(n-i+1)+10})^{z_1},$$
$$(K^c_{16(n-i+1)+11})^{z_1}, (K^c_{16(n-i+1)+12})^{z_1}, (K^c_{16(n-i+1)+13})^{z_1}, (K^c_{16(n-i+1)+14})^{z_1}, (K^c_{16(n-i+1)+15})^{z_1},), i = \overline{1...n}.$$

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 $-K \boxplus K = 0$, $K \oplus K = 1$.

Ключи расшифрования выходного преобразования вышеприведенных сетей связаны с раундовыми ключами зашифрования следующим образом:

$$(K^d_{16n}, K^d_{16n+1}, K^d_{16n+2}, K^d_{16n+3}, K^d_{16n+4}, K^d_{16n+5}, K^d_{16n+6}, K^d_{16n+7}, K^d_{16n+8}, K^d_{16n+9}, K^d_{16n+10},$$
$$K^d_{16n+11}, K^d_{16n+12}, K^d_{16n+13}, K^d_{16n+14}, K^d_{16n+15}) = ((K^c_0)^{z_0}, (K^c_1)^{z_0}, (K^c_2)^{z_0}, (K^c_3)^{z_0}, (K^c_4)^{z_0}, \quad (3)$$
$$(K^c_5)^{z_0}, (K^c_6)^{z_0}, (K^c_7)^{z_0}, (K^c_8)^{z_1}, (K^c_9)^{z_1}, (K^c_{10})^{z_1}, (K^c_{11})^{z_1}, (K^c_{12})^{z_1}, (K^c_{13})^{z_1}, (K^c_{14})^{z_1},$$
$$(K^c_{15})^{z_1}).$$

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^c_0, K^c_1, …, K^{16}_0 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. $K^d_{16n} = (K^c_0)^{z_0}$, $K^d_{16n+1} = (K^c_1)^{z_0}$, ..., $K^d_{16n+15} = (K^c_{15})^{z_1}$.

Полученные результаты. В статье на основе сети PES16–8 разработаны сети RFWKPES16–8, RFWKPES16–4, RFWKPES16–2 и RFWKPES16–1. В разработанных сетях, в качестве раундовых функций можно выбрать любые преобразования, в том числе однонаправленные функции. Потому что при расшифровании нет необходимости вычисления обратной функции к раундовым функциям. Кроме этого, в разработанных сетях в качестве раундовых функций можно выбрать функции с двумя, четырьмя и восьмью входных и выходных блоков.

На основе приведенных сетей, при длине подблоков равным 32 битам, можно построить алгоритм зашифрования длиной блока 512 бит, при длине подблоков равных 16 битам, можно построить алгоритм зашифрования длиной блока 256 бит и при длине подблоков равных 8 битам, можно построить алгоритм шифрования длиной блока 128 бит. Если выбрать в качестве операций z_0, z_1 операции mul, add и xor, все возможные варианты данного выбора равны 3^2. Кроме этого, в каждой сети имеются 16 вариантов. Характеристика сетей приведена в таблице 1.

Таблица 1

Характеристика сетей

Сеть	Число раундовых ключей	Число раундовых функций
RFWKPES16–8	$16n+16$	8
RFWKPES16–4	$16n+16$	4
RFWKPES16–2	$16n+16$	2
RFWKPES16–1	$16n+16$	1

Заключение. Преимущество разработанных сетей состоит в том, что при зашифровании и расшифровании используется один и тот же алгоритм. Это даёт удобство при создании аппаратных и программно–аппаратных средств. Кроме этого, в качестве раундовых функций используя раундовые функции существующих алгоритмов шифрования, например, алгоритмы шифрования основанные на сети Фейстеля, можно перевести эти алгоритмы на основе вышеприведенных сетей.

ЛИТЕРАТУРА

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

[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 IDEA8–4, состоящая из четырех раундовых функции //Инфокоммуникации: Сети–Технологии–Решения. –Тошкент, 2013, №2, с. 55–59.

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

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

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

[7]. Туйчиев Г.Н. О сети PES16–8, состоящей из восьми раундовых функций // Защита информация. - Киев, 2014, №3, с. 167-173.

[8]. Туйчиев Г.Н. Сеть PES32–16, состоящая из шестнадцати раундовых функции // Безпека информации. –Киев, 2014, №1, с. 43–47.

[9]. Туйчиев Г.Н. О сетях IDEA8–2, IDEA8–1 и RFWKIDEA8–4, RFWKIDEA8–2, RFWKIDEA8–1, разработанные на основе сети IDEA8–4 // Узбекский математический журнал. – Ташкент, 2014, №3, с. 104-118.

[10]. Туйчиев Г.Н. О сетях RFWKPES8-4, RFWKPES8-2, RFWKPES8-1, разработанные на основе сети PES8-4 //Материалы международной научной конференции «Актуальные проблемы прикладной математики и информационных технологий–Аль–Хоразми 2014». Том № II, –Ташкент, 2014, с. 32–36.

[11]. Туйчиев Г.Н. О сетях RFWKPES32–8, RFWKPES32–4, RFWKPES32–2 и RFWKPES32–1, созданных на основе сети PES32–16 // Сборник тезисов и докладов республиканского семинара «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения». –Ташкент, 2014.

[12]. 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

[13]. 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.

REFERENCES

[1]. Aripov M.M. Tuychiev G.N. The network IDEA4–2, consists from two round functions // Infocommunications: Networks–Technologies–Solutions. –Tashkent , 2012, №4, pp. 55–59.

[2]. Aripov M.M. Tuychiev G.N. The network PES8–4, consists from four round functions // Materials of the international scientific conference «Modern problems of applied mathematics and information technologies–Al–khorezmiy 2012». Volume № II, –Tashkent, 2012, pp. 16–19.

[3]. Tuychiev G.N. The network IDEA8–4, consists from four round functions // Infocommunications: Networks–Technologies–Solutions. –Tashkent. 2013, №2, pp. 55–59.

[4]. Tuychiev G.N. The network IDEA16–8, consisted of eight round functions // Acta TSTU. –Tashkent, 2014, №1, pp. 183–187

[5]. Tuychiev G.N. The network IDEA32–16, consists from sixteen round functions // Acta NUUz. –Tashkent, 2013, №4. pp. 57–61.

[6]. Tuychiev G.N. The network PES4–2, consists from two round functions // Uzbek journal of the problems of informatics and energetics. –Tashkent,, 2013, №5–6, pp. 17–111.

[7]. Tuychiev G.N. About the network PES16–8, consisting of eight round function // Ukrainian Information Security Research Journal,

[8]. Tuychiev G.N. The network PES32–16, consisting of sixteen round functions // Ukrainian Scientific Journal of Information Security. 2014, vol. 20, issue 1, pp. 43–47

[9]. Tuychiev G.N. About networks IDEA8–2, IDEA8–1 and RFWKIDEA8–4, RFWKIDEA8–2, RFWKIDEA8–1, developed on the basis of network IDEA8–4 // Uzbek mathematical journal. –Tashkent, 2014, №3, pp. 104–118

[10]. Tuychiev G.N. About networks RFWKPES8–4, RFWKPES8–2, RFWKPES8–1, developed on the basis of network PES8–4// Transactions of the international scientific conference «Modern problems of applied mathematics and information technologies–Al–Khorezmiy 2012». Volume № 2, –Tashkent, 2014, pp. 32–36.

[11]. Tuychiev G.N. About networks RFWKPES32–8, RFWKPES32–4, RFWKPES32–2 and RFWKPES32–1, created on the basis of network PES32–16// Compilation of theses and reports republican seminar «Information security in the sphere communication and information. Problems and their solutions». –Tashkent, 2014

[12]. 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
[13]. 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.

ПРО МЕРЕЖІ RFWKPES16–8, RFWKPES16–4, RFWKPES16–2 ТА RFWKPES16–1, СТВОРЕНІ НА ОСНОВІ МЕРЕЖІ PES16–8

У статті на осное мережі PES16–8 розроблені мережі RFWKPES16–8, RFWKPES16–4, RFWKPES16–2 і RFWKPES16–1 складаються з восьми, чотирьох, двох і однієї раундових функцій. Основна перевага запропонованих мереж в тому, що при зашифрованих і расшифровании використовується один і той же алгоритм, а також як раундових функцій можна використовувати будь– які перетворення. В розроблених мережах довжина подблоков дорівнює 8, 16 і 32 бітам і на основі цієї мережі можна створити алгоритм шифрування довжиною блоку 128, 256 і 512 бітам. Крім цього, 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, раундова функція, зашифрование, розшифрування, мультиплікативна інверсія, аддитивная інверсія.

ABOUT NETWORKS RFWKPES16–8, RFWKPES16–4, RFWKPES16–2 AND RFWKPES16–1, CREATED ON THE BASIS NETWORK PES16–8

In the paper on the basis of the network PES16–8 developed networks RFWKPES16–8, RFWKPES16–4, RFWKPES16–2 and RFWKPES16–1 consisting of eight, four, two, and one round function. The main advantage of the proposed network that during encryption and decryption using the same algorithm as well as a round function can be 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
Index terms: Feistel network, Lai–Massey scheme, round function, encryption, decryption, 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.

УДК 004.027

МЕТОДИ ШИФРУВАННЯ НА ОСНОВІ ПЕРЕСТАНОВКИ БЛОКІВ ЗМІННОЇ ДОВЖИНИ

Володимир Лужецький, Іван Горбенко

Однією з основних операцій, яка використовується в багатьох блокових шифрах, є перестановка. Сучасні блокові шифри здійснюють операцію перестановки лише в межах окремого блоку або невеликої групи блоків. В одній з попередній публікацій було запропоновано метод псевдовипадкової перестановки блоків в межах усього повідомлення, однак у сучасних шифрах довжина блоку є фіксованою, тому, навіть після перестановки блоків, початкові та кінцеві позиції блоків залишаються відомими. Для підвищення криптографічної стійкості запропоновано здійснювати розбиття повідомлення на блоки змінної довжини. Розроблено методи шифрування на основі перестановки блоків змінної довжини, сформовано рекомендації стосовно кількості можливих значень довжини блоку та діапазону цих значень, запропоновано правила формування псевдовипадкових значень довжин блоків, наведено їх порівняння з точки зору забезпечення стійкості.
Ключові слова: *перестановка, блоки змінної довжини, відкрите повідомлення, шифротекст, генератор псевдовипадкових чисел.*

Вступ. Відомо [1], що перестановка є однією з базових (разом з підстановкою) операцій алгоритмів шифрування. Зокрема, операція перестановки використовується у сучасних архітектурах блокових шифрів (таких як мережа Фейстеля, SP-мережа, "квадрат"). Однак, ці архітектури передбачають здійснення перестановки частин окремого блоку або перестановки блоків в межах невеликої групи. Так, мережа Фейстеля передбачає розбиття блоку даних на дві або чотири частини і здійснення фіксованої перестановки цих частин [2]. SP-мережа здійснює перестановку чотирьох і