© Tuychiev G. On the network PES2m-m, consisting of m round function and its modifications // Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 1, p. 52-63.

О СЕТИ PES2*m*–*m*, СОСТОЯЩЕЙ ИЗ *m* РАУНДОВЫХ ФУНКЦИЙ И ЕЁ МОДИФИКАЦИИ

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 30 научных публикаций.
E-mail: blasterjon@gmail.com

Аннотация. *На сегодняшний день одним из наиболее эффективных методов построения симметричных блочных шифров является использование так называемых сетей Фейстеля. В этой статье на основе схемы Лай-Месси разработаны сети, состоящие из 2m подблоков. В разработанных сетях, аналогично сети Фейстеля, при зашифровании и расшифровании используется один и тот же алгоритм и в качестве раундовых функций можно использовать любые преобразования. На основе этих разработанных сетей можно построить алгоритм блочного шифрования длиной блока 64m бит при длине подблока равной 32 битам, длиной блока 32m бит при длине подблока равной 16 битам и длиной блока 16m бит при длине подблока равной 8 битам.*

Ключевые слова: *симметричная криптография, 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 тот факт, что при зашифровании и расшифровании используется один и тот же алгоритм.

В 1990 году Х. Лай и Дж. Мэсси взамен алгоритма DES разработали новый алгоритм блочного шифрования PES [16]. Однако после публикации работ Э. Бихама и А. Шамира по дифференциальному криптоанализу PES был модифицирован усилением его криптостойкости и назван IPES [17]. Через год его переименовали в IDEA [18]. Эти алгоритмы основаны на схеме Лай-Мэсси и в конструкции алгоритмов лежит «смешение операций различных алгебраических групп». В алгоритмах шифрования PES, IDEA при зашифровании и расшифровании используется один и тот же алгоритм, но раундовая функция не используется, вместо неё применены MA преобразования.

На основе IDEA разработан алгоритм шифрования IDEA–128 [19], 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 в которых длина блока равна 64, 96, 128 битам соответственно [20, 21]. В алгоритмах шифрования PES, IDEA, IDEA–128, MESH–64, MESH–96, MESH–128 при зашифровании и расшифровании, аналогично как у алгоритмов блочного шифрования, основанных на сети Фейстеля, используется один и тот же алгоритм.

Разработаны расширенные схемы Лай-Мэсси, в которых имеются раундовые функции. Алгоритмы шифрования FOX [15], Мухомор [14] разработан на основе расширенной схемы Лай-Мэсси. Отличие от вышеприведенных алгоритмов шифрования в алгоритмах шифрования FOX, Мухомор алгоритмы зашифрования и расшифрования отличаются.

В алгоритмах шифрования PES, IDEA, MESH–64, MESH–96, MESH–128 раундовые ключи умножаются по модулю $2^{16}+1$ и суммируются по модулю 2^{16} на соответствующие подблоки. В MA 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 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 сетях PESX-Y, IDEAX-Y X-означает число подблоков, Y-число раундовых функций. В разработанных сетях при зашифровании и расшифровании используется один и тот же

алгоритм и в качестве раундовой функции можно использовать любые преобразования.

В сетях PESX-Y, IDEAX-Y 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 сетей 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.

Поэтому, на основе сети PES4–2 разработана сеть PES4–1 [9], состоящая из одной раундовой функции, в которой раундовая функция имеет по два входных и выходных блока. А на основе сети PES8–4 разработаны сети PES8–2, PES8–1 [10] состоящие из двух и одной раундовой функций, в которых раундовые функции имеют по два и четыре входных и выходных блоков. Аналогичным образом, на основе сети PES16–8 разработаны сети PES16–4, PES16–2, PES16–1 [11] состоящие из четырех, двух и одной раундовой функции, в которой раундовые функции имеют по два, четыре и восемь входных и выходных блоков.

На основе сети PES4–2 разработаны сети RFWKPES4–2 (round function without key PES4–2), RFWKPES4–1 (round function without key PES4–1), состоящие из двух и одной раундовой функции, в которых раундовые функции имеют по одному и два входных и выходных блоков [9]. А на основе сети PES8–4 разработаны сети RFWKPES8–4, RFWKPES8–2, RFWKPES8–1 состоящие из четырех, двух и одной раундовых функции, в которых раундовые функции имеют по одному, два и четыре входных и выходных блоков [12]. Таким же образом, на основе сети PES32–16 разработаны сети RFWKPES32–16, RFWKPES32–8, RFWKPES32–4, RFWKPES32–2 и RFWKPES32–1, состоящие из шестнадцати, восьми, четырех, двух и одной раундовых функций, в которых раундовые функции имеют по одному, два, четыре, восемь и шестнадцать входных и выходных блоков [13]. Во всех разработанных сетях в раундовых функциях не использованы раундовые ключи.

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 том числе однонаправленные функции. В данной статье обобщены сети PESX-Y и в ней приведены новые сети PES2m–m, RFWKPES2m–m, PES2m–(m/2), RFWKPES2m–(m/2), PES2m–(m/4), RFWKPES2m–(m/4) и PES2m–1, RFWKPES2m–1 состоящие из 2m подблоков и m, m/2, m/4 и одной раундовой функции.

Структура сети PES2m–m

В сети PES2m–m длина подблоков X^0, X^1, …, X^{2m-1}, длина раундовых ключей $K_{3m(i-1)}$, $K_{3m(i-1)+1}$, …, $K_{3m(i-1)+2m-1}$, $i=\overline{1...n+1}$, а также длина входных и выходных подблоков раундовых функций F_0, F_1, …, F_{m-1} равна 32 (16, 8) битам. Длина раундовых ключей $K_{3m(i-1)+2m}$, $K_{3m(i-1)+2m+1}$, …, $K_{3m(i-1)+3m-1}$, $i=\overline{1...n}$, необязательно должна быть равной 32 (16, 8) битам. Процесс зашифрования сети PES2m–m приведен в (1) формуле, а схема сети приведена на рис. 1.

$$
\begin{cases}
X_i^0 = (X_{i-1}^m(z_0)K_{3m(i-1)}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-1} \\
X_i^1 = (X_{i-1}^{m+1}(z_0)K_{3m(i-1)+2m-2}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-2} \\
X_i^2 = (X_{i-1}^{m-2}(z_0)K_{3m(i-1)+2m-3}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-3} \\
..... \\
X_i^{m-1} = (X_{i-1}^{2m-1}(z_0)K_{3m(i-1)+m}) \oplus Y^0 \\
X_i^m = (X_{i-1}^0(z_1)K_{3m(i-1)+m-1}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-1} \\
X_i^{m+1} = (X_{i-1}^1(z_1)K_{3m(i-1)+m-2}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-2} \\
X_i^{m+2} = (X_{i-1}^2(z_1)K_{3m(i-1)+m-3}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-3} \\
..... \\
X_i^{2m-1} = (X_{i-1}^{m-1}(z_1)K_{3m(i-1)+2m-1}) \oplus Y^0
\end{cases}
, \; i=\overline{1...n}; \qquad (1)
$$

$$
\begin{cases}
X_{n+1}^0 = (X_n^0(z_0)K_{3mn}) \\
X_{n+1}^1 = (X_n(z_0)K_{3mn+1}) \\
X_{n+1}^2 = (X_n^2(z_0)K_{3mn+2}) \\
..... \\
X_{n+1}^{m-1} = (X_n^{m-1}(z_0)K_{3mn+m-1}) \\
X_{n+1}^m = (X_n^m(z_1)K_{3mn+m}) \\
X_{n+1}^{m+1} = (X_n^{m+1}(z_1)K_{3mn+m+1}) \\
X_{n+1}^{m+2} = (X_n^{m+2}(z_1)K_{3mn+m+2}) \\
..... \\
X_{n+1}^{2m-1} = (X_n^{2m-1}(z_1)K_{3mn+2m-1})
\end{cases}
\text{, } \textit{в выходном преобразовании.}
$$

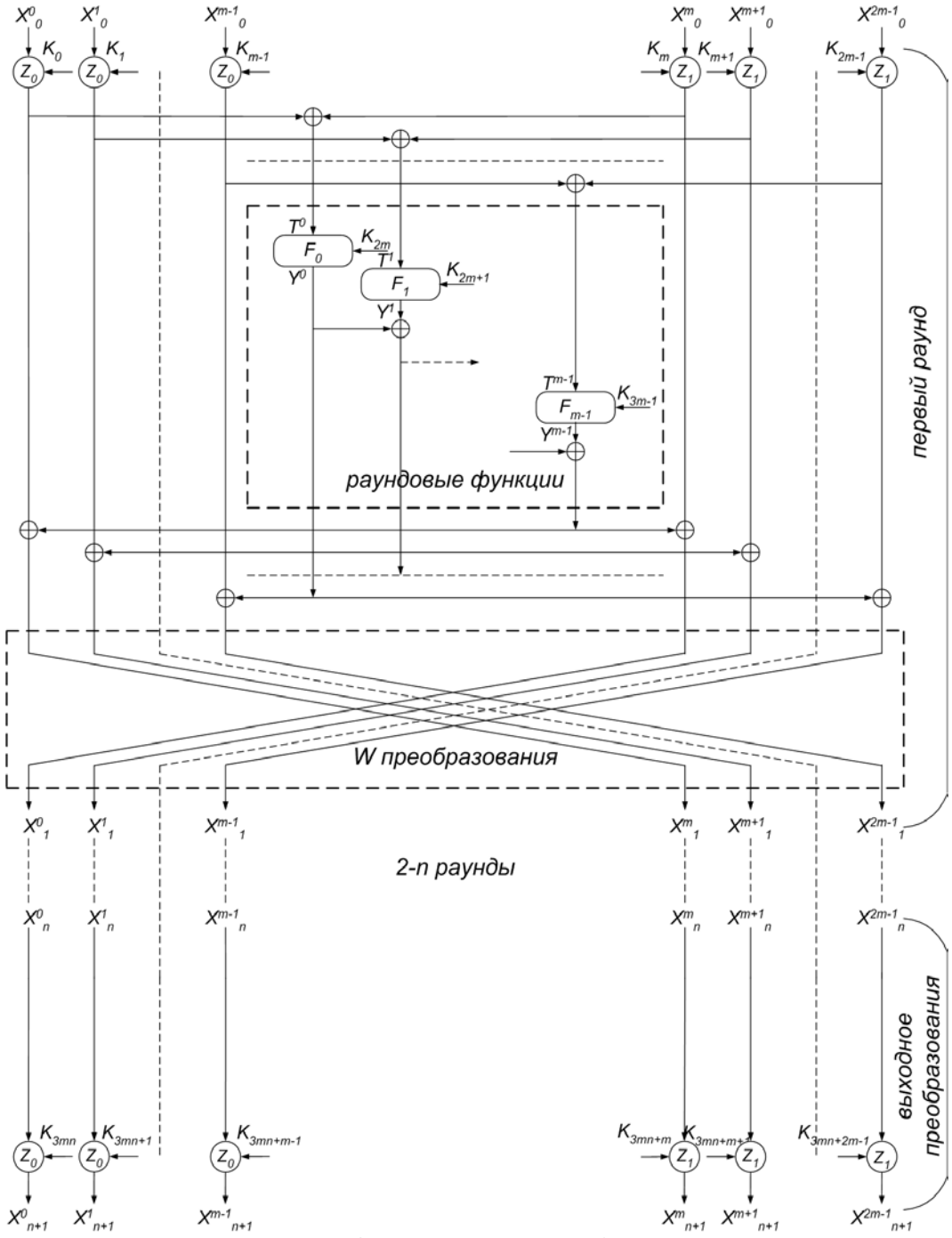

Рис. 1. Схема *n*–раундовой сети PES2m–m

В (3) формуле $Y^j = F_j(T^j, K_{3m(i-1)+2m-1+j})$, $j = \overline{0...m-1}$–выходные значения раундовых функций и $T^j = (X_{i-1}^j(z_0)K_{3m(i-1)+j}) \oplus (X_{i-1}^{j+m}(z_1)K_{3m(i-1)+m+j})$, $j = \overline{0...m-1}$–входные значения раундовых функций F_0, F_1, …, F_{m-1}.

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 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 ⊕ – операция суммирования по XOR 32 (16, 8) битных подблоков. На основе этой сети можно построить алгоритм блочного шифрования длиной блока *64m* бит при длине подблока равной 32 битам, длиной блока *32m* бит при длине подблока равной 16 битам и длиной блока 16*m* бит при длине подблока равной 8 битам.

Как видно из рис. 1, в *W* преобразовании кроме подблоков X^j и X^{j+m}, $j = \overline{0...m-1}$ все подблоки заменяются между собой. В качестве первого варианта сети PES2m–m выбираем схему, приведенную на рис. 1, тогда:

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

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

– если заменить между собой только подблоки X^i ва X^{i+m}, $i=\overline{0...m-4}$, то полученную сеть можно выбрать в качестве 4–варианта,

– …,

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

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

– если в сети не менять места подблоков, то её можно выбрать в качестве m+1–варианта,

– если заменить между собой только подблоки X^i ва X^{i+m}, $i=\overline{1...m-1}$, то полученную сеть можно выбрать в качестве m+2–варианта,

– если заменить между собой только подблоки X^i ва X^{i+m}, $i=\overline{2...m-1}$, то полученную сеть можно выбрать в качестве m+3–варианта,

– …

– если заменить между собой только подблоки X^i ва X^{i+m}, $i=\overline{m-2...m-1}$, то полученную сеть можно выбрать в качестве 2m-1–варианта,

– если заменить между собой только подблоки X^{m-1} ва X^{2m-1}, то полученную сеть можно выбрать в качестве 2m–варианта.

Генерация ключей сети PES2m–m

В n–раундовой сети PES2m–m в каждом раунде применяются 3m раундовые ключи и в выходном преобразовании 2m раундовых ключей, т.е., число всех ключей равно 3mn+2m. При зашифровании из ключа K генерируются 3mn+2m 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 зашифрования K_i^c, а при расшифровании раундовые ключи расшифрования K_i^d, т.е., при зашифровании и расшифровании используется один и тот же алгоритм, меняются только раундовые ключи. В сети PES2m–m ключи расшифрования выходного преобразования привязаны к ключам зашифрования по формуле (2).

$$(K_{3mn}^d, K_{3mn+1}^d, K_{3mn+2}^d, ..., K_{3mn+m-1}^d, K_{3mn+m}^d, K_{3mn+m+1}^d, K_{3mn+m+2}^d, ..., K_{3mn+2m-1}^d) = ((K_0^c)^{z_0}, (K_1^c)^{z_0}, (K_2^c)^{z_0}, ..., (K_{m-1}^c)^{z_0}, (K_m^c)^{z_1}, (K_{m+1}^c)^{z_1}, (K_{m+2}^c)^{z_1}, ..., (K_{2m-1}^c)^{z_1}). \quad (2)$$

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

Таким же образом, ключи расшифрования первого, второго, третьего и n–раунда привязаны к ключам зашифрования по формуле (3).

$$\begin{aligned}&(K_{3m(i-1)}^d, K_{3m(i-1)+1}^d, K_{3m(i-1)+2}^d, ..., K_{3m(i-1)+m-2}^d, K_{3m(i-1)+m-1}^d, K_{3m(i-1)+m}^d, K_{3m(i-1)+m+1}^d, K_{3m(i-1)+m+2}^d, ...,\\ &K_{3m(i-1)+2m-2}^d, K_{3m(i-1)+2m-1}^d, K_{3m(i-1)+2m}^d, K_{3m(i-1)+2m+1}^d, K_{3m(i-1)+2m+2}^d, ..., K_{3m(i-1)+3m-1}^d) = ((K_{3m(n-i+1)}^c)^{z_0},\\ &(K_{3m(n-i+1)+1}^c)^{z_0}, (K_{3m(n-i+1)+2}^c)^{z_0}, ..., (K_{3m(n-i+1)+m-1}^c)^{z_0}, (K_{3m(n-i+1)+m}^c)^{z_1}, (K_{3m(n-i+1)+m+1}^c)^{z_1},\\ &(K_{3m(n-i+1)+m+2}^c)^{z_1}, ..., (K_{3m(n-i+1)+2m-1}^c)^{z_1}, K_{3m(n-i)+2m}^c, K_{3m(n-i)+2m+1}^c, K_{3m(n-i)+2m+2}^c, ..., K_{3m(n-i)+3m-1}^c),\\ &i=\overline{1...n}.\end{aligned} \quad (3)$$

В 2, 3 и 2m–вариантов сети ключи расшифрования выходного преобразования, первого, второго, третьего и n–раунда привязаны к ключам зашифрования по формуле (2) и (3).

В приведёной сети PES2m–m число раундовых функций равно m и раундовые функции F_0, F_1, …, F_{m-1} имеют одно входное и выходное значение. В качестве раундовых функции можно использовать функции с двумя входными и выходными значениями, с четырьмя входными и выходными значениями и с m входными и выходными значениями. Если в качестве раундовых функции использовать функцию с двумя входными и выходными значениями, то число раундовых функции равно $m/2$ и сеть называется PES2m–(m/2), в качестве раундовых функций использовать функцию с четыремя входными и выходными значениями, то число раундовых функции равно $m/4$ и сеть называется PES2m–(m/4), и т.п. в качестве раундовых функций использовать функцию с m входными и выходными значениями, то число раундовых функции равно одному и сеть называется PES2m–1.

Структура сети PES2m–(m/2)

В сети PES2m–(m/2) длина подблоков X^0, X^1, …, X^{2m-1}, длина раундовых ключей $K_{(2m+m/2)(i-1)}$,

$K_{(2m+m/2)(i-1)+1}$, …, $K_{(2m+m/2)(i-1)+2m-1}$, $i=\overline{1...n+1}$ равно 32 (16, 8) битам. Раундовые функции F_0, F_1, …, $F_{(m/2)-1}$ имеют два входа и выхода, в которых длина входных и выходных блоков функций равна 32 (16, 8) битам. Длина раундовых ключей $K_{(2m+m/2)(i-1)+2m}$, $K_{(2m+m/2)(i-1)+2m+1}$, …, $K_{(2m+m/2)(i-1)+(2m+m/2)-1}$, $i=\overline{1...n}$, необязательно должна быть равной 32 (16, 8) битам.

Схема раундовой функции сети PES2m–(m/2) приведена на рис. 2, а процесс зашифрования сети приведён в (4).

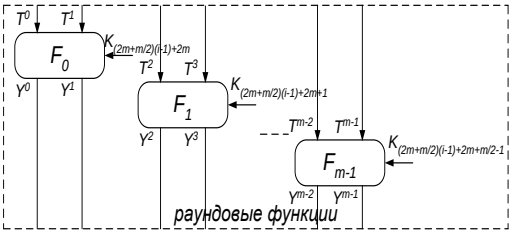

Рис. 2. Схема раундовой функции сети PES2m–(m/2)

В данной сети число общих раундовых ключей равно $(2m+m/2)n+2m$, в раундовых функциях применены раундовые ключи $K_{(2m+m/2)(i-1)+2m}$, $K_{(2m+m/2)(i-1)+2m+1}$, …, $K_{(2m+m/2)(i-1)+(2m+m/2)-1}$, $i=\overline{1...n}$, а в выходном преобразовании применены раундовые ключи $K_{(2m+m/2)n}$, $K_{(2m+m/2)n+1}$, ..., $K_{(2m+m/2)n+2m-1}$.

$$\begin{cases} X_i^0=(X_{i-1}^m(z_0)K_{(2m+m/2)(i-1)})\oplus Y^{m-1} \\ X_i^1=(X_{i-1}^{m+1}(z_0)K_{(2m+m/2)(i-1)+2m-2})\oplus Y^{m-2} \\ X_i^2=(X_{i-1}^{m+2}(z_0)K_{(2m+m/2)(i-1)+2m-3})\oplus Y^{m-3} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_i^{m-1}=(X_{i-1}^{2m-1}(z_0)K_{(2m+m/2)(i-1)+m})\oplus Y^0 \\ X_i^m=(X_{i-1}^0(z_1)K_{(2m+m/2)(i-1)+m-1})\oplus Y^{m-1} \\ X_i^{m+1}=(X_{i-1}^1(z_1)K_{(2m+m/2)(i-1)+m-2})\oplus Y^{m-2} \\ X_i^{m+2}=(X_{i-1}^2(z_1)K_{(2m+m/2)(i-1)+m-3})\oplus Y^{m-3} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_i^{2m-1}=(X_{i-1}^{m-1}(z_1)K_{(2m+m/2)(i-1)+2m-1})\oplus Y^0 \end{cases}, \; i=\overline{1...n}; \tag{4}$$

$$\begin{cases} X_{n+1}^0=(X_n^m(z_0)K_{(2m+m/2)n}) \\ X_{n+1}^1=(X_n^{m+1}(z_0)K_{(2m+m/2)n+1}) \\ X_{n+1}^2=(X_n^{m+2}(z_0)K_{(2m+m/2)n+2}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{m-1}=(X_n^{2m-1}(z_0)K_{(2m+m/2)n+m-1}) \\ X_{n+1}^m=(X_n^0(z_1)K_{(2m+m/2)n+m}) \\ X_{n+1}^{m+1}=(X_n^1(z_1)K_{(2m+m/2)n+m+1}) \\ X_{n+1}^{m+2}=(X_n^2(z_1)K_{(2m+m/2)n+m+2}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{2m-1}=(X_n^{m-1}(z_1)K_{(2m+m/2)n+2m-1}) \end{cases}, \textit{ в выходном преобразовании.}$$

Если $T0=[T^0,T^1]$, $T1=[T^2,T^3]$, ..., $T(m/2-1)=[T^{m-2},T^{m-1}]$ – входной подблок, $Y0=[Y^0,Y^1]$, $Y1=[Y^2,Y^3]$, ..., $Y(m/2-1)=[Y^{m-2},Y^{m-1}]$ – выходной подблок раундовой функции, то раундовую функцию можно представить в виде $Y0=F_0(T0,K_{(2m+m/2)(i-1)+2m})$, $Y1=F_1(T1,K_{(2m+m/2)(i-1)+2m+1})$, ..., $Y(m/2-1)=F_{m/2-1}(T(m/2-1),K_{(2m+m/2)(i-1)+2m+m/2-1})$. Здесь $T^j=(X_{i-1}^j(z_0)K_{(2m+m/2)(i-1)+j})\oplus(X_{i-1}^{m+j}(z_1)K_{(2m+m/2)(i-1)+m+j})$, $j=\overline{0...m-1}$. Для корректности формулы алгоритма шифрования раундовую функцию $Y0=F_0(T0,K_{(2m+m/2)(i-1)+2m})$ представим в виде $Y^0=F_0^0(T^0,T^1,K_{(2m+m/2)(i-1)+2m})$, $Y^1=F_0^1(T^0,T^1,K_{(2m+m/2)(i-1)+2m})$, раундовую функцию $Y1=F_1(T1,K_{(2m+m/2)(i-1)+2m+1})$ представим в виде $Y^2=F_1^0(T^2,T^3,K_{(2m+m/2)(i-1)+2m+1})$, $Y^3=F_1^1(T^2,T^3,K_{(2m+m/2)(i-1)+2m+1})$ и так далее раундовую функцию $Y(m/2-1)=F_{m/2-1}(T(m/2-1),K_{(2m+m/2)(i-1)+2m+m/2-1})$ представим в виде $Y^{m-2}=F_{m-1}^0(T^{m-2},T^{m-1},K_{(2m+m/2)(i-1)+2m+m/2-1})$, $Y^{m-1}=F_{m-1}^1(T^{m-2},T^{m-1},K_{(2m+m/2)(i-1)+2m+m/2-1})$, здесь F_i^j –выходной $j+1$ –блок раундовой функции F_i.

Генерация ключей сети PES2m–(m/2)

В сети PES2m–(m/2) в каждом раунде применяются $2m+(m/2)$ раундовые ключи и в последнем преобразовании $2m$ раундовых ключей, т.е., число всех ключей равно $(2m+m/2)n+2m$. При зашифровании из ключа K генерируются $(2m+m/2)n+2m$ раундовые ключи зашифрования K_i^c. А раундовые ключи расшифрования K_i^d вычисляются на основе K_i^c.

В сети PES2m–(m/2) ключи расшифрования выходного преобразования привязаны к ключам зашифрования следующим образом (5). Таким же образом, ключи расшифрования первого, второго, третьего и n–раунда привязаны к ключам зашифрования по формуле (6):

$$(K^d_{(2m+m/2)n}, K^d_{(2m+m/2)n+1}, K^d_{(2m+m/2)n+2}, ..., K^d_{(2m+m/2)n+m-1}, K^d_{(2m+m/2)n+m}, K^d_{(2m+m/2)n+m+1}, K^d_{(2m+m/2)n+m+2}, ...,$$
$$K^d_{(2m+m/2)n+2m-1}) = ((K^c_0)^{z_0}, (K^c_1)^{z_0}, (K^c_2)^{z_0}, ..., (K^c_{m-1})^{z_1}, (K^c_m)^{z_1}, (K^c_{m+1})^{z_1}, (K^c_{m+2})^{z_1}, ..., (K^c_{2m-1})^{z_1}). \quad (5)$$

$$(K^d_{(2m+m/2)(i-1)}, K^d_{(2m+m/2)(i-1)+1}, K^d_{(2m+m/2)(i-1)+2}, ..., K^d_{(2m+m/2)(i-1)+m-2}, K^d_{(2m+m/2)(i-1)+m-1}, K^d_{(2m+m/2)(i-1)+m},$$
$$K^d_{(2m+m/2)(i-1)+m+1}, K^d_{(2m+m/2)(i-1)+m+2}, ..., K^d_{(2m+m/2)(i-1)+2m-2}, K^d_{(2m+m/2)(i-1)+2m-1}, K^d_{(2m+m/2)(i-1)+2m}, K^d_{(2m+m/2)(i-1)+2m+1},$$
$$K^d_{(2m+m/2)(i-1)+2m+2}, ..., K^d_{(2m+m/2)(i-1)+3m-1}) = ((K^c_{(2m+m/2)(n-i+1)})^{z_0}, (K^c_{(2m+m/2)(n-i+1)+1})^{z_0}, (K^c_{(2m+m/2)(n-i+1)+2})^{z_0},$$
$$..., (K^c_{(2m+m/2)(n-i+1)+m-1})^{z_0}, (K^c_{(2m+m/2)(n-i+1)+m})^{z_1}, (K^c_{(2m+m/2)(n-i+1)+m+1})^{z_1}, (K^c_{(2m+m/2)(n-i+1)+m+2})^{z_1}, ...,$$
$$(K^c_{(2m+m/2)(n-i+1)+2m-1})^{z_1}, K^c_{(2m+m/2)(n-i)+2m}, K^c_{(2m+m/2)(n-i)+2m+1}, K^c_{(2m+m/2)(n-i)+2m+2}, ..., K^c_{(2m+m/2)(n-i)+3m-1}), \quad (6)$$
$$i = \overline{1...n}.$$

В 2, 3 и 2m–вариантов сети ключи расшифрования выходного преобразования, первого, второго, третьего и n–раунда привязаны к ключам зашифрования по формуле (5) и (6).

Структура сети PES2m–(m/4)

В сети PES2m–(m/4) длина подблоков X^0, X^1, …, X^{2m-1}, длина раундовых ключей $K_{(2m+m/4)(i-1)}$, $K_{(2m+m/4)(i-1)+1}$, …, $K_{(2m+m/4)(i-1)+2m-1}$, $i = \overline{1...n+1}$ равно 32 (16, 8) битам. Раундовые функции F_0, F_1, …, $F_{(m/4)-1}$ имеют четыре входа и выхода, в которые длина входных и выходных блоков функций равна 32 (16, 8) битам. Длина раундовых ключей $K_{(2m+m/4)(i-1)+2m}$, $K_{(2m+m/4)(i-1)+2m+1}$, …, $K_{(2m+m/4)(i-1)+2m+m/4-1}$, $i = \overline{1...n}$ необязательно должна быть равной 32 (16, 8) битам. Схема раундовой функции сети PES2m–(m/4) приведена на рис. 3 и процесс зашифрования приведен в (7) формуле.

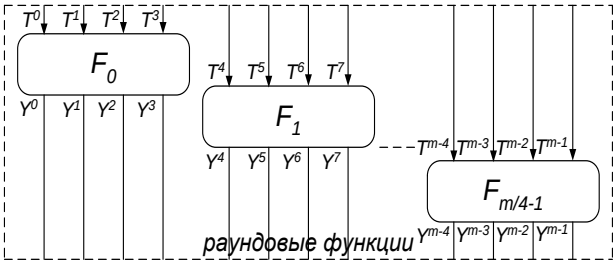

Рис. 3. Схема раундовой функции сети PES2m–(m/4)

В данной сети число общих раундовых ключей равно (2m+m/4)n+2m, в раундовых функциях применены раундовые ключи $K_{(2m+m/4)(i-1)+2m}$, $K_{(2m+m/4)(i-1)+2m+1}$, …, $K_{(2m+m/4)(i-1)+2m+m/4-1}$, $i = \overline{1...n}$, а в выходном преобразовании применены раундовые ключи $K_{(2m+m/4)n}$, $K_{(2m+m/4)n+1}$, $K_{(2m+m/4)n+2}$, …, $K_{(2m+m/4)n+2m-1}$.

Если $T0 = [T^0, T^1, T^2, T^3]$, $T1 = [T^4, T^5, T^6, T^7]$, …, $T(m/4-1) = [T^{m-4}, T^{m-3}, T^{m-2}, T^{m-1}]$ – входной подблок, $Y0 = [Y^0, Y^1, Y^2, Y^3]$, $Y1 = [Y^4, Y^5, Y^6, Y^7]$, …, $Y(m/4-1) = [Y^{m-4}, Y^{m-3}, Y^{m-2}, Y^{m-1}]$ – выходной подблок раундовой функции, то раундовую функцию можно представить в виде

$$Yj = F_j(Tj, K_{(2m+m/4)(i-1)+2m+j}), \quad j = \overline{0...(m/4)-1}.$$

Здесь $T^j = (X^j_{i-1}(z_j))K_{(2m+m/4)(i-1)+j}) \oplus (X^{m+j}_{i-1}(z_{m-1-j}))K_{(2m+m/4)(i-1)+m+j})$, $j = \overline{0...m-1}$.

Для корректности формулы алгоритма шифрования раундовую функцию $Y0 = F_0(T0, K_{(2m+m/4)(i-1)+2m})$ представим в виде

$$Y^0 = F^0_0(T^0, T^1, T^2, T^3, K_{(2m+m/2)(i-1)+2m}),$$
$$Y^1 = F^1_0(T^0, T^1, T^2, T^3, K_{(2m+m/2)(i-1)+2m}),$$
$$Y^2 = F^2_0(T^0, T^1, T^2, T^3, K_{(2m+m/2)(i-1)+2m}),$$
$$Y^3 = F^3_0(T^0, T^1, T^2, T^3, K_{(2m+m/2)(i-1)+2m}),$$

раундовую функцию $Y1 = F_1(T1, K_{(2m+m/4)(i-1)+2m})$ представим в виде

$$Y^4 = F^0_0(T^4, T^5, T^6, T^7, K_{(2m+m/2)(i-1)+2m+1}),$$
$$Y^5 = F^1_0(T^4, T^5, T^6, T^7, K_{(2m+m/2)(i-1)+2m+1}),$$
$$Y^6 = F^2_0(T^4, T^5, T^6, T^7, K_{(2m+m/2)(i-1)+2m+1}),$$
$$Y^7 = F^3_0(T^4, T^5, T^6, T^7, K_{(2m+m/2)(i-1)+2m+1})$$

и так далее раундовую функцию $Y(m/4-1) = F_{m/4-1}(T(m/4-1), K_{(2m+m/4)(i-1)+2m+m/4-1})$ представим в виде

$$Y^{m-4} = F^0_{m/4-1}(T^{m-4}, T^{m-3}, T^{m-2}, T^{m-1}, K_{(2m+m/4)(i-1)+2m+m/4-1}),$$
$$Y^{m-3} = F^1_{m/4-1}(T^{m-4}, T^{m-3}, T^{m-2}, T^{m-1}, K_{(2m+m/4)(i-1)+2m+m/4-1}),$$
$$Y^{m-2} = F^2_{m/4-1}(T^{m-4}, T^{m-3}, T^{m-2}, T^{m-1}, K_{(2m+m/4)(i-1)+2m+m/4-1}),$$
$$Y^{m-1} = F^3_{m/4-1}(T^{m-4}, T^{m-3}, T^{m-2}, T^{m-1}, K_{(2m+m/4)(i-1)+2m+m/4-1}).$$

$$\begin{cases} X_i^0 = (X_{i-1}^m(z_0)K_{(2m+m/4)(i-1)}) \oplus Y^{m-1} \\ X_i^1 = (X_{i-1}^{m+1}(z_0)K_{(2m+m/4)(i-1)+2m-2}) \oplus Y^{m-2} \\ X_i^2 = (X_{i-1}^{m+2}(z_0)K_{(2m+m/4)(i-1)+2m-3}) \oplus Y^{m-3} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_i^{m-1} = (X_{i-1}^{2m-1}(z_0)K_{(2m+m/4)(i-1)+m}) \oplus Y^0 \\ X_i^m = (X_{i-1}^0(z_1)K_{(2m+m/4)(i-1)+m-1}) \oplus Y^{m-1} \\ X_i^{m+1} = (X_{i-1}^1(z_1)K_{(2m+m/4)(i-1)+m-2}) \oplus Y^{m-2} \\ X_i^{m+2} = (X_{i-1}^2(z_1)K_{(2m+m/4)(i-1)+m-3}) \oplus Y^{m-3} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_i^{2m-1} = (X_{i-1}^{m-1}(z_1)K_{(2m+m/4)(i-1)+2m-1}) \oplus Y^0 \end{cases}, \ i = \overline{1...n};$$

$$\begin{cases} X_{n+1}^0 = (X_n^m(z_0)K_{(2m+m/4)n}) \\ X_{n+1}^1 = (X_n^{m+1}(z_0)K_{(2m+m/4)n+1}) \\ X_{n+1}^2 = (X_n^{m+2}(z_0)K_{(2m+m/4)n+2}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{m-1} = (X_n^{2m-1}(z_0)K_{(2m+m/4)n+m-1}) \\ X_{n+1}^m = (X_n^0(z_1)K_{(2m+m/4)n+m}) \\ X_{n+1}^{m+1} = (X_n^1(z_1)K_{(2m+m/4)n+m+1}) \\ X_{n+1}^{m+2} = (X_n^2(z_1)K_{(2m+m/4)n+m+2}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{2m-1} = (X_n^{m-1}(z_1)K_{(2m+m/4)n+2m-1}) \end{cases}, \textit{ в выходном преобразовании.} \quad (7)$$

Генерация ключей сети PES2m–(m/4)

В n–раундовой сети PES2m–(m/4) в каждом раунде применяются $2m+(m/4)$ раундовые ключи и в последнем преобразовании $2m$ раундовых ключей, т.е., число всех ключей равно $(2m+m/4)n+2m$.

Ключи расшифрования выходного преобразования привязаны к ключам зашифрования следующим образом:

$$(K_{(2m+m/4)n}^d, K_{(2m+m/4)n+1}^d, K_{(2m+m/4)n+2}^d, ..., K_{(2m+m/4)n+m-1}^d, K_{(2m+m/4)n+m}^d, K_{(2m+m/4)n+m+1}^d, K_{(2m+m/4)n+m+2}^d, ...,$$
$$K_{(2m+m/4)n+2m-1}^d) = ((K_0^c)^{z_0}, (K_1^c)^{z_0}, (K_2^c)^{z_0}, ..., (K_{m-1}^c)^{z_0}, (K_m^c)^{z_1}, (K_{m+1}^c)^{z_1}, (K_{m+2}^c)^{z_1}, ..., (K_{2m-1}^c)^{z_1}). \quad (8)$$

$$(K_{(2m+m/4)(i-1)}^d, K_{(2m+m/4)(i-1)+1}^d, K_{(2m+m/4)(i-1)+2}^d, ..., K_{(2m+m/4)(i-1)+m-2}^d, K_{(2m+m/4)(i-1)+m-1}^d, K_{(2m+m/4)(i-1)+m}^d,$$
$$K_{(2m+m/4)(i-1)+m+1}^d, K_{(2m+m/4)(i-1)+m+2}^d, ..., K_{(2m+m/4)(i-1)+2m-2}^d, K_{(2m+m/4)(i-1)+2m-1}^d, K_{(2m+m/4)(i-1)+2m}^d,$$
$$K_{(2m+m/4)(i-1)+2m+1}^d, K_{(2m+m/4)(i-1)+2m+2}^d, ..., K_{(2m+m/4)(i-1)+3m-1}^d) = ((K_{(2m+m/4)(n-i+1)}^c)^{z_0}, (K_{(2m+m/4)(n-i+1)+1}^c)^{z_0},$$
$$(K_{(2m+m/4)(n-i+1)+2}^c)^{z_0}, ..., (K_{(2m+m/4)(n-i+1)+m-1}^c)^{z_0}, (K_{(2m+m/4)(n-i+1)+m}^c)^{z_1}, (K_{(2m+m/4)(n-i+1)+m+1}^c)^{z_1},$$
$$(K_{(2m+m/4)(n-i+1)+m+2}^c)^{z_1}, ..., (K_{(2m+m/4)(n-i+1)+2m-1}^c)^{z_1}, K_{(2m+m/4)(n-i)+2m}^c, K_{(2m+m/4)(n-i)+2m+1}^c,$$
$$K_{(2m+m/4)(n-i)+2m+2}^c, ..., K_{(2m+m/4)(n-i)+3m-1}^c), \ i = \overline{1...n}. \quad (9)$$

Таким же образом, ключи расшифрования второго, третьего и n–раунда привязаны к ключам зашифрования по формуле (9).

Структура сети PES2m–1

В сети PES2m–1 длина подблоков X^0, X^1, …, X^{2m-1} и длина раундовых ключей $K_{(2m+1)(i-1)}$, $K_{(2m+1)(i-1)+1}$, …, $K_{(2m+1)(i-1)+2m-1}$, $i = \overline{1...n+1}$ равна 32 (16, 8) битам. Раундовая функции F имеет m входа и выхода, в которых длина входных и выходных блоков функций равна 32 (16, 8) битам. Длина раундового ключа $K_{(2m+1)(i-1)+2m}$, $i = \overline{1...n}$, необязательно должна быть равной 32 (16, 8) битам. Схема раундовой функции сети PES2m–1 приведена на рис. 4, а процесс зашифрования приведен в (10) формуле.

В данной сети число общих раундовых ключей равно $(2m+1)n+2m$, в раундовой функции применен раундовый ключ $K_{(2m+1)(i-1)+2m}$, $i = \overline{1...n}$, а в выходном преобразовании применены раундовые ключи $K_{(2m+1)n}$, $K_{(2m+1)n+1}$, …, $K_{(2m+1)n+2m-1}$.

$$
\begin{cases}
X_i^0 = (X_{i-1}^m(z_0)K_{(2m+1)(i-1)}) \oplus Y^{m-1} \\
X_i^1 = (X_{i-1}^{m+1}(z_0)K_{(2m+1)(i-1)+2m-2}) \oplus Y^{m-2} \\
X_i^2 = (X_{i-1}^{m+2}(z_0)K_{(2m+1)(i-1)+2m-3}) \oplus Y^{m-3} \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_i^{m-1} = (X_{i-1}^{2m-1}(z_0)K_{(2m+1)(i-1)+m}) \oplus Y^0 \\
X_i^m = (X_{i-1}^0(z_1)K_{(2m+1)(i-1)+m-1}) \oplus Y^{m-1} \\
X_i^{m+1} = (X_{i-1}^1(z_1)K_{(2m+1)(i-1)+m-2}) \oplus Y^{m-2} \\
X_i^{m+2} = (X_{i-1}^2(z_1)K_{(2m+1)(i-1)+m-3}) \oplus Y^{m-3} \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_i^{2m-1} = (X_{i-1}^{m-1}(z_1)K_{(2m+1)(i-1)+2m-1}) \oplus Y^0
\end{cases}, \; i = \overline{1...n};
$$

$$
\begin{cases}
X_{n+1}^0 = (X_n^m(z_0)K_{(2m+m/4)n}) \\
X_{n+1}^1 = (X_n^{m+1}(z_0)K_{(2m+m/4)n+1}) \\
X_{n+1}^2 = (X_n^{m+2}(z_0)K_{(2m+m/4)n+2}) \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_{n+1}^{m-1} = (X_n^{2m-1}(z_0)K_{(2m+m/4)n+m-1}) \\
X_{n+1}^m = (X_n^0(z_1)K_{(2m+m/4)n+m}) \\
X_{n+1}^{m+1} = (X_n^1(z_1)K_{(2m+m/4)n+m+1}) \\
X_{n+1}^{m+2} = (X_n^2(z_1)K_{(2m+m/4)n+m+2}) \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_{n+1}^{2m-1} = (X_n^{m-1}(z_1)K_{(2m+m/4)n+2m-1})
\end{cases}, \textit{ в выходном преобразовании.}
\tag{10}
$$

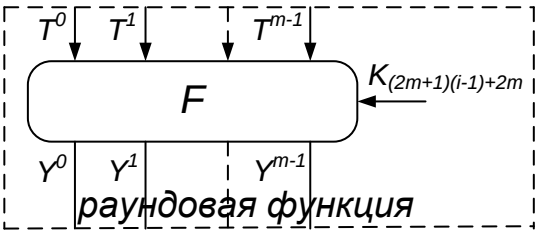

Рис. 4. Схема раундовой функции сети PES2m–1

Если берем $T = [T^0, T^1, T^2, ..., T^{m-1}]$ – в качестве входного подблока, $Y = [Y^0, Y^1, Y^3, ..., Y^{m-1}]$ – в качестве выходного подблока раундовой функции, то раундовую функцию можно представить в виде $Y = F(T, K_{(2m+1)(i-1)+2m})$. Здесь $T^j = (X_{i-1}^j(z_0)K_{(2m+1)(i-1)+j}) \oplus (X_{i-1}^{m+j}(z_1)K_{(2m+1)(i-1)+m+j})$, $j = \overline{0...m-1}$. Для корректности формулы алгоритма шифрования раундовую функцию $Y = F(T, K_{(2m+1)(i-1)+2m})$ представим в виде $Y^0 = F^0(T^0, T^1, ..., T^{m-1}, K_{(2m+1)(i-1)+2m})$, $Y^1 = F^1(T^0, T^1, ..., T^{m-1}, K_{(2m+1)(i-1)+2m})$, ..., $Y^{m-1} = F^{m-1}(T^0, T^1, ..., T^{m-1}, K_{(2m+1)(i-1)+2m})$.

Генерация ключей сети PES2m–1

В n–раундовой сети PES2m–1 в каждом раунде применяются $2m+1$ раундовые ключи и в последнем преобразовании $2m$ раундовых ключей, т.е., число всех ключей равно $(2m+1)n+2m$.

Ключи расшифрования выходного преобразования привязаны к ключам зашифрования следующим образом (11). Таким же образом ключи расшифрования второго, третьего и n–раунда привязаны к ключам зашифрования по формуле (12).

$$
\begin{aligned}
&(K_{(2m+1)n}^d, K_{(2m+1)n+1}^d, K_{(2m+1)n+2}^d, ..., K_{(2m+1)n+m-1}^d, K_{(2m+1)n+m}^d, K_{(2m+1)n+m+1}^d, K_{(2m+1)n+m+2}^d, ..., \\
&K_{(2m+1)n+2m-1}^d) = ((K_0^c)^{z_0}, (K_1^c)^{z_0}, (K_2^c)^{z_0}, ..., (K_{m-1}^c)^{z_0}, (K_m^c)^{z_1}, (K_{m+1}^c)^{z_1}, (K_{m+2}^c)^{z_1}, ..., (K_{2m-1}^c)^{z_1}).
\end{aligned}
\tag{11}
$$

$$
\begin{aligned}
&(K_{(2m+1)(i-1)}^d, K_{(2m+1)(i-1)+1}^d, K_{(2m+1)(i-1)+2}^d, ..., K_{(2m+1)(i-1)+m-2}^d, K_{(2m+1)(i-1)+m-1}^d, K_{(2m+1)(i-1)+m}^d, K_{(2m+1)(i-1)+m+1}^d, \\
&K_{(2m+1)(i-1)+m+2}^d, ..., K_{(2m+1)(i-1)+2m-2}^d, K_{(2m+1)(i-1)+2m-1}^d, K_{(2m+1)(i-1)+2m}^d, K_{(2m+1)(i-1)+2m+1}^d, K_{(2m+1)(i-1)+2m+2}^d, ..., \\
&K_{(2m+1)(i-1)+3m-1}^d) = ((K_{(2m+1)(n-i+1)}^c)^{z_0}, (K_{(2m+1)(n-i+1)+1}^c)^{z_0}, (K_{(2m+1)(n-i+1)+2}^c)^{z_0}, ..., (K_{(2m+1)(n-i+1)+m-1}^c)^{z_0}, \\
&(K_{(2m+1)(n-i+1)+m}^c)^{z_1}, (K_{(2m+1)(n-i+1)+m+1}^c)^{z_1}, (K_{(2m+1)(n-i+1)+m+2}^c)^{z_1}, ..., (K_{(2m+1)(n-i+1)+2m-1}^c)^{z_1}, K_{(2m+1)(n-i)+2m}^c, \\
&K_{(2m+1)(n-i)+2m+1}^c, K_{(2m+1)(n-i)+2m+2}^c, ..., K_{(2m+1)(n-i)+3m-1}^c), \; i = \overline{1...n}.
\end{aligned}
\tag{12}
$$

Структура сети RFWKPES2m–m

В сети RFWKPES2m–m длина подблоков X_i^0, X_i^1, …, X_i^{2m-1}, длина раундовых ключей, а также длина входных и выходных блоков раундовых функций F_0, F_1, …, F_{m-1}. равна 32 (16, 8) бит. Схема n–раундовой сети RFWKPES2m–m приведена на рис. 5 и процесс шифрования приведен в (13) формуле.

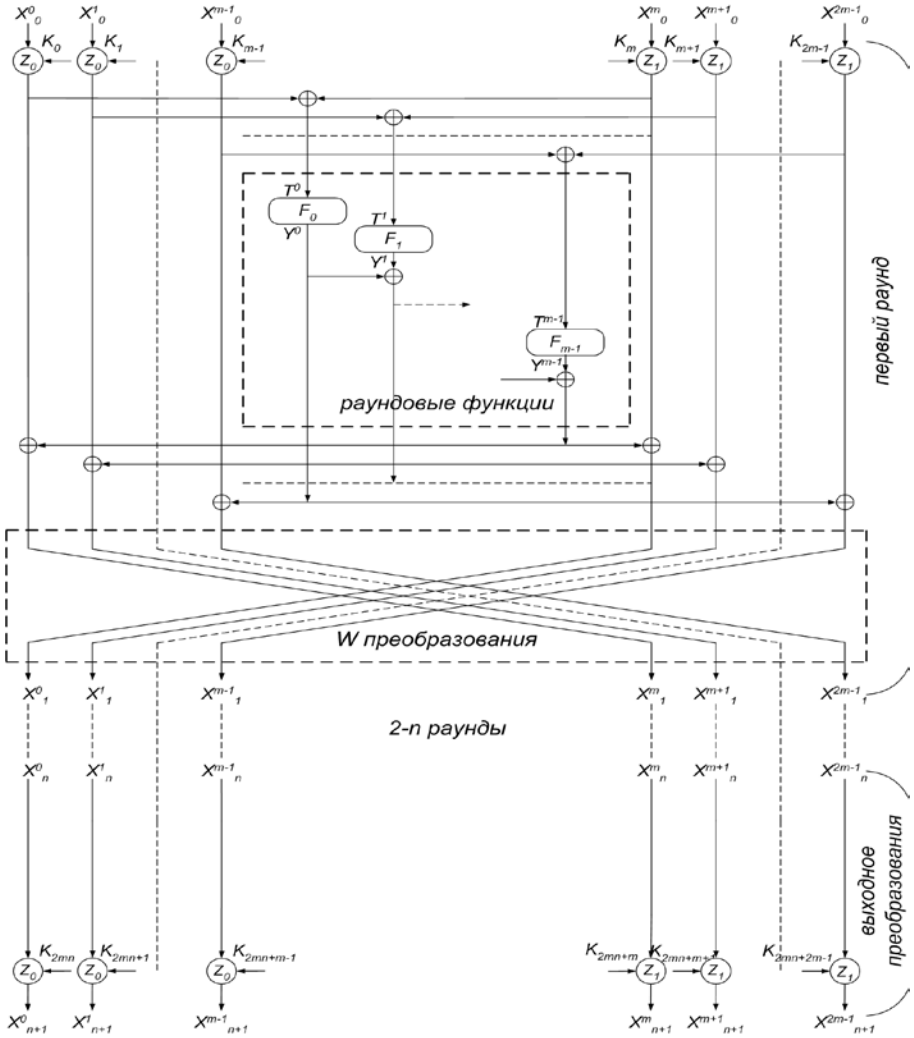

Рис. 5. Схема *n*–раундовой сети RFWKPES2m–m

В сети RFWKPES2m–m раундовые функции можно представит в виде $Y^j = F_j(T^j)$, $j = \overline{0...m-1}$. Здесь $T^j = (X_{i-1}^j(z_0)K_{2m(i-1)+j}) \oplus (X_{i-1}^{j+m}(z_1)K_{2m(i-1)+m+j})$ – входные значения раундовых функций F_0, F_1, …, F_{m-1}.

$$
\begin{cases}
X_i^0 = (X_{i-1}^m(z_0)K_{2m(i-1)}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-1} \\
X_i^1 = (X_{i-1}^{m+1}(z_0)K_{2m(i-1)+2m-2}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-2} \\
X_i^2 = (X_{i-1}^{m-2}(z_0)K_{2m(i-1)+2m-3}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-3} \\
..... \\
X_i^{m-1} = (X_{i-1}^{2m-1}(z_0)K_{2m(i-1)+m}) \oplus Y^0 \quad , \ i = \overline{1...n}; \\
X_i^m = (X_{i-1}^0(z_1)K_{2m(i-1)+m-1}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-1} \\
X_i^{m+1} = (X_{i-1}^1(z_1)K_{2m(i-1)+m-2}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-2} \\
X_i^{m+2} = (X_{i-1}^2(z_1)K_{2m(i-1)+m-3}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-3} \\
..... \\
X_i^{2m-1} = (X_{i-1}^{m-1}(z_1)K_{2m(i-1)+2m-1}) \oplus Y^0
\end{cases}
$$

$$
\begin{cases}
X_{n+1}^0 = (X_n^0(z_0)K_{2mn}) \\
X_{n+1}^1 = (X_n(z_0)K_{2mn+1}) \\
X_{n+1}^2 = (X_n^2(z_0)K_{2mn+2}) \\
..... \\
X_{n+1}^{m-1} = (X_n^{m-1}(z_0)K_{2mn+m-1}) \quad , \textit{в выходном преобразовании.} \\
X_{n+1}^m = (X_n^m(z_1)K_{2mn+m}) \\
X_{n+1}^{m+1} = (X_n^{m+1}(z_1)K_{2mn+m+1}) \\
X_{n+1}^{m+2} = (X_n^{m+2}(z_1)K_{2mn+m+2}) \\
..... \\
X_{n+1}^{2m-1} = (X_n^{2m-1}(z_1)K_{2mn+2m-1})
\end{cases}
\qquad (13)
$$

Структура сети RFWKPES2m–(m/2)

В сети RFWKPES2m–(m/2), как у сети RFWKPES2m–m, длина подблоков X_i^0, X_i^1, …, X_i^{2m-1}, длина раундовых ключей, а также длина входных и выходных блоков функций F_0, F_1, …, $F_{(m/2)-1}$ равна 32 (16, 8) битам. Схема раундовой функции сети RFWKPES2m–(m/2) приведена на рис. 6 и процесс шифрования приведен в (14) формуле.

$$\begin{cases} X_i^0 = (X_{i-1}^m(z_0)K_{2m(i-1)}) \oplus Y^{m-1} \\ X_i^1 = (X_{i-1}^{m+1}(z_0)K_{2m(i-1)+2m-2}) \oplus Y^{m-2} \\ X_i^2 = (X_{i-1}^{m-2}(z_0)K_{2m(i-1)+2m-3}) \oplus Y^{m-3} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_i^{m-1} = (X_{i-1}^{2m-1}(z_0)K_{2m(i-1)+m}) \oplus Y^0 \\ X_i^m = (X_{i-1}^0(z_1)K_{2m(i-1)+m-1}) \oplus Y^{m-1} \\ X_i^{m+1} = (X_{i-1}^1(z_1)K_{2m(i-1)+m-2}) \oplus Y^{m-2} \\ X_i^{m+2} = (X_{i-1}^2(z_1)K_{2m(i-1)+m-3}) \oplus Y^{m-3} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_i^{2m-1} = (X_{i-1}^{m-1}(z_1)K_{2m(i-1)+2m-1}) \oplus Y^0 \end{cases}, \; i = \overline{1...n}; \quad (14)$$

$$\begin{cases} X_{n+1}^0 = (X_n^0(z_0)K_{2mn}) \\ X_{n+1}^1 = (X_n(z_0)K_{2mn+1}) \\ X_{n+1}^2 = (X_n^2(z_0)K_{2mn+2}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{m-1} = (X_n^{m-1}(z_0)K_{2mn+m-1}), \textit{в выходном преобразовании.} \\ X_{n+1}^m = (X_n^m(z_1)K_{2mn+m}) \\ X_{n+1}^{m+1} = (X_n^{m+1}(z_1)K_{2mn+m+1}) \\ X_{n+1}^{m+2} = (X_n^{m+2}(z_1)K_{2mn+m+2}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{2m-1} = (X_n^{2m-1}(z_1)K_{2mn+2m-1}) \end{cases}$$

Если берем $T0 = [T^0, T^1]$, $T1 = [T^2, T^3]$, …, $T(m/2-1) = [T^{m-2}, T^{m-1}]$ в качестве входного значения, $Y0 = [Y^0, Y^1]$, $Y1 = [Y^2, Y^3]$, …, $Y(m/2-1) = [Y^{m-2}, Y^{m-1}]$ в качестве выходного значения раундовой функции, то раундовую функцию можно представить в виде $Yj = F_j(Tj)$, $j = \overline{0...(m/2)-1}$. Здесь $T^j = (X_{i-1}^j(z_0)K_{2m(i-1)+j}) \oplus (X_{i-1}^{m+j}(z_1)K_{2m(i-1)+m+j})$, $j = \overline{0...m-1}$.

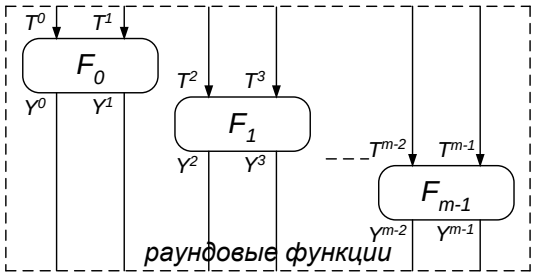

Рис. 6. Схема раундовой функции сети RFWKPES2m–(m/2)

Для корректности формулы алгоритма шифрования раундовую функцию $Y0 = F_0(T0)$ представим в виде $Y^0 = F_0^0(T^0, T^1)$, $Y^1 = F_0^1(T^0, T^1)$, 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 т.д. раундовую функцию $Y(m/2-1) = F_{(m/2)-1}(T(m/2-1))$ представим в виде $Y^{m-2} = F_{m-1}^0(T^{m-2}, T^{m-1})$, $Y^{m-1} = F_{m-1}^1(T^{m-2}, T^{m-1})$.

Структура сети RFWKPES2m–(m/4)

В сети RFWKPES2m–(m/4) длина подблоков X_i^0, X_i^1, …, X_i^{2m-1}, длина раундовых ключей, а также длина входных и выходных блоков функций F_0, F_1, …, $F_{(m/4)-1}$ равна 32 (16, 8) битам. Схема раундовой функции сети RFWKPES2m–(m/4) приведена на рис. 7 и процесс шифрования приведен в (14) формуле.

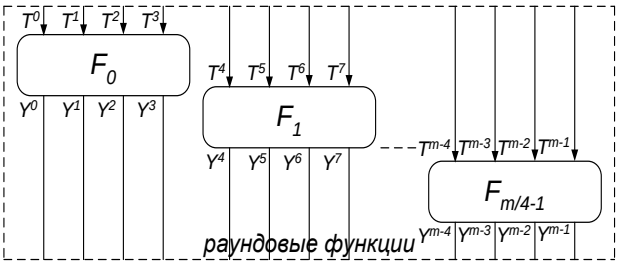

Рис. 7. Схема раундовой функции сети RFWKPES2m–(m/4)

Если берем $T0 = [T^0, T^1, T^2, T^3]$, $T1 = [T^4, T^5, T^6, T^7]$, …, $T(m/4-1) = [T^{m-4}, T^{m-3}, T^{m-2}, T^{m-1}]$ в качестве входного значения, $Y0 = [Y^0, Y^1, Y^2, Y^3]$, $Y1 = [Y^4, Y^5, Y^6, Y^7]$, …, $Y(m/4-1) = [Y^{m-4}, Y^{m-3}, Y^{m-2}, Y^{m-1}]$ в качестве выходного значения раундовой функции, то раундовую функцию можно представить в виде $Yj = F_j(Tj)$, $j = \overline{0...(m/4)-1}$. Для корректности формулы алгоритма шифрования раундовую функцию $Y0 = F_0(T0)$ представим в виде $Y^0 = F_0^0(T^0, T^1, T^2, T^3)$, $Y^1 = F_0^1(T^0, T^1, T^2, T^3)$, $Y^2 = F_0^2(T^0, T^1, T^2, T^3)$, $Y^3 = F_0^3(T^0, T^1, T^2, T^3)$, раундовую функцию $Y1 = F_1(T1)$ представим в виде $Y^4 = F_0^0(T^4, T^5, T^6, T^7)$, $Y^5 = F_0^1(T^4, T^5, T^6, T^7)$, $Y^6 = F_0^2(T^4, T^5, T^6, T^7)$, $Y^7 = F_0^3(T^4, T^5, T^6, T^7)$ и т.п. раундовую функцию $Y(m/4-1) = F_{m/4-1}(T(m/4-1))$ представим в виде $Y^{m-4} = F_{m/4-1}^0(T^{m-4}, T^{m-3}, T^{m-2}, T^{m-1})$, $Y^{m-3} = F_{m/4-1}^1(T^{m-4}, T^{m-3}, T^{m-2}, T^{m-1})$, $Y^{m-2} = F_{m/4-1}^2(T^{m-4}, T^{m-3}, T^{m-2}, T^{m-1})$, $Y^{m-1} = F_{m/4-1}^3(T^{m-4}, T^{m-3}, T^{m-2}, T^{m-1})$.

Структура сети RFWKPES2m–1

В сети RFWKPES2m–1 длина подблоков X_i^0, X_i^1, …, X_i^{2m-1}, длина раундовых ключей, а также длина входных и выходных блоков функции F равна 32 (16, 8) битам. Схема раундовой функции сети RFWKPES2m–1 приведена на рис. 8 и процесс шифрования приведен в (14) формуле.

Если берем $T = [T^0, T^1, ..., T^{m-1}]$ в качестве входного значения, $Y = [Y^0, Y^1, ..., Y^{m-1}]$ в качестве выходного значения раундовой функции, то раундовую функцию можно представить в виде $Y = F(T)$. Для корректности формулы алгоритма шифрования раундовую функцию $Y = F(T)$

представим в виде $Y^0 = F^0(T^0,T^1,...,T^{m-1})$, $Y^1 = F^1(T^0,T^1,...,T^{m-1})$, ..., $Y^{m-1} = F^{m-1}(T^0,T^1,...,T^{m-1})$.

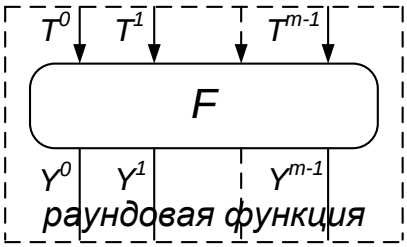

Рис. 8. Схема раундовой функции сети RFWKPES2m–1

В сетях RFWKPES2m–(m/2), RFWKPES2m–(m/4) и RFWKPES2m–1 формула шифрования одинакова, только отличается видом функции. Например, если в сети RFWKPES2m–1 $Y^0 = F^0(T^0,T^1,...,T^{m-1})$, $Y^1 = F^1(T^0,T^1,...,T^{m-1})$, в сети RFWKPES2m–(m/2) $Y^0 = F_0^0(T^0,T^1)$, $Y^1 = F_0^1(T^0,T^1)$ и в сети RFWKPES2m–(m/4) $Y^0 = F_0^0(T^0,T^1,T^2,T^3)$, $Y^1 = F_0^1(T^0,T^1,T^2,T^3)$.

Как у сети PES2m–m, на сетях RFWKPES2m–m, PES2m–(m/2), RFWKPES2m–(m/2), PES2m–(m/4), RFWKPES2m–(m/4) и PES2m–1, RFWKPES2m–1 имеет 2*m* вариантов сети на основе замены подблоков.

Генерация ключей RFWKPES2m–m, RFWKPES2m–(m/2), RFWKPES2m–(m/4), RFWKPES2m–1

В *n*-раундовой сети RFWKPES2m–m, RFWKPES2m–(m/2), RFWKPES2m–(m/4), RFWKPES2m–1 в каждом раунде применяются 2*m* раундовые ключи и в последнем преобразовании 2*m* раундовых ключей, т.е., число всех ключей равно 2*mn*+2*m*.

В сетях RFWKPES2m–m, RFWKPES2m–(m/2), RFWKPES2m–(m/4) и RFWKPES2m–1 ключи расшифрования выходного преобразования привязаны к ключам зашифрования следующим образом:

$$(K_{2mn}^d, K_{2mn+1}^d, K_{2mn+2}^d, ..., K_{2mn+m-1}^d, K_{2mn+m}^d,$$
$$K_{2mn+m+1}^d, K_{2mn+m+2}^d, ..., K_{2mn+2m-1}^d) = ((K_0^c)^{z_0}, (K_1^c)^{z_0},$$
$$(K_2^c)^{z_0}, ..., (K_{m-1}^c)^{z_0}, (K_m^c)^{z_1}, (K_{m+1}^c)^{z_1}, (K_{m+2}^c)^{z_1}, ..., (K_{2m-1}^c)^{z_1}). \quad (15)$$

Таким же образом ключи расшифрования первого, второго, третьего и *n*–раунда привязаны к ключам зашифрования по формуле (16).

$$(K_{2m(i-1)}^d, K_{2m(i-1)+1}^d, K_{2m(i-1)+2}^d, ..., K_{2m(i-1)+m-2}^d, K_{2m(i-1)+m-1}^d, K_{2m(i-1)+m}^d, K_{2m(i-1)+m+1}^d, K_{2m(i-1)+m+2}^d, ...,$$
$$K_{2m(i-1)+2m-2}^d, K_{2m(i-1)+2m-1}^d) = ((K_{2m(n-i+1)}^c)^{z_0}, (K_{2m(n-i+1)+1}^c)^{z_0}, (K_{2m(n-i+1)+2}^c)^{z_0}, ..., (K_{2m(n-i+1)+m-1}^c)^{z_0},$$
$$(K_{2m(n-i+1)+m}^c)^{z_1}, (K_{2m(n-i+1)+m+1}^c)^{z_1}, (K_{2m(n-i+1)+m+2}^c)^{z_1}, ..., (K_{2m(n-i+1)+2m-1}^c)^{z_1}), i = \overline{1...n}. \quad (16)$$

Заключение

В статье разработаны сети, состоящие из 2m подблоков. Характеристика сетей приведена в табл. 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.

Характеристика сетей Таблица 1

Сеть	Число раундовых функции	Число раундовых ключей	Число раундовых ключей, применяемых в функциях
PES2m–m	m	3mn+2m	m
PES2m–(m/2)	m/2	(2m+m/2)n+2m	m/2
PES2m–(m/4)	m/4	(2m+m/4)n+2m	m/4
PES2m–1	1	(2m+1)n+2m	1
RFWKPES2m–m	m	2mn+2m	0
RFWKPES2m–(m/2)	m/2	2mn+2m	0
RFWKPES2m–(m/4)	m/4	2mn+2m	0
RFWKPES2m–1	1	2mn+2m	0

На основе приведенных сетей, при длине подблоков X_i^0, X_i^1, …, X_i^{2m-1} равным 32 бит можно построить алгоритм шифрования длиной блока *64m* бит, при длине подблоков равным 16 битам можно построить алгоритм шифрования длиной блока *32m* бит и при длине подблоков равным 8 битам можно построить алгоритм шифрования длиной блока *16m* бит. Если выбрать в качестве операций z_0, z_1 операции mul, add и xor, все возможные варианты данного выбора равны 9. Кроме этого, в сети имеются 2*m* варианта.

Выводы

Преимущество сетей состоит в том, что при зашифровании и расшифровании используется единственный алгоритм. Это даёт удобство при создании аппаратного и программно–аппаратных средств. Потому что, при зашифровании и расшифровании используется одно аппаратное или программно–аппаратное средство.

Литература

[1] Арипов М.М., Туйчиев Г.Н. Сеть IDEA4–2, состоящая из двух раундовых функции // Инфокоммуникации: Сети–Технологии–Решения. – Ташкент, 2012 г., №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 г., с. 16–19.

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

[4] Туйчиев Г.Н. Сеть IDEA8–4, состоящая из четырех раундовых функции // Инфоком-муникации: Сети–Технологии–Решения. – Ташкент, 2013 г.. №2, с. 55-59.

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

[6] Туйчиев Г.Н. О сети PES16–8, состоящей из восьми раундовых функций // Защита информации, Киев, 2014 г, Том 16, №4, с. 318-322.

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

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

[9] Туйчиев Г.Н. О сетях PES4–1 и RFWKPES4–2, RFWKPES4–1, разработанных на основе сети PES4–2 // Проблемы информатики и энергетики, – Ташкент, 2015 г., №1, с. 97–103.

[10] Туйчиев Г.Н. О сетях PES8-2 и PES8-1, разработанные на основе сети PES8-4 // Материалы международной научной конференции «Актуаль-ные проблемы прикладной математики и информационных технологий Аль–Хоразми 2014», Том № II, Ташкент, 2014 г., с. 28–32.

[11] Туйчиев Г.Н. О сетях PES32–8, PES32–4, PES32–2 и PES32–1, созданных на основе сети PES32–16 // Безпека інформації, К., 2014. Том 20, №2, 164-168 стр.

[12] 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 г., с. 32–36.

[13] 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.

[14] Горбенко І.Д. Перспективний блоковий симетричний шифр «Мухомор». Основні положення та специфікація / І.Д. Горбенко, В.І. Долгов, Р.В. Олійников та ін. // Прикладная радио-электроника. – 2007. – Т. 6, № 2. – С. 147-157.

[15] Junod P., Vaudenay S. FOX: a new family of block ciphers. // In 11th Selected Areas in Cryptography (SAC) Workshop, LNCS 3357, Springer–Verlag, pp. 114–129.

[16] 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

[17] Lai X., Massey J.L. and Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology, Proceedings of Eurocrypt 1991, pp. 17-38, 1991

[18] 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.

[19] Nakahara J. On the Design of IDEA-128 // http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2005/00.pdf

[20] 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.

[21] Nakahara J., Rijmen V., Preneel B., Vandewalle J. The MESH Block Ciphers // WISA 2003. LNCS, vol. 2908, pp. 458–473.

УДК 003.056.55 (045)

Туйчієв Г.Н. Про мережу PES2m-m, що складаються з m раундових функцій та її модифікації

Анотація. *На сьогодні одним з найбільш ефективних методів побудови симетричних блокових шифрів є використання так званих мереж Фейстеля. У цій статті на основі схеми Лай-Массі розроблені мережі, складаються з 2m підблоків. У розроблених мережах, аналогічно мережі Фейстеля, при зашифруванні і розшифруванні використовується один і той же алгоритм і в якості раундових функцій можна використовувати будь-які перетворення. На основі цих розроблених мереж можна побудувати ефективні алгоритми блокового шифрування довжиною блоку 64m біт при довжині підблоку 32 біти, довжиною блоку 32m біт при довжині підблоку рівною 16 біт, а також довжиною блоку 16m біт при довжині підблоку рівною 8 біт.*

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

Tuychiev G. On the network PES2m-m, consisting of m round function and its modifications

Abstract. *Today one of the most effective methods of symmetric block cipher construction is the use of so-called Feistel network. This article based on Lai-Massey scheme developed network subblocks composed of 2m. In proposed networks, similar network Feistel, when encryption and decryption used same algorithm and as round function use any conversion. Based on these networks designed build a block encryption algorithm block length 64m bit sub-block at length of 32 bits, 32m length block sub-block length in bits equal to 16 bits and the length of the block with a length of 16m-bit sub-block of 8 bits.*

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

Отримано *3 лютого 2015 року*, затверджено редколегією *19 лютого 2015 року*