УДК 004.056.55

Г.Н. Туйчиев

Национальный университет Узбекистана, Ташкент, Республика Узбекистан

О СЕТИ IDEA2m–m, СОСТОЯЩЕЙ ИЗ m РАУНДОВЫХ ФУНКЦИЙ И ЕЕ МОДИФИКАЦИИ

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

Введение

Алгоритмы блочного шифрования как ГОСТ 28147–89, DES, Blowfish, E2 разработаны на основе сети Фейстеля. Преимуществом сети Фейстеля является, то что при зашифровании и расшифровании используется один и тот же алгоритм. Процесс зашифрования и расшифрования можно представить в виде формул (1), (2):

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

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

Для сети Фейстеля выполняется равенство

$$L_{i-1} = R_i \oplus F(L_i, K_i) = L_{i-1} \oplus F(R_{i-1}, K_i) \oplus F(L_i, K_i) = L_{i-1}.$$

Это равенство означает, что при расшифровании нет необходимости вычисления обратной функции F^{-1}, т.е., в качестве раундовой функции F можно выбрать любые преобразования [2].

В 1990 году Х. Лай и Дж. Мэсси взамен алгоритма DES разработали новый алгоритм блочного шифрования PES [1]. 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 [2]. 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 равна 64 битам. 64 битный блок делится на четыре 16 битных подблока 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 $\oplus$;

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

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

На основе модификации алгоритма IDEA разработан алгоритм шифрования IDEA-128, 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 [3, 4]. 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.

Кроме этого разработаны расширенные схемы Лай-Мэсси, в которых имеются раундовые функции и алгоритмы шифрования FOX, Мухомор разработан на основе этой схемы. Отличие от вышеприведенных сетей, в алгоритмах шифрования FOX, Мухомор алгоритм 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 МА преобразовании ограничиваются использованием опе-

рации 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 работах [5, 7, 9, 11] авторами на основе структуры алгоритма шифрования IDEA разработана сеть под названием IDEA4–2, IDEA8–4, IDEA16–8, IDEA32–16 состоящая из двух, четырех, восьми и шестнадцати раундовых функций.

В сетях IDEA4–2, IDEA8–4, IDEA16–8, IDEA32–16 раундовые функции имеют по одному входному и выходному блоку. 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 IDEA4–2 разработана сеть IDEA4–1, состоящая из одной раундовой функции, в которой раундовая функция имеет по два входных и выходных подблока [6]. На основе сети IDEA8–4 разработаны сети IDEA8–2, IDEA8–1, состоящая из двух, одной раундовой функции, в которых раундовая функция имеет по два и четыре входных и выходных подблока [8]. На основе сети IDEA16–8 разработаны сети IDEA16–4, IDEA16–2, IDEA16–1 состоящая из четырех, двух, одной раундовой функции, в которых раундовая функция имеет по два, четыре и восьми входных и выходных подблока [10], а на основе сети IDEA32–16 разработаны сети IDEA32–8, IDEA32–4, IDEA32–2, IDEA32–1 [12].

Кроме этого, в разработанных сетях раундовые ключи умножаются и суммируются с подблоками. За счет умножения и суммирования раундовых ключей к подблокам, раундовые функции указанных сетях можно применять без ключа. Поэтому, на основе сети IDEA4–2, IDEA4–1 разработаны сети RFWKIDEA4–2 (round function without key IDEA4–2), RFWKIDEA4–1, в который в раундовых функциях не использовано раундовые ключи [6].

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.

Данная статья является обобщением сетей IDEA4–2, IDEA8–4, IDEA16-8, IDEA32–16 и в ней приведена новая сеть под названием

– IDEA2m–m, состоящая из 2m подблоков и m раундовых функций,

– IDEA2m–(m/2) состоящая из 2m подблоков и m/2 раундовых функций,

– IDEA2m–(m/4) состоящая из 2m подблоков и m/4 раундовых функций,

– IDEA2m–1 состоящая из 2m подблоков и одной раундовой функции,

– RFWKIDEA2m–m, состоящая из 2m подблоков и m раундовых функций,

– RFWKIDEA2m–(m/2) состоящая из 2m подблоков и m/2 раундовых функций,

– RFWKIDEA2m–(m/4) состоящая из 2m подблоков и m/4 раундовых функций,

– RFWKIDEA2m–1 состоящая из 2m подблоков и одной раундовой функции.

Структура сети IDEA2m–m

В сети IDEA2m–m длина подблоков X^0, X^1, X^2,…, 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_2,…, 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 IDEA2m–m приведен в [3], а схема сети приведена на рис. 1.

В [3] $Y^j=F_j(T^j, K_{3m(i-1)+2m+j})$, $j=\overline{0...m-1}$ – выходные значениz раундовых функций, а

$$T^j=(X_{i-1}^j(z_j)K_{3m(i-1)+j})\oplus$$
$$\oplus(X_{i-1}^{m+j}(z_{m-1-j})K_{3m(i-1)+m+j}) -$$

входные значения раундовых функций F_0, F_1, F_2, …, F_{m-1}.

$$\begin{cases} X_i^0=(X_{i-1}^0(z_0)K_{3m(i-1)})\oplus Y^0\oplus Y^1\oplus Y^2\oplus...\oplus Y^{m-1};\\ X_i^1=(X_{i-1}^{2m-2}(z_1)K_{3m(i-1)+2m-2})\oplus Y^0\oplus Y^1;\\ X_i^2=(X_{i-1}^{2m-3}(z_2)K_{3m(i-1)+2m-3})\oplus Y^0\oplus Y^1\oplus Y^2;\\ .....\\ X_i^{m-1}=(X_{i-1}^m(z_{m-1})K_{3m(i-1)+m})\oplus Y^0\oplus Y^1\oplus Y^2\oplus...\oplus Y^{m-1};\\ X_i^m=(X_{i-1}^{m-1}(z_{m-1})K_{3m(i-1)+m-1})\oplus Y^0;\\ X_i^{m+1}=(X_{i-1}^{m-2}(z_{m-2})K_{3m(i-1)+m-2})\oplus Y^0\oplus Y^1;\\ X_i^{m+2}=(X_{i-1}^{m-3}(z_{m-3})K_{3m(i-1)+m-3})\oplus Y^0\oplus Y^1\oplus Y^2;\\ .....\\ X_i^{2m-1}=(X_{i-1}^{2m-1}(z_0)K_{3m(i-1)+2m-1})\oplus Y^0, \end{cases} \quad (3)$$

$i=\overline{1...n}$.

В качестве операции z_i, $i=\overline{0...m-1}$ 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 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.

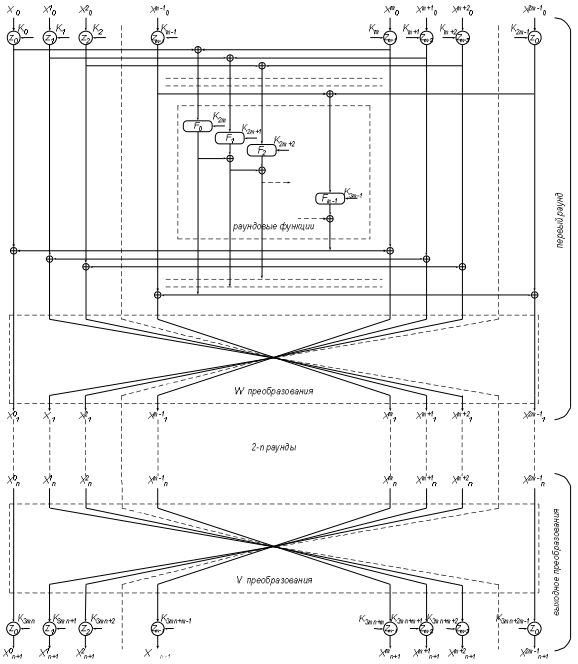

Рис. 1. Схема n-раундовой сети IDEA2m–m

Как видно из рис. 1, в V и W преобразовании кроме подблоков X^0, X^{2m-1} все подблоки заменяется между собой. В качестве первого варианта сети IDEA2m–m выбираем схему, приведенную на рис. 1, тогда

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

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

– если заменить между собой только подблоки X_{i-1}^j и X_{i-1}^{2m-1-j}, $j=\overline{4...m-1}$, $i=\overline{1...n+1}$, то полученную сеть можно выбрать в качестве 4–варианта,

– …,

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

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

– если заменить между собой все подблоки, то полученную сеть можно выбрать в качестве $m+1$–варианта.

Генерация ключей сети IDEA2m–m

В n – раундовой сети IDEA2m–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 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 IDEA2m–m раундовые ключи расшифрования первого раунда связаны с ключами зашифрования по формуле (4).

$$\begin{aligned}&(K_0^d, K_1^d, K_2^d, ..., K_{m-1}^d, K_m^d, K_{m+1}^d, K_{m+2}^d, ...,\\ &K_{2m-1}^d, K_{2m}^d, K_{2m+1}^d, K_{2m+2}^d, ..., K_{3m-1}^d) =\\ &((K_{3mn}^c)^{z0}, (K_{3mn+1}^c)^{z1}, (K_{3mn+2}^c)^{z2}, ...,\\ &(K_{3mn+m-1}^c)^{z_{m-1}}, (K_{3mn+m}^c)^{z_{m-1}}, (K_{3mn+m+1}^c)^{z_{m-2}},\\ &(K_{3mn+m+2}^c)^{z_{m-3}}, ...(K_{3mn+2m-1}^c)^{z0}, K_{3m(n-1)+2m},\\ &K_{3m(n-1)+2m+1}^c, K_{3m(n-1)+2m+2}^c, ..., K_{3m(n-1)+3m-1}^c).\end{aligned} \quad (4)$$

Если в качестве операции z_i, $i=\overline{0...m-1}$ 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 связаны к ключам зашифрования следующим образом:

$$\begin{aligned}&(K_{3mn}^d, K_{3mn+1}^d, K_{3mn+2}^d, ..., K_{3mn+m-1}^d, K_{3mn+m}^d,\\ &K_{3mn+m+1}^d, K_{3mn+m+2}^d, ..., K_{3mn+2m-1}^d) =\\ &=((K_0^c)^{z0}, (K_1^c)^{z1}, (K_2^c)^{z2}, ..., (K_{m-1}^c)^{z_{m-1}}, (K_m^c)^{z_{m-1}},\\ &(K_{m+1}^c)^{z_{m-2}}, (K_{m+2}^c)^{z_{m-3}}, ..., (K_{2m-1}^c)^{z0}).\end{aligned} \quad (5)$$

Таким же образом ключи расшифрования второго, третьего и n–раунда связаны к ключам зашифрования по формуле:

$$(K^d_{3m(i-1)}, K^d_{3m(i-1)+1}, K^d_{3m(i-1)+2}, \ldots, K^d_{3m(i-1)+m-1}, K^d_{3m(i-1)+m}, K^d_{3m(i-1)+m+1}, K^d_{3m(i-1)+m+2}, \ldots, K^d_{3m(i-1)+2m-1}, K^d_{3m(i-1)+2m}, K^d_{3m(i-1)+2m+1}, K^d_{3m(i-1)+2m+2}, \ldots, K^d_{3m(i-1)+3m-1}) = ((K^c_{3m(n-i+1)})^{z_0}, (K^c_{3m(n-i+1)+2m-2})^{z_1}, (K^c_{3m(n-i+1)+2m-3})^{z_2}, \ldots, (K^c_{3m(n-i+1)+m})^{z_{m-1}}, (K^c_{3m(n-i+1)+m-1})^{z_{m-1}}, (K^c_{3m(n-i+1)+m-2})^{z_{m-2}}, (K^c_{3m(n-i+1)+m-3})^{z_{m-3}}, \ldots, (K^c_{3m(n-i+1)+2m-1})^{z_0}, K^c_{3m(n-i)+2m}, K^c_{3m(n-i)+2m+1}, K^c_{3m(n-i)+2m+2}, \ldots, K^c_{3m(n-i)+3m-1}), \quad i = \overline{2...n}. \qquad (6)$$

В 2, 3 и $m+1$–вариантов сети ключи расшифрования первого раунда и выходного преобразования связаны с ключами зашифрования по формуле (4) и (5). Вычисление ключей расшифрования второго, третьего и n–раунда похоже на (6), только

– в 2–варианте ключи $K^c_{3m(n-i+1)+1}$ и $K^c_{3m(n-i+1)+2m-2}$,

– в 3–варианте ключи $K^c_{3m(n-i+1)+1}$ и $K^c_{3m(n-i+1)+2m-2}$, $K^c_{3m(n-i+1)+2}$ и $K^c_{3m(n-i+1)+2m-3}$,

– в 4–варианте ключи $K^c_{3m(n-i+1)+1}$ и $K^c_{3m(n-i+1)+2m-2}$, $K^c_{3m(n-i+1)+2}$ и $K^c_{3m(n-i+1)+2m-3}$, $K^c_{3m(n-i+1)+3}$ и $K^c_{3m(n-i+1)+2m-4}$,

– ……

– в (m – 1)–варианте ключи $K^c_{3m(n-i+1)+1}$ и $K^c_{3m(n-i+1)+2m-2}$, $K^c_{3m(n-i+1)+2}$ и $K^c_{3m(n-i+1)+2m-3}$, $K^c_{3m(n-i+1)+3}$ и $K^c_{3m(n-i+1)+2m-4}$, …, $K^c_{3m(n-i+1)+m-3}$ и $K^c_{3m(n-i+1)+m+2}$, $K^c_{3m(n-i+1)+m-2}$ и $K^c_{3m(n-i+1)+m+1}$,

– в m–варианте ключи $K^c_{3m(n-i+1)+1}$ и $K^c_{3m(n-i+1)+2m-2}$, $K^c_{3m(n-i+1)+2}$ и $K^c_{3m(n-i+1)+2m-3}$, $K^c_{3m(n-i+1)+3}$ и $K^c_{3m(n-i+1)+2m-4}$, …, $K^c_{3m(n-i+1)+m-2}$ и $K^c_{3m(n-i+1)+m+1}$, $K^c_{3m(n-i+1)+m-1}$ и $K^c_{3m(n-i+1)+m}$,

– в (m + 1)–варианте ключи $K^c_{3m(n-i+1)}$ и $K^c_{3m(n-i+1)+2m-1}$ заменяются между собой.

В приведённой сети IDEA2m–m число раундовых функций равно m и раундовые функции F_0, F_1, $F_2, \ldots, F_{m-1}$ имеет одно входное и выходное значение. В качестве раундовых функций 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 функций равно m/2 и сеть называется IDEA2m–(m/2), в качестве раундовых функций использовать функцию с четырьмя входными и выходными значениями, то число раундовых функции равно m/4 и сеть называется IDEA2m–(m/4), и т.п., если в качестве раундовых функций использовать функцию с m входными и выходными значениями, то число раундовых функции равно одному и сеть называется IDEA2m–1.

Структура сети IDEA2m–(m/2)

В сети IDEA2m–(m/2) длина подблоков X^0, X^1, …, X^{2m-1}, длина раундовых ключей $K_{(2m+m/2)(i-1)}$, $K_{(2m+m/2)(i-1)+1}$, $K_{(2m+m/2)(i-1)+2}, \ldots, K_{(2m+m/2)(i-1)+2m-1}$, $i = \overline{1...n+1}$ равно 32 (16, 8) битам. Раундовые функции F_0, F_1, $F_2, \ldots, F_{(m/2)-1}$ имеют два входа и выхода, в которых длина входных и выходных блоков функций равна 32 (16, 8) битам. Длина раундовых ключей $K_{(2m+m/2)(i-1)+2m}$, $K_{(2m+m/2)(i-1)+2m+1}$, $K_{(2m+m/2)(i-1)+2m+2}, \ldots, K_{(2m+m/2)(i-1)+(2m+m/2)-1}$, $i = \overline{1...n}$, необязательно должна быть равной 32 (16, 8) битам. Схема i – раунда сети IDEA2m–(m/2) приведена на рис. 2.

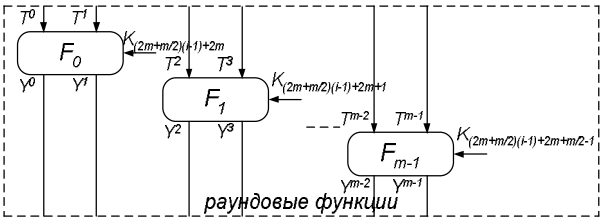

Рис. 2. Схема i – раунда сети IDEA2m–(m/2)

Если берем $T0 = [T^0, T^1]$, $T1 = [T^2, T^3]$, $T2 = [T^4, T^5]$, ..., $T(m/2-1) = [T^{m-2}, T^{m-1}]$ в качестве входного значения, $Y0 = [Y^0, Y^1]$, $Y1 = [Y^2, Y^3]$, $Y2 = [Y^4, Y^5]$, ..., $Y(m/2-1) = [Y^{m-2}, Y^{m-1}]$ – в качестве выходного значения раундовой функции, то раундовую функцию можно представить в виде $Yj = F_j(Tj, K_{(2m+m/2)(i-1)+2m+j})$, $j = \overline{0...(m/2)-1}$. Здесь $T^j = (X^j_{i-1}(z_j)K_{(2m+m/2)(i-1)+j}) \oplus (X^{m+j}_{i-1}(z_{m-1-j})K_{(2m+m/2)(i-1)+m+j})$, $j = \overline{0...m-1}$ –

входные значения раундовых функций F_0, F_1, F_2,…, $F_{(m/2)-1}$. 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 $Y(m/2-1) = F_7(T(m/2-1), K_{(2m+m/2)(i-1)+2m+m/2-1})$ представим в виде $Y^{m-2} = F_{m-1}^0(T^{m-2}, T^{m-1}, K_{(2m+m/2)(i-1)+2m+m/2-1})$, $Y^{m-1} = F_{m-1}^1(T^{m-2}, T^{m-1}, K_{(2m+m/2)(i-1)+2m+m/2-1})$. Процесс зашифрования сети IDEA2m–(m/2) приведён в (7).

Как видно из рис. 2, в V и W преобразовании кроме подблоков X^0, X^{2m-1} все подблоки заменяются между собой. Как у сети IDEA2m–m, на сети IDEA2m–(m/2) имеется $m+1$ вариантов сети на основе замены подблоков.

$$\begin{cases} X_i^0 = (X_{i-1}^0(z_0)K_{(2m+m/2)(i-1)}) \oplus Y^{m-1}; \\ X_i^1 = (X_{i-1}^{2m-2}(z_1)K_{(2m+m/2)(i-1)+2m-2}) \oplus Y^1; \\ X_i^2 = (X_{i-1}^{2m-3}(z_2)K_{(2m+m/2)(i-1)+2m-3}) \oplus Y^2; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_i^{m-1} = (X_{i-1}^m(z_{m-1})K_{(2m+m/2)(i-1)+m}) \oplus Y^{m-1}; \\ X_i^m = (X_{i-1}^{m-1}(z_{m-1})K_{(2m+m/2)(i-1)+m-1}) \oplus Y^0; \\ X_i^{m+1} = (X_{i-1}^{m-2}(z_{m-2})K_{(2m+m/2)(i-1)+m-2}) \oplus Y^1; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_i^{2m-1} = (X_{i-1}^{2m-1}(z_0)K_{(2m+m/2)(i-1)+2m-1}) \oplus Y^0, \end{cases}$$

$$i = \overline{1...n}, \qquad (7)$$

$$\begin{cases} X_{n+1}^0 = (X_n^0(z_0)K_{(2m+m/2)n}); \\ X_{n+1}^1 = (X_n^{2m-2}(z_1)K_{(2m+m/2)n+1}); \\ X_{n+1}^2 = (X_n^{2m-3}(z_2)K_{(2m+m/2)n+2}); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{m-1} = (X_n^m(z_{m-1})K_{(2m+m/2)n+m-1}); \\ X_{n+1}^m = (X_n^{m-1}(z_{m-1})K_{(2m+m/2)n+m}); \\ X_{n+1}^{m+1} = (X_n^{m-2}(z_{m-2})K_{(2m+m/2)n+m+1}); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{2m-1} = (X_n^{2m-1}(z_0)K_{(2m+m/2)n+2m-1}) \end{cases}$$

в выходном преобразовании.

Генерация ключей сети IDEA2m–(m/2)

В сети IDEA2m–(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 $n-$раундовой сети IDEA2m–(m/2) раундовые ключи первого раунда расшифрования связаны с ключами зашифрования по формуле

$$\begin{aligned} &(K_0^d, K_1^d, K_2^d, \ldots, K_{m-1}^d, K_m^d, K_{m+1}^d, K_{m+2}^d, \ldots, K_{2m-1}^d, \\ &K_{2m}^d, K_{2m+1}^d, K_{2m+2}^d, \ldots, K_{(2m+m/2)-1}^d) = \\ &(K_{(2m+m/2)n}^c)^{z_0}, (K_{(2m+m/2)n+1}^c)^{z_1}, \\ &(K_{(2m+m/2)n+2}^c)^{z_2}, \ldots, (K_{(2m+m/2)n+m-1}^c)^{z_{m-1}}, \\ &(K_{(2m+m/2)n+m}^c)^{z_{m-1}}, (K_{(2m+m/2)n+m+1}^c)^{z_{m-2}}, \\ &(K_{(2m+m/2)n+m+2}^c)^{z_{m-3}}, \ldots, (K_{(2m+m/2)n+2m-1}^c)^{z_0}, \\ &K_{(2m+m/2)(n-1)+2m}^c, K_{(2m+m/2)(n-1)+2m+1}^c, \\ &K_{(2m+m/2)(n-1)+2m+2}^c, \ldots, K_{(2m+m/2)(n-1)+(2m+m/2)-1}^c). \end{aligned} \qquad (9)$$

Ключи расшифрования выходного преобразования связаны к ключам зашифрования следующим образом:

$$\begin{aligned} &(K_{(2m+m/2)n}^d, K_{(2m+m/2)n+1}^d, K_{(2m+m/2)n+2}^d, \ldots, \\ &K_{(2m+m/2)n+m-1}^d, K_{(2m+m/2)n+m}^d, K_{(2m+m/2)n+m+1}^d, \\ &K_{(2m+m/2)n+m+2}^d, \ldots, K_{(2m+m/2)n+2m-1}^d) = \\ &((K_0^c)^{z_0}, (K_1^c)^{z_1}, (K_2^c)^{z_2}, \ldots, (K_{m-1}^c)^{z_{m-1}}, (K_m^c)^{z_{m-1}}, \\ &(K_{m+1}^c)^{z_{m-2}}, (K_{m+2}^c)^{z_{m-3}}, \ldots, (K_{2m-1}^c)^{z_0}). \end{aligned} \qquad (10)$$

Таким же образом ключи расшифрования второго, третьего и n–раунда связаны к ключам зашифрования по формуле (11).

В 2, 3 и $m+1$–вариантов сети ключи расшифрования первого раунда и выходного преобразования связаны к ключам зашифрования по формуле (9) и (10). Ключи расшифрования второго, третьего и n–раунда вычисляется как у сети IDEA2m–m, только в индексе взамен 3m используется $2m+m/2$.

$$\begin{aligned} &(K_{(2m+m/2)(i-1)}^d, K_{(2m+m/2)(i-1)+1}^d, K_{(2m+m/2)(i-1)+2}^d, \\ &\ldots, K_{(2m+m/2)(i-1)+m-2}^d, K_{(2m+m/2)(i-1)+m}^d, \\ &K_{(2m+m/2)(i-1)+m+1}^d, K_{(2m+m/2)(i-1)+m+2}^d, \ldots, \\ &K_{(2m+m/2)(i-1)+(2m+m/2)-2}^d, K_{(2m+m/2)(i-1)+(2m+m/2)-1}^d, \\ &K_{(2m+m/2)(i-1)+2m}^d, K_{(2m+m/2)(i-1)+2m+1}^d, \\ &K_{(2m+m/2)(i-1)+2m+2}^d, \ldots, K_{(2m+m/2)(i-1)+(2m+m/2)-1}^d) = \end{aligned} \qquad (11)$$

$$((K^c_{(2m+m/2)(n-i+1)})^{Z0},(K^c_{(2m+m/2)(n-i+1)+2m-2})^{Z1},$$

$$(K^c_{(2m+m/2)(n-i+1)+2m-3})^{Z2},...,$$

$$(K^c_{(2m+m/2)(n-i+1)+m+1})^{Z_{m-2}},(K^c_{(2m+m/2)(n-i+1)+m})^{Z_{m-1}},$$

$$(K^c_{(2m+m/2)(n-i+1)+m-1})^{Z_{m-1}},(K^c_{(2m+m/2)(n-i+1)+m-2})^{Z_{m-2}},$$

$$(K^c_{(2m+m/2)(n-i+1)+m-3})^{Z_{m-3}},...,(K^c_{(2m+m/2)(n-i+1)+1})^{Z1},$$

$$(K^c_{(2m+m/2)(n-i+1)+(2m+m/2)-1})^{Z0},K^c_{(2m+m/2)(n-i)+2m},$$

$$K^c_{(2m+m/2)(n-i)+2m+1},K^c_{(2m+m/2)(n-i)+2m+2},...,$$

$$K^c_{(2m+m/2)(n-i)+(2m+m/2)-1}),\ i=\overline{2...n}.$$

Структура сети IDEA2m–(m/4)

В сети IDEA2m–(m/4) длина подблоков X^0, X^1, …, X^{2m-1}, длина раундовых ключей

$$K_{(2m+m/4)(i-1)},\ K_{(2m+m/4)(i-1)+1},$$

$$K_{(2m+m/4)(i-1)+2},\ldots,\ K_{(2m+m/4)(i-1)+2m-1},$$

$$i=\overline{1...n+1}$$

равно 32 (16, 8) битам. Раундовые функции F_0, F_1, $F_2,\ldots,F_{(m/4)-1}$ имеют четыре входа и выхода, в которые длина входных и выходных блоков функций равна 32 (16, 8) битам. Длина раундовых ключей

$$K_{(2m+m/4)(i-1)+2m},\ K_{(2m+m/4)(i-1)+2m+1},\ \ldots,$$

$$K_{(2m+m/4)(i-1)+2m+m/4-1},\ i=\overline{1...n},$$

необязательно должна быть равной 32 (16, 8) битам. Схема $i-$раунда сети IDEA2m–(m/4) приведена на рис. 3.

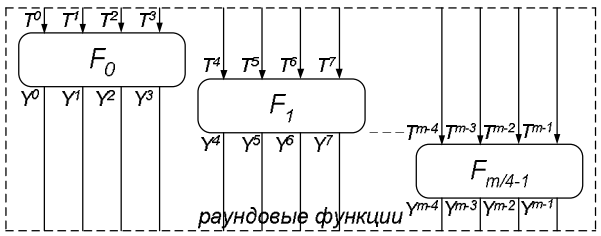

Рис. 3. Схема $i-$раунда сети IDEA2m–(m/4)

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

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

Здесь $T^j=(X^j_{i-1}(z_j)K_{(2m+m/4)(i-1)+j})\oplus(X^{m+j}_{i-1}(z_{m-1-j})$ $K_{(2m+m/4)(i-1)+m+j})$, $j=\overline{0...m-1}$ входные значения раундовые функции F_0, F_1, $F_2,\ldots,F_{(m/4)-1}$. 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 $Y^{m-4}=$

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

$$Y^{m-3}=F^1_{m/4-1}(T^{m-4},T^{m-3},T^{m-2},T^{m-1},$$

$$K_{(2m+m/4)(i-1)+2m+m/4-1}),$$

$$Y^{m-2}=F^2_{m/4-1}(T^{m-4},T^{m-3},T^{m-2},T^{m-1},$$

$$K_{(2m+m/4)(i-1)+2m+m/4-1}),$$

$$Y^{m-1}=F^3_{m/4-1}(T^{m-4},T^{m-3},T^{m-2},T^{m-1},$$

$K_{(2m+m/4)(i-1)+2m+m/4-1})$. Процесс зашифрования сети IDEA2m–(m/4) приведен в (12).

$$\begin{cases}X^0_i=(X^0_{i-1}(z_0)K_{(2m+m/4)(i-1)})\oplus Y^{m-1};\\ X^1_i=(X^{2m-2}_{i-1}(z_1)K_{(2m+m/4)(i-1)+2m-2})\oplus Y^1;\\ X^2_i=(X^{2m-3}_{i-1}(z_2)K_{(2m+m/4)(i-1)+2m-3})\oplus Y^2;\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ X^{m-1}_i=(X^m_{i-1}(z_{m-1})K_{(2m+m/4)(i-1)+m})\oplus Y^{m-1};\\ X^m_i=(X^{m-1}_{i-1}(z_{m-1})K_{(2m+m/4)(i-1)+m-1})\oplus Y^0;\\ X^{m+1}_i=(X^{m-2}_{i-1}(z_{m-2})K_{(2m+m/4)(i-1)+m-2})\oplus Y^1;\\ X^{m+2}_i=(X^{m-3}_{i-1}(z_{m-3})K_{(2m+m/4)(i-1)+m-3})\oplus Y^2;\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ X^{2m-1}_i=(X^{2m-1}_{i-1}(z_0)K_{(2m+m/4)(i-1)+2m-1})\oplus Y^0,\end{cases},$$

$$i=\overline{1...n}\qquad(12)$$

$$\begin{cases} X_{n+1}^{0} = (X_n^{0}(z_0)K_{(2m+m/4)n}); \\ X_{n+1}^{1} = (X_n^{2m-2}(z_1)K_{(2m+m/4)n+1}); \\ X_{n+1}^{2} = (X_n^{2m-3}(z_2)K_{(2m+m/4)n+2}); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{m-1} = (X_n^{m}(z_{m-1})K_{(2m+m/4)n+m-1}); \\ X_{n+1}^{m} = (X_n^{m-1}(z_{m-1})K_{(2m+m/4)n+m}); \\ X_{n+1}^{m+1} = (X_n^{m-2}(z_{m-2})K_{(2m+m/4)n+m+1}); \\ X_{n+1}^{m+2} = (X_n^{m-3}(z_{m-3})K_{(2m+m/4)n+m+2}); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{2m-1} = (X_n^{2m-1}(z_0)K_{(2m+m/4)n+2m-1}) \end{cases},$$

в выходном преобразовании

Как видно из рис. 3, в V и W преобразовании кроме подблоков X^0, X^{2m-1} все подблоки заменяются между собой. Как у сети IDEA2m–(m/2), на сети IDEA2m–(m/4) имеет $m+1$ вариантов сети на основе замены подблоков.

Генерация ключей сети IDEA2m–(m/4)

В n – раундовой сети IDEA2m–(m/4) в каждом раунде применяются 2m+(m/4) раундовые ключи и в последнем преобразовании 2m раундовых ключей, т.е., число всех ключей равно $(2m+m/4)n+2m$.

В n – раундовой сети IDEA2m–(m/4) ключи расшифрования первого раунда связаны с ключами зашифрования по формуле (13).

$$\begin{gathered}(K_0^d, K_1^d, K_2^d, \ldots, K_{m-1}^d, K_m^d, K_{m+1}^d, K_{m+2}^d, \ldots, K_{2m-1}^d, \\ K_{2m}^d, K_{2m+1}^d, K_{2m+2}^d, \ldots, \\ K_{(2m+m/4)-1}^d) = (K_{(2m+m/4)n}^c)^{z_0}, (K_{(2m+m/4)n+1}^c)^{z_1}, \\ (K_{(2m+m/4)n+2}^c)^{z_2}, \ldots, \\ (K_{(2m+m/4)n+m-1}^c)^{z_{m-1}}, (K_{(2m+m/4)n+m}^c)^{z_{m-1}}, \\ (K_{(2m+m/4)n+m+1}^c)^{z_{m-2}}, (K_{(2m+m/4)n+m+2}^c)^{z_{m-3}}, \\ \ldots (K_{(2m+m/4)n+2m-1}^c)^{z_0}, K_{(2m+m/4)(n-1)+2m}^c, \\ K_{(2m+m/4)(n-1)+2m+1}^c, K_{(2m+m/4)(n-1)+2m+2}^c, \ldots, \\ K_{(2m+m/4)(n-1)+(2m+m/4)-1}^c).\end{gathered} \quad (13)$$

Ключи расшифрования выходного преобразования связаны к ключам зашифрования следующим образом:

$$\begin{gathered}(K_{(2m+m/4)n}^d, K_{(2m+m/4)n+1}^d, K_{(2m+m/4)n+2}^d, \ldots, \\ K_{(2m+m/4)n+m-1}^d, K_{(2m+m/4)n+m}^d, K_{(2m+m/4)n+m+1}^d, \\ K_{(2m+m/4)n+m+2}^d, \ldots, K_{(2m+m/4)n+2m-1}^d) = \\ ((K_0^c)^{z_0}, (K_1^c)^{z_1}, (K_2^c)^{z_2}, \ldots, (K_{m-1}^c)^{z_{m-1}}, (K_m^c)^{z_{m-1}}, \\ (K_{m+1}^c)^{z_{m-2}}, (K_{m+2}^c)^{z_{m-3}}, \ldots, (K_{2m-1}^c)^{z_0}).\end{gathered} \quad (14)$$

Таким же образом ключи расшифрования второго, третьего и n–раунда связаны к ключам зашифрования по формуле (15):

$$\begin{gathered}(K_{(2m+m/4)(i-1)}^d, K_{(2m+m/4)(i-1)+1}^d, K_{(2m+m/4)(i-1)+2}^d, \\ \ldots, K_{(2m+m/4)(i-1)+m-2}^d, K_{(2m+m/4)(i-1)+m-1}^d, \\ K_{(2m+m/4)(i-1)+m}^d, K_{(2m+m/4)(i-1)+m+1}^d, \\ K_{(2m+m/4)(i-1)+m+2}^d, \ldots, K_{(2m+m/4)(i-1)+(2m+m/4)-2}^d, \\ K_{(2m+m/4)(i-1)+(2m+m/4)-1}^d, K_{(2m+m/2)(i-1)+2m}^d, \\ K_{(2m+m/4)(i-1)+2m+1}^d, K_{(2m+m/4)(i-1)+2m+2}^d, \ldots, \\ K_{(2m+m/4)(i-1)+(2m+m/4)-1}^d) = ((K_{(2m+m/4)(n-i+1)}^c)^{z_0}, \\ (K_{(2m+m/4)(n-i+1)+2m-2}^c)^{z_1}, \\ (K_{(2m+m/4)(n-i+1)+2m-3}^c)^{z_2}, \ldots, \\ (K_{(2m+m/4)(n-i+1)+m+1}^c)^{z_{m-2}}, (K_{(2m+m/4)(n-i+1)+m}^c)^{z_{m-1}}, \\ (K_{(2m+m/4)(n-i+1)+m-1}^c)^{z_{m-1}}, (K_{(2m+m/4)(n-i+1)+m-2}^c)^{z_{m-2}}, \\ (K_{(2m+m/4)(n-i+1)+m-3}^c)^{z_{m-3}}, \\ \ldots, (K_{(2m+m/4)(n-i+1)+1}^c)^{z_1}, (K_{(2m+m/4)(n-i+1)+(2m+m/2)-1}^c)^{z_0}, \\ K_{(2m+m/4)(n-i)+2m}^c, \\ K_{(2m+m/4)(n-i)+2m+1}^c, K_{(2m+m/4)(n-i)+2m+2}^c, \ldots, \\ K_{(2m+m/4)(n-i)+(2m+m/4)-1}^c), i = \overline{2...n}.\end{gathered} \quad (15)$$

В 2, 3 и $m+1$ –вариантов сети ключи расшифрования первого раунда и выходного преобразования связан к ключам зашифрования по формуле (13) и (14). Ключи расшифрования второго, третьего и *n*–раунда вычисляется как у сети IDEA2m–m, только в индексе взамен 3m используется $2m+m/4$.

Структура сети IDEA2m–1

В сети IDEA2m–1 длина подблоков X^0, X^1, …, X^{2m-1} и длина раундовых ключей $K_{(2m+1)(i-1)}$, $K_{(2m+1)(i-1)+1}$, $K_{(2m+1)(i-1)+2}$, …, $K_{(2m+1)(i-1)+2m-1}$, $i = \overline{1...n+1}$ равна 32 (16, 8) битам. Раундовые функции F_0, F_1, F_2, …, $F_{(m/4)-1}$ имеют четыре 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 i – раунда сети IDEA2m–(m/2) приведена на рис. 4.

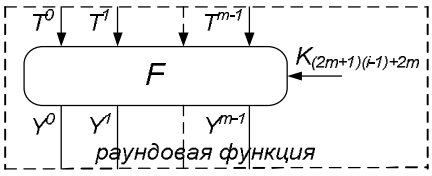

Рис. 4. Схема n–раундовой сети IDEA2m–1

Если берем $T=[T^0,T^1,T^2,...,T^{m-1}]$ – в качестве входного значения, $Y=[Y^0,Y^1,Y^3,...,Y^{m-1}]$ – в качестве выходного значения раундовой функции, то раундовую функцию можно представить в виде

$$Y=F\ (T,K_{(2m+1)(i-1)+2m}).$$

Здесь

$T^j=(X_{i-1}^j(z_j)K_{(2m+1)(i-1)+j})\oplus\ (X_{i-1}^{m+j}(z_{m-1-j})K_{(2m+1)(i-1)+m+j})$, $j=\overline{0...m-1}$ – входные значения раундовой функции F. Для корректности формулы алгоритма шифрования раундовую функцию

$$Y=F\ (T,K_{(2m+1)(i-1)+2m})$$

представим в виде

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

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

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

Процесс зашифрования сети IDEA2m–1 приведен в (16).

$$\begin{cases} X_i^0=(X_{i-1}^0(z_0)K_{(2m+1)(i-1)})\oplus Y^{m-1};\\ X_i^1=(X_{i-1}^{2m-2}(z_1)K_{(2m+1)(i-1)+2m-2})\oplus Y^1;\\ X_i^2=(X_{i-1}^{2m-3}(z_2)K_{(2m+1)(i-1)+2m-3})\oplus Y^2;\\ .....\\ X_i^{m-1}=(X_{i-1}^m(z_{m-1})K_{(2m+1)(i-1)+m})\oplus Y^{m-1};\\ X_i^m=(X_{i-1}^{m-1}(z_{m-1})K_{(2m+1)(i-1)+m-1})\oplus Y^0;\\ X_i^{m+1}=(X_{i-1}^{m-2}(z_{m-2})K_{(2m+1)(i-1)+m-2})\oplus Y^1;\\ X_i^{m+2}=(X_{i-1}^{m-3}(z_{m-3})K_{(2m+1)(i-1)+m-3})\oplus Y^2;\\ .....\\ X_i^{2m-1}=(X_{i-1}^{2m-1}(z_0)K_{(2m+1)(i-1)+2m-1})\oplus Y^0, \end{cases}$$

$$i=\overline{1...n} \qquad (16)$$

$$\begin{cases} X_{n+1}^0=(X_n^0(z_0)K_{(2m+1)n});\\ X_{n+1}^1=(X_n^{2m-2}(z_1)K_{(2m+1)n+1});\\ X_{n+1}^2=(X_n^{2m-3}(z_2)K_{(2m+1)n+2};)\\ .....\\ X_{n+1}^{m-1}=(X_n^m(z_{m-1})K_{(2m+1)n+m-1});\\ X_{n+1}^m=(X_n^{m-1}(z_{m-1})K_{(2m+1)n+m});\\ X_{n+1}^{m+1}=(X_n^{m-2}(z_{m-2})K_{(2m+1)n+m+1});\\ X_{n+1}^{m+2}=(X_n^{m-3}(z_{m-3})K_{(2m+1)n+m+2});\\ .....\\ X_{n+1}^{2m-1}=(X_n^{2m-1}(z_0)K_{(2m+1)n+2m-1}) \end{cases}$$

в выходном преобразовании

Как видно из рис. 4, в V и W преобразовании кроме подблоков X^0, X^{2m-1} все подблоки заменяются между собой. Как у сети IDEA2m–(m/2), на сети IDEA2m–1 имеется $m+1$ вариантов сети на основе замены подблоков.

Генерация ключей сети IDEA2m–1

В n – раундовой сети IDEA2m–1 в каждом раунде применяются 2m+1 раундовые ключи и в последнем преобразовании 2m раундовых ключей, т.е., число всех ключей равно $(2m+1)n+2m$.

В сети IDEA2m–1 раундовые ключи расшифрования первого раунда связаны с ключами зашифрования по формуле (17).

$$\begin{aligned} &(K_0^d,K_1^d,K_2^d,...,K_{m-1}^d,K_m^d,K_{m+1}^d,K_{m+2}^d,...,\\ &K_{2m-1}^d,K_{2m}^d,K_{2m+1}^d)=(K_{(2m+1)n}^c)^{z_0},\\ &(K_{(2m+1)n+1}^c)^{z_1},(K_{(2m+1)n+2}^c)^{z_2},...,\\ &(K_{(2m+1)n+m-1}^c)^{z_{m-1}},(K_{(2m+1)n+m}^c)^{z_{m-1}},\\ &(K_{(2m+1)n+m+1}^c)^{z_{m-2}},(K_{(2m+1)n+m+2}^c)^{z_{m-3}},\\ &...(K_{(2m+1)n+2m-1}^c)^{z_0},K_{(2m+1)(n-1)+2m}^c). \end{aligned} \qquad (17)$$

Ключи расшифрования выходного преобразования связаны к ключам зашифрования следующим образом:

$$\begin{aligned} &(K_{(2m+1)n}^d,K_{(2m+1)n+1}^d,K_{(2m+1)n+2}^d,...,K_{(2m+1)n+m-1}^d,\\ &K_{(2m+1)n+m}^d,K_{(2m+1)n+m+1}^d,K_{(2m+1)n+m+2}^d,...,\\ &K_{(2m+1)n+2m-1}^d)=((K_0^c)^{z_0},(K_1^c)^{z_1},(K_2^c)^{z_2},...,\\ &(K_{m-1}^c)^{z_{m-1}},(K_m^c)^{z_{m-1}},(K_{m+1}^c)^{z_{m-2}},(K_{m+2}^c)^{z_{m-3}},...,\\ &(K_{2m-1}^c)^{z_0}). \end{aligned} \qquad (18)$$

Таким же образом ключи расшифрования второго, третьего и n–раунда связаны к ключам зашифрования по формуле (19):

$$\begin{aligned} &(K_{(2m+1)(i-1)}^d,K_{(2m+1)(i-1)+1}^d,K_{(2m+1)(i-1)+2}^d,...,\\ &K_{(2m+1)(i-1)+m-2}^d,K_{(2m+1)(i-1)+m-1}^d,K_{(2m+1)(i-1)+m}^d,\\ &K_{(2m+1)(i-1)+m+1}^d,K_{(2m+1)(i-1)+m+2}^d,...,\\ &K_{(2m+1)(i-1)+2m-1}^d,K_{(2m+1)(i-1)+2m}^d)=\\ &=((K_{(2m+1)(n-i+1)}^c)^{z_0},(K_{(2m+1)(n-i+1)+2m-2}^c)^{z_1},\\ &(K_{(2m+1)(n-i+1)+2m-3}^c)^{z_2},...,(K_{(2m+1)(n-i+1)+m+1}^c)^{z_{m-2}},\\ &(K_{(2m+1)(n-i+1)+m}^c)^{z_{m-1}},(K_{(2m+1)(n-i+1)+m-1}^c)^{z_{m-1}},\\ &(K_{(2m+1)(n-i+1)+m-2}^c)^{z_{m-2}},(K_{(2m+1)(n-i+1)+m-3}^c)^{z_{m-3}},\\ &...,(K_{(2m+1)(n-i+1)+1}^c)^{z_1},\\ &(K_{(2m+1)(n-i+1)+2m-1}^c)^{z_0},K_{(2m+1)(n-i)+2m}^c),\ i=\overline{2...n}. \end{aligned} \qquad (19)$$

В 2, 3 и $m+1$ –вариантов сети ключи расшифрования первого раунда и выходного преобразова-

ния связан к ключам зашифрования по формуле (17) и (18). Ключи расшифрования второго, третьего и n–раунда вычисляются как у сети IDEA2m–m, только в индексе взамен 3m используется $2m+1$.

Как видно из схемы сетей IDEA2m–m, IDEA2m–(m/2), IDEA2m–(m/4) и IDEA2m–1 в каждом раунде раундовые ключи на подблок умножаются и складываются, кроме этого в каждой раундовой функции применены раундовые ключи. За счет применение раундовых ключей к подблоку раундовые функции можно использовать без ключа. Использованные раундовые функции без ключа в сети IDEA2m–m обозначаются как RFWKIDEA2m–m (round function without key IDEA2m–m), раундовой функция без ключа использованная сеть IDEA2m–(m/2) обозначается как RFWKIDEA2m–(m/2), и т.д. RFWKIDEA2m–1.

Структура сети RFWKIDEA2m–m

В сети RFWKIDEA2m–m длина подблоков X_i^0, X_i^1, X_i^2,..., X_i^{2m-1}, длина раундовых ключей, а также длина входных и выходных блоков функций F_0, F_1, F_2,..., F_{m-1} равна 32 (16, 8) бит.

Схема n–раундовой сети RFWKIDEA2m–m приведена на рис. 5 и процесс шифрования приведен в (20)-й формуле.

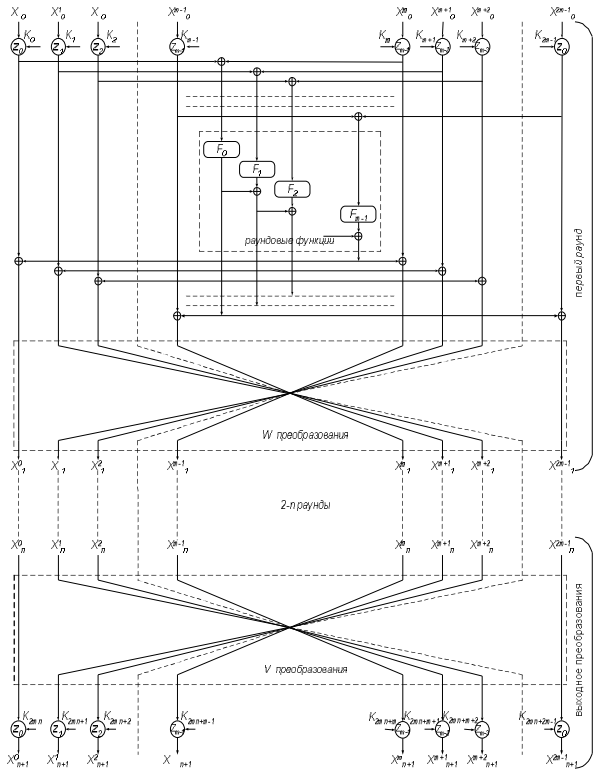

Рис. 5. Схема n–раундовой сети RFWKIDEA2m–m

В сети RFWKIDEA2m–m раундовые функции можно представит в виде $Y^j = F_j(T^j)$, $j = \overline{0...m-1}$.

Здесь

$$T^j = (X_{i-1}^j(z_j)K_{2m(i-1)+j}) \oplus \oplus (X_{i-1}^{j+m}(z_{15-j})K_{2m(i-1)+m+j})$$

– входные значения раундовых функций F_0, F_1, F_2,..., F_{m-1}.

Как видно из рис. 5, в V и W преобразовании кроме подблоков X^0, X^{2m-1} все подблоки заменяются между собой.

Как у сети IDEA2m–m, на сети RFWKIDEA2m–m имеет $m+1$ вариантов сети на основе замены подблоков.

$$\begin{cases} X_i^0 = (X_{i-1}^0(z_0)K_{2m(i-1)}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^{m-1}; \\ X_i^1 = (X_{i-1}^{2m-2}(z_1)K_{2m(i-1)+2m-2}) \oplus Y^0 \oplus Y^1; \\ X_i^2 = (X_{i-1}^{2m-3}(z_2)K_{2m(i-1)+2m-3}) \oplus Y^0 \oplus Y^1 \oplus Y^2; \\ ..... \\ X_i^{m-1} = (X_{i-1}^m(z_{m-1})K_{2m(i-1)+m}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus \\ \quad \oplus ... \oplus Y^{m-1}; \\ X_i^m = (X_{i-1}^{m-1}(z_{m-1})K_{2m(i-1)+m-1}) \oplus Y^0; \\ X_i^{m+1} = (X_{i-1}^{m-2}(z_{m-2})K_{2m(i-1)+m-2}) \oplus Y^0 \oplus Y^1; \\ X_i^{m+2} = (X_{i-1}^{m-3}(z_{m-3})K_{2m(i-1)+m-3}) \oplus Y^0 \oplus Y^1 \oplus Y^2; \\ ..... \\ X_i^{2m-1} = (X_{i-1}^{2m-1}(z_0)K_{2m(i-1)+2m-1}) \oplus Y^0, \end{cases}$$

$$i = \overline{1...n} \qquad (20)$$

$$\begin{cases} X_{n+1}^0 = (X_n^0(z_0)K_{2mn}) \\ X_{n+1}^1 = (X_n^{2m-2}(z_1)K_{2mn+1}) \\ X_{n+1}^2 = (X_n^{2m-3}(z_2)K_{2mn+2}) \\ ..... \\ X_{n+1}^{m-1} = (X_n^m(z_{m-1})K_{2mn+m-1}) \\ X_{n+1}^m = (X_n^{m-1}(z_{m-1})K_{2mn+m}) \\ X_{n+1}^{m+1} = (X_n^{m-2}(z_{m-2})K_{2mn+m+1}) \\ X_{n+1}^{m+2} = (X_n^{m-3}(z_{m-3})K_{2mn+m+2}) \\ ..... \\ X_{n+1}^{2m-1} = (X_n^{2m-1}(z_0)K_{2mn+2m-1}), \end{cases}$$

в выходном преобразовании

Структура сети RFWKIDEA2m–(m/2)

В сети RFWKIDEA2m–(m/2), как у сети RFWKIDEA2m–m, длина подблоков X_i^0, X_i^1, X_i^2,..., X_i^{2m-1}, длина раундовых ключей, а также длина входных и выходных блоков функций F_0, F_1, F_2,..., $F_{(m/2)-1}$ равна 32 (16, 8) битам.

Схема $i-$раунда сети RFWKIDEA2m–(m/2) приведена на рис. 6.

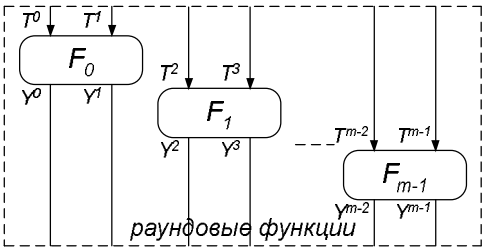

Рис. 6. Схема i – раунда сети RFWKIDEA2m–(m/2)

Если берем $T0 = [T^0, T^1]$, $T1 = [T^2, T^3]$, $T2 = [T^4, T^5]$, ..., $T(m/2-1) = [T^{m-2}, T^{m-1}]$ – в качестве входного значения, $Y0 = [Y^0, Y^1]$, $Y1 = [Y^2, Y^3]$, $Y2 = [Y^4, Y^5]$, ..., $Y(m/2-1) = [Y^{m-2}, Y^{m-1}]$ – в качестве выходного значения раундовой функции, то раундовую функцию можно представить в виде

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

Здесь

$T^j = (X_{i-1}^j(z_j)K_{2m(i-1)+j}) \oplus (X_{i-1}^{m+j}(z_{m-1-j})K_{2m(i-1)+m+j})$, $j = \overline{0...m-1}$ входные значения раундовые функции F_0, F_1, $F_2, \ldots, F_{(m/2)-1}$. 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 $Y(m/2-1) = F_7(T(m/2-1))$ представим в виде $Y^{m-2} = F_{m-1}^0(T^{m-2}, T^{m-1})$, $Y^{m-1} = F_{m-1}^1(T^{m-2}, T^{m-1})$. Процесс шифрования сети RFWKIDEA2m–(m/2) приведен в (21).

$$\begin{cases} X_i^0 = (X_{i-1}^0(z_0)K_{2m(i-1)}) \oplus Y^{m-1}; \\ X_i^1 = (X_{i-1}^{2m-2}(z_1)K_{2m(i-1)+2m-2}) \oplus Y^1; \\ X_i^2 = (X_{i-1}^{2m-3}(z_2)K_{2m(i-1)+2m-3}) \oplus Y^2; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_i^{m-1} = (X_{i-1}^m(z_{m-1})K_{2m(i-1)+m}) \oplus Y^{m-1}; \\ X_i^m = (X_{i-1}^{m-1}(z_{m-1})K_{2m(i-1)+m-1}) \oplus Y^0; \\ X_i^{m+1} = (X_{i-1}^{m-2}(z_{m-2})K_{2m(i-1)+m-2}) \oplus Y^1; \\ X_i^{m+2} = (X_{i-1}^{m-3}(z_{m-3})K_{2m(i-1)+m-3}) \oplus Y^2; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_i^{2m-1} = (X_{i-1}^{2m-1}(z_0)K_{2m(i-1)+2m-1}) \oplus Y^0, \end{cases}$$

$$i = \overline{1...n}, \qquad (21)$$

$$\begin{cases} X_{n+1}^0 = (X_n^0(z_0)K_{2mn}) \\ X_{n+1}^1 = (X_n^{2m-2}(z_1)K_{2mn+1}) \\ X_{n+1}^2 = (X_n^{2m-3}(z_2)K_{2mn+2}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{m-1} = (X_n^m(z_{m-1})K_{2mn+m-1}) \\ X_{n+1}^m = (X_n^{m-1}(z_{m-1})K_{2mn+m}) \\ X_{n+1}^{m+1} = (X_n^{m-2}(z_{m-2})K_{mn+m+1}) \\ X_{n+1}^{m+2} = (X_n^{m-3}(z_{m-3})K_{2mn+m+2}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n+1}^{2m-1} = (X_n^{2m-1}(z_0)K_{(2m+1)n+2m-1}), \end{cases}$$

в выходном преобразовании

Структура сети RFWKIDEA2m–(m/4)

В сети RFWKIDEA2m–(m/4) длина подблоков X_i^0, X_i^1, X_i^2, ..., X_i^{2m-1}, длина раундовых ключей, а также длина входных и выходных блоков функций F_0, F_1, $F_2, \ldots, F_{(m/4)-1}$ равна 32 (16, 8) битам.

Схема i – раунда сети RFWKIDEA2m–(m/4) приведена на рис. 7.

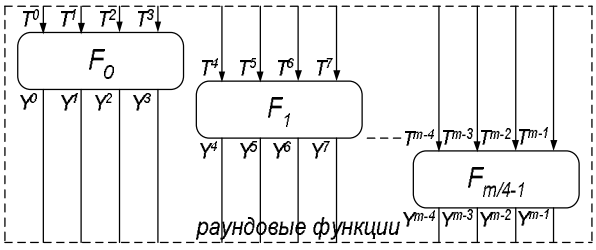

Рис. 7. Схема n–раундовой сети RFWKIDEA2m–(m/4)

Если $T0 = [T^0, T^1, T^2, T^3]$, $T1 = [T^4, T^5, T^6, T^7]$, ..., $T(m/4-1) = [T^{m-4}, T^{m-3}, T^{m-2}, T^{m-1}]$ –входное значение, $Y0 = [Y^0, Y^1, Y^2, Y^3]$, $Y1 = [Y^4, Y^5, Y^6, Y^7]$, ..., $Y(m/4-1) = [Y^{m-4}, Y^{m-3}, Y^{m-2}, Y^{m-1}]$ – выходное значение 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

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

Процесс зашифрования сети RFWKIDEA2m–(m/4) приведен в (21).

Структура сети RFWKIDEA2m–1

В сети RFWKIDEA2m–1 длина подблоков X_i^0, X_i^1, X_i^2,…, X_i^{2m-1}, длина раундовых ключей, а также длина входных и выходных блоков функции F равна 32 (16, 8) битам. Схема i – раунда сети RFWKIDEA2m–1 приведена на рис. 8.

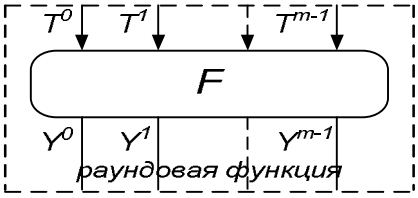

Рис. 8. Схема i – раунда сети RFWKIDEA2m–1

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

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

Процесс зашифрования сети IDEA2m–1 – (20).

В сетях RFWKIDEA2m–(m/2), RFWKIDEA2m–(m/4) и RFWKIDEA2m–1 формула шифрования одинакова, только видом функции отличается.

Генерация ключей RFWKIDEA2m–m, RFWKIDEA2m–(m/2), RFWKIDEA2m–(m/4), RFWKIDEA2m–1

В n – раундовой сети RFWKIDEA2m–m, RFWKIDEA2m–(m/2), RFWKIDEA2m–(m/4), RFWKIDEA2m–1 в каждом раунде применяются $2m$ раундовые ключи и в последнем преобразовании $2m$ раундовых ключей, т.е., число всех ключей равно $2mn + 2m$. В сетях RFWKIDEA2m–m, RFWKIDEA2m–(m/2), RFWKIDEA2m–(m/4) и RFWKIDEA2m–1 ключи расшифрования первого раунда связаны с ключами зашифрования по формуле (22):

$$\begin{aligned}(K_0^d, K_1^d, K_2^d, ..., K_{m-1}^d, K_m^d, K_{m+1}^d, K_{m+2}^d, ..., K_{2m-1}^d) = \\ ((K_{2mn}^c)^{z_0}, (K_{2mn+1}^c)^{z_1}, (K_{2mn+2}^c)^{z_2}, ..., \\ (K_{2mn+m-1}^c)^{z_{m-1}}, (K_{2mn+m}^c)^{z_{m-1}}, (K_{2mn+m+1}^c)^{z_{m-2}}, \\ (K_{2mn+m+2}^c)^{z_{m-3}}, ...(K_{2mn+2m-1}^c)^{z_0}).\end{aligned} \quad (22)$$

Ключи расшифрования выходного преобразования связаны к ключам зашифрования следующим образом:

$$\begin{aligned}(K_{2mn}^d, K_{2mn+1}^d, K_{2mn+2}^d, ..., K_{2mn+m-1}^d, K_{2mn+m}^d, \\ K_{2mn+m+1}^d, K_{2mn+m+2}^d, ..., K_{2mn+2m-1}^d) = ((K_0^c)^{z_0}, \\ (K_1^c)^{z_1}, (K_2^c)^{z_2}, ..., (K_{m-1}^c)^{z_{m-1}}, (K_m^c)^{z_{m-1}}, \\ (K_{m+1}^c)^{z_{m-2}}, (K_{m+2}^c)^{z_{m-3}}, ..., (K_{2m-1}^c)^{z_0}).\end{aligned} \quad (23)$$

Таким же образом ключи расшифрования второго, третьего и n–раунда связаны к ключам зашифрования по формуле (5).

$$\begin{aligned}(K_{2m(i-1)}^d, K_{2m(i-1)+1}^d, K_{2m(i-1)+2}^d, ..., K_{2m(i-1)+m-2}^d, \\ K_{2m(i-1)+m-1}^d, K_{2m(i-1)+m}^d, K_{2m(i-1)+m+1}^d, \\ K_{2m(i-1)+m+2}^d, ..., K_{2m(i-1)+2m-2}^d, K_{2m(i-1)+2m-1}^d) = \\ ((K_{2m(n-i+1)}^c)^{z_0}, (K_{2m(n-i+1)+2m-2}^c)^{z_1}, \\ (K_{2m(n-i+1)+2m-3}^c)^{z_2}, ..., (K_{2m(n-i+1)+m+1}^c)^{z_{m-2}}, \\ (K_{2m(n-i+1)+m}^c)^{z_{m-1}}, (K_{2m(n-i+1)+m-1}^c)^{z_{m-1}}, \\ (K_{2m(n-i+1)+m-2}^c)^{z_{m-2}}, (K_{2m(n-i+1)+m-3}^c)^{z_{m-3}}, ..., \\ (K_{2m(n-i+1)+1}^c)^{z_1}, (K_{2m(n-i+1)+2m-1}^c)^{z_0}).\end{aligned} \quad (24)$$

В 2, 3 и (m+1)–вариантов сети ключи расшифрования первого раунда и выходного преобразования связан к ключам зашифрования по формуле (21) и (22). Ключи расшифрования второго, третьего и *n*–раунда вычисляется как у сети IDEA2m–m, только в индексе взамен 3m используется 2m.

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.

На основе приведенных сетей, при длине подблоков X_i^0, X_i^1, X_i^2,…, X_i^{2m-1} равной 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 3^m. Кроме этого, в сети имеются m+1 варианта.

Таблица 1

Характеристика сетей

Сеть	Число раундовых функций	Число раундовых ключей	Число раундовых ключей, применяемых в функциях
IDEA2m–m	m	$3mn + 2m$	m
IDEA2m–(m/2)	m/2	$(2m+m/2)n+2m$	m/2
IDEA2m–(m/4)	m/4	$(2m+m/4)n+2m$	m/4
IDEA2m–1	1	$(2m+1)n + 2m$	1
RFWKIDEA2m–m	m	$2mn + 2m$	0
RFWKIDEA2m–(m/2)	m/2	$2mn + 2m$	0
RFWKIDEA2m–(m/4)	m/4	$2mn + 2m$	0
RFWKIDEA2m–1	1	$2mn + 2m$	0

Вывод. Если раундовые функции постоянные, выбирая операции add, mul, xor 3^m способом и варианты m+1 способом, но основе разработанных сетей можно построить $3^m(m+1)$ алгоритмов блочного шифрования. 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.

Список литературы

1. Lai X. A proposal for a new block encryption standard. Advances in Cryptology / X. Lai, J.L. Massey // Proc. Eurocrypt'90, LNCS 473, Springer–Verlag, 1991. – P. 389-404.

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

3. Nakahara J., The MESH Block Ciphers / J. Nakahara, Jr. V. Rijmen, B. Preneel, J. Vandewalle //The 4th International Workshop on Info. Security Applications, WISA 2003, Springer–Verlag, LNCS 2908, 2003. – P. 458-473.

4. Nakahara J. Faster Variants MESH Block Ciphers / J. Nakahara // The 5th International Conference on Cryptology in India, INDOCRYPT 2004, Springer–Verlag, LNCS 3348, 2004. – P. 162-174.

5. Арипов М.М. Сеть IDEA4–2, состоящая из двух раундовых функций / М.М. Арипов, Г.Н. Туйчиев // Инфокоммуникации: Сети–Технологии–Решения. – Ташкент, 2012. – №4 (24). – С. 55-59.

6. Туйчиев Г.Н. Сети RFWKIDEA4–2, IDEA4–1 и RFWKIDEA4–1 / Г.Н. Туйчиев // Вестник Туринского политехнического университета в городе Ташкент. – 2013. – №3. – С. 71-77.

7. Туйчиев Г.Н. Сеть IDEA8–4, состоящая из четырех раундовых функций / Г.Н. Туйчиев // Инфокоммуникации: Сети–Технологии–Решения. – Ташкент, 2013. – №2 (26). – С. 55-59.

8. Туйчиев Г.Н. О сетях IDEA8–2, IDEA8–1 и RFWKIDEA8–4, RFWKIDEA8–2, RFWKIDEA8–1, разработанных на основе сети IDEA8–4 / Г.Н. Туйчиев // Узбекский математический журнал. – Ташкент, 2014. – №3. – С. 104-118.

9. Туйчиев Г.Н. Сеть IDEA16–8, состоящая из восьми раундовых функций / Г.Н. Туйчиев // Вестник ТАШГТУ. – Ташкент, 2014. – №1. – С. 183-187.

10. Туйчиев Г.Н. О сетях IDEA16–4, IDEA16–2, IDEA16–1, созданных на основе сети IDEA16–8 / Г.Н. Туйчиев // Республиканскbq семинар «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения». – Ташкент, 2014 г.

11. Туйчиев Г.Н. Сеть IDEA32–16, состоящая из шестнадцати раундовых функций / Г.Н. Туйчиев // Вестник НУУз. – Ташкент, 2013. – №4/1. – С. 57-61.

12. Туйчиев Г.Н. О сетях IDEA32–8, IDEA32–4, IDEA32–2, IDEA32–1, созданных на основе сети IDEA32–16 / Г.Н. Туйчиев // Инфокоммуникации: Сети–Технологии–Решения. – Ташкент, 2014. – №2 (30). – С. 45-50.

Поступила в редколлегию 14.05.2015

Рецензент: д-р экон. наук, доц. С.В. Кавун, Харьковский институт банковского дела Университета банковского дела НБУ (Київ), Харьков.

ПРО МЕРЕЖУ IDEA2m–m, ЩО СКЛАДАЄТЬСЯ З m РАУНДОВИХ ФУНКЦІЙ ТА ЇЇ МОДИФІКАЦІЇ

Г.Н. Туйчиєв

У статті на основі схеми Лай-Мессі розроблені мережі, що складаються з 2m підблоків. У розроблених мережах, аналогічно мережі Фейстеля, при зашифруванні і розшифруванні використовується один і той же алгоритм і як раундові функції можна використовувати будь-які перетворення. На основі цього в розроблених мережах можна побудувати алгоритм блокового шифрування довжиною блоку 64m біт при довжині підблоку, рівній 32 бітам, довжиною блоку 32m біт при довжині підблоку, рівній 16 бітам і довжиною блоку 16m біт при довжині підблоку, рівній 8 бітам.

Ключові слова: *мережа Фейстеля, схема Лай–Мессі, зашифрування, розшифрування, алгоритм блокового шифрування, раунд, раундовая функція, раундові ключі, вихідне перетворення, блок, підблок, множення по модулю, складання по модулю, мультиплікативна інверсія, аддитивна інверсія.*

ABOUT NETWORK Of IDEA2m–m, CONSISTING OF m ROUND OF FUNCTIONS AND ITS MODIFICATION

G.N. Tuychiev

In the article on the basis of chart Lay-Messi networks, consisting of 2m subblocks, are developed. In the developed networks, like the network of Feystelya, for encoding and decryption a the same algorithm is used and as round functions it is possible to utillize any transformations. On the basis of it in the developed networks it is possible to build the algorithm of block encryption of block of 64m length beaten at length of subblock, equal to 32 bats, beaten block of 32m length at length of subblock, equal to 16 bats and beaten block of 16m length at length of subblock, equal to 8 bats.

Keywords: *network of Feystelya, chart of Lay–Messi, encoding, decryptions, algorithm of block encryption, round, round function, round keys, output transformation, block, subblock, increases on the module, additions on the module, multiplicative inversion, additive inversion.*