© Tuychiev G. About RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2 & RFWKIDEA16-1 networks, created on the basis of IDEA16-8 network // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 259-263.

О СЕТЯХ RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2 и RFWKIDEA16-1, СОЗДАННЫХ НА ОСНОВЕ СЕТИ IDEA16-8

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

Аннотация. *В статье на основе сети IDEA16-8 разработаны сети RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2, RFWKIDEA16-1 состоящие из восьми, четырех, двух и одной раундовых функций. Основное преимущество предложенных сетей в том, что при зашифровании и расшифровании используется один и тот же алгоритм, а также в качестве раундовых функций можно использовать любые криптографические преобразования. В разработанных сетях алгебраические операции являются переменными, в качестве этих операции можно использовать операции сложения и умножения по модулю и XOR. В сетях длина подблоков равна 8, 16 и 32 битам и на основе сетей можно создать алгоритм шифрования длиной блока 128, 256 и 512 битам.*

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

Введение

В 1990 году Х. Лай и Дж. Мэсси взамен алгоритма DES разработали новый алгоритм блочного шифрования PES [5]. 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 [6]. Эти алгоритмы основаны на схемы Лай-Мэсси и в основе конструкции алгоритмов лежит «смешение операций различных алгебраических групп».

В алгоритмах шифрования PES и IDEA, аналогично DES, длина блока равна 64 битам. Каждый 64-битный блок делится на четыре 16-битных подблоков и операции производятся над 16-битными подблоками. В процессе шифрования PES и IDEA к парам 16-битных подблоков применяются три различные групповые операции:

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

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

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

В алгоритмах шифрования PES и IDEA раундовые ключи умножаются по модулю $2^{16}+1$ и суммируются по модулю 2^{16} с соответствующими подблоками. В МА преобразовании ограничиваются использованием операции умножения по модулю $2^{16}+1$ и суммированием по модулю 2^{16}, т.е. не используются такие операции как сдвиг, подстановка с помощью S-блоков и т.д. В работах [1-4] 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 соответственно. В разработанных сетях при зашифровании и расшифровании, аналогично сети Фейстеля, используется один и тот же алгоритм, а в качестве раундовых функций можно использовать любые преобразования.

В сети IDEA16-8 в каждом раунде применяются 24 раундовых ключа, причем 8 раундовых ключей применяются в раундовых функциях, 16 раундовых ключей умножаются и суммируются с подблоками. За счет применения 16 раундовых ключей в подблоках, раундовые функции сети IDEA16-8 можно использовать без ключа. Кроме этого, в сети IDEA16-8 раундовые функции имеют по одному входному и выходному блоку. В качестве раундовых функций можно использовать функции, в которых имеются по два входных и выходных блока, по четыре входных и выходных блока, по

восемь входных и выходных блоков, а также по шестнадцать входных и выходных блоков.

В этой статье на основе сети IDEA16-8 разрабатываются:

– сеть RFWKIDEA16-8 (round function without key IDEA16-8), состоящая из восьми раундовых функций,

– сеть RFWKIDEA16-4 (round function without key IDEA16-4), состоящая из четырех раундовых функций,

– сеть RFWKIDEA16-2 (round function without key IDEA16-2), состоящая из двух раундовых функций,

– сеть RFWKIDEA16-1 (round function without key IDEA16-1), состоящая из одной раундовой функции.

Структура сети RFWKIDEA16–8

В сети RFWKIDEA16-8 длина подблоков X^0, X^1, …, X^{15}, длина раундовых ключей, а также длина входных и выходных блоков функций F_0, F_1, …, F_7 равна 32 (16, 8) битам. Схема *n*–раундовой сети RFWKIDEA32-16 приведена на рис. 1, а процесс зашифрования приведен в следующей цепочке преобразований:

$$\begin{cases} X_i^0 = (X_{i-1}^0(z_0)K_{16(i-1)}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^7 \\ X_i^1 = (X_{i-1}^{14}(z_1)K_{16(i-1)+14}) \oplus Y^0 \oplus Y^1 \\ X_i^2 = (X_{i-1}^{13}(z_2)K_{16(i-1)+13}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \\ ..... \\ X_i^7 = (X_{i-1}^{8}(z_7)K_{16(i-1)+8}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \oplus ... \oplus Y^7 \\ X_i^8 = (X_{i-1}^{7}(z_7)K_{16(i-1)+7}) \oplus Y^0 \\ X_i^9 = (X_{i-1}^{6}(z_6)K_{16(i-1)+6}) \oplus Y^0 \oplus Y^1 \\ X_i^{10} = (X_{i-1}^{5}(z_5)K_{16(i-1)+5}) \oplus Y^0 \oplus Y^1 \oplus Y^2 \\ ..... \\ X_i^{15} = (X_{i-1}^{15}(z_0)K_{16(i-1)+15}) \oplus Y^0 \end{cases},$$

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

$$\begin{cases} X_{n+1}^0 = (X_n^0(z_0)K_{16n}) \\ X_{n+1}^1 = (X_n^{14}(z_1)K_{16n+1}) \\ X_{n+1}^2 = (X_n^{13}(z_2)K_{16n+2}) \\ ..... \\ X_{n+1}^7 = (X_n^8(z_7)K_{16n+8}) \\ X_{n+1}^8 = (X_n^7(z_7)K_{16n+9}) \\ X_{n+1}^9 = (X_n^6(z_6)K_{16n+10}) \\ X_{n+1}^{10} = (X_n^5(z_5)K_{16n+11}) \\ ..... \\ X_{n+1}^{15} = (X_n^{15}(z_0)K_{16n+15}) \end{cases}, \textit{в выходном преобразовании}$$

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

Как и у сети IDEA16-8, в сети RFWKIDEA16-8 в зависимости от замены подблоков, в *V* и *W* преобразованиях имеются 9 вариантов сети.

Структура сети RFWKIDEA16-4, RFWK-IDEA16-2, RFWKIDEA16-1

В вышеприведенной сети (RFWKIDEA16-8) раундовые функции имеют один вход и один выход. Кроме этого, в блочных шифрах применяются раундовые функции, имеющие по два входных и выходных блока. На основе сети RFWKIDEA16-8 можно построить сети, в которых раундовые функции имеют по четыре входных и выходных блоков и по восемь входных и выходных блоков. Сеть, для которой раундовые функции имеют по два входных и выходных блока, а также в которой применяется четыре раундовых функции, называется RFWKIDEA16-4. Аналогично, сеть, для которой раундовые функции имеют по четыре входных и выходных блока, а также применяется две раундовые функции, называется RFWKIDEA16-2 и т.д.

Таким же образом определяется сеть RFW-KIDEA16-1. Схемы сети RFWKIDEA16-4, RFW-KIDEA16-2, RFWKIDEA16-1 приведены на рис. 2-4.

В сети RFWKIDEA16-4 раундовые функции F_0, F_1, F_2, F_3 имеют по два входных и выходных блока, длина которых равна 32 (16, 8) битам. Если в качестве входного блока положим $T0 = [T^0, T^1]$, $T1 = [T^2, T^3]$, $T2 = [T^4, T^5]$, $T3 = [T^6, T^7]$, и в качестве выходного блока раундовой функции берём $Y0 = [Y^0, Y^1]$, $Y1 = [Y^2, Y^3]$, $Y2 = [Y^4, Y^5]$, $Y3 = [Y^6, Y^7]$, то раундовую функцию можно представить в виде $Y0 = F_0(T0)$, $Y1 = F_1(T1)$, $Y2 = F_2(T2)$, $Y3 = F_3(T3)$. Для корректности процесса зашифрования раундовую функцию $Y0 = F_0(T0)$ представим в виде $Y^0 = F_0^0(T^0, T^1)$, $Y^1 = F_0^1(T^0, T^1)$, а раундовую функцию $Y1 = F_1(T1)$ представим в виде $Y^2 = F_1^0(T^2, T^3)$, $Y^3 = F_1^1(T^2, T^3)$ и так далее … раундовую функцию $Y3 = F_7(T3)$ представим в виде $Y^6 = F_3^0(T^6, T^7)$, $Y^7 = F_3^1(T^6, T^7)$.

В сети RFWKIDEA16-2 раундовые функции F_0, F_1 имеют четыре входных и выходных блока по 32 (16, 8) бита соответственно. Если $T0 = [T^0, T^1, T^2, T^3]$, $T1 = [T^4, T^5, T^6, T^7]$ – входной блок, $Y0 = [Y^0, Y^1, Y^2, Y^3]$, $Y1 = [Y^4, Y^5, Y^6, Y^7]$ – выходной блок раундовых функции, то раундовую функцию можно представить в виде $Y0 = F_0(T0)$, $Y1 = F_1(T1)$. Для корректности процесса зашифрования раундовую функцию $Y0 = F_0(T0)$ представим в виде $Y^0 = F_0^0(T^0, T^1, T^2, T^3)$, $Y^1 = F_0^1(T^0, T^1, T^2, T^3)$, … , $Y^3 = F_0^3(T^0, T^1, T^2, T^3)$, раундовую функцию $Y1 = F_1(T1)$ представим в виде $Y^4 = F_1^0(T^4, T^5, T^6, T^7)$, $Y^5 = F_1^1(T^4, T^5, T^6, T^7)$, … , $Y^7 = F_1^3(T^4, T^5, T^6, T^7)$.

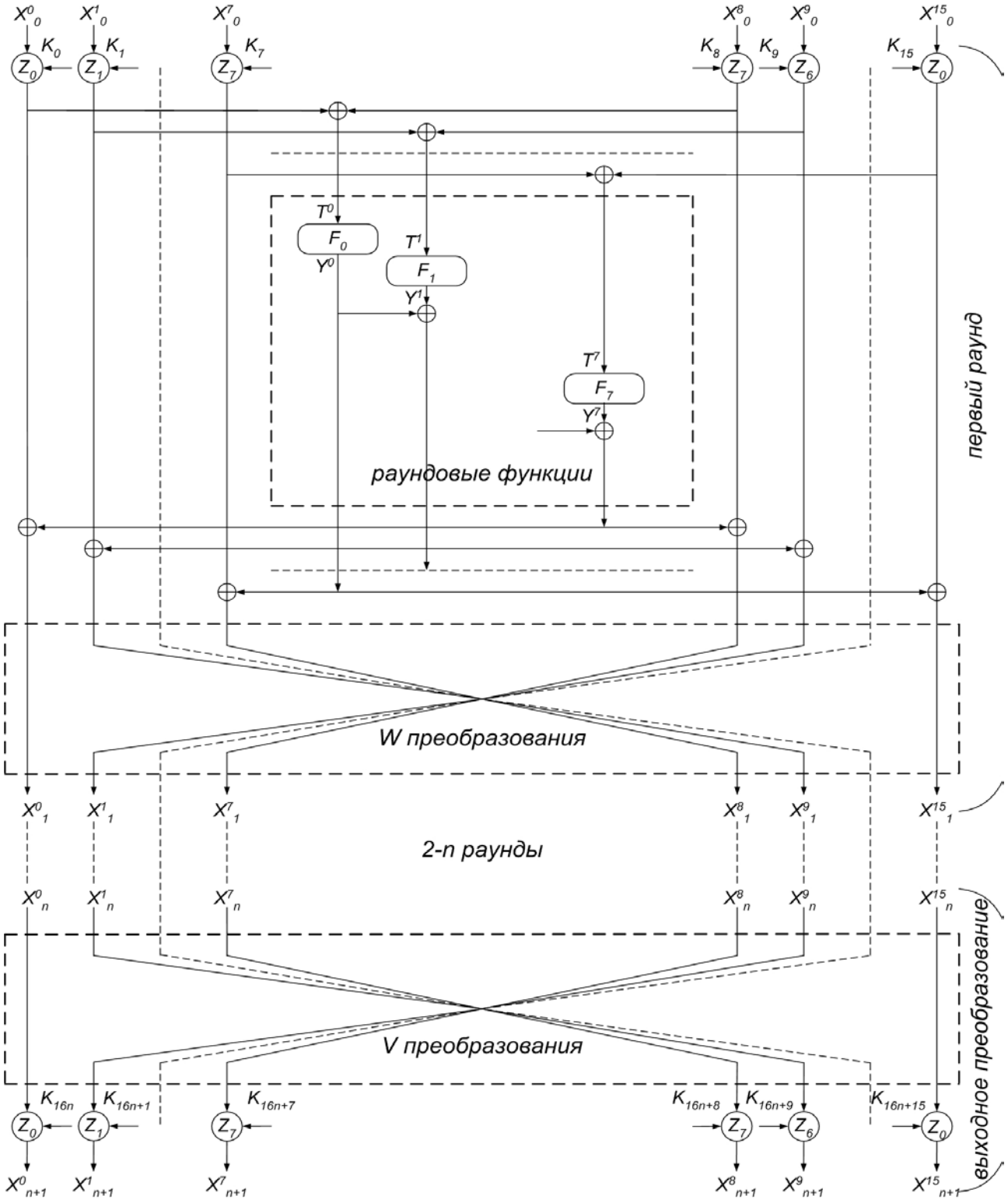

Рис. 1. Схема *n*–раундовой сети RFWKIDEA16-8

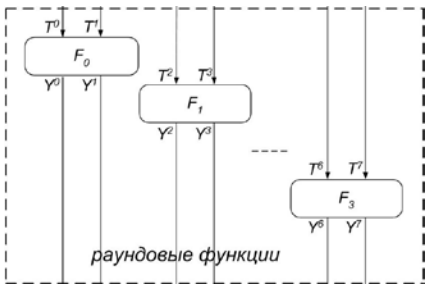

Рис. 2. Схема раундовой функции сети RFWKIDEA16-4

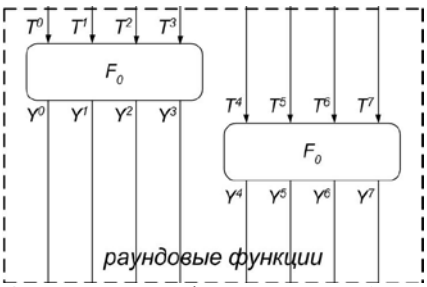

Рис. 3. Схема раундовой функции сети RFWKIDEA16-2

Рис. 4. Схема раундовой функции сети RFWKIDEA16-1

Аналогично сети RFWKIDEA16-2, если в сети RFWKIDEA16-1 в качестве входного блока берем $T=[T^0,T^1,...,T^7]$ и в качестве выходного блока раундовой функции берем $Y=[Y^0,Y^1,...,Y^7]$, то раундовую функцию можно представить в виде $Y=F(T)$. Для корректности процесса зашифрования раундовую функцию $Y=F(T)$ представим в виде $Y^0=F^0(T^0,T^1,...,T^7)$, $Y^1=F^1(T^0,T^1,...,T^7)$, ..., $Y^7=F^7(T^0,T^1,...,T^7)$. В сетях RFWKIDEA32-8, RFWKIDEA32-4, RFWKIDEA32-2, RFWKIDEA32-1 F_i^j – выходной $j+1$ блок раундовой функции F_i.

Процесс зашифрования RFWKIDEA32-8, RFWKIDEA32-4, RFWKIDEA32-2, RFWKIDEA32-1 похож на цепочку преобразований (1), только вместо $Y^0\oplus Y^1$ ставится Y^1, вместо $Y^0\oplus Y^1\oplus Y^2$ ставится Y^2 и т. д., … вместо $Y^0\oplus Y^1\oplus Y^2\oplus...\oplus Y^7$ ставится Y^7.

Генерация ключей сети RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2, RFWKIDEA16-1

В $n-$раундовой сети RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2, RFWKIDEA16-1 в каждом раунде применяются 16 раундовых ключей и в последнем преобразовании 16 раундовых ключей, т.е., число всех ключей равно $32n+32$. В $n-$раундовой сети RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2, RFWKIDEA16-1 раундовые ключи расшифрования первого раунда связаны с ключами зашифрования по формуле (2).

$$\begin{aligned}&(K_0^d,K_1^d,K_2^d,K_3^d,K_4^dK_5^d,K_6^d,K_7^d,K_8^d,K_9^d,K_{10}^d,K_{11}^d,\\&K_{12}^d,K_{13}^d,K_{14}^d,K_{15}^d)=((K_{16n}^c)^{z_0},(K_{16n+1}^c)^{z_1},(K_{16n+2}^c)^{z_2},\\&(K_{16n+3}^c)^{z_3},(K_{16n+4}^c)^{z_4},(K_{16n+5}^c)^{z_5},(K_{16n+6}^c)^{z_6},\\&(K_{16n+7}^c)^{z_7},(K_{16n+8}^c)^{z_7},(K_{16n+9}^c)^{z_6},(K_{16n+10}^c)^{z_5},\\&(K_{16n+11}^c)^{z_4},(K_{16n+12}^c)^{z_3},(K_{16n+13}^c)^{z_2},(K_{16n+14}^c)^{z_1},\\&K_{16n+15}^c)^{z_0})\end{aligned}\quad(2)$$

Если в качестве операции z_i, $i=\overline{0...7}$ 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 выполняется $K\otimes K^{-1}=1\bmod(2^{32}+1)$, $K\otimes K^{-1}=1\bmod(2^{16}+1)$, $K\otimes K^{-1}=1\bmod(2^8+1)$ и $-K\boxplus K=0$, $K\oplus K=1$.

Ключи расшифрования выходного преобразования связаны с ключами зашифрования следующим образом:

$$\begin{aligned}&(K_{16n}^d,K_{16n+1}^d,K_{16n+2}^d,K_{16n+3}^d,K_{16n+4}^d,K_{16n+5}^d,K_{16n+6}^d,\\&K_{16n+7}^d,K_{16n+8}^d,K_{16n+9}^d,K_{16n+10}^d,K_{16n+11}^d,K_{16n+12}^d,\\&K_{16n+13}^d,K_{16n+14}^d,K_{16n+15}^d)=((K_0^c)^{z_0},(K_1^c)^{z_1},(K_2^c)^{z_2},\\&(K_3^c)^{z_3},(K_4^c)^{z_4},(K_5^c)^{z_5},(K_6^c)^{z_6},(K_7^c)^{z_7},(K_8^c)^{z_7},\\&(K_9^c)^{z_6},(K_{10}^c)^{z_5},(K_{11}^c)^{z_4},(K_{12}^c)^{z_3},(K_{13}^c)^{z_2},(K_{14}^c)^{z_1},\\&(K_{15}^c)^{z_0}).\end{aligned}\quad(3)$$

Таким же образом, ключи расшифрования второго, третьего и n–раунда связаны с ключами зашифрования по формуле (4):

$$\begin{aligned}&(K_{16(i-1)}^d,K_{16(i-1)+1}^d,K_{16(i-1)+2}^d,K_{16(i-1)+3}^d,K_{16(i-1)+4}^d,\\&K_{16(i-1)+5}^d,K_{16(i-1)+6}^d,K_{16(i-1)+7}^d,K_{16(i-1)+8}^d,K_{16(i-1)+9}^d,\\&K_{16(i-1)+10}^d,K_{16(i-1)+11}^d,K_{16(i-1)+12}^d,K_{16(i-1)+13}^d,\\&K_{16(i-1)+14}^d,K_{16(i-1)+15}^d)=((K_{16(n-i+1)}^c)^{z_0},\\&K_{16(n-i+1)+14}^c)^{z_1},(K_{16(n-i+1)+13}^c)^{z_2},(K_{16(n-i+1)+12}^c)^{z_3},\\&(K_{16(n-i+1)+11}^c)^{z_4},(K_{16(n-i+1)+10}^c)^{z_5},(K_{16(n-i+1)+9}^c)^{z_6},\\&(K_{16(n-i+1)+8}^c)^{z_7},(K_{16(n-i+1)+7}^c)^{z_7},(K_{16(n-i+1)+6}^c)^{z_6},\\&(K_{16(n-i+1)+5}^c)^{z_5},(K_{16(n-i+1)+4}^c)^{z_4},(K_{16(n-i+1)+3}^c)^{z_3},\\&(K_{16(n-i+1)+2}^c)^{z_2},(K_{16(n-i+1)+1}^c)^{z_1},(K_{16(n-i+1)+15}^c)^{z_0}),\\&i=\overline{2...n}\end{aligned}\quad(4)$$

Полученные результаты

Таким образом, в этой статье, на основе сети IDEA16-8, разработаны 4 класса сетей: RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2 и RFWKIDEA16-1. В разработанных сетях, в качестве раундовых функций можно выбрать любые преобразования, в том числе однонаправленные функции, так как при расшифровании нет необходимости вычисления обратной функции к раундовым функциям.

На основе приведенных сетей, при длине подблоков 32 бит, можно построить алгоритм зашифрования длиной блока 512 бит, при длине подблоков 16 бит, можно построить алгоритм зашифрования длиной блока 256 бит и при длине подблоков 8 битам, а также можно построить алгоритм шифрования длиной блока 128 бит. Если выбрать в качестве операций z_i, $i=\overline{0...7}$ операции mul, add и xor, все возможные варианты данного выбора равны 3^8. Кроме этого, в каждой сети имеются 9 вариантов.

Преимущество разработанных сетей состоит в том, что при зашифровании и расшифровании используется один и тот же алгоритм – это даёт удобство при создании аппаратных и программно–аппаратных средств.

Литература

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

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

[3] Туйчиев Г.Н. Сеть IDEA16–8, состоящая из восьми раундовых функций // Вестник ТашГТУ. — Ташкент, 2014. — №1. — С. 184-187.

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

[5] 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

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

УДК 003.056.55 (045)

Туйчієв Г.Н. Про мережі RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2 та RFWKIDEA16-1, створені на основі мережі IDEA16-8

Анотація. *У статті на основі мережі IDEA16-8 розроблені мережі RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2 та RFWKIDEA16-1, які складаються з восьми, чотирьох, двох і однієї раундової функції відповідно. Основна перевага запропонованих мереж полягає у тому, що при зашифруванні та розшифруванні використовується один і той же алгоритм, а також перевагою є те, що у якості раундових функцій можна використовувати будь-які криптографічні перетворення. У розроблених мережах алгебраїчні операції є змінними, у якості цих операції можна використовувати операції додавання і множення за модулем та XOR. У цих мережах довжина підблоків дорівнює 8, 16 і 32 біти відповідно. Крім цього, на основі запропонованих у статті мереж можна створити алгоритми шифрування із довжиною блоку 128, 256 та 512 біт.*

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

Tuychiev G. About RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2 &RFWKIDEA16-1 networks created on the basis of IDEA16-8 network

Abstract. *In the paper on the basis of the IDEA16-8 network were developed networks RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2 and RFWKIDEA16-1 that consist of eight, four, two and one round function. The main advantage of the proposed networks is that during encryption and decryption using the same algorithm as well as a round function can be used any cryptographic transformations. In the developed networks algebraic operations are variable, as these operations can be used the operations of addition and multiplication in modulo & XOR. Lengths of subblocks in these networks are 8, 16 and 32 bits. Besides using proposed in paper networks can be created encryption algorithm with lengths of block 128, 256 and 512 bits.*

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

Отримано *3 жовтня 2014 року*, затверджено редколегією *20 жовтня 2014 року*