УДК 621.391:519.2:519.7

ОЦЕНКА СЛОЖНОСТИ РАЗЛИЧЕНИЯ СХЕМЫ ЛЕЙ-МЕССИ И СЛУЧАЙНОЙ ПЕРЕСТАНОВКИ

Р.В. ОЛЕЙНИКОВ, Д.С. КАЙДАЛОВ

Выполнен анализ эффективности трехраундовой схемы Лей-Месси – высокоуровневой конструкции симметричного блочного шифра. Оценка получена на основе определения сложности проведения атаки с выбранными открытыми текстами, направленной на различение конструкции криптографического преобразования и модели идеального шифра – случайной перестановки. Обоснована верхняя граница преимущества для произвольного алгоритма-различителя и точные значения преимущества для двух конкретных методов.

Ключевые слова: блочный шифр, схема Лей-Месси, случайная перестановка.

ВВЕДЕНИЕ

Схема Лей-Месси является альтернативной высокоуровневой конструкцией блочных симметричных шифров. На ее основе построены алгоритмы FOX, «Мухомор» и др. Основным преимуществом схемы Лей-Месси, как и цепи Фейстеля, является возможность построения инволютивного преобразования, т.е. расшифрование реализовано практически аналогично зашифрованию при использовании обратного порядка раундовых подключей. Дополнительным преимуществом этой конструкции является отсутствие требований к биективности раундовой функции (как у SPN-структур), что упрощает разработку и реализацию.

Как и цепь Фейстеля, схема Лей-Месси представляет собой итеративную структуру. Операции шифрования можно выразить следующим образом [1]:

$$L_i = \sigma(L_{i-1} \oplus F(L_{i-1} \oplus R_{i-1}, K_{i-1})),$$

$$R_i = R_{i-1} \oplus F(L_{i-1} \oplus R_{i-1}, K_{i-1}), \text{ при } i \in 1...n-1.$$

На последнем раунде преобразование σ отсутствует:

$$L_n = L_{n-1} \oplus F(L_{n-1} \oplus R_{n-1}, K_{n-1}),$$

$$R_n = R_{n-1} \oplus F(L_{n-1} \oplus R_{n-1}, K_{n-1}).$$

Здесь R_i и L_i – это правая и левая части сообщения на i-ом раунде (соответственно R_0 и L_0 – открытое сообщение, а R_n и L_n – зашифрованное сообщение, где n – количество раундов). σ –некоторое ортоморфное преобразование [1], а отображение F – это функция усложнения, зависимая от ключа. Общая схема одного раунда приведена на рис. 1.

Далее предполагается, что σ построена на основе одного раунда цепи Фейстеля с тождественной раундовой функцией (рис. 2), поскольку в шифрах, построенных по схеме Лей-Месси (FOX, Мухомор), используется именно такая конструкция.

Блочный шифр реализует определенное подмножество перестановок, количество которых равняется количеству возможных ключей шифрования. Т.к. выбор такого подмножества определяется структурой шифра и не является случайным, то возможно построение алгоритма-различителя, который мог бы определить, является ли конкретная перестановка случайно выбранной из общего множества, либо полученной в результате действия блочного шифра. Таким образом, анализируя входные данные, поданные на вход алгоритма-различителя, на выходе алгоритма мы будем иметь «1» либо «0». «1» в том случае, если считается, что входные данные были получены с помощью блочного шифра (схемы Лей-Месси в данном случае) и «0», если считается, что это результат действия случайной функции. Для схемы Лей-Месси вероятность появления «1» будет иметь определенное значение. Однако и для случайной функции вероятность появления «1» на выходе алгоритма-различителя не равна нулю, поскольку возможен случайный выбор произвольной перестановки, аналогичной сформированной схемой Лей-Месси.

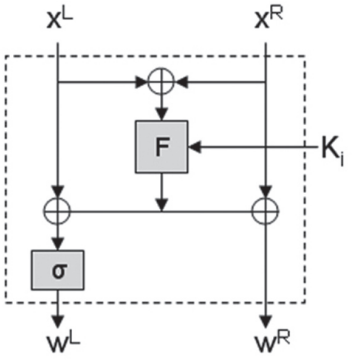

Рис. 1. Схема Лей-Месси

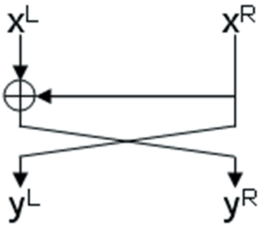

Рис. 2. Функция σ

Детально модель алгоритма-различителя и характеристики его эффективности рассмотрены в нашей предыдущей статье [2].

1. ВЕРХНЯЯ ГРАНИЦА ВЕРОЯТНОСТИ РАЗЛИЧЕНИЯ СХЕМЫ ЛЕЙ-МЕССИ И СЛУЧАЙНОЙ ФУНКЦИИ

Далее будет рассмотрена максимальная вероятность различения случайной функции и схемы Лей-Месси с количеством раундов $r \geq 3$. Доказательство будет приводиться для 3-раундовой схемы Лей-Месси, однако итоговое неравенство будет справедливо и для конструкций с большим количеством раундов, поскольку сложность различения будет только увеличиваться.

3-раундовая схема Лей-Месси приведена на рис. 3.

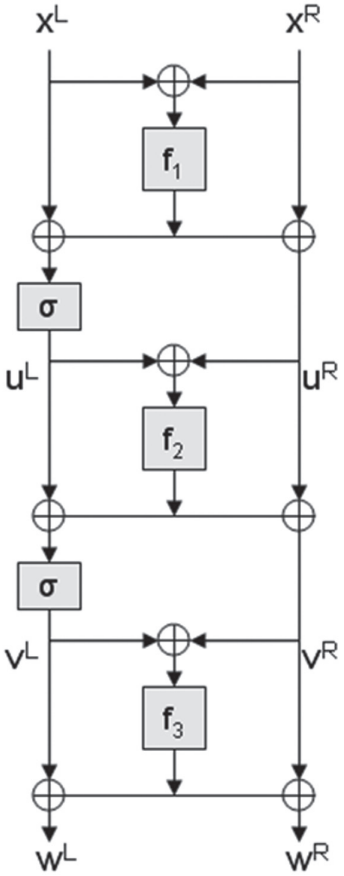

Рис. 3. Схема Лей-Месси

Далее используются следующие обозначения:

x^L, x^R – левая и правая половины входного блока данных, каждая по n бит. Соответственно общая длина входного блока составляет $2n$ бит;

$\Delta x = x^L \oplus x^R$ – XOR-разность между левой и правой половинами битового вектора;

u^L, u^R – левая и правая половины промежуточного результата после 1-го раунда преобразований;

v^L, v^R – левая и правая половины промежуточного результата после 2-го раунда преобразований;

w^L, w^R – левая и правая половины выходного значения;

f_1, f_2, f_3 – случайные функции;

$\sigma^2(x) = \sigma(\sigma(x))$.

Кроме того, вводится функция $\sigma'(x) = \sigma(x) + x$. Если σ – линейная, то σ' тоже линейная.

Отметим, что рассматриваемый алгоритм-различитель будет иметь смысл для любой линейной функции (т.е. такой, что $\sigma(x+y) = \sigma(x) + \sigma(y)$).

Теорема 1. Максимальная вероятность различения схемы Лей-Месси (рис. 3) с количеством раундов $r \geq 3$ и случайных раундовых функциях при k запросах не превышает значения

$$Adv_{\max}(LM, PRF) \leq 1 - \left(\frac{2^n - 2}{2^n - 1}\right)^{\frac{k(k-1)}{2}}.$$

Доказательство.

Сначала необходимо доказать, что при $\Delta U_i \neq \Delta U_j$ (рис. 1) различение невозможно.

Итак, пусть $\Delta U_i \neq \Delta U_j$ для всех возможных пар запросов. Тогда

$$W_i^L = V_i^L \oplus f_3(\Delta V_i) =$$
$$= \sigma^2(x_i^L \oplus f_1(\Delta x_i)) \oplus \sigma(f_2(\Delta U_i)) \oplus f_3(\Delta V_i),$$
$$W_i^R = V_i^R \oplus f_3(\Delta V_i) =$$
$$= x_i^R \oplus f_1(\Delta x_i) \oplus f_2(\Delta U_i) \oplus f_3(\Delta V_i),$$
$$W_j^L = V_j^L \oplus f_3(\Delta V_j) =$$
$$= \sigma^2(x_j^L \oplus f_1(\Delta x_j)) \oplus \sigma(f_2(\Delta U_j)) \oplus f_3(\Delta V_j),$$
$$W_j^R = V_j^R \oplus f_3(\Delta V_j) =$$
$$= x_j^R \oplus f_1(\Delta x_j) \oplus f_2(\Delta U_j) \oplus f_3(\Delta V_j).$$

Поскольку f_2 – случайная функция (перестановка), то $f_2(\Delta U_i)$ и $f_2(\Delta U_j)$ – случайные величины. Следовательно, выходные значения схемы Лей-Месси также будут случайными.

Кроме того, рассмотрим значения ΔW_i и ΔW_i:

$$\Delta W_i = W_i^L \oplus W_i^R = \sigma^2(x_i^L \oplus f_1(\Delta x_i)) \oplus \sigma(f_2(\Delta U_i)) \oplus$$
$$\oplus x_i^R \oplus f_1(\Delta x_i) \oplus f_2(\Delta U_i) = \sigma^2(x_i^L \oplus f_1(\Delta x_i)) \oplus$$
$$\oplus x_i^R \oplus f_1(\Delta x_i) \oplus \sigma'(f_2(\Delta U_i)),$$

$$\Delta W_j = W_j^L \oplus W_j^R = \sigma^2(x_j^L \oplus f_1(\Delta x_j)) \oplus$$
$$\oplus \sigma(f_2(\Delta U_j)) \oplus x_j^R \oplus f_1(\Delta x_j) \oplus f_2(\Delta U_j) =$$
$$= \sigma^2(x_j^L \oplus f_1(\Delta x_j)) \oplus x_j^R \oplus f_1(\Delta x_j) \oplus \sigma'(f_2(\Delta U_j)).$$

Поскольку f_2 – случайная функция (перестановка), то $\sigma'(f_2(\Delta U_i))$ и $\sigma'(f_2(\Delta U_j))$ – случайные величины. Соответственно ΔW_i и ΔW_i в таком случае тоже случайные значения.

Вероятность выполнения условия $\Delta U_i = \Delta U_j$ можно оценить следующим образом.

$$\sigma(x_i^L \oplus f_1(\Delta x_i)) \oplus x_i^R \oplus f_1(\Delta x_i) =$$
$$= \sigma(x_j^L \oplus f_1(\Delta x_j)) \oplus x_j^R \oplus f_1(\Delta x_j),$$

$$\sigma(x_i^L) \oplus \sigma(f_1(\Delta x_i)) \oplus x_i^R \oplus f_1(\Delta x_i) =$$
$$= \sigma(x_j^L) \oplus \sigma(f_1(\Delta x_j)) \oplus x_j^R \oplus f_1(\Delta x_j),$$

$$\begin{aligned}\sigma(f_1(\Delta x_i))\oplus\sigma(f_1(\Delta x_j))\oplus f_1(\Delta x_i)\oplus f_1(\Delta x_j)=\\ =\sigma(x_j^L)\oplus\sigma(x_i^L)\oplus x_j^R\oplus x_i^R,\\ \sigma^{/}(f_1(\Delta x_i))\oplus\sigma(f_1(\Delta x_j))=\\ =\sigma(x_j^L)\oplus\sigma(x_i^L)\oplus x_j^R\oplus x_i^R.\end{aligned} \quad (1)$$

Если f_1 – случайная функция, то максимальная вероятность выполнения (1) (при подобранных открытых текстах) не превышает

$$P_1 \le \frac{1}{2^n}.$$

Если же f_1 – случайная перестановка, то максимальная вероятность выполнения (1) (при подобранных открытых текстах) не превышает

$$P_2 \le \frac{1}{2^n-1}. \quad (2)$$

Формула (2) учитывает условие

$$\sigma^{/}(f_1(\Delta x_i))\oplus\sigma(f_1(\Delta x_j))\neq 0.$$

Поскольку определяется верхняя граница различения, то $P(\Delta U_i=\Delta U_j)=P_2$. Тогда для двух запросов вероятность выполнения условия $\Delta U_i\neq\Delta U_j$ равна

$$P(\Delta U_i\neq\Delta U_j)=1-P_2\le 1-\frac{1}{2^n-1}=\frac{2^n-2}{2^n-1}.$$

Для k запросов вероятность того, что для каждой пары выполняется условие $\Delta U_i\neq\Delta U_j$, имеет следующее значение:

$$P(\Delta U_i\neq\Delta U_j)\le\left(\frac{2^n-2}{2^n-1}\right)^{\frac{k(k-1)}{2}}. \quad (3)$$

Отсюда вероятность различения схемы Лей-Месси не превышает значения (3).

Максимальное преимущество алгоритма-различителя равно

$$Adv_{\max}(LM,PRF)=|P_{\max}(LM)-P_{\max}(PRF)|.$$

Можно сделать предположение в пользу криптоаналитика о том, что для случайной функции вероятность появления «1» на выходе алгоритма-различителя равна нулю (ложное срабатывание не допускается). Тогда преимущество равно

$$\begin{aligned}Adv_{\max}(LM,PRF)=|P_{\max}(LM)-P_{\max}(PRF)\le|\\ \le 1-\left(\frac{2^n-2}{2^n-1}\right)^{\frac{k(k-1)}{2}}.\end{aligned} \quad (4)$$

Доказательство окончено.

На рис. 4 и 5 приведены теоретически максимальные вероятности различения цепи Фейстеля (пунктиром) и схемы Лей-Месси. Формула для максимальной вероятности различения цепи Фейстеля рассматривалась в [2]. Для схемы Лей-Месси (сплошная линия) использовалась формула (4).

Из рис. 4 и 5 видно, что при одинаковом количестве запросов вероятность различения схемы Лей-Месси ниже, что свидетельствует о более высокой эффективности схемы Лей-Месси как высокоуровневой конструкции блочного шифра.

Рассмотренная вероятность является всего лишь теоретической верхней границей различения. Это значит, что реальная максимальная вероятность различения может быть и меньше.

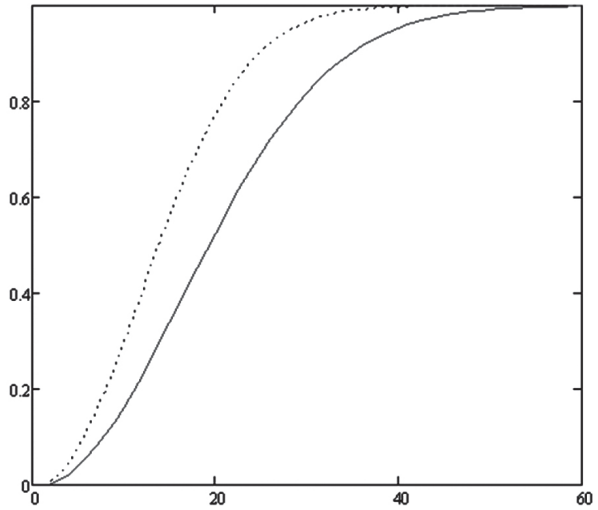

Рис. 4. Максимальные вероятности различения для цепи Фейстеля и схемы Лей-Месси для блока n=8

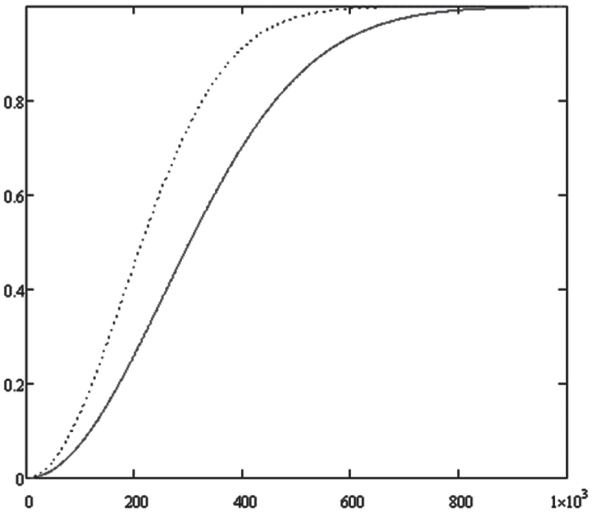

Рис. 5. Максимальные вероятности различения для цепи Фейстеля и схемы Лей-Месси для блока n=16

2. АЛГОРИТМ-РАЗЛИЧИТЕЛЬ ДЛЯ 3-РАУНДОВОЙ СХЕМЫ ЛЕЙ-МЕССИ СО СЛУЧАЙНЫМИ ФУНКЦИЯМИ В КАЧЕСТВЕ РАУНДОВЫХ ПРЕОБРАЗОВАНИЙ

Оценка вероятности различения, приведенная в теореме 1, является теоретически максимально возможной вероятностью различения. Однако для практически реализуемых алгоритмов различения данная вероятность будет меньше. Кроме того, с ростом числа раундов вероятность различения также будет уменьшаться. Стоит отметить, что высокоуровневая конструкция может иметь несколько различителей одновременно, каждый из которых позволяет получить определенную вероятность.

Алгоритм-различитель №1 для 3-раундовой схемы Лей-Месси со случайными функциями в качестве раундовых преобразований.

Алгоритм-различитель для k пар входных аргументов (x_i, x_j) проверяет выполнение равенства

$$\Delta W_i \oplus \Delta W_j = \sigma(x_i^R \oplus x_j^R) \oplus x_i^R \oplus x_j^R . \qquad (5)$$

В случае выполнения хотя бы для одной пары возвращаемое значение будет «1» (определена схема Лей-Месси), иначе – «0» (случайная перестановка).

Теорема 2. Для k запросов вида (x_i, x_j), соответствующих условиям $\sigma(x_i^L \oplus x_j^L) = x_i^R \oplus x_j^R$ и $\Delta x_i \neq \Delta x_j$, при проверке выполнения равенства $\Delta W_i \oplus \Delta W_j = \sigma(x_i^R \oplus x_j^R) \oplus x_i^R \oplus x_j^R$, $0 \le i < j < k$ вероятность различения 3-раундовой схемы Лей-Месси на основе случайных функций как раундового преобразования и случайной перестановки не превышает значения

$$Adv(LM, PRP) \le$$

$$\le \left| \left(1 - \frac{2^n}{2^{2n}-1}\right)^{\frac{k(k-1)}{2}} - \left(1 - \frac{2^{n+1}-1}{2^{2n}}\right)^{\frac{k(k-1)}{2}} \right|. \qquad (6)$$

Доказательство.

При $k = 2$ для схемы Лей-Месси вероятность выполнения равенства (5) при использовании случайных функций в раундовом преобразовании равна значению

$$P(LM) = 1 - \left(1 - \frac{1}{2^n}\right)^2 = \frac{2^{n+1}-1}{2^{2n}} .$$

Результат получается из следующих выводов. Полные выражения для ΔW_i и ΔW_j представляются в виде

$$\Delta W_i = W_i^L \oplus W_i^R = V_i^L \oplus V_i^R =$$
$$= \sigma(\sigma(x_i^L \oplus f_1(\Delta x_i)) \oplus f_2(\Delta U_i)) \oplus \qquad (7)$$
$$\oplus x_i^R \oplus f_1(\Delta x_i) \oplus f_2(\Delta U_i),$$

$$\Delta W_j = W_j^L \oplus W_j^R = V_j^L \oplus V_j^R =$$
$$= \sigma(\sigma(x_j^L \oplus f_1(\Delta x_j)) \oplus f_2(\Delta U_j)) \oplus \qquad (8)$$
$$\oplus x_j^R \oplus f_1(\Delta x_j) \oplus f_2(\Delta U_j).$$

Учитывая, что функция - линейная, выражения (7) и (8) можно представить следующим образом:

$$\Delta W_i = W_i^L \oplus W_i^R = V_i^L \oplus V_i^R =$$
$$= \sigma^2(x_i^L) \oplus \sigma^2(f_1(\Delta x_i)) \oplus \qquad (9)$$
$$\oplus \sigma(f_2(\Delta U_i)) \oplus x_i^R \oplus f_1(\Delta x_i) \oplus f_2(\Delta U_i),$$

$$\Delta W_j = W_j^L \oplus W_j^R = V_j^L \oplus V_j^R =$$
$$= \sigma^2(x_j^L) \oplus \sigma^2(f_1(\Delta x_j)) \oplus \sigma(f_2(\Delta U_j)) \oplus \qquad (10)$$
$$\oplus x_j^R \oplus f_1(\Delta x_j) \oplus f_2(\Delta U_j).$$

Таким образом, равенство (5) будет выполняться в двух случаях:

1. В случае возникновения коллизии на функции f_1: если произошла коллизия и $f_1(\Delta x_i) = f_1(\Delta x_j)$, то также выполняется условие $\Delta U_i = \Delta U_j$, соответственно и $f_2(\Delta U_i) = f_2(\Delta U_j)$.

Для равенства $\Delta U_i = \Delta U_j$:

$$\Delta U_i = U_i^L \oplus U_i^R =$$
$$= \sigma(x_i^L \oplus f_1(\Delta x_i)) \oplus x_i^R \oplus f_1(\Delta x_i),$$
$$\Delta U_j = U_j^L \oplus U_j^R =$$
$$= \sigma(x_j^L \oplus f_1(\Delta x_j)) \oplus x_j^R \oplus f_1(\Delta x_j).$$

Соответственно, если $\Delta U_i = \Delta U_j$, то справедливо следующее выражение:

$$\sigma(x_i^L) \oplus \sigma(f_1(\Delta x_i)) \oplus x_i^R \oplus f_1(\Delta x_i) =$$
$$= \sigma(x_j^L) \oplus \sigma(f_1(\Delta x_j)) \oplus x_j^R \oplus f_1(\Delta x_j).$$

Из $f_1(\Delta x_i) = f_1(\Delta x_j)$ следует

$$\sigma(x_i^L) \oplus x_i^R = \sigma(x_j^L) \oplus x_j^R .$$

Это соответствует условию, по которому отбираются пары открытых текстов, поэтому при возникновении коллизии на f_1 также выполняется $f_2(\Delta U_i) = f_2(\Delta U_j)$.

В этом случае разность выражений (9) и (10) равна

$$\Delta W_i \oplus \Delta W_j = \sigma^2(x_i^L) \oplus x_i^R \oplus \sigma^2(x_j^L) \oplus x_j^R =$$
$$= \sigma^2(x_i^L \oplus x_j^L) \oplus x_i^R \oplus x_j^R ,$$

что соответствует (5). Это означает, что при коллизии на функции f_1 выражение (5) действительно выполняется.

f_1 – случайная функция и $\Delta x_i \neq \Delta x_j$ по условию, поэтому вероятность коллизии равна

$$P(f_1(\Delta x_i) = f_1(\Delta x_j)) = \frac{1}{2^n} .$$

2. В случае отсутствия коллизии на функции f_1 и выполнения следующего равенства:

$$\sigma^2(f_1(\Delta x_i) \oplus f_1(\Delta x_j)) \oplus f_1(\Delta x_i) \oplus f_1(\Delta x_j) =$$
$$= \sigma'(f_2(\Delta U_i) \oplus f_2(\Delta U_j)).$$

Полное уравнение для $\Delta W_i \oplus \Delta W_j$ имеет вид

$$\Delta W_i \oplus \Delta W_j = \sigma^2(x_i^L) \oplus \sigma^2(f_1(\Delta x_i)) \oplus$$
$$\oplus \sigma(f_2(\Delta U_i)) \oplus x_i^R \oplus f_1(\Delta x_i) \oplus f_2(\Delta U_i) \oplus$$
$$\oplus \sigma^2(x_j^L) \oplus \sigma^2(f_1(\Delta x_j)) \oplus \sigma(f_2(\Delta U_j)) \oplus$$
$$\oplus x_j^R \oplus f_1(\Delta x_j) \oplus f_2(\Delta U_j) =$$
$$= \sigma^2(x_i^L \oplus x_j^L) \oplus x_i^R \oplus x_j^R \oplus \sigma^2(f_1(\Delta x_i) \oplus$$
$$\oplus f_1(\Delta x_j)) \oplus \sigma(f_2(\Delta U_i) \oplus f_2(\Delta U_j)) \oplus$$
$$\oplus f_1(\Delta x_i) \oplus f_1(\Delta x_j) \oplus f_2(\Delta U_i) \oplus f_2(\Delta U_j).$$

Отсюда следует

$$\Delta W_i \oplus \Delta W_j \oplus \sigma^2(x_i^L \oplus x_j^L) \oplus x_i^R \oplus x_j^R =$$
$$= \sigma^2(f_1(\Delta x_i) \oplus f_1(\Delta x_j)) \oplus f_1(\Delta x_i) \oplus$$
$$\oplus f_1(\Delta x_j) \oplus \sigma'(f_2(\Delta U_i) \oplus f_2(\Delta U_j)).$$

Таким образом, для выполнения условия (5) должно выполняться равенство:

$$\sigma^2(f_1(\Delta x_i) \oplus f_1(\Delta x_j)) \oplus f_1(\Delta x_i) \oplus$$
$$\oplus f_1(\Delta x_j) \oplus \sigma'(f_2(\Delta U_i) \oplus f_2(\Delta U_j)) = 0,$$

$$\sigma^2(f_1(\Delta x_i)\oplus f_1(\Delta x_j))\oplus f_1(\Delta x_i)\oplus f_1(\Delta x_j)= \\ =\sigma'(f_2(\Delta U_i)\oplus f_2(\Delta U_j)). \quad (11)$$

Поскольку функции f_1 и f_2 – случайные, то вероятность выполнения уравнения (11) имеет значение

$$P=\frac{1}{2^n}.$$

Исходя из двух описанных случаев, можно найти общую вероятность выполнения равенства (5) для схемы Лей-Месси при одной паре входных запросов:

$$P_1(LM)=1-(1-\frac{1}{2^n})^2=\frac{2^{n+1}-1}{2^{2n}}.$$

Если принять, что вероятность выполнения равенства (5) для всех пар запросов одинаковая, то общую вероятность получения «1» на выходе алгоритма-различителя можно получить с помощью следующего выражения:

$$P_2(LM)=1-(1-\frac{2^{n+1}-1}{2^{2n}})^{\frac{k(k-1)}{2}}, \quad (12)$$

где k – количество запросов. Вероятность определяется по формуле для независимых событий, т.к. одновременно несколько независимых пар могут удовлетворять заданному равенству. Общее количество возможных пар составляет $C_k^2=\frac{k(k-1)}{2}$.

Формула (12) является аппроксимационным значением, имеющим минимальную погрешность при количестве запросов, значительно меньшим мощности множества открытых (шифрованных) текстов.

Точное значение вероятности можно получить с помощью формулы

$$P_3(LM)=1-\prod_{i=0}^{k-2}(1-\frac{1}{2^n-i})^{2(k-(i+1))}. \quad (13)$$

Это связано с тем, что пары запросов не являются независимыми и равновероятными. Однако отличия в вероятностях минимальны, поэтому для упрощения целесообразно пользоваться аппроксимированным значением (12). Зависимости между запросами рассматривались в нашей предыдущей работе [2].

Т.к. аппроксимационная формула дает большее значение вероятности различения, чем точная формула, то верхнюю границу целесообразно задать как неравенство, что и сделано в формуле (6). В дальнейшем для упрощения формул будет использоваться именно аппроксимационное значение вероятности.

Для случайной перестановки вероятность выполнения равенства (5) при $k=2$ запросах равна

$$P(PRP)=\frac{2^n}{2^{2n}-1}.$$

Вычитание единицы из знаменателя обусловлено тем, что в перестановке при разных входных значениях не повторяются выходные значения. Т.е. $W_i\neq W_j$, и соответственно, невозможен случай, когда $W_i^L\oplus W_j^L=W_i^R\oplus W_j^R=0$. Поскольку правая часть выражения (5) никогда не равна нулю (по условию для линейного ортоморфного преообразования), то вероятность увеличивается.

Если принять, что вероятность выполнения равенства (5) для всех пар запросов одинаковая, то общую вероятность получения «1» на выходе алгоритма-различителя для случайной перестановки можно получить с помощью выражения:

$$P_2(LM)=1-(1-\frac{2^n}{2^{2n}-1})^{\frac{k(k-1)}{2}}.$$

Способ нахождения такой вероятности аналогичен описанному выше. Точное значение вероятности можно получить, используя следующее выражение:

$$P_3(LM)=1-\prod_{i=0}^{k-2}(1-\frac{2^n}{2^{2n}-1-i\cdot 2^n})^{k-(i+1)}. \quad (14)$$

Доказательство этой формулы уже приводилось в нашей предыдущей статье [2] и здесь опускается.

Преимущество алгоритма-различителя находится как модуль разности значений (13) и (14):

$$Adv(LM,PRP)=|\prod_{i=0}^{k-2}(1-\frac{1}{2^n-i})^{2(k-(i+1))}- \\ -\prod_{i=0}^{k-2}(1-\frac{2^n}{2^{2n}-1-i\cdot 2^n})^{k-(i+1)}|\leq \\ \leq|(1-\frac{2^n}{2^{2n}-1})^{\frac{k(k-1)}{2}}-(1-\frac{2^{n+1}-1}{2^{2n}})^{\frac{k(k-1)}{2}}|.$$

Доказательство окончено.

Следует отметить, что увеличение количества запросов до определенного порогового значения приводит к возрастанию вероятности различения. Дальнейшие запросы снижают эффективность различения.

На рис. 6 и 7 приведен график зависимости вероятности (ось ординат) различения для $n=8$ и $n=16$ от количества входных запросов (ось абсцисс).

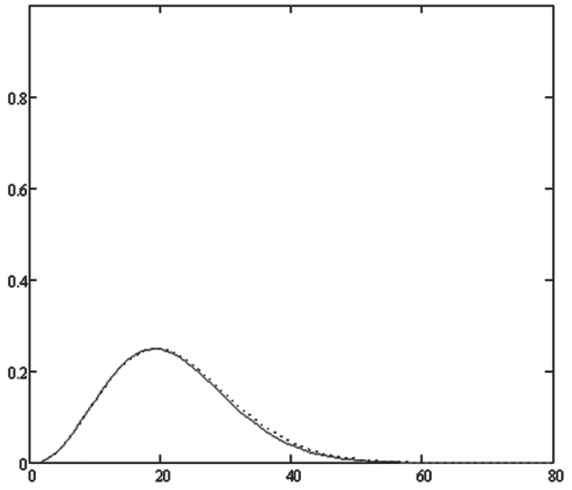

Рис. 6. Зависимость вероятности различения от количества входных запросов для $n=8$

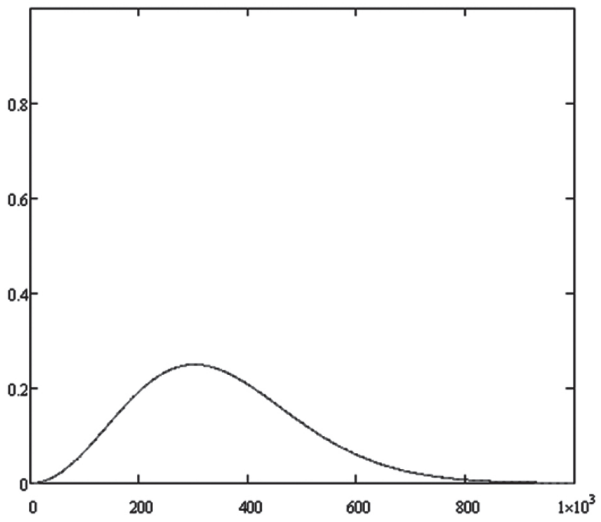

Рис. 7. Зависимость вероятности различения от количества входных запросов для $n = 16$

Как следует из графиков, для выбранных параметров с помощью описанного алгоритма-различителя можно достичь вероятности различения порядка $P_{\max} \approx 0.3$. При этом требуется порядка $\sqrt{2^n}$ выбранных открытых текстов.

3. АЛГОРИТМ-РАЗЛИЧИТЕЛЬ ДЛЯ 3-РАУНДОВОЙ СХЕМЫ ЛЕЙ-МЕССИ СО СЛУЧАЙНЫМИ ПЕРЕСТАНОВКАМИ В КАЧЕСТВЕ РАУНДОВЫХ ПРЕОБРАЗОВАНИЙ

Используется та же схема (рис. 3), только раундовые функции f_1, f_2, f_3 – случайные перестановки. В этом случае более эффективно использовать следующий алгоритм-различитель.

Алгоритм-различитель №2 для 3-раундовой схемы Лей-Месси со случайными перестановками в качестве раундовых преобразований.

Алгоритм-различитель для k пар входных аргументов (x_i, x_j) проверяет выполнение равенства

$$\Delta W_i \oplus \Delta W_j = \sigma(x_i^R \oplus x_j^R \oplus x_i^L \oplus x_j^L),$$
$$0 \le i < j < k. \qquad (15)$$

Если хотя бы для одной пары данное равенство выполняется, то на выходе алгоритм выдает «1» (определена цепь Лей-Месси), иначе – «0» (случайная перестановка).

Теорема 3. Для k запросов вида (x_i, x_j), соответствующих условиям

$$\sigma(x_i^L \oplus x_j^L) \oplus x_i^R \oplus x_j^R \neq 0 \text{ и } \Delta x_i \neq \Delta x_j,$$

при проверке выполнения равенства

$$\Delta W_i \oplus \Delta W_j = \sigma(x_i^R \oplus x_j^R \oplus x_i^L \oplus x_j^L),$$

$0 \le i < j < k$ вероятность различения 3-раундовой схемы Лей-Месси на основе случайных перестановок как раундового преобразования и случайной перестановки не превышает значения

$$Adv(LM, PRP) \le \left|(1 - \frac{2^n}{2^{2n}-1})^{\frac{k(k-1)}{2}} - (1 - \frac{1}{2^n - 1})^{k(k-1)}\right|.$$

Доказательство.

Вероятность выполнения условия

$$\Delta W_i \oplus \Delta W_j = \sigma(x_i^R \oplus x_j^R \oplus x_i^L \oplus x_j^L)$$

для схемы Лей-Месси при $k = 2$ равна

$$P(LM) = 1 - (1 - \frac{1}{2^n - 1})^2.$$

Результат получается из следующих выводов. Равенство (15) выполняется в двух случаях:

1. В случае возникновения коллизии $\Delta U_i = \Delta U_j$. Тогда справедливо следующее:

$$\begin{gathered}\sigma(x_i^L \oplus f_1(\Delta x_i)) \oplus x_i^R \oplus f_1(\Delta x_i) = \\ = \sigma(x_j^L \oplus f_1(\Delta x_j)) \oplus x_j^R \oplus f_1(\Delta x_j), \\ \sigma(x_i^L) \oplus \sigma(f_1(\Delta x_i)) \oplus x_i^R \oplus f_1(\Delta x_i) = \\ = \sigma(x_j^L) \oplus \sigma(f_1(\Delta x_j)) \oplus x_j^R \oplus f_1(\Delta x_j), \\ \sigma(f_1(\Delta x_i)) \oplus \sigma(f_1(\Delta x_j)) \oplus f_1(\Delta x_i) \oplus f_1(\Delta x_j) = \\ = \sigma(x_j^L) \oplus \sigma(x_i^L) \oplus x_j^R \oplus x_i^R. \end{gathered} \qquad (16)$$

Поскольку $\Delta x_i \neq \Delta x_j$, а f_1, f_2, f_3 – это перестановки, то для всех запросов

$$\sigma(f_1(\Delta x_i)) \oplus \sigma(f_1(\Delta x_j)) \oplus f_1(\Delta x_i) \oplus f_1(\Delta x_j) \neq 0. \qquad (17)$$

Из (16) и (17) также следует, что $\sigma(x_j^L) \oplus \sigma(x_i^L) \oplus x_j^R \oplus x_i^R \neq 0$ – начальное условие для входных текстов.

Если произошла коллизия и равенство (16) выполняется, то

$$\begin{gathered}\Delta W_i \oplus \Delta W_j = \sigma^2(x_i^L) \oplus \sigma^2(f_1(\Delta x_i)) \oplus \\ \oplus \sigma(f_2(\Delta U_i)) \oplus x_i^R \oplus f_1(\Delta x_i) \oplus f_2(\Delta U_i) \oplus \\ \oplus \sigma^2(x_j^L) \oplus \sigma^2(f_1(\Delta x_j)) \oplus \sigma(f_2(\Delta U_j)) \oplus \\ \oplus x_j^R \oplus f_1(\Delta x_j) \oplus f_2(\Delta U_j) = \\ = \sigma^2(x_i^L \oplus x_j^L) \oplus x_i^R \oplus x_j^R \oplus \sigma^2(f_1(\Delta x_i) \oplus \\ \oplus f_1(\Delta x_j)) \oplus f_1(\Delta x_i) \oplus f_1(\Delta x_j). \end{gathered} \qquad (18)$$

Из (16) и (18) следует

$$\Delta W_i \oplus \Delta W_j = \sigma(x_i^L \oplus x_j^L \oplus x_i^R \oplus x_j^R). \qquad (19)$$

Равенство (19) соответствует условию различения, т.е. оно справедливо при выполнении (16). Вероятность выполнения (16) равна

$$P_1(LM) = \frac{1}{2^n - 1}.$$

Уменьшение знаменателя на единицу обусловлена $\sigma(x_j^L) \oplus \sigma(x_i^L) \oplus x_j^R \oplus x_i^R \neq 0$ для входных текстов. Это увеличивает вероятность, поскольку левая часть (16) никогда не равна нулю.

2. В случае отсутствия коллизии $\Delta U_i = \Delta U_j$ и при выполнении следующего равенства:

$$\begin{gathered}\Delta W_i \oplus \Delta W_j = \sigma^2(x_i^L) \oplus \sigma^2(f_1(\Delta x_i)) \oplus \\ \oplus \sigma(f_2(\Delta U_i)) \oplus x_i^R \oplus f_1(\Delta x_i) \oplus f_2(\Delta U_i) \oplus \\ \oplus \sigma^2(x_j^L) \oplus \sigma^2(f_1(\Delta x_j)) \oplus \sigma(f_2(\Delta U_j)) \oplus \\ \oplus x_j^R \oplus f_1(\Delta x_j) \oplus f_2(\Delta U_j) = \\ = \sigma(x_i^L \oplus x_i^R \oplus x_j^L \oplus x_j^R). \end{gathered} \qquad (20)$$

Поскольку функции f_1 и f_2 – это случайные перестановки, а $\Delta W_i \oplus \Delta W_j$ – случайное значение (с некоторыми оговорками), то вероятность выполнения уравнения (20) имеет следующее значение:

$$P = \frac{2^n + 1}{2^{2n} - 1} = \frac{1}{2^n - 1}.$$

Из двух описанных условий можно найти общую вероятность выполнения равенства (15) для схемы Лей-Месси со случайными раундовыми перестановками при одной паре входных запросов. Сумма вероятностей находится по формуле для независимых событий:

$$P_1(LM) = 1 - (1 - \frac{1}{2^n - 1})^2.$$

Если принять, что вероятность выполнения равенства (15) для всех пар запросов одинаковая, то общую вероятность получения «1» на выходе алгоритма-различителя можно получить с помощью следующего выражения:

$$P_2(LM) = 1 - (1 - \frac{1}{2^n - 1})^{2^{\frac{k(k-1)}{2}}}, \qquad (21)$$

где k – количество запросов. Вероятность определяется по формуле сложения для совместимых событий, т.к. одновременно несколько пар могут удовлетворять заданному равенству. Общее количество возможных пар составляет $C_k^2 = \frac{k(k-1)}{2}$.

Формула (21) является аппроксимационным значением, имеющим минимальную погрешность при количестве запросов, значительно меньшим мощности множества открытых (шифрованных) текстов.

Точное значение вероятности можно получить с помощью формулы

$$P_3(LM) = 1 - \prod_{i=0}^{k-2} (1 - \frac{1}{2^n - 1 - i})^{2(k-(i+1))}. \qquad (22)$$

Это связано с тем, что пары запросов не являются независимыми и равновероятными. Однако отличия в вероятностях минимальны, поэтому для упрощения целесообразно пользоваться аппроксимированным значением (21). Зависимости между запросами рассматривались в нашей предыдущей работе [2].

Для случайной перестановки вероятность выполнения равенства (15) при $k = 2$ запросах равна

$$P(PRP) = \frac{2^n}{2^{2n} - 1}.$$

Вычитание единицы из знаменателя обусловлено тем, что в перестановке при разных входных значениях не повторяются выходные значения. Соответственно, $W_i \neq W_j$ и невозможено выполнение условия $W_i^L \oplus W_j^L = W_i^R \oplus W_j^R = 0$. Поскольку правая часть выражения (15) никогда не равна нулю (по условию для линейного ортоморфного преообразования), то вероятность увеличивается.

Поскольку правая часть выражения (15) никогда не равна нулю (по условию, для цепи Фейстеля в качестве линейной функции), то невозможен один из неподходящих вариантов, т.е. вероятность увеличивается.

Если принять, что вероятность выполнения равенства (15) для всех пар запросов одинаковая, то общую вероятность получения «1» на выходе алгоритма-различителя для случайной перестановки можно получить с помощью выражения:

$$P_2(LM) = 1 - (1 - \frac{2^n}{2^{2n} - 1})^{\frac{k(k-1)}{2}}.$$

Способ нахождения такой вероятности аналогичен описанному выше. Точное значение вероятности можно получить используя следующее выражение:

$$P_3(LM) = 1 - \prod_{i=0}^{k-2} (1 - \frac{2^n}{2^{2n} - 1 - i \cdot 2^n})^{k-(i+1)}. \qquad (23)$$

Доказательство этой формулы уже приводилось в нашей предыдущей статье [2] и здесь опускается.

Преимущество алгоритма-различителя находится как модуль разности значений (22) и (23):

$$Adv(LM, PRP) = |\prod_{i=0}^{k-2} (1 - \frac{1}{2^n - 1 - i})^{2(k-(i+1))} -$$
$$- \prod_{i=0}^{k-2} (1 - \frac{2^n}{2^{2n} - 1 - i \cdot 2^n})^{k-(i+1)}| \leq$$
$$\leq |(1 - \frac{1}{2^n - 1})^{k(k-1} - (1 - \frac{2^n}{2^{2n} - 1})^{\frac{k(k-1)}{2}}|.$$

Доказательство окончено.

Аналогично предыдущему алгоритму, увеличение количества запросов до определенного порогового значения приводит к возрастанию вероятности различения. Дальнейшие запросы снижают эффективность различения.

На рис. 8 и 9 приведен график зависимости вероятности (ось ординат) различения для $n = 8$ и $n = 16$ от количества входных запросов (ось абсцисс).

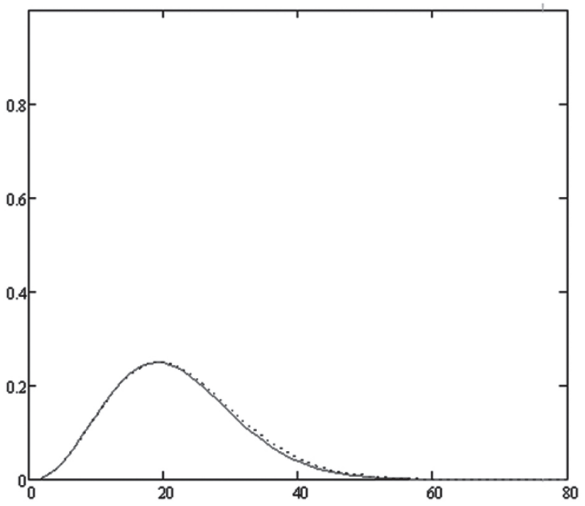

Рис. 8. Зависимость вероятности различения от количества входных запросов для $n = 8$

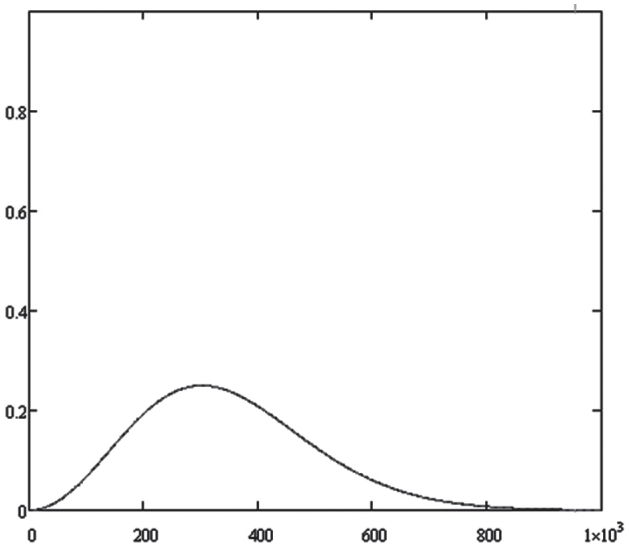

Рис. 9. Зависимость вероятности различения от количества входных запросов для $n = 16$

Как следует из графиков, для выбранных параметров с помощью описанного алгоритма-различителя можно достичь вероятности различения порядка $P_{\max} \approx 0.3$. При этом требуется порядка $\sqrt{2^n}$ выбранных открытых текстов.

Рассматриваемый алгоритм имеет практически такую же эффективность, как и предыдущий для 3-раундовой схемы Лей-Месси со случайными функциями в качестве раундовых преобразований.

ВЫВОДЫ

Использование модели идеального блочного шифра как случайной перестановки позволяет получить численную оценку эффективности высокоуровневой конструкции алгоритма шифрования, в рассмотренном случае – схемы Лей-Месси.

Для исключения влияния свойств конкретной цикловой функции в качестве раундового преобразования целесообразно брать случайную функцию или случайную перестановку. Полученные результаты позволяют точно оценить верхнюю границу эффективности (преимущества) произвольного алгоритма-различителя для 3 раундовой схемы Лей-Месси.

Для рассмотренных конкретных алгоритмов выведены точные значения преимущества, определен метод расчета оптимального количества запросов, при котором преимущество будет максимальным.

Для алгоритмов различения схемы Лей-Месси на основе случайных функций и случайных перестановок существует конкретное значение количества запросов, на котором преимущество будет максимальным.

В то же время, для алгоритма различения цепи Фейстеля на основе случайных перестановок увеличение количества запросов непрерывно ведет к максимизации преимущества.

Дополнительные аппроксимационные соотношения позволяют значительно упростить расчет вероятностей различения и преимущества алгоритмов-различителей с высокой точностью.

Критерий эффективности высокоуровневой конструкции блочного шифра на основе сравнения сложности различения 3-раундового преобразования позволяет сделать вывод о большей эффективности схемы Лей-Месси по сравнению с цепью Фейстеля.

Литература

[1] *Vaudenay S.* On the Lai-Massey Scheme / Technical report LIENS-99-3, Ecole Normale Superieure, 1999.

[2] *Р.В. Олейников, Д.С. Кайдалов.* Уточнение эффективности различения цепи Фейстеля и случайной перестановки. Радиотехника / вып. 167, Харьков: ХНУРЭ, 2011 г., стр. 190-202.

Поступила в редколлегию 11.03.2012

Олейников Роман Васильевич, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: анализ и синтез симметричных криптографических преобразований

Кайдалов Дмитрий Сергеевич, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: анализ стойкости блочных симметричных шифров.

УДК 621.391:519.2:519.7

Оцінка складності розрізнення схеми Лей-Мессі та випадкової перестановки / Р.В. Олійников, Д.С. Кайдалов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2012. – Том 11. № 2. – С. 152–159.

Виконаний аналіз ефективності трьохраундової схеми Лей-Мессі – високорівневої конструкції симетричного блокового шифра. Оцінка отримана на основі визначення складності виконання атаки з обраними відкритими текстами, яка спрямована на розрізнення конструкції криптографічного перетворення і моделі ідеального шифра – випадкової перестановки.

Ключевые слова: блочний шифр, схема Лей-Мессі, випадкова перестановка.

Іл. 9. Бібліогр.: 2 назв.

UDC 621.391:519.2:519.7

Evaluation of complexity of distinguishing the Lai-Massey scheme and random permutation / R.V. Oliynykov, D.S. Kaidalov // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 152–159.

An efficiency analysis of the 3-round Lai-Massey scheme as a high level construction of a symmetric block cipher is performed. The evaluation is based on the complexity estimation of a chosen plaintext attack directed at distinguishing the construction of cryptographic transformation and a model of the ideal cipher as a random permutation. The upper bound of advantage for an arbitrary algorithm-distinguisher and precise values of advantage for two methods are grounded.

Keywords: block cipher, Lai-Massey scheme, random permutation.

Fig. 9. Ref.: 2 items.