УДК 621. 391:519.2:519.7

Свойства законов распределения XOR таблиц и таблиц линейных аппроксимаций случайных подстановок

И. В. Лисицкая

Харьковский национальный университет имени В.Н. Каразина, Украина

Изучаются свойства законов распределения XOR таблиц и таблиц линейных аппроксимаций случайных подстановок, в частности, устанавливаются связи между дискретными (соседними или смежными) значениями каждого из этих законов.

Ключевые слова: *случайная подстановка, XOR таблица подстановки, линейная аппроксимационная таблица подстановки, закон распределения вероятностей.*

Вивчаються властивості законів розподілу XOR таблиць і таблиць лінійних апроксімацій випадкових підстановок, зокрема, встановлюються зв'язки між дискретними (сусідніми або суміжними) значеннями кожного з цих законів.

Ключові слова*: випадкова підстановка, XOR таблиця підстановки, лінійна апроксимаційна таблиця підстановки, закон розподілу ймовірностей.*

Properties of laws of distributing of XOR of tables and tables of linear approximations of random substitutions are studied, in particular, affiliated between discrete (nearby or contiguous) values each of these laws.

Key words: *random substitutions, table of linear approximations, distributing of XOR of tables, law probability distribution.*

1. Введение

В работах [1-4] были доказаны теоремы, определяющие законы распределения вероятностей XOR таблиц и таблиц линейных аппроксимаций случайных подстановок. Было также показано, что полученные законы справедливы и для шифрующих преобразований, рассматриваемых для каждого ключа зашифрования как подстановка. В последующих работах [5,6] эти законы распределения вероятностей были использованы для построения дополнительных критериев отбора случайных подстановок.

На наш взгляд представляет несомненный научный и практический интерес дальнейшее изучение свойств подстановок случайного типа с предельными дифференциальными и линейными показателями, приближающимися к теоретическим законам распределения вероятностей XOR таблиц и таблиц линейных аппроксимаций. Настоящая работа посвящена установлению связей между дискретными (соседними или смежными) значениями каждого из этих законов, а также дальнейшему анализу свойств ″предельных″ распределений, которые могут оказаться полезными при изучении (определении) показателей стойкости шифров к атакам дифференциального и линейного криптоанализа.

2. Понятийный аппарат дифференциального и линейного криптоанализа

Напомним сначала смысл теорем, доказанных в работах [1-4] и необходимый понятийный аппарат.

В обозначениях работ [1,2] пусть $\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$ будет вероятностью того, что значение ячейки дифференциальной таблицы случайно взятой подстановки π порядка 2^n для перехода входной разности ΔX в выходную разность ΔY будет равно $2k$. Эта вероятность определяется теоремой.

Утверждение 1. *Для любых ненулевых фиксированных* ΔX, $\Delta Y \in Z_2^n$ *в предположении, что подстановка* π *выбрана равновероятно из множества* S_2^n *и* $0 \le k \le 2^{n-1}$,

$$\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)= \\ =\begin{pmatrix}2^{n-1}\\ k\end{pmatrix}^2 \cdot \frac{k!\cdot 2^k \cdot \Phi(2^{n-1}-k)}{2^n!}, \tag{1}$$

где функция $\Phi(d)$ *определяется выражением*

$$\Phi(d)=\sum_{i=0}^{d}(-1)^i \cdot \begin{pmatrix}d\\ i\end{pmatrix}^2 \cdot 2^i \cdot i!\cdot(2d-2i)!\cdot \tag{2}$$

Закон распределения вероятностей (1) получен для полного множества подстановок, однако замечательным его свойством является то, что он оказывается справедливым и для усеченного (причем, существенно) множества подстановок, формируемых симметричными шифрами. Такие преобразования, осуществляемые на различных ключах зашифрования, как известно, формируют множество подстановок случайного типа. Об этом, как уже отмечалось в нашей работе [7], свидетельствуют многочисленные результаты экспериментов. И это еще не все! Получается, что для множества подстановок, определяемых шифрующими преобразованиями, выполняется свойство, напоминающее эргодическое свойство случайных процессов (среднее по множеству реализаций совпадает со средним по времени для одной достаточно длинной реализации [8]). Это свойство проявляется в том, что закон распределения (1), полученный на основе анализа всего множества $2^n!$ равновероятных подстановок степени 2^n, оказывается справедливым (с весьма высокой точностью) и для заполнений ячеек таблиц XOR разностей шифрующих преобразований. Этот результат подтвержден экспериментально на малых версиях шифров, однако мы надеемся показать в ближайшее время, что этим свойством обладают и соответствующие большие прототипы.

Хорошим подтверждением того, что для закона распределения вероятностей $\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$, полученного для ансамбля случайных подстановок, рассматриваемого применительно к отдельно взятой подстановке, с высокой точностью выполняется условие нормировки характерное для полной группы событий:

$$\sum_{k=0}^{k^*}\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)=1. \tag{3}$$

Здесь $\Lambda_\pi(\Delta X, \Delta Y)$ – значение XOR таблицы для пары значений разностей входов и выходов ΔX, $\Delta Y \in S_2^n$, $\Delta X = X + X'$, $\Delta Y = \pi(X) + \pi(X')$ подстановки $\pi \in S_2^n$. Значение k^* представляет собой половину от максимального числа переходов XOR таблицы случайной подстановки. Выполненные многочисленные проверки подтверждает и это теоретический результат.

Совершенно аналогичное по содержанию утверждение справедливо для вероятностей значений линейных аппроксимационных таблиц $LAT_\pi^*(\alpha, \beta)$ случайных подстановок [3,4].

Утверждение 2. Пусть $\lambda^*(\alpha, \beta)$ будет случайным значением распределения $LAT_\pi^*(\alpha, \beta) = \left| LAT_\pi(\alpha, \beta) - 2^{n-1} \right|$, когда подстановка π выбрана равновероятно из множества 2^n и маски α, β не нулевые. Тогда $\lambda^*(\alpha, \beta)$ для $|k| \le 2^{n-2}$ принимает только четные значения и

$$\Pr\left(\lambda^*(\alpha, \beta) = 2k\right) = \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ 2^{n-2} - k \end{pmatrix}^2. \quad (4)$$

Заметим здесь, что в соответствии со свойствами биномиальных коэффициентов:

$$\begin{pmatrix} 2^{n-1} \\ 2^{n-2} - k \end{pmatrix} = \begin{pmatrix} 2^{n-1} \\ 2^{n-2} + k \end{pmatrix}.$$

И для этого распределения справедлива нормировка:

$$\sum_{k=0}^{k^*} \Pr\left(\lambda^*(\alpha, \beta) = 2k^*\right) = 1. \quad (5)$$

Здесь k^* – половинное значение максимального для таблицы $LAT_\pi^*(\alpha, \beta)$ смещения.

Более того, мы далее покажем, что для распределения (4) справедлива также нормировка вида:

$$\sum_{\hat{e}=-2^{n-1}}^{2^{n-1}} \left(\frac{2k}{2^{n-1}} \right)^2 \cdot (2^n - 1) \cdot \Pr\left(\lambda^*(\alpha, \beta) = 2k\right) = 1,$$

которая при соответствующей интерпретации повторяет известное условие [7]:

$$\sum_{\tilde{A}y \in Y} LP^\pi(\tilde{A}x \to \tilde{A}y) = 1. \quad (6)$$

Напомним, что дифференциальная и линейная вероятности здесь определяются в соответствии с обозначениями принятыми в [7] следующим образом.

Дифференциальная вероятность DP^f и линейная вероятность LP^f соответственно для ключезависимой функции f с n-битным входом x и n-битным выходом y ($x, y \in GF(2)^n$) есть

$$DP^f(\Delta x \to \Delta y) = \\ = \frac{\#\{x \in GF(2)^n \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^n}, \quad (7)$$

$$LP^f(\Gamma y \to \Gamma x) = \\ = \left(\frac{\#\{x \in GF(2)^n \mid x \cdot \tilde{A}x = f(x) \cdot \tilde{A}y\}}{2^{n-1}} - 1 \right)^2, \quad (8)$$

где Δx и Δy являются входным и выходным различием (разностью), а Гx и Гy входной и выходной масками; x Гx обозначает результат побитного произведения x и Гx.

В этой работе мы покажем и докажем ряд важных свойств, которым подчиняются законы распределения вероятностей (1) и (4). Нас будут здесь интересовать соотношения, связывающие соседние (ближайшие) значения законов распределения вероятностей (отношение вероятностей для заполнений ячеек таблиц дифференциальных разностей и таблиц линейных аппроксимаций, равных соответственно значениям 2k и 2(k –1)).

3. Свойства таблицы XOR разностей случайных подстановок

Рассмотрим сначала закон вероятностей (1) с его доопределением (2). Будем интересоваться отношением соседних значений этого закона распределения:

$$\frac{\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2(k-1)\right)}{\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right)}, \quad k = 1, \ldots, k^*. \quad (9)$$

Подставим в это соотношение значения фигурирующих в нем законов распределения вероятностей:

$$\frac{\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2(k-1)\right)}{\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right)} = \\ = \frac{\binom{2^{n-1}}{k-1}^2 \cdot \frac{(k-1)!\, 2^{k-1} \cdot \Phi(2^{n-1} - k + 1)}{2^n!}}{\binom{2^{n-1}}{k}^2 \cdot \frac{k!\, 2^k \cdot \Phi(2^{n-1} - k)}{2^n!}} = \\ = \frac{k^2}{(2^{n-1} - k + 1)^2} \cdot \frac{\Phi(2^{n-1} - k + 1)}{k \cdot 2 \cdot \Phi(2^{n-1} - k)}.$$

Если теперь воспользоваться аппроксимацией функции $\Phi(d)$ в виде [2]:

$$\Phi(d) \approx (2d)!/e^{\frac{1}{2}},$$

то для отношения функций $\Phi(d)$ с аргументами, отличающимися на единицу, имеем:

$$\frac{\Phi(2^{n-1}-k+1)}{\Phi(2^{n-1}-k)} \approx \frac{(2\cdot(2^{n-1}-k+1))!}{(2\cdot(2^{n-1}-k))!} =$$

$$= (2^n - 2k + 2)(2^n - 2k + 1).$$

С учетом этой аппроксимации, выполняющейся с весьма высокой точностью, отношение (9) приводится к результату:

$$\frac{\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2(k-1)\right)}{\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right)} =$$

$$= k \cdot \frac{(2^n - 2k + 1)}{2^{n-1} - k + 1} \approx 2k.$$

Зафиксируем его в виде утверждения.

Утверждение 3. Для отношения дифференциальных вероятностей соседних значений ячеек таблицы XOR разностей случайных подстановок для k = 1,…,k* справедливо соотношение:

$$\frac{\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2(k-1)\right)}{\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right)} \approx 2k \tag{10}$$

или

$$\#\left\{\Lambda_\pi(\Delta X, \Delta Y) = 2(k-1)\right\} = 2k \cdot \#\left\{\Lambda_\pi(\Delta X, \Delta Y) = 2k\right\}.$$

Полученное соотношение позволяет очень просто реконструировать закон распределения вероятностей (1) по максимальному значению полного дифференциала случайной подстановки или по числу нулевых ячеек дифференциальной таблицы. В частности, если вспомнить [2], что для числа нулевых ячеек дифференциальной таблицы случайной подстановки справедлива оценка, выполняющаяся с большой точностью:

$$\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 0\right) = e^{-1/2} = 0,6065...,$$

то можно прийти к выводу, что для закона распределения вероятностей значений переходов таблицы XOR разностей случайной подстановки справедлива аппроксимация:

$$\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right) = e^{-1/2}\,\frac{1}{2^k\, k!}. \tag{11}$$

Для числа ячеек таблицы XOR разностей случайной подстановки степени 2^n соответственно получим расчетное соотношение:

$$\Lambda_{n,2k} = (2^n - 1)^2 \times \frac{e^{-1/2}}{2^k\, k!}.$$

Очевидно, что для значений заполнений ячеек таблицы должна выполняться нормировка:

$$\sum_{k=0}^{k^*} \Lambda_{n,2k} = \sum_{k=0}^{k^*} (2^n - 1)^2 \times \frac{e^{-1/2}}{2^k\, k!} = (2^n - 1)^2 .$$

$$(2^n - 1)^2 e^{-1/2}\left(1 + \frac{1}{2} + \frac{1}{2\cdot 4} + \ldots + \frac{1}{2^{k^*}\, k^*!}\right) = (2^n - 1)^2,$$

и, значит, должно выполняться соотношение:

$$e^{-1/2}\left(1+\frac{1}{2}+\frac{1}{2\cdot 4}+\ldots+\frac{1}{2^{k^*}k^*!}\right)=1.$$

Его справедливость следует из представления $\sqrt{e}$ через сумму ряда

$$\sqrt{e}=\sum_{i=1}^{\infty}\frac{1}{2^i i!}\ .$$

В результате можно сделать вывод, что практически закон распределения вероятностей переходов таблицы XOR разностей случайной подстановки (11) не зависит от её степени. Он является одинаковым для подстановок различных степеней.

Можно также прийти к общему правилу, определяющему распределение значений любой таблицы XOR разностей случайной подстановки (подстановки любой степени), в соответствии с которым таблица XOR разностей такой подстановки (а в интересующем нас приложении таблица полных дифференциалов итеративного шифра) будет содержать в среднем:

60% нулевых значений (каждая вторая ячейка таблицы является нулем);

30% двоек (каждая третья ячейка является двойкой);

7,5% четверок (каждая 13-я ячейка четверка);

1,25% шестерок (каждая 80-я ячейка шестерка);

0,156% восьмерок (каждая 640-я ячейка восьмерка) и т.д.

Последнее значение буде равно максимуму таблицы дифференциальных разностей и оно, скорее всего (но не обязательно), будет единственным!

Остается отметить, что это среднее значение будет мало отличаться от среднего значения максимумов реального многоциклового итеративного шифрующего преобразования.

4. Свойства таблиц линейных аппроксимаций случайных подстановок

Рассмотрим теперь закон вероятностей (4). Убедимся, что для него справедлива нормировка (6), которая в этом случае записывается в виде

$$\frac{2^n-1}{\left(2^{n-1}\right)^2}\sum_{k=-2^{n-2}}^{2^{n-2}}(2k)^2\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+k}^2=2^n. \qquad (12)$$

(сумма квадратов смещений любой строки дает полное множество пар текстов с фиксированной разностью − полное множество возможных входов в каждую строку таблицы)

Ниже приведено доказательство этого свойства. Рассмотрим сумму в левой части равенства (12):

$$\sum_{k=-2^{n-2}}^{2^{n-2}}\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+k}^2. \qquad (13)$$

Перейдем при суммировании к новой переменной $s=2^{n-2}+k\rightarrow\ k=s-2^{n-2}$, и, следовательно, при изменении k от $k=-2^{n-2}$ до $k=2^{n-2}$ новая переменная s изменяется в пределах от 0 до $k=2^{n-1}$.

В результате вместо суммы (13) будем рассматривать сумму

$$\sum_{s=0}^{2^{n-1}} \left(2s - 2^{n-1}\right)^2 \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \binom{2^{n-1}}{s}^2 = \sum_{s=0}^{2^{n-1}} \left(4s^2 - 2^n s + 2^{2n-2}\right) \cdot \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \binom{2^{n-1}}{s}^2. \quad (14)$$

Раскрывая скобки в первом сомножителе под знаком суммы в правой части (13), рассмотрим слагаемое:

$$\sum_{s=1}^{2^{n-1}} s^2 \cdot \binom{2^{n-1}}{s}^2 = \left[\frac{s \cdot \left(2^{n-1}\right)!}{\left(2^{n-1} - s\right)! \cdot (s)!}\right]^2.$$

Выражение в квадратных скобках этого слагаемого можно представить в виде:

$$\frac{s \cdot \left(2^{n-1}\right)!}{\left(2^{n-1} - s\right)! \cdot s!} = \frac{2^{n-1} \cdot \left(2^{n-1} - 1\right)!}{\left(2^{n-1} - s\right)! \cdot (s-1)!} = 2^{n-1} \cdot \binom{2^{n-1} - 1}{s-1}.$$

С учетом полученного представления имеем:

$$\sum_{s=1}^{2^{n-1}} 4s^2 \cdot \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \binom{2^{n-1}}{s}^2 =$$

$$= 4 \cdot \sum_{s=1}^{2^{n-1}} \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot 2^{2(n-1)} \cdot \binom{2^{n-1} - 1}{s-1}^2 =$$

$$= 4 \cdot \sum_{k=0}^{2^{n-1}-1} \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot 2^{2(n-1)} \cdot \binom{2^{n-1} - 1}{k}^2 =$$

$$= 4 \cdot \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot 2^{2(n-1)} \cdot \binom{2^n - 2}{2^{n-1} - 1} =$$

$$= 4 \cdot \frac{\left(2^{n-1}\right)^2 \cdot 2^{2n-2}}{2^n (2^n - 1)} = \frac{2^{2n-2}}{2^n - 1} = \frac{2^n \cdot 2^{n-2}}{2^n - 1}.$$

При получении этого результата использовано известное представление для суммы квадратов биномиальных коэффициентов [8]:

$$\binom{a}{0}^2 + \binom{a}{1}^2 + \ldots + \binom{a}{a}^2 = \binom{2a}{a}.$$

Рассмотрим второе слагаемое

$$2^n \cdot \sum_{s=1}^{2^{n-1}} s \cdot \binom{2^{n-1}}{s}^2 =$$

$$= 2^n \cdot \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \sum_{s=1}^{2^{n-1}} \left[\frac{s \cdot \left(2^{n-1}\right)!}{\left(2^{n-1} - s\right)! \cdot (s)!}\right] \cdot \binom{2^{n-1}}{s} =$$

$$= 2^n \cdot \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \sum_{s=1}^{2^{n-1}} \left[\frac{s \cdot \left(2^{n-1}\right)!}{\left(2^{n-1}-s\right)! \cdot (s)!} \right] \cdot \binom{2^{n-1}}{s} =$$

$$= 2^n \cdot \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \sum_{s=1}^{2^{n-1}} 2^{n-1} \cdot \binom{2^{n-1}-1}{s-1} \binom{2^{n-1}}{s}.$$

Произведение биномиальных коэффициентов дает

$$\sum_{s=1}^{2^{n-1}} \binom{2^{n-1}-1}{s-1} \binom{2^{n-1}}{s} = \binom{2^{n-1}-1}{0} \binom{2^{n-1}}{1} +$$

$$+ \binom{2^{n-1}-1}{1} \binom{2^{n-1}}{2} + \ldots +$$

$$+ \binom{2^{n-1}-1}{2^{n-1}-1} \binom{2^{n-1}}{2^{n-1}} =$$

$$= \binom{2^{n-1}-1}{0} \binom{2^{n-1}}{2^{n-1}-1} + \binom{2^{n-1}-1}{1} \binom{2^{n-1}}{2^{n-1}-2} + \ldots +$$

$$+ \binom{2^{n-1}-1}{2^{n-1}-1} \binom{2^{n-1}}{0} = \binom{2^n-1}{2^{n-1}-1}.$$

При получении и этого результата использовано известное соотношение для суммы произведений биномиальных коэффициентов [8]:

$$\binom{a}{0} \binom{b}{k} + \binom{a}{1} \binom{b}{k-1} + \ldots + \binom{a}{k} \binom{b}{0} = \binom{a+b}{k}.$$

В результате имеем

$$2^n \cdot \sum_{s=1}^{2^{n-1}} 2^{n-1} \cdot \binom{2^{n-1}-1}{s-1} \binom{2^{n-1}}{s} = 2^{2n-1} \cdot \binom{2^n-1}{2^{n-1}-1}.$$

$$= 2^{2n-1} \cdot \frac{\left(2^{n-1}!\right)^2 (2^n-1)!}{2^n! \left(2^{n-1}-1\right)! \left(2^{n-1}\right)!} = \frac{2^{2n-1} \cdot 2^{n-1}}{2^n}.$$

Третье слагаемое

$$2^{2n-2} \cdot \sum_{s=0}^{2^{n-1}} \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \binom{2^{n-1}}{s}^2 =$$

$$= 2^{2n-2} \cdot \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \sum_{s=0}^{2^{n-1}} \binom{2^{n-1}}{s}^2 =$$

$$= 2^{2n-2} \cdot \frac{\left(2^{n-1}!\right)^2 2^n!}{2^n! \cdot \left(2^{n-1}!\right)^2} = 2^{2n-2}.$$

Общим результатом будет:

$$\sum_{s=0}^{2^{n-1}} \left(4s^2 - 2^n s + 2^{2n-2}\right) \cdot \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ s \end{pmatrix}^2 =$$

$$= \frac{2^n \cdot 2^{n-2}}{2^n - 1} - \frac{2^{2n-1} \cdot 2^{n-1}}{2^n} + 2^{2n-2} = \frac{2^{3n-2}}{2^n - 1}.$$

Таким образом, можно прийти к выводу, что справедливо соотношение:

$$\frac{2^n - 1}{\left(2^{n-1}\right)^2} \cdot \frac{2^{3n-2}}{2^n - 1} = 2^n.$$

Этот результат полностью подтверждает свойство (6), так как представляет сумму значений квадратов заполнений (ячеек) таблицы дифференциальных разностей с ненулевыми входами и выходами (с исключением первого столбца и первой строки таблицы). Он складывается из суммы заполнений строк усеченной таблицы (сумма квадратов элементов по любой строке таблицы равна квадрату половинного значения числа входов в неё $\left(2^{n-1}\right)^2$, умноженному на общее число ее ненулевых строк равное $2^n - 1$). В результате справедливо утверждение.

Утверждение 4. *Для закона распределения смещений таблицы линейных аппроксимаций случайной подстановки выполняется условие нормировки:*

$$\frac{2^n - 1}{\left(2^{n-1}\right)^2} \cdot \sum_{k=-2^{n-2}}^{2^{n-2}} (2k)^2 \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ 2^{n-2} + k \end{pmatrix}^2 = 2^n.$$

В качестве третьего результата покажем, что для закона распределения смещений таблицы линейных аппроксимаций случайной подстановки (4) справедливо отношение:

$$\frac{\Pr\left(\lambda^*(\alpha,\beta) = 2(k-1)\right)}{\Pr\left(\lambda^*(\alpha,\beta) = 2k\right)} = \left(\frac{2^{n-2} + k}{2^{n-2} - k + 1}\right)^2. \qquad (15)$$

Действительно, подставим в левую часть равенства явные представления для фигурирующих здесь законов распределения вероятностей $\Pr\left(\lambda^*(\alpha,\beta) = 2(k-1)\right)$ и $\Pr\left(\lambda^*(\alpha,\beta) = 2k\right)$:

$$\frac{\frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ 2^{n-2} + k - 1 \end{pmatrix}^2}{\frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ 2^{n-2} + k \end{pmatrix}^2} = \frac{\begin{pmatrix} 2^{n-1} \\ 2^{n-2} + k - 1 \end{pmatrix}^2}{\begin{pmatrix} 2^{n-1} \\ 2^{n-2} + k \end{pmatrix}^2}.$$

Дробь в правой части последнего равенства приводится к виду:

$$\frac{\binom{2^{n-1}}{2^{n-2}+k-1}^2}{\binom{2^{n-1}}{2^{n-2}+k}^2} =$$

$$= \left(\frac{\left(2^{n-2}+k\right)!\cdot\left(2^{n-2}-k\right)!}{\left(2^{n-2}+k-1\right)!\cdot\left(2^{n-2}-k+1\right)!} \right)^2 .$$

Раскрывая факториалы в числителе и знаменателе полученного результата, и для положительных и для отрицательных значений k приходим к итогу (15).

Из (15) следует, что поскольку $k = 1,\ldots, k^*$, причем $k^* \le 2^{n-2}$, то отношение

$$\frac{\Pr\left(\lambda^*(\alpha,\beta) = 2(k-1)\right)}{\Pr\left(\lambda^*(\alpha,\beta) = 2k\right)}$$

с ростом n быстро стремится к единице (при $n = 8 \to 1{,}09$; при $n = 16 \to 1{,}000015$). Это значит, что значения смещений таблиц линейных аппроксимаций в области близкой к максимумам мало отличаются друг от друга.

5. Заключение

Полученные соотношения для законов распределения вероятностей таблиц XOR разностей и таблиц линейных аппроксимаций могут оказаться полезными при изучении свойств шифрующих преобразований.

Из приведенных результатов можно сделать вывод, что если для полных дифференциалов значения максимумов являются ярко выраженными, то для линейных корпусов (для значений смещений таблиц LAT) значения ячеек в области максимумов смещений практически не отличаются. Их получается достаточно много, и они имеют значения на порядок и более превышающие максимальные значения таблицы полных дифференциалов.

Естественно приобретает важность проведение дальнейших исследований по изучению возможностей и оценке реальной сложности выполнения соответствующих атак. Что касается атак дифференциального криптоанализа, то нам уже удалось реализовать атаку на полный дифференциал уменьшенной версии шифра Baby-Rijndael. Построить атаку на линейный корпус малой версии шифра пока не удалось. Работа продолжается.

ЛИТЕРАТУРА

1. Олейников Р.В. Дифференциальные свойства подстановок / Олейников Р.В., Олешко О.И., Лисицкий К.Е., Тевяшев А.Д. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 326–333.
2. L. J. O'Connor. On the Distribution of Characteristics in Bijective Mappings. Advances in Cryptology. EUROCRIPT 93, Lecture Notes in Computer Science, vol. 795, T. Hellesethed., Springer-Verlag, pages 360–370, 1994.

3. Долгов В.И. Свойства таблиц линейных аппроксимаций случайных подстановок / Долгов В.И., Лисицкая И.В., Олешко О.И // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 334–340.
4. Luke O'Connor. Properties of Linear Approximation Tables. Email: oconnor@dsts. Edu. au, 1995.
5. Лисицкая И.В. Случайные подстановки в криптографии. / Долгов В.И., Лисицкая И.В., Лисицкий К.Е.// Радіоелектронні та комп'ютерні системи, 2010, № 5 (46), С. 79-84.
6. Лисицкая И.В. Экспериментальная проверка работоспособности новых критериев отбора случайных подстановок. / Лисицкая И.В., Лисицкий К.Е., Широков А.В., Мельничук Е.Д.// Радіоелектронні та комп'ютерні системи, 2010, № 6 (47), С. 87-93.
7. Горбенко И.Д. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / Горбенко І.Д., Долгов В.И., Лисицкая И.В., Олейников Р.В.//Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 212-320.
8. Бронштейн И.Н. Справочник по математике для инженеров и учащихся вузов./ Бронштейн И.Н., Семендяев К.А. // Изд-во М:. ″Наука″ 1980, стр. 976 с., 2007.

Надійшла у першій редакції 28.12.2010, в останній - 11.01.2011.