УДК 621.3.06

К.Е. ЛИСИЦКИЙ

ЗАКОН РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ СМЕЩЕНИЙ ТАБЛИЦ ЛИНЕЙНЫХ АППРОКСИМАЦИЙ СЛУЧАЙНЫХ ПОДСТАНОВОК

Введение

В соответствии с развиваемой в последнее время новой методологией оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа [1] обострился интерес к математическому описанию случайных подстановок. Он вызван тем, что оказалось, что все блочные симметричные шифры асимптотически приобретают свойства случайных подстановок. В этом направлении был получен ряд важных результатов [2 – 6].

Здесь возвратимся к работе [3], посвященной построению закона распределения вероятностей переходов таблиц линейных аппроксимаций случайных подстановок. В этой работе была представлена оригинальная версия доказательства теоремы, сформулированной еще Люком О'Конором [7]. Сегодня стало понятно, что представленное доказательство теоремы в ней выполнено не совсем аккуратно. В работе не хватает обоснований некоторых важных моментов, и явно не выдерживает критики Утверждение 2, точнее, его доказательство нельзя считать правильным (убедительным). Учитывая теоретическую важность результата, которому посвящена работа, здесь предлагается уточненная версия доказательства теоремы и дополнительные подходы к интерпретации ее результатов. Для уменьшения неоднозначности трактовок и повышения прозрачности доказательств излагаемого материала здесь вводятся и доказываются дополнительные утверждения, устраняющие имеющиеся в работе [3] недоработки и пробелы.

Уточненное доказательство теоремы

Следуя [3, 7], напомним обозначения, использованные в этих работах и саму теорему.

Пусть $\pi : Z_2^n \to Z_2^n$ – биективное n-битное отображение и пусть S_2^n будет множеством всех таких отображений. Для n-битного вектора $X \in Z_2^n$ пусть X_i обозначает i-й бит вектора X. Линейная аппроксимационная таблица для подстановки π обозначается LAT_π и является таблицей размера $2^n \times 2^n$ с элементами $LAT_\pi(\alpha, \beta)$, определяемыми соотношением

$$LAT_\pi(\alpha,\beta) \overset{def}{=} \overset{def}{=} \#\left\{ X / X \in Z_2^n,\ \bigoplus_{i=1}^{n} X[i]\cdot\alpha[i] = \bigoplus_{i=1}^{n} \pi\big(X[i]\big)\cdot\beta[i] \right\}, \quad (1)$$

где $\alpha, \beta \in Z_2^n$ и $'\cdot'$ обозначает операцию скалярного произведения.

В соответствии с приведенным определением $LAT_\pi(\alpha, \beta)$ представляет собой число равенств четности между линейной комбинацией входных битов (определяемых маской α по входу в LAT_π подстановки по строкам) и линейной комбинацией выходных битов (определяемых маской β по входу в таблицу LAT_π подстановки по столбцам).

Теорема, о которой идет речь, сформулирована в [3, 7] следующим образом.

Теорема 1: *Пусть $\lambda(\alpha, \beta)$ будет случайным числом, соответствующим значению линейной аппроксимационной таблицы подстановки $LAT_\pi(\alpha, \beta)$, когда подстановка π выбрана равновероятно из множества S_2^n и маски α, β ненулевые. Тогда $\lambda(\alpha, \beta)$ для целых значений k, $0 \le k \le 2^{n-1}$ принимает только четные значения и вероятность, что*

$\lambda(\alpha,\beta)=2k$
определяется выражением

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

Далее излагается новый (уточненный) вариант ее доказательства.

Д о к а з а т е л ь с т в о. Нас интересует число подстановок из общего их числа $2^n!$, ячейки таблиц $LAT_\pi(\alpha,\beta)$ которых для заданного значения входа в таблицы по строкам α и заданного значения входа в таблицы по столбцам β (заданного сочетания пары входов в LAT_π) имеют заполнением (значением) число $2k$.

По определению, если подстановка π имеет значение ячейки таблицы $LAT_\pi(\alpha,\beta)$ равное $\lambda(\alpha,\beta)=2k$, то это означает, что число входов в подстановку X из общего их числа 2^n, прошедших при построении таблицы маску α с признаками чет и нечет (имеющих результатом скалярного произведения $\alpha\cdot X$ нуль или единицу), совпадающих с числом соответствующих выходов подстановки $\pi(X)$, прошедших маску β с признаками чет и нечет (имеющих результатом скалярного произведения $\beta\cdot\pi(X)$ нуль или единицу), равно $2k$, т.е. число входов и выходов, удовлетворяющих равенству четности $\alpha\cdot X=\beta\cdot\pi(X)$ равно $2k$.

Итак, интересующее нас событие связано с совпадением признаков чет или нечет для входных текстов подстановки и ее выходных текстов, прошедших соответствующие маски.

В дальнейшем нам потребуется несколько дополнительных утверждений.

Утверждение 1. *Для любого сочетания масок входа α и масок выхода β ровно половина* (2^{n-1}) *из общего числа скалярных произведений для всего множества входов в подстановку (как и для всего множества выходов подстановки) принимают значения "чет"* (0), *а остальные* 2^{n-1} *скалярных произведений принимают значения "нечет"* (1).

Предварительно докажем еще одно утверждение

Утверждение 2

Сумма по модулю 2 *двоичных символов полного набора из* 2^l *l-битных векторов на всем наборе этих векторов в половине случае равна нулю, а в другой половине случаев равна* 1.

Д о к а з а т е л ь с т в о. Число единиц в векторах полного набора из 2^l двоичных векторов меняется от 0 до l, причем число векторов без единиц $C_l^0=1$, число векторов с одной единицей $C_l^1=l$, с двумя единицами $C_l^2=\frac{l(l-1)}{2}$, …, число векторов с k единицами C_l^k, . . ., число векторов с l единицами будет $C_l^l=1$. Но векторы с нечетным числом единиц при сложении битов по модулю 2 (при вычислении скалярных произведений) будут давать результатом единицу, а векторы с четным числом единиц при сложении битов по модулю 2 будут давать результатом нуль.

Тогда на полном множестве из 2^l векторов число результатов "чет" (0) и "нечет" (1) для $l=2s$ (четного) будет определяться выражением $\sum_{k=0}^{s}C_l^{2k}$ для векторов с четным числом единиц, либо соответственно $\sum_{k=0}^{s}C_l^{2k-1}$ для векторов с нечетным числом единиц, а для $l=2s+1$` (нечетного) будет соответственно определяться выражением $\sum_{k=0}^{s}C_l^{2k}$ для векторов

с четным числом единиц и $\sum_{k=0}^{s} C_l^{2k+1}$ для векторов с нечетным числом единиц. Нетрудно убедиться (непосредственной проверкой), что $\sum_{k=0}^{s} C_l^{2k} = \sum_{k=0}^{s} C_l^{2k-1} = 2^{l-1}$ для $l = 2s$ (четного), как и то, что $\sum_{k=0}^{s} C_l^{2k} = \sum_{k=0}^{s} C_l^{2k+1} = 2^{l-1}$ для $l = 2s+1$` (нечетного). Тем самым доказана справедливость утверждения 2.

Вернемся к Утверждению 1.

Д о к а з а т е л ь с т в о. Будем интерпретировать маски входа в подстановку и маски выхода подстановки как *l*-битные и *m*-битные единичные вектора, наложенные на *n*-битные блоки входов и выходов в подстановку. Тогда скалярные произведения $\alpha \cdot X$ для масок, содержащих *l* единиц, (также как и скалярные произведения $\beta \cdot \pi(X)$ для масок, содержащих *m* единиц), наложенных на полный набор *n*-битных блоков входов и выходов) независимо от расположения единичных символов маски будут включать полные наборы из *l*-битных (*m*-битных) двоичных последовательностей, которые повторяются на полном наборе *n*-битных векторов $2^n / 2^l = 2^{n-l}$ ($2^n / 2^m = 2^{n-m}$) раз.

Учитывая, что в соответствии с Утверждением 2 сумма по модулю 2 двоичных символов для полного набора из 2^l *l*-битных векторов на всем наборе этих векторов в половине случаев равна нулю, а в другой половине случаев равна 1, т.е. имеем 2^{l-1} нулей и столько же единиц, приходим к выводу, что для любой *l*-битной маски входа на всем множестве *n*-битных векторов $2^{l-1} \times 2^{n-l} = 2^{n-1}$ скалярных произведений будут давать результатом нуль и столько же 2^{n-1} скалярных произведений будут давать результатом единицу. Аналогичный результат следует и для скалярных произведений с *m*-битными масками выхода. Тем самым доказано утверждение 1.

Таким образом, в соответствии с доказанным выше положением ровно половина (2^{n-1}) из общего числа скалярных произведений для всего множества входов в подстановку (как и для всего множества выходов из подстановки) принимают значения "чет" (нуль), а остальные 2^{n-1} скалярных произведений принимают значения "нечет" (единица). В результате различные подстановки при вычислении $LAT_\pi(\alpha, \beta)$ практически будут отличаться только распределением четных (нулевых) и нечетных (единичных) значений множеств скалярных произведений $\alpha \cdot X$ и $\beta \cdot \pi(X)$ из одного и того же набора, включающего 2^{n-1} четных и 2^{n-1} нечетных значений этих произведений.

Результирующее число "проходов" (выполнений равенства $\alpha \cdot X = \beta \cdot \pi(X)$) для любой пары входов в таблицу α и β будет определяться числом совпадений признаков чет или нечет в "списках" соответствующих наборов скалярных произведений для входов и выходов подстановки, причем одно и то же значение числа "проходов" будут иметь подстановки, которые отличаются переходами (перестановками), сохраняющими четность (нечетность) компонент, формирующих значение $\lambda(\alpha, \beta)$. Напомним, что параметр $\lambda(\alpha, \beta)$ фиксирует число случаев выполнения равенства $\alpha \cdot X = \beta \cdot \pi(X)$ для каждой пары α, β.

Нам потребуется еще два утверждения.

Утверждение 3. *Две последовательности, составленные из* 2^n *двоичных элементов, содержащие одинаковое число* 2^{n-1} *символов каждого типа, имеют только четное число совпадений* (*несовпадений*).

Д о к а з а т е л ь с т в о. Пусть $\xi = \{0,1\}^{2^n}$ и $\zeta = \{0,1\}^{2^n}$ – две случайно взятые 2^n-битные последовательности с одинаковым числом нулей и единиц. Доказательство будем вести

«от противного». Предположим, что последовательности ξ и ζ имеют нечетное число совпадений. Пусть для конкретности совпадающие символы имеют четное число нулей и нечетное число единиц. Тогда оставшиеся (несовпадающие) символы последовательностей для одной из них будут иметь нечетное число нулей и четное число единиц, в то время как вторая последовательность тогда должна иметь четное число нулей и нечетное число единиц (ведь они противоположные). В результате получается, что в одной последовательности должно быть четное число нулей и четное число единиц, в то время как во второй должно быть нечетное число нулей и нечетное число единиц, а это противоречит исходному предположению, что обе последовательности состоят из одинакового четного числа нулей и четного числа единиц. Следовательно, наше предположение о том, что последовательности ξ и ζ могут иметь нечетное число совпадений не верно.

Из доказанного следует справедливость утверждения первой части теоремы о том, что параметр $\lambda(\alpha,\beta)$ линейных аппроксимационных таблиц подстановок принимает только четные значения, так как наборы признаков чет и нечет в скалярных произведениях можно интерпретировать как соответствующие двоичные последовательности.

Справедливо также и такое утверждение.

Утверждение 4. *Для двух последовательностей, составленных из* 2^n *числа двоичных элементов и содержащих одинаковое число* 2^{n-1} *символов каждого типа, совпадающие* (*несовпадающие*) *последовательности символов содержат для каждой из последовательностей одинаковое число единиц и нулей.*

Д о к а з а т е л ь с т в о. Пусть $\xi = \{0,1\}^{2^n}$ и $\zeta = \{0,1\}^{2^n}$ – две случайно взятые 2^n-битные последовательности с одинаковым числом нулей и единиц и пусть $2k = s+t$, $s \neq t$ будет числом совпадающих символов. Пусть далее для конкретности совпадающие символы содержат *s* единиц и *t* нулей (в обеих частях равенства четности содержится по *s* единиц и *t* нулей). Но каждая последовательность состоит из одинакового числа 2^{n-1} символов каждого типа. Опять доказательство от противного. Пусть теперь, скажем, для первой последовательности ξ в числе несовпадающих символов оказывается $2^{n-1} - s$ единиц и $2^{n-1} - t$ нулей. Но это несовпадающие символы и, значит, вторая последовательность должна содержать $2^{n-1} - s$ нулей и $2^{n-1} - t$ единиц (противоположные символы).

В результате получается, что первая последовательность содержит, как и положено, $2^{n-1} - s + s = 2^{n-1}$ единиц и $2^{n-1} - t + t = 2^{n-1}$ нулей, а вторая – $2^{n-1} - s + t$ нулей и $2^{n-1} - t + s$ единиц, что при $s \neq t$ противоречит исходному положению, что каждая из последовательностей состоит из одинакового числа нулей и единиц, т.е. мы должны считать, что $s = t$.

Таким образом, среди $2k$ пар совпадений признаков ″чет″ ″нечет″ в равенствах $\lambda(\alpha,\beta)$ для каждой подстановки половина совпадений ″четы″ и еще половина ″нечеты″.

Перейдем теперь к определению значений интересующего нас числа $\lambda(\alpha,\beta)$ для подстановки степени 2^n.

Заметим сразу, что подстановки с одним и тем же значением параметра $\lambda(\alpha,\beta)$ отличаются друг от друга распределением в левой и правой части равенств $\alpha \cdot X = \beta \cdot \pi(X)$ четных и нечетных компонент.

Ранее уже отмечалось, что из 2^n скалярных произведений в правых частях равенств (как и в левых) половина произведений имеют признак ″чет″, а другая половина признак ″нечет″ (их 2^{n-1} каждого типа). Причем равенство сохраняется, если меняются местами между собой переходы (выходы) подстановки, которые дают результатами скалярные произведения с одинаковым признаком четности.

Для 2^{n-1} входов в подстановку с одинаковым признаком четности соответствующие 2^{n-1} выходов образуют подстановку степени 2^{n-1}, т.е. саму подстановку степени 2^n можно

рассматривать как две подстановки степени 2^{n-1} (ведь переходы случайной подстановки формируются независимо друг от друга). Это значит, что для каждого значения маски выходов β существует $2^{n-1}!$ различных подстановок, отличающихся между собой закреплением (расстановкой) выходов, формирующих признаки ″чет″ и столько же, т.е. $2^{n-1}!$ различных подстановок, отличающихся между собой закреплением выходов, формирующих признаки ″нечет″. Действительно, выходы подстановки, соответствующие входам с одинаковым признаком четности для фиксированной маски α, сохраняются по числу четов и нечетов для выходной маски β при их перестановке между собой.

В силу независимости распределения выходов подстановок по входам всего получается, что существует $(2^{n-1}!)^2$ вариантов различных подстановок, имеющих одно и то же распределение признаков ″чет″ и ″нечет″ (2^{n-1} скалярных произведений $\beta \cdot C$ каждого типа четности), отличающихся расстановкой выходов подстановки по своим входам.

Теперь каждая из таких подстановок реализует интересующее нас значение параметра $\lambda(\alpha, \beta) = 2k$ привязкой (совпадениями признаков ″чет″ и ″нечет″) входящих в $2k$ равенств $\alpha \cdot X = \beta \cdot \pi(X)$.

В соответствии с утверждением 4 таких совпадений будет в $2k$ переходах $\lambda(\alpha, \beta)$ по k каждого типа четности. Эти два набора по из одинакового числа переходов каждого типа (k равенств $\alpha \cdot X = \beta \cdot \pi(X)$ каждого из типов) могут быть осуществлены для каждого уникального набора из 2^{n-1} скалярных произведений $\beta \cdot C$ одного типа четности $C_{2^{n-1}}^{k}$ вариантами расстановки выходов подстановки по ее входам, а всего получается, что равенства обоих типов четности, образующих $2k$ интересующих нас переходов $\lambda(\alpha, \beta)$, могут быть реализованы $\left(C_{2^{n-1}}^{k}\right)^2$ различными способами ($C_{2^{n-1}}^{k} = \binom{2^{n-1}}{k}$ – биномиальный коэффициент).

В результате приходим к результату, который и утверждается в теореме.

Далее уже цитируются результаты работы [3].

В линейном криптоанализе интересуются входами (значениями) в линейную аппроксимационную таблицу подстановки порядка 2^n, которые после вычитания нормировочного значения 2^{n-1} являются отличием (смещением) действительного значения на число 2^{n-1} и, как отмечается в [3, 7, 8], представляют собой корреляцию линейных комбинаций входов и выходов подстановки. В результате приходят к так называемым линеаризованным таблицам подстановок, которые в [3, 7] обозначены $LAT_{\pi}^{*}(\alpha, \beta)$. Они определяются выражением

$$LAT_{\pi}^{*}(\alpha, \beta) = \left| LAT_{\pi}(\alpha, \beta) - 2^{n-1} \right|. \qquad (3)$$

В этом случае модуль в правой части записанного соотношения приводит к тому, что значение $\lambda(\alpha, \beta) = 2k$ для $2k' = 2k - 2^{n-1}$, $0 \le k \le 2^{n-1}$ может быть получено как при положительном смещении $k' = k - 2^{n-2}$ ($2^{n-2} \le k \le 2^{n-1}$), так и при отрицательном смещении $k' = k - 2^{n-2}$ ($0 \le k \le 2^{n-2}$), причем возможны и нулевые значения смещений ($\lambda^*(\alpha, \beta) = 0$), когда $k = 2^{n-2}$. Возвращаясь к старому обозначению переменной k (теперь уже для смещения), теорему 1 теперь можем переписать в виде теоремы 2.

Теорема 2: *Пусть $\lambda^*(\alpha, \beta)$ будет случайным числом, соответствующим значению линейной аппроксимационной таблицы подстановки $LAT_{\pi}^{*}(\alpha, \beta) = \left| LAT_{\pi}(\alpha, \beta) - 2^{n-1} \right|$, когда подстановка π выбрана равновероятно из множества S_2^n и маски α, β ненулевые. Тогда*

$\lambda^*(\alpha,\beta)$ для целых значений k, $|k| \le 2^{n-2}$ принимает только четные значения и вероятность, что $\lambda^*(\alpha,\beta) = 2k$ определяется выражением

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

Определение наибольшего значения входа *в* LAT_π^*

Наша цель - определить наибольшее значение таблицы LAT_π^*.

Пусть теперь, как и в [3,7], $\lambda(\pi)$ будет наибольшим значением таблицы LAT_π^* взятым над всеми невырожденными α и β:

$$\lambda(\pi) \overset{def}{=} \max_{\alpha,\beta \ne 0} LAT_\pi^*(\alpha,\beta).$$

Здесь пропустим ряд соображений, представленных в работе [1], в частности проверку условий нормировок для полученного закона распределения вероятностей.

Обозначим $\mathrm{E}[\lambda(\pi,2k)]$ ожидаемое число ячеек таблицы LAT_π^*, имеющих значение $2k$.

В этом месте, повторяя рассуждения работы [3], сделаем переход от свойств ансамбля подстановок к свойствам отдельной подстановки. Считая, что полученный закон распределения вероятностей (4) справедлив для каждой отдельно взятой подстановки, рассмотрим его теперь применительно к множеству $(2^n-1)^2$ ячеек таблицы LAT_π^*, соответствующих ненулевым ее входам и выходам.

В результате можем получить выражение для вычисления $\mathrm{E}[\lambda^*(\pi,2k)]$ как простое умножение формулы (4) на общее число ячеек таблицы подстановки, исключая первую строку и первый столбец

$$\mathrm{E}[\lambda^*(\pi,2k)] = \frac{(2^n-1)^2 \cdot \left(2^{n-1}!\right)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ 2^{n-2} + |k| \end{pmatrix}^2, \qquad (5)$$

(для положительных и отрицательных значений смещения k результат будет один и тот же).

Выражение (5) имеет тенденцию быстро стремиться к нулю с ростом k. Среднему значению максимума таблицы LAT_π^* подстановки, как следует из сопоставления результатов вычислений с экспериментальными данными, будет соответствовать значение k^*, при котором получается наименьшее значение $\mathrm{E}[\lambda^*(\pi,2k)]$, превышающее или равное единице, т.е. для определения k^* необходимо найти округленное в сторону увеличения до ближайшего целого решение уравнения

$$\frac{(2^n-1)^2 \cdot \left(2^{n-1}!\right)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ 2^{n-2} - |k^*| \end{pmatrix}^2 = 1. \qquad (6)$$

Сравнение расчетных и экспериментальных результатов

Варианты решения уравнения (6) (переборным методом, который существенно упрощается при использовании результатов экспериментов), вместе с данными экспериментов заимствованные из [3] иллюстрирует табл. 1.

Как следует из результатов, представленных в табл. 1, найденные значения максимумов смещений таблиц линейных аппроксимаций случайных подстановок хорошо согласуются с данными, полученными экспериментальным путем.

Заметим, что в правой колонке таблицы представлены и результаты расчетов по предлагаемой в [9] упрощенной формуле

$$\mathrm{E}\left[\lambda(\pi,2k)\right]=\left(\frac{3}{2}\right)^{n}. \qquad (7)$$

Таблица 1

Сравнение теоретических
и экспериментальных результатов

n	$2k$*	$\mathrm{E}\left[\lambda(\pi,2k)\right]$	Эксперимент
4	4 6 8	3,89 1,118 0,017	5,498 $\left(\frac{3}{2}\right)^{8}=5{,}06$
6	12 14 16	9,013 1,7 0,239	14,48 $\left(\frac{3}{2}\right)^{6}=11{,}39$
8	32 34	2,12 0,7457	34,68 $\left(\frac{3}{2}\right)^{8}=25{,}62$
10	74 76	1,16 0,64	78,8 $\left(\frac{3}{2}\right)^{10}=57{,}66$
12	162 164	1,129 0,82	116,24 $\left(\frac{3}{2}\right)^{12}=129{,}74$
14	350 352	1,069 0,900	314 $\left(\frac{3}{2}\right)^{14}=291$
16	748 750	1,027 0,93	720 $\left(\frac{3}{2}\right)^{16}=657$

Если идти далее, то видно, что выражение (4) можно рассматривать как закон распределения вероятностей значений $\lambda^*(\alpha,\beta)$ таблицы $LAT_{\pi}^{*}(\alpha,\beta)$ отдельной взятой случайной подстановки π. В работе [3] показано, что для него выполняется условие нормировки ($\Pr\left(\left|\lambda(\pi)\right|\le 2^{n-1}\right)=1$).

Далее приводятся дополнительные материалы из работы [9].

Как показывает анализ, полученное расчетное соотношение хорошо работает для значений $n\le 32$. Для получения практических результатов при больших значениях n в работе [9] предложено воспользоваться теоремой 9 из работы [10], в которой обосновывается допустимость аппроксимациb соотношения (4) нормальным законом распределения вероятностей. Эта теорема здесь приводится под номером 3.

Теорема. 3: *Для случайной n-битовой подстановки, с* $n \ge 5$ *дисбаланс* $\mathrm{Imb}(v,u)$ *аппроксимации является случайным значением с распределением, которое может быть аппроксимировано в виде*

$$\Pr(\mathrm{Imb}(v, u) = z) \approx 2Z\left(\frac{z}{2^{(n-2)/2}}\right) \tag{8}$$

для z четного и нуль для z нечетного.

Если в (8) подставить $z = 2x$, то его можно переписать в виде

$$\Pr(\mathrm{Imb}(v, u) = 2x) \approx Z\left(\frac{x}{2^{(n-4)/2}}\right).$$

При выводе этого соотношения авторы пользуются леммой, повторяющей наш результат (2):

$$\Pr(\mathrm{Imb}(v, u) = 2x) = \frac{\binom{2^{n-1}}{2^{n-2}+x}^2}{\binom{2^n}{2^{n-1}}}, \tag{9}$$

т.е. в наших обозначениях дисбаланс $\mathrm{Imb}(v, u) = z$ при $z = 2k$ как раз соответствует $\lambda(\pi) = 2k$.

В табл. 2, заимствованной из [9], приводятся для сравнения результаты оценки максимальных значений смещений линейной таблицы случайной подстановки (половинных значений), полученных при использовании аппроксимирующего выражения (7), аппроксимации, использованной в выражении (8), и точного расчета по формуле (4).

Таблица 2

Сравнение результатов, полученных различными путями

n	Значение $x = k_L^*$ для нормального закона	Значение x для нашей аппроксимации	Расчетное значение k_L^*
8	16	12,81	16-17
16	334	328,42	374
20	1466	1662,62	1670
24	6342	8417	7302
28	27142	42611,346	31504
32	115080	215719	135649
128	62316975567822669939 $\approx 2^{67} \rightarrow \approx 2^{-120}$	17324119207854702237560 $\approx 2^{75} \rightarrow \approx 2^{-104}$	-

Как следует из представленных результатов расчетов, итоговая аппроксимация в виде нормального закона (8) оказывается достаточно хорошей. Видно также, что если аппроксимация нормальным законом дает оценки заниженные, то предлагаемая в [9] аппроксимация приводит к завышенным оценкам.

Для значений $n > 32$ остается ориентироваться на аппроксимирующие соотношения. Если полагать, что соотношение граничных (оценочных) значений, следующих из соответствующих аппроксимирующих выражений, с истинными значениями сохраняется и для значений $n > 32$, то в соответствии с идеологией, развиваемой в работе [9], можно перейти к расчетам ожидаемых значений максимумов линейных вероятностей для полномасштабных шифров.

Например, использование представленных аппроксимирующих соотношений для 128-битного шифра позволяет получить граничные значения для максимальной линейной вероятности (слева и справа) вида

$$2^{-120} \le LP_{\max}^{f} \le 2^{-104}.$$

Заметим, однако, что аппроксимация нормальным законом для значений $n \ge 32$ получается существенно точнее предлагаемой аппроксимации (судя по приведенным данным, отношение расчетного и аппроксимирующего выражений для аппроксимации в виде нормального закона принимает значения: при $n = 20 \rightarrow \frac{1670}{1466} = 1{,}139$ при $n = 24 \rightarrow \frac{7302}{6384} = 1{,}144$, при $n = 32 \rightarrow \frac{135649}{115080} = 1{,}178$). Если считать, что близкое к этому соотношение (отношение меньше двойки) сохранится и для больших значений n, то можно прийти к ожидаемому значению вероятности, более близкому к левой из двух приведенных границ, т.е. в качестве достаточно точной оценки линейной вероятности для интересующего нас битового размера входа в шифр $n = 128$ следует рассматривать значение $LP_{\max}^{f} \approx 2^{-119}$. Предложенная аппроксимация в этом случае дает ошибку в 2^{15} раза. Она оказывается хорошей для малых версий шифров. Работа по уточнению результатов продолжается.

Заключение

Приведенный закон распределения вероятностей для числа смещений таблиц линейных аппроксимаций случайных подстановок позволяет, как показано в работах [1, 9], ввести более строгие критерии отбора случайных подстановок, вплотную приближающих их свойства к свойствам шифрующих преобразований блочных симметричных шифров.

Выведенные расчетные соотношения для средних значений максимумов таблиц линейных аппроксимаций позволяют более обоснованно подойти к оценке показателей стойкости блочных симметричных шифров к атакам линейного криптоанализа.

Список литературы: 1. *Лисицкая, И. В.* Методология оценки стойкости блочных симметричных криптопреобразований на основе уменьшенных моделей : дис. … д-ра техн. наук : 05.13.05 / Лисицкая Ирина Викторовна. – 2012. – 293 с. 2. *Олейников, Р.В.* Дифференциальные свойства подстановок / Р.В. Олейников, О.И. Олешко, К.Е. Лисицкий, А.Д. Тевяшев // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 326-333. 3. *Долгов, В.И.* Свойства таблиц линейных аппроксимаций случайных подстановок / В.И. Долгов, И.В. Лисицкая, О.И. Олешко // Прикладная радиоэлектроника. – Харьков : ХНУРЭ, 2010. – Т. 9, №3. – С. 334-340. 4. *Долгов, В.И.* Случайные подстановки в криптографии / В.И. Долгов, И.В. Лисицкая, К.Е. Лисицкий // Радіоелектронні та комп'ютерні системи. – 2010. – № 5 (46). – С. 79-85. 5. *Лисицкая, И.В.* Оценка числа случайных подстановок с заданным распределением парных разностей XOR таблиц и смещений таблиц линейных аппроксимаций / И.В. Лисицкая, А.В. Широков, Е.Д. Мельничук, К.Е. Лисицкий // Прикладная радиоэлектроника. – Харьков : ХНУРЭ. – 2010. – Т. 9, № 3. – С. 341-345. 6. *Олейников, Р. В., Лисицкий, К. Е.* Исследование дифференциальных свойств подстановок различных цикловых классов // Двенадцатая Междунар. науч.-практ. конф. "Безопасность информации в информационно-телекоммуникационных системах ", 19-22 мая 2009 г., Тезисы докладов. – К. : ЧП "ЕКМО", НИЦ "ТЕЗИС" НТУУ "КПИ", 2009. – С. 24-25. 7. *Luke O'Connor*. Properties of Linear Approximation Tables. Email: oconnor@dsts. Edu. au, 1995. 8. *Luke O'Connor*. On Linear Approximation Tables and Ciphers secure against Linear Cryptanalysis. Email: oconnor@dsts. Edu. au, 1995. 9. *Долгов, В. И.* Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа : монография / В.И. Долгов, И.В. Лисицкая. – Харьков : Форт, 2013. – 420 с. 10. *Joan Daemen, Vincent Rijmen* Probability distributions of Correlation and Differentials in Block Ciphers / Joan Daemen, Vincent Rijmen // April 13, 2006, pp. 1–38.

Харьковский национальный университет имени В.Н. Каразина

Поступила в редколлегию 07.04.2017