УДК 621. 391:519.2:519.7

# СВОЙСТВА ТАБЛИЦ ЛИНЕЙНЫХ АППРОКСИМАЦИЙ СЛУЧАЙНЫХ ПОДСТАНОВОК

*В.И. ДОЛГОВ, И.В. ЛИСИЦКАЯ, О.И. ОЛЕШКО*

Выводятся расчетные соотношения для среднего значения максимумов таблиц линейных аппроксимаций случайных подстановок. Показывается, что линейные свойства шифрующих преобразований современных блочных симметричных шифров (при заявленном числе циклов преобразования) являются одним из проявлений свойств случайных подстановок. Предлагается подход к сравнению эффективности решений по построению алгоритмов шифрования в виде минимального числа циклов алгоритма, при котором реализуется асимптотический показатель среднего значения максимума линейного корпуса.

*Ключевые слова:* линейные аппроксимации, случайные подстановки.

## ВВЕДЕНИЕ

Интерес и внимание к исследованию и разработке процедур генерации криптографически стойких S-блоков возник в начале 90-х годов прошедшего столетия [1, 2, 3, 4, 5, 6 и др.]. Он стал закономерным исходом изучения и исследования специалистами надежности американского стандарта симметричного шифрования DES, завоевавшим к тому времени мировой авторитет и признание (ставшим фактически всемирным стандартом). К этому же времени относится появление работы израильских ученых-криптографов Бихама и Шамира [7], предложивших атаку дифференциального криптоанализа на шифр DES, а двумя годами позже работы Мацуи [8], посвященной линейному криптоанализу – второму новому типу криптонападения на DES. Эти работы стали заметным стимулом дальнейшего разворачивания работ, посвященных исследованию и анализу S-блоковых конструкций и алгоритмов [9-16 и мн. другие], может быть часто не опирающиеся прямо на S-блоковые конструкции, но, тем не менее, имеющие к ним самое непосредственное отношение. Сегодня эти работы, конечно уже вышли далеко за рамки шифра DES. Появилось множество новых решений по построению алгоритмов шифрования. На смену самого шифра DES в США не так уж и давно принят новый стандарт шифрования AES (FIPS-197). Естественно, что параллельно с развитием техники конструирования шифров происходило и совершенствование методов криптоанализа, направленных на преодоление показателей стойкости, закладываемых в шифр его разработчиками. Это значит, что и сегодня вопросы построения более совершенных процедур шифрования и алгоритмов криптографической защиты информации в целом не потеряли своей актуальности, а, следовательно, в центре внимания криптографов и математиков продолжают оставаться методы и алгоритмы конструирования новых шифров и в том числе методы (генерации) более совершенных S-блоковых конструкций.

Мы хотим здесь обратить внимание читателей на то, что многие исследователи связывают показатели стойкости шифров к атакам дифференциального и линейного криптоанализа с соответствующими показателями S-блоков, с помощью которых осуществляются нелинейные преобразования во многих шифрах. Так, в работах [17,18 и др.] результирующие показатели стойкости шифров к указанным атакам напрямую выражаются через значения максимумов таблиц XOR разностей и линейных аппроксимаций входящих в шифр S-блоковых преобразований. Наши эксперименты с малыми версиями шифров, однако, показывают, что асимптотические характеристики устойчивости шифров не совпадают с показателями, определяемыми через максимумы таблиц XOR разностей или соответственно максимумы таблиц линейных аппроксимаций подстановочных конструкций. Более того, наши эксперименты с уменьшенными копиями современных шифров показывают, что их асимптотические характеристики вообще не зависят от максимумов таблиц XOR разностей и таблиц линейных аппроксимаций используемых в шифрах S-блоков.

Здесь мы продолжаем исследования, начатые в нашей работе [19], где мы рассматривали свойства таблиц XOR разностей случайных подстановок. Теперь мы будем интересоваться свойствами таблиц линейных аппроксимаций случайных подстановок. В этой работе ставится задача получить распределение значений ячеек таблиц линейных аппроксимаций S-блоков расчетным путем.

## 1. ЗАКОН РАСПРЕДЕЛЕНИЯ СМЕЩЕНИЙ ТАБЛИЦ ЛИНЕЙНЫХ АППРОКСИМАЦИЙ СЛУЧАЙНЫХ ПОДСТАНОВОК

Отметим, что и в этом случае (имеется в виду наша работа [19]), близкую по постановке задачу нам удалось найти также в работах Luka O'Connora [20, 21] 1995-го года, в которых приводятся интересующие нас расчетные соотношения без доказательств. Кроме того, нас не удовлетворила и авторская интерпретация конечных результатов, что определило целесообразность изложения собственной позиции по этому вопросу.

И в этой работе мы воспользуемся центральной идеей развиваемого в [20, 21] подхода, а именно будем считать, что свойства отдельной

случайной подстановки однозначно выражаются через свойства ансамбля случайных подстановок, и на этой основе представим свою версию доказательств и интерпретации соответствующих результатов.

Далее рассматриваются подстановки общего вида порядка $2^n$, к которым можно отнести и шифрующие преобразования, осуществляемые для каждого $n$-битного блока данных $P$ и фиксированного значения ключа $K$ симметричными шифрами. Заметим, однако, сразу, что множество подстановок (с операцией умножения подстановок) в классическом понимании образуют симметрическую группу, обозначаемую в математической литературе как $S_2^n$, порядок которой равен $2^n!$, в то время как множество подстановок, образуемое симметричными шифрами, не является группой и их число ограничено значением $2^n$ (числом ключей).

В линейном криптоанализе интересуются значениями (входами) в так называемые линейные аппроксимационные таблицы ($LAT$) S-блоков, которые, как отмечается в [20, 21], после вычитания нормировочного значения $2^{n-1}$ представляют собой корреляции линейных комбинаций с входами и выходами S-блоков.

Напомним ряд определений.

Следуя работе [21], 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 $i$-тый бит вектора $X$. Линейная аппроксимационная таблица для подстановки $p$ обозначается $LAT_\pi$ и является таблицей размера $2^n \times 2^n$ с элементами $LAT_\pi(\alpha,\beta)$, определяемыми соотношением

$$LAT_\pi(\alpha,\beta) \stackrel{def}{=}$$

$$\stackrel{def}{=} \#\left\{ X / X \in Z_2^n, \stackrel{n}{\oplus}_{i=1} X[i]\cdot\alpha[i] = \stackrel{n}{\oplus}_{i=1} \pi(X[i])\cdot\beta[i] \right\},$$

где $\alpha,\beta \in Z_2^n$ и $'\cdot'$ обозначает операцию побитного логического ИЛИ.

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

Нас будет интересовать теорема, которая приведена в работе [20] без доказательства.

**Теорема 1**: *Пусть* $\lambda(\alpha,\beta)$ *будет случайным числом, соответствующим значению линейной аппроксимационной таблицы подстановки* $LAT_\pi(\alpha,\beta)$, *когда подстановка p выбрана равновероятно из множества* $S_2^n$ *и маски* $\alpha,\beta$ *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*

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

Мы далее здесь предлагаем свой вариант ее доказательства.

Доказательство. 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 $\alpha$ и заданного значения входа в таблицы по столбцам $\beta$ (заданного сочетания пары входов в $LAT_\pi$) имеют заполнением (значением) число $2k$.

По определению, если подстановка $p$ имеет значение ячейки $LAT_\pi(\alpha,\beta)$ равное $\lambda(\alpha,\beta) = 2k$, то это означает, что число плайнтекстов $P$ из общего их числа $2^n$, прошедших при построении таблицы маску $\alpha$ с признаками чет и нечет (имеющих результатом скалярного произведения $\alpha \cdot P$ ноль или единицу), совпадающих с числом соответствующих шифртекстов $C$, прошедших маску $\beta$ с признаками чет и нечет, равно $2k$ (число плайнтекстов, удовлетворяющих равенству четности $\alpha \cdot P = \beta \cdot C$, равно $2k$).

Итак, интересующее нас событие связано с совпадением признаков чет или нечет для плайнтекстов и шифртекстов, прошедших соответствующие маски.

Обратим в связи с этим внимание на то, что для любого из вариантов сочетаний масок $\alpha,\beta \in Z_2^n$ скалярные произведения $\alpha \cdot P$ также как и $\beta \cdot C$ формируются с использованием всех $2^n$ $n$-битных возможных значения входов и выходов. Причем ровно половина ($2^{n-1}$) из общего числа скалярных произведений для всего множества плайнтекстов (как и для всего множества шифртекстов) принимают значения "чет", а остальные $2^{n-1}$ скалярных произведений принимают значения "нечет". В результате различные подстановки при вычислении $LAT_\pi(\alpha,\beta)$ практически будут отличаться только распределением четных и нечетных значений множеств скалярных произведений $\alpha \cdot P$ и $\beta \cdot C$ из одного и того же набора (включающего $2^{n-1}$ четных и $2^{n-1}$ нечетных значений этих произведений).

Это означает, что каждая пара $\alpha$ и $\beta$ значений масок для входов (по строкам и столбцам) в таблицы $LAT_\pi$ при переборе по всем возможным значениям входов $P$ в подстановку (при вариации по всем значениям плайнтекстов) будет приводить к одному и тому же закону распределения вероятностей параметра $\lambda(\alpha,\beta)$ – числа выполнения линейных соотношений $\alpha \cdot P = \beta \cdot C$ независимо от конкретных значений масок $\alpha$ и $\beta$.

Результирующее число "проходов" (выполнений равенства $\alpha \cdot P = \beta \cdot C$ для пары $\alpha$ и $\beta$ будет определяться числом совпадений четов или нечетов в "списках" соответствующих наборов скалярных произведений, 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 $\alpha \cdot P = \beta \cdot C$ для каждой подстановки.

Докажем сначала дополнительное утверждение.

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

Доказательство. Пусть $\xi = \{0,1\}^n$ и $\zeta = \{0,1\}^n$ – две случайно взятые $2^n$-битные последовательности с одинаковым числом нулей и единиц.

Доказательство будем вести от противного. Предположим, что последовательности $\xi$ и $\zeta$ 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 $\xi$ и $\zeta$ 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 скалярных произведений можно интерпретировать как соответствующие двоичные последовательности.

Справедливо также и такое утверждение.

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

Доказательство. Пусть $\xi = \{0,1\}^n$ и $\zeta = \{0,1\}^n$ – 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 (снова доказательство ведется от противного). Пусть далее для конкретности совпадающие символы содержат $s$ единиц и $t$ нулей. Тогда несовпадающие символы каждой из последовательностей $\xi$ и $\zeta$ должны содержать $2^{n-1} - s$ единиц и $2^{n-1} - t$ нулей, причем $2^{n-1} - s \neq 2^{n-1} - t$ (разное число нулей и единиц). Но одинаковые наборы из нулей и единиц в ″хвостах″ каждой из последовательностей могут дать $2^{n-1} - 2k$ несовпадений только тогда, когда сравниваемые ″хвосты″ последовательностей имеют одинаковое число $2^{n-2} - 2$ единиц и нулей. Мы пришли к противоречию, и, следовательно, предположение, что $s \neq t$ неверно.

Таким образом, среди $2k$ пар совпадений признаков ″чет″ и ″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 порядка $2^n$.

Заметим сразу, что подстановки с одним и тем же значением параметра $\lambda(\alpha,\beta)$ отличаются друг от друга распределением в левой и правой сторонах равенств $\alpha \cdot P = \beta \cdot C$ 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.

Это значит, что для каждого значения маски выходов $\beta$ 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″.

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 закрепленными за ними выходами подстановок.

Теперь каждая из таких подстановок реализует интересующее нас значение параметра $\lambda(\alpha,\beta) = 2k$ привязкой (совпадениями признаков ″чет″ и ″нечет″) $2k$ скалярных произведений $\beta \cdot C$ выходов к $2k$ скалярным произведениям входов $\alpha \cdot P$.

В соответствии с утверждением 2 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 $\alpha \cdot P = \beta \cdot C$ каждого из типов) могут быть осуществлены для каждого уникального набора из $2^{n-1}$ скалярных произведений $\beta \cdot C$ одного типа четности $C^k_{2^{n-1}}$ 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

$$\left(C_{2^{n-1}}^{k}\right)^2 \qquad (2)$$

различными способами ( $C_{2^{n-1}}^{k} = \begin{pmatrix} 2^{n-1} \\ k \end{pmatrix}$ – биномиальный коэффициент).

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

В линейном криптоанализе интересуются входами (значениями) в линейную аппроксимационную таблицу подстановки порядка $2^n$, которые являются отличием (смещением) действительного значения на число $2^{n-1}$, что представляет собой корреляцию между линейными комбинациями входов и выходов.

Поэтому рассматриваются так называемые линеаризованные таблицы подстановок, которые в [20] 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 $LAT_\pi^*(\alpha,\beta) = 2k$, $k > 0$ может быть получено и при $k' = k + 2^{n-1}$, и при $k' = 2^{n-1} - k$ (значение $k' = k - 2^{n-1}$ может быть как положительным, так и отрицательным). Причем, возможны и нулевые значения $LAT_\pi^*(\alpha,\beta)$, когда $k' = 2^{n-1}$. С учетом отмеченного приходим к утверждению 3.

**Утверждение 3.** *Пусть* $\lambda^*(\alpha,\beta)$ *будет случайным значением линейной аппроксимационной таблицы* $LAT_\pi^*(\alpha,\beta)$ *для пары её входов б и в, когда подстановка р выбрана равновероятно из множества* $2^n$ *и* $\alpha,\beta$ *не нулевые. Тогда* $\lambda^*(\alpha,\beta)$ *принимает только четные значения и для* $|k| \le 2^{n-2}$

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

Утверждение следует непосредственно из теоремы 1 и приведенных выше соображений.

## 2. СРАВНЕНИЕ РАСЧЕТНЫХ И ЭКСПЕРИМЕНТАЛЬНЫХ РЕЗУЛЬТАТОВ

Наша цель определить границу для наибольшего значения входа в $LAT_\pi^*$.

Пусть теперь, как и в [20], $\lambda(\pi)$ – будет наибольшим входом $LAT_\pi^*$ для отображения $\pi$, взятого над всеми невырожденными $\alpha$ и $\beta$:

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

Рассуждения автора цитируемой работы [20] по определению $\lambda(\pi)$ не все представляются достаточно аккуратными. Кроме того, автор допускает ошибки в записи некоторых принципиальных соотношений. Поэтому мы, не игнорируя его отдельных соображений и рассуждений, представим свой вариант вывода расчетного выражения для определения $\lambda(\pi)$.

Итак, пусть теперь $E[\lambda(\pi,2k)]$ обозначает ожидаемое число ячеек таблицы $LAT_\pi^*$, имеющих значение $2k$.

В этом месте, как и в работе [20], мы и сделаем переход от свойств ансамбля подстановок к свойствам отдельной подстановки, о чем говорилось в предыдущем разделе. 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 $LAT_\pi^*$, соответствующих ненулевым ее входам и выходам.

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

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

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

Аналогичный результат получен и в работе [21], однако, и в записи этого выражения, как и в записи выражения аналогичного выражению (4), в цитируемой работе имеются погрешности.

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

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

Аналогичный результат представлен в работе [20] в виде условия для определения границы для вероятности того, что $\lambda(\pi)$ достигает самое большее значение $2t$ в виде

$$\Pr(\lambda(\pi) \le 2t) > 1 - \sum_{k=2^{n-2}+t}^{2^{n-1}} E[\lambda(\pi,2k)].$$

В частности, автором определялось наименьшее значение $t$, для которого $\Pr(\lambda(\pi) \le 2t) > \frac{1}{2}$, и это граничное значение им было обозначено $t_n$ и определено как медиана распределения. Результаты расчетов, приведенные в его работе, отличаются от полученных нами в два раза (из-за лишнего сомножителя двойки в представлении выражения (5)).

Варианты решения уравнения (6) (переборным методом, который резко упрощается при использовании результатов экспериментов), вместе с данными экспериментов иллюстрирует табл. 1.

Как следует из результатов, представленных в табл. 1, найденные значения максимумов таблиц

линейных аппроксимаций случайных подстановок хорошо согласуются с данными, полученными экспериментальным путем.

**Таблица 1**

Сравнение теоретических и экспериментальных результатов

| $n$ | $2k^*$ | $E[\lambda(\pi,2k)]$ | Эксперимент |
|---|---|---|---|
| 4 | 4<br>6<br>8 | 3,89<br>1,118<br>0,017 | 5,498<br>$\left(\frac{3}{2}\right)^8 = 5{,}06$ |
| 6 | 12<br>14<br>16 | 9,013<br>1,7<br>0,239 | 14,48<br>$\left(\frac{3}{2}\right)^6 = 11{,}39$ |
| 8 | 32<br>34 | 2,12<br>0,7457 | 34,68<br>$\left(\frac{3}{2}\right)^8 = 25{,}62$ |
| 10 | 74<br>76 | 1,16<br>0,64 | 78,8<br>$\left(\frac{3}{2}\right)^8 = 57{,}66$ |
| 12 | 162<br>164 | 1,129<br>0,82 | 116,24<br>$\left(\frac{3}{2}\right)^8 = 129{,}74$ |
| 14 | 350<br>352 | 1,069<br>0,900 | 314<br>$\left(\frac{3}{2}\right)^{14} = 291$ |
| 16 | 748<br>750 | 1,027<br>0,93 | 720<br>$\left(\frac{3}{2}\right)^{17} = 657$ |

Если идти далее, то можно убедиться, что закон распределения вероятностей (4) с ограничением по числу слагаемых можно рассматривать как закон распределения вероятностей значений $\lambda^*(\alpha,\beta)$ таблицы $LAT_\pi^*(\alpha,\beta)$ отдельной взятой случайной подстановки $\pi$ (к аналогичному результату в отношении закона распределения вероятностей значений ячеек XOR таблиц мы пришли и в работе [19] при анализе дифференциальных свойств случайных подстановок).

Убедимся, что для найденной нами вероятности (4) выполняется условие нормировки (проверка результата).

Запишем для этого более аккуратное выражение для вероятности того, что $\lambda(\pi)$ имеет значение не превышающее $2t$ в виде

$$\Pr\left(\lambda^*(\alpha,\beta)\le 2t\right)=\sum_{k=-t}^{t}\Pr\left(\lambda^*(\alpha,\beta)=2k\right)= \\ =\sum_{k=2^{n-2}-t}^{2^{n-2}+t}\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{k}^2, \qquad (7)$$

для $t\le 2^{n-2}$.

Если воспользоваться известным свойством биномиальных коэффициентов:

$$\left(C_n^0\right)^2+\left(C_n^1\right)^2+\ldots+\left(C_n^n\right)^2=C_{2n}^n$$

(см., например, [21]), то приходим к результату $\Pr\left(|\lambda(\pi)|\le 2^{n-1}\right)=1$, т.е. условие нормировки для закона распределения вероятностей (4) выполнено.

Более того, легко убедиться также в том, что

$$2\cdot\sum_{k=k^*+1}^{2^{n-2}}\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+k}^2<<1. \qquad (8)$$

Здесь мы рассматриваем только положительные значения смещения, а наличие и отрицательных значений учитывается введением множителя двойки. В таблице 2 представлены результаты расчетов суммы в левой части выражения (8), выполненные для различных сочетаний параметров $n$ и $k^*$.

**Таблица 2**

Оценка "Хвостов" распределений

| $n$ | $2k^*$ | $\sum_{k=k^*+1}^{2^{n-2}}\Pr\left(\lambda^*(\alpha,\beta)=2k\right)$ | $\left(2^{n-1}-1\right)^2\sum_{k=k^*+1}^{2^{n-2}}\Pr\left(\lambda^*(\alpha,\beta)\right)$ |
|---|---|---|---|
| 4 | 8 | 0,00007 | 0,016 |
| 6 | 16 | $1{,}66\cdot 10^{-6}$ | 0,0065 |
| 8 | 34 | 0,0000168 | 1,09 |
| 10 | 72 | $4{,}4\cdot 10^{-6}$ | 4,6 |
| 12 | 156 | $6{,}299\cdot 10^{-7}$ | 11,065 |
| 14 | 336 | $8{,}24\cdot 10^{-8}$ | 8,69 |

И в этом случае, как и в предыдущей нашей работе [19], мы экспериментально установили, что отмеченные выше результаты характерны не только для случайных подстановок, но и для многоцикловых шифрующих преобразований, свойственных блочным симметричным шифрам во блочным симметричным шифрам вообще. Наши эксперименты показывают, что шифрующее преобразование (любой современный шифр) асимптотически (для Rijndael подобных шифров уже после 4-х циклов) для различных ключей зашифрования ведет себя как случайная подстановка, т.е. и для них оказываются справедливыми расчетные соотношения, представленные в этой работе, относящиеся теперь к линейным аппроксимациям. Для иллюстрации этого факта в табл. 3 представлены результаты определения значений числа "переходов" $\lambda^*(\alpha,\beta)$ таблицы $LAT_\pi^*(\alpha,\beta)$ линейного корпуса (таблицы $LAT_\pi^*$ для 4-х циклового шифрующего 16-битного преобразования) уменьшенной модели шифра Лабиринт (одного из шифров, представленных на Украинский конкурс по выбору нового стандарта блочного симметричного преобразования). Аналогичные результаты получаются и для уменьшенных моделей других шифров: Baby Rijendael, Baby ADE и др.

Luka O'Connor и в работе [21] применяет свои результаты только к шифрам, использующим случайные подстановки, и как во многих известных работах, посвященных оценке стойкости БСШ к атакам линейного криптоанализа,

**Таблица 3**

| Отклонение | 0 | 2 | 100 | 200 | 300 | 400 | 500 | 600 | 720 |
|---|---|---|---|---|---|---|---|---|---|
| Количество | 81839 | 163317 | 120328 | 48060 | 10378 | 1232 | 82 | 1 | 1 |

показатели стойкости шифров он связывает с линейными свойствами подстановочных преобразований, использованных при их построении. Как мы уже отмечали в предыдущей нашей работе [19], полученные нами с использованием уменьшенных моделей шифров Rijndael, Камелия, а также шифров Мухомор, Лабиринт, Калина и ADE, представленных на Украинский конкурс по выбору национального стандарта блочного симметричного шифрования, а также ряда других шифров, экспериментальные результаты свидетельствуют о том, что реальные асимптотические (при полных наборах цикловых преобразований) значения максимальных и средних вероятностей дифференциальных и линейных характеристик (полных дифференциалов и линейных корпусов) для этих шифров являются свойством, не зависящим ни от свойств S-блоков, ни от числа циклов (после определенного их числа), ни от способа введения в цикловые функции подключей [22]. Они определяются, как уже было отмечено выше, свойствами шифрующего преобразования именно как случайной подстановки, несмотря даже на то, что БСШ реализует существенно меньшую часть всего множества подстановок соответствующего порядка.

## ЗАКЛЮЧЕНИЕ

Перейдем теперь к выводам в отношении формирования оценок показателей стойкости БСШ к атакам линейного криптоанализа.

Представляется, что и в этом случае (как и в работе [19]) в качестве показателя эффективности, позволяющего сравнивать между собой различные решения по построению БСШ, можно использовать число циклов шифрования, после которого достигается асимптотическое значение максимума таблицы линейных аппроксимаций шифра.

Для определения этого асимптотического значения предлагается рассматривать наряду с приведенными выше расчетными соотношениями, воспользоваться которыми для больших шифров по-видимому не удастся, более простое соотношение, возникшее в процессе изучения результатов вычислительных экспериментов в виде

$$\lambda(\pi)=\left(\frac{3}{2}\right)^n.$$

Остается привести расчетное соотношение для определения максимума линейной вероятности.

Напомним, что в обозначениях работы [17] максимальная линейная вероятность $DL^f_{\max}$ для ключезависимой функции $f$ с $n$-битным входом $x$ и $n$-битным выходом $y$ ( $(x, y \in GF(2)^n)$ есть

$$DL^f_{\max} = \max_{Ax, AY \neq 0} DL^f(Ay \to Ax),$$

где

$$DL^f(\ y \to\ x) =$$

$$= \left( \frac{\#\{x \in GF(2)^n / x \cdot Ax = f(x) \cdot Ay\}}{2^{n-1}} - 1 \right)^2.$$

Связь записанных соотношений с приведенными в работе очевидна

$$DL^f_{\max} = \left( \frac{\lambda(\pi)}{2^{n-1}} \right)^2.$$

В заключение остается еще раз напомнить, что линейные свойства шифрующих преобразований современных блочных симметричных шифров (при заявленном числе циклов преобразования) являются одним из проявлений свойств случайных подстановок, и в этом смысле шифр Rijendael и шифры, представленные на Украинский конкурс, являются эквивалентными. Все они реализуют наибольшую вероятность максимума линейного корпуса (для 128 битных версий) близкую к значению

$$\left( \frac{\left(\frac{3}{2}\right)^{128}}{2^{127}} \right)^2 = 2^{-104}.$$

**Литература.**


[1] *C.M. Adams.* A formal and practical design procedure for Substitution-Permutation network cryptosystem. PhD thesis, Department of Electrical Engineering, Queen's University at Kingston, 1990.

[2] *C. M. Adams. And S.E. Tavares.* The Structured design of cryptographically good S-boxes. Journal of Cryptology, 3 (1): 27-41, 1990.

[3] *R. Forré.* Methods and instruments for designing S-boxes. Journal of Cryptology, 2(3): 115-130,1990.

[4] *K. Nyberg.* Perfect nonlinear S-boxes. In Advances in cryptology - EUROCRYPT91, volume 547, Lecture Notes in Computer Science, pp. 378-386. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[5] *E.F. Brickell, J.H. Moore, and M.R. Purtill.* Structure in the S-boxes DES. Advances in cryptology, CRYPTOZb, Lecture Notes in Computer Science, vol. 263.A.M. Odlyzko ed., Springer-Verlag, pages 3-8, 1987.

[6] *M.H. Dawson.* A unified framework for substitution box design based on information theory. Vaster's thesis, Queen's University, Kingston, Ontario, Canada, 1991.

[7] *E. Biham, A. Shamir.* Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, Vol. 4 No.l, 1991, pp. 3-72.

[8] *Matsui, M.:* Linear cryptanalysis method for DES cipher. In Advances in Cryptology.- EUROCRYPT'93 (1994) vol. 765. Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 386-397.

[9] *K. Nyberg and L.R. Knudsen*. Provable security against differential cryptanalysis. In Advances in cryptology - EUROCRYPT'92, volume Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, 1992, pp. 566-574.

[10] *T. Beth and C. Ding*. On permutations against differential cryptanalysis. In Advances in cryptology - EUROCRYPT'93. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[11] *K. Nyberg*. Differentially uniform mappings for cryptography. In Advances in cryptology - Proceedings of EUROCRYPT'93 (1994) vol. 765, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York, pp. 55-65.

[12] *Seberry J., Zhang X.M., Zheng Y.* "Pitfalls in Designing Boxes (Extended Abstract)"//, Copyright © Springer-Verlag, 1998, pp. 383-396.

[13] *Seberry J., Zhang X.M., Zheng Y.:* Relationships among nonlinearity criteria. Presented at EUROCRYPTV4, 1994.

[14] *Zhang X.M, Zheng Y, Imai. H.:* Non-existence of Certain Quadratic S-boxes and Two Bounds on Nonlinear Characteristics of General S-boxes // October 1997, pp. 1-18.

[15] *K. Nyberg*. On the construction of highly nonlinear permutations. In Advances in cryptology - Proceedings of EUROCRYPT'92 (1993) vol. 740, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 92-98.

[16] *Seberry J., Zhang X.M., Zheng Y.* Improving the strict avalanche characteristics of cryptographic functions. Information Processing Letttrs, 50:37-41, 1994.

[17] *F. Sano, K. Ohkuma, H. Chimisu, and S. Rawamura*. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis, IEISE Trans. Fundamentals, VOL. E86-A, No.1, pp. 37–46, Janiary 2003.

[18] *Алексийчук А.Н., Ковальчук Л.В., Скрыпник Е.В., Шевцов А.С.* Оценки практической стойкости блочного шифра "Калина" относительно методов разностного, линейного криптоанализа и относительно алгебраических атак, основанных на гомоморфизмах // Прикладная радиоэлектроника: научн.-техн. журнал. – 2008, Т. 7, № 3. – С. 203–209.

[19] *Олейников Р.В., Олешко О.И., Лисицкий К.Е., Тевяшев А.Д.* Дифференциальные свойства случайных подстановок. // Прикладная радиоэлектроника: научн.-техн. журнал. – 2010. – Т.9. – № 3. – С. 326–333.

[20] *Luke O'Connor*. Properties of Linear Approximation Tables. Email: oconnor@dsts. Edu. au, 1995.

[21] *Luke O'Connor*. On Linear Approximation Tables and Ciphers secure against Linear Cryptanalysis. Email: oconnor@dsts. Edu. au, 1995. (семь страниц).

[21] *Бронщтейн И.Н., Семендяев К.А.* Справочник по математике для инженеров и учащихся вузов. – М.: "Наука", 1980. – 197 с.

[22] *Долгов В. И., Лисицкая И. В., Олешко О. И., Золочевская А. Ю., Дроботько Е. В.* К вопросу оценки стойкости БСШ к атакам линейного и дифференциального криптоанализа. Сборник трудов Первой Международной научно-технической конференции "Компьютерные науки и технологии", 8-10 октября 2009 г., Белгород, Ч. II. – С. 35-39.

Поступила в редколлегию 25.06.2010.

**Долгов Виктор Иванович,** доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: математические методы защиты информации.

**Лисицкая Ирина Викторовна,** кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, теория сложности.

**Олешко Олег Иванович,** старший преподаватель кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.

---

УДК 621. 391:519.2:519.7

**Властивості таблиць лінійних апроксимацій випадкових підстановок** / В.І. Долгов, І.В. Лисицька, О.І. Олешко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 334-340.

Виводяться розрахункові співвідношення для середнього значення максимумів таблиць лінійних апроксімацій випадкових підстановок. Показується, що лінійні властивості шифруючих перетворень сучасних блокових симетричних шифрів (при заявленому числі циклів перетворення) є одним із проявів властивостей випадкових підстановок. Пропонується підхід до порівняння ефективності рішень з побудови алгоритмів шифрування у вигляді мінімального числа циклів алгоритму, при якому реалізується асимптотичний показник середнього значення максимуму лінійного корпусу.

Ключові слова: лінійні апроксимації, випадкові підстановки.

Табл. 03. Бібліогр.: 22 найм.

UDC 621. 391:519.2:519.7

**Properties of tables of linear approximations of random substitutions** / V.I. Dolgov, I.V. Lisitskaya, O.I. Oleshko // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 334-340.

Computational relations for the average maximum value of tables of linear approximations of random substitutions are derived. It is shown that the linear properties of encryption transformations of modern block symmetric ciphers (with the declared number of transformation cycles) are one of the manifestations of properties of random substitutions. The paper suggests an approach to comparing the efficiency of solutions on construction of encryption algorithms in the form of a minimum number of cycles of an algorithm, which implements an asymptotic index of the average maximum value of a linear hull.

*Key words:* linear approximation, random substitutions.

Tab. 03. Ref.: 22 items.