**УДК 621. 3.06**

*И.В. ЛИСИЦКАЯ, д-р техн. наук*

# ВЫРОЖДЕННЫЕ ПОДСТАНОВКИ

## Введение

Одним из основных положений, развиваемых в новой методологии оценки показателей стойкости блочных симметричных шифров (БСШ) к атакам дифференциального и линейного криптоанализа, является положение, состоящее в том, что все БСШ после определенного индивидуального для каждого БСШ числа циклов приходят по дифференциальным и линейным показателям к свойствам случайных подстановок соответствующей степени. В концентрированном виде эти идеи выражены в работе [1] следующим образом.

*Все современные блочные симметричные шифры через определенное число циклов независимо от используемых в шифрах S блоков (здесь идет речь не о вырожденных их конструкциях) приходят к свойствам случайных подстановок, то есть по комбинаторным показателям (числу инверсий, циклов и возрастаний), а также по законам распределения переходов XOR таблиц (таблиц полных дифференциалов) и законам распределения смещений таблиц линейных аппроксимаций (линейных корпусов) повторяют соответствующие показатели случайных подстановок. Вследствие этого значения максимумов полных дифференциалов и линейных корпусов могут быть получены расчетным путем из формул для законов распределения вероятностей переходов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок.*

*При этом проверка показателей случайности больших шифров может быть выполнена на основе разработки и последующего анализа показателей случайности уменьшенных моделей, которые допускают проведение вычислительных экспериментов в реальные временные сроки.*

В качестве возражений выдвинутому положению существует мнение о том, что это всё частные результаты, и можно без труда найти подстановки, которые не укладываются в его рамки.

Проведенные многочисленные эксперименты свидетельствуют, однако, о том, что сформулированное положение выполняется практически для всех известных шифров, а подстановки, его не подтверждающие, – это ограниченное множество по сравнению с общим числом возможных подстановок, существенно не влияющее на достоверность сформулированного утверждения.

Из сказанного следует, что предлагаемая методология работает для произвольных S-блоковых конструкций, исключая вырожденные подстановки. Возникает вопрос, а какие же S-блоки считать вырожденными ?

Одним из простых ответов на этот вопрос может стать следующее: вырожденными S-блоками следует считать те, которые либо не позволяют шифру в пределах ограниченного числа циклов, однозначно определенного для каждого шифра, достичь показателей случайной подстановки, либо стационарное значение, к которому приходит шифр, не соответствует ожидаемому, свойственному случайной подстановке.

Эта работа посвящена изучению представителей множества вырожденных подстановок, а также оценке мощности этого множества, что позволит удостовериться в выполнении сформулированного положения с весьма высоким уровнем доверия.

## Примеры вырожденных подстановок

Здесь представляются результаты экспериментов с малыми (16-битными) моделями шифров. Подтверждение адекватности малых моделей своим большим прототипам можно найти в [2, 3 и др.]. Соответственно разговор будет идти о полубайтовых S-блоках, изученных наиболее всесторонне [4, 5 и др.].

Эксперименты показывают, что к вырожденным подстановкам следует отнести, прежде всего, подстановки с показателями нелинейности, равными или близкими к нулю (максимальное значение смещения таблиц ЛАТ равно $2^{n-1}$). В табл. 1 и 2 представлено поцикловое поведение полных дифференциалов 16-битного шифра Хеуса из работы [6] (шифра со слабым линейным преобразованием).

Таблица 1

| Подстановка | | Значения максимумов ТР в зависимости от числа циклов | | | | | |
|---|---|---|---|---|---|---|---|
| Тождественная подстановка | | Число циклов | | | | | |
| 1 | 1,2,3,4,5,6,7,8,9,1A,B,C,D,E,F ЛАТ – 8, ДТ – 16 (15) | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 57617,07 | 50364,40 | 45675,60 | 40971,40 | 37338,80 | 39267,00 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 41487,80 | 43386,53 | 44803,13 | 46411,40 | 47075,40 | 47872,93 |
| Подстановка 14 из работы [] | | Число циклов | | | | | |
| 2 | 5,A,C,6,0,F,3,9,8,D,B,1,7,2,E,4 ЛАТ – 8, ДТ – 8 (12) | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 32768 | 16384 | 5043,20 | 1327,87 | 369,60 | 151,07 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 61,53 | 32,60 | 24,20 | 23,87 | 23,93 | 24,13 |
| Подстановка 1 из работы [22] | | Число циклов | | | | | |
| 3 | C,D,5,1,A,B,6,2,E,3,7,F,4,0,8,9 ЛАТ – 8, ДТ – 12 (3) | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 49152,00 | 27648,00 | 15552,00 | 3616,00 | 1016,00 | 451,27 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 209,27 | 106,60 | 53,07 | 27,53 | 20,07 | 19,07 |

В качестве первого примера взята тождественная подстановка (единичная подстановка симметрической группы). Результаты её применения для построения процедуры зашифрования (шифра) приведены в верхней части табл. 1 (первый пример). Этот пример свидетельствует, что без применения подстановочной нелинейной операции шифр (любой) просто разваливается (он далёк от случайной подстановки).

Второй и третий примеры подстановок взяты из работ [5, 7]. Они свидетельствуют, что действительно существуют и нетождественные подстановки со значением показателя максимума смещения линейной аппроксимационной таблицы (ЛАТ), равным 8 (максимально возможным значением для полубайтовой подстановки), которые также не позволяют реализовать эффективную процедуру зашифрования. Заметим, что вторая подстановка приходит к асимптотическому значению максимума таблицы дифференциалов (ТД) равному 24, отличающемуся от теоретического значения максимума дифференциала для случайной подстановки (18 – 20).

В табл. 2 представлены результаты поцикловой оценки максимумов смещений таблиц линейных аппроксимаций (линейных оболочек) шифра Хеуса с этими же подстановками. И в этом случае результаты свидетельствуют о практической непригодности рассмотренных первых двух подстановок для построения шифрующих преобразований. Последняя подстановка приходит после семи циклов к показателям случайной подстановки, однако для достижения необходимых дифференциальных свойств (см. табл. 1) ей требуется более 11 циклов зашифрования. В то же время здесь можно сослаться на результаты работ [7, 8 и др.], из которых следует, что случайно взятые подстановки с большой вероятностью приводят к эффективному шифрующему преобразованию (число циклов, необходимое для перехода к случайной подстановке для шифра Хеуса, не превышает шести).

Таблица 2

| Подстановка | | Значения максимумов ЛАТ в зависимости от числа циклов | | | | | |
|---|---|---|---|---|---|---|---|
| Тождественная подстановка | | Число циклов | | | | | |
| 1 | 0,1,2,3,4,5,6,7,8,9,1A,B,C,D,E,F ЛАТ – 8, ДТ – 16 (15) | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 32768 | 32768 | 32768 | 32768 | 32768 | 32768 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 32768 | 32768 | 32768 | 32768 | 32768 | 32768 |
| Подстановка 14 из работы [5] | | Число циклов | | | | | |
| 2 | 5,A,C,6,0,F,3,9,8,D,B,1,7,2,E,4 | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 32768 | 32768 | 32768 | 32768 | 32768 | 32768 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 32768 | 32768 | 32768 | 32768 | 32768 | 32768 |
| Подстановка 1 из работы [8] | | Число циклов | | | | | |
| 3 | C,D,5,1,A,B,6,2,E,3,7,F,4,0,8,9 | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 32768 | 24576 | 12288 | 5244 | 2044 | 1080 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 792 | 872 | 826 | 816 | 842 | 816 |

Таблица 3

| Подстановка | | Значения максимумов ТР в зависимости от числа циклов | | | | | |
|---|---|---|---|---|---|---|---|
| Тождественная подстановка | | Число циклов | | | | | |
| 1 | 1,2,3,4,5,6,7,8,9,1A,B,C,D,E,F ЛАТ – 8, ДТ – 16 (15) | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 57617,07 | 50364,40 | 45675,60 | 40971,40 | 37338,80 | 39267,00 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 41487,80 | 43386,53 | 44803,13 | 46411,40 | 47075,40 | 47872,93 |
| Подстановка 14 из табл. 2 | | Число циклов | | | | | |
| 2 | 5,A,C,6,0,F,3,9,8,D,B,1,7,2,E,4 ЛАТ – 8, ДТ – 8 (12) | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 32768 | 16384 | 5043,20 | 1327,87 | 369,60 | 151,07 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 61,53 | 32,60 | 24,20 | 23,87 | 23,93 | 24,13 |
| Подстановка 1 из работы [22] | | Число циклов | | | | | |
| 3 | C,D,5,1,A,B,6,2,E,3,7,F,4,0,8,9 ЛАТ – 8, ДТ – 12 (3) | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 49152,00 | 27648,00 | 15552,00 | 3616,00 | 1016,00 | 451,27 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 209,27 | 106,60 | 53,07 | 27,53 | 20,07 | 19,07 |

В табл. 3 приведены поцикловые распределения максимумов числа переходов XOR таблиц для шифров с сильным линейным преобразованием. Они реализуются с помощью уменьшенной (16-битной) конструкции шифра baby-Rijndael, в котором используются те же S-блоки, что и в предыдущих экспериментах. Первая вырожденная подстановка (тождественная) конечно и в этом случае приводит к развалу процедуры шифрования. В то же время другие две подстановки (по крайней мере, последняя на 11-ти циклах выходит к свойствам случайной подстановки). В то же время по линейным свойствам (см. табл. 4) вторая подстановка повторяет показатели, продемонстрированные шифром Хеуса (см. табл. 3). Она явно не подходит для построения шифра.

Далее было изучено влияние на качество шифрующего преобразования и дифференциальных свойств S-блоков. В табл. 5 приведены примеры подстановок с предельными (по максимуму) дифференциальными показателями. По результатам табл. 5 можно сделать

вывод, что плохими могут быть подстановки и со значением максимумов дифференциальных таблиц превышающих 8-10 (они, как правило, свойственны подстановкам с максимальными значениями смещения ЛАТ).

Вырожденными могут быть подстановки и с немаксимальными значениями дифференциальных и линейных показателей. Пример такой подстановки представлен в табл. 6.

Таблица 4

| Подстановки | | Значения максимумов ЛАТ в зависимости от числа циклов | | | | | |
|---|---|---|---|---|---|---|---|
| Тождественная подстановка | | Число циклов | | | | | |
| 1 | 1,2,3,4,5,6,7,8,9,1A,B,C,D,E,F | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 32768 | 32768 | 32768 | 32768 | 32768 | 32768 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 32768 | 32768 | 32768 | 32768 | 32768 | 32768 |
| Подстановка 14 из табл. 2 | | Число циклов | | | | | |
| 2 | 5,A,C,6,0,F,3,9,8,D,B,1,7,2,E,4 | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 32768 | 32768 | 32768 | 32768 | 32768 | 32768 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 32768 | 32768 | 32768 | 32768 | 32768 | 32768 |
| Подстановка 1 из работы [22] | | Число циклов | | | | | |
| 3 | C,D,5,1,A,B,6,2,E,3,7,F,4,0,8,9 ЛАТ – 8, ДТ – 12 (3) | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 32768 | 24576 | 12288 | 5244 | 2044 | 1080 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 792 | 872 | 826 | 816 | 842 | 816 |

Таблица 5

| Подстановка с тремя переходами с вероятностью 1 | | Число циклов | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | F,D,9,B,1,3,2,0,4,6,7,5,A,8,C,E ЛАТ – 8, ДТ – 16 (3) | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 58112,00 | 16827,00 | 8192,00 | 8192,27 | 8192,47 | 8193,93 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 8195,87 | 8195,47 | 8197,47 | 8198,20 | 8198,47 | 8200,87 |
| Подстановка с одним переходом с вероятностью 1 | | Число циклов | | | | | |
| 5 | 6,4,1,3,0,2,7,5,E,C,D,F,8,A,9,B ЛАТ – 8, ДТ – 16 (1) | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 57617,07 | 10290,13 | 8192,00 | 8193,67 | 8192,47 | 8196,93 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 8198,67 | 8199,27 | 8200,27 | 8202,93 | 8204,13 | 8207,27 |

Таблица 6

| Подстановка | | Число циклов | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | C,9,4,6,8,E,D,5,3,F,B,0,A,2,1,7 ЛАТ – 6, ДТ – 8 (5) | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 32768,00 | 1536,00 | 139,07 | 23,53 | 24,20 | 23,73 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 23,80 | 24,07 | 23,80 | 23,93 | 24,00 | 23,80 |

В этом случае шифр пришёл к другому стационарному значению равному 24. Это второй пример подстановки с таким свойством (см. табл. 1). Заметим, что при другой конструкции линейного преобразования (линейным преобразованием MixColumn и ShiftRows $GF(2^8)$) шифр приходит к асимптотическому значению, соответствующему случайной подстановке. Нам пока не удалось объяснить этот эффект. Табл.7 демонстрирует линейные показатели шифра baby-Rijndael с этим же S-блоком (S-блоками).

Таблица 7

| Подстановка | | Значения максимумов ЛАТ в зависимости от числа циклов | | | | | |
|---|---|---|---|---|---|---|---|
| | | Число циклов | | | | | |
| 6 | C,9,4,6,8,E,D,5,3,F,B,0,A,2,1,7<br>ЛАТ – 6, ДТ – 8 (5) | 1 | 2 | 3 | 4 | 5 | 6 |
| | | 32768,00 | 32768,00 | 32768,00 | 32768,00 | 32768,00 | 32768,00 |
| | | Число циклов | | | | | |
| | | 7 | 8 | 9 | 10 | 11 | 12 |
| | | 32768,00 | 32768,00 | 32768,00 | 32768,00 | 32768,00 | 32768,00 |

Результат говорит о том, что этот S-блок нельзя применять для построения шифра.

**Оценка доли вырожденных подстановок среди подстановок симметрической группы**

Здесь покажем, что вероятность попасть на вырожденную подстановку при их случайном формировании весьма мала. Начнём с того, что вероятность получения подстановки с показателем нелинейности равным нулю, можно определить из формулы для соответствующего закона распределения вероятностей из работы [9]. В соответствии с этой работой для случайной подстановки степени $2^n$ справедлива теорема:

Теорема 1. *Пусть* $\lambda^*(\alpha,\beta)$ *будет случайным значением смещения линейной аппроксимационной таблицы* $LAT_\pi^*(\alpha,\beta)$ *для пары её входов α и β, когда подстановка π выбрана равновероятно из множества* $2^n$ *и* $\alpha,\beta$ *не нулевые. Тогда смещения* $\lambda^*(\alpha,\beta)$ *принимают только четные значения и для* $|l| \le 2^{n-2}$

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

При $l = 2^{n-2}$ (показатель нелинейности 0) из этого соотношения получаем

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

$$= \frac{\left(2^{n-1}!\right)^2}{2^n!} = \begin{pmatrix} 2^n \\ 2^{n-1} \end{pmatrix}^{-1} \approx \left(2^{2^n}\,\frac{2^{-(n-2)/2}}{\sqrt{2\pi}}\right)^{-1}.$$

Здесь использована аппроксимация биномиального коэффициента из работы [10].

Из полученного результата следует, что для вероятности получить путём случайного выбора полубайтовую подстановку ($n$ = 4) со значением максимума смещения таблицы линейных аппроксимаций равным $k = 2^3 = 8$ имеем

$$\Pr\left(\lambda(\alpha,\beta) = 2\cdot 2^3\right) = 7{,}65\cdot 10^{-5},$$

т.е. как показывают расчёты, эта вероятность меньше одной десятитысячной.

Эти расчёты сделаны для вероятности соответствующего заполнения одной ячейки таблицы, а таких ячеек в таблице (исключая нулевые маски по входу и выходу) $(2^n-1)^2$. Поэтому для вероятности получить полубайтовую подстановку со значением смещения $k = 2^3 = 8$ приходим к результату

$$7{,}65\cdot 10^{-5}\cdot(2^4-1)^2 = 0{,}0172.$$

Для генерации байтовой подстановки с таким же (нулевым) показателем нелинейности соответственно приходим к вероятности

$$\Pr\left(\lambda(\alpha,\beta) = 2\cdot 2^7\right) = 1{,}73\cdot 10^{-76}.$$

С учётом числа ячеек таблицы

$$1{,}73\cdot 10^{-76}\cdot(2^8-1)^2 = 1{,}13\cdot 10^{-71},$$

т.е. получить путём отбора такую подстановку практически невозможно.

Аналогично можно выполнить оценку вероятности порождения случайной подстановки с теоретически максимально возможным значением перехода XOR таблицы подстановки. Для этого воспользуемся теоремой из работы [11]. Она определяет вероятность события, заключающегося в том, что значение дифференциальной таблицы случайно взятой подстановки $\pi$ порядка $2^n$ для перехода входной разности $\Delta X$ в соответствующую выходную разность $\Delta Y$ будет равно $2k$. Эта вероятность в работе обозначена $\Pr(\Lambda_\pi(\Delta X, \Lambda Y) = 2k)$. Сама теорема звучит так:

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

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

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

$$\Phi(d) = \sum_{i=0}^{d}(-1)^i \cdot \binom{d}{i}^2 \cdot 2^i \cdot i!\,(2d-2i)!$$

Здесь для $k = 2^{n-1}$ получим расчётное соотношение

$$\Pr(\Lambda_\pi(\Delta X, \Lambda Y) = 2\cdot 2^{n-1}) =$$

$$= \binom{2^{n-1}}{2^{n-1}}^2 \frac{2^{n-1}!\,2^{2^{n-1}} \cdot \Phi(2^{n-1}-2^{n-1})}{2^n!}.$$

Поскольку, как отмечено в [10], $\Phi(d) \approx (2d)!\,e^{-\frac{1}{2}}$, то $\Phi(2^{n-1}-2^{n-1}) = \Phi(0) \approx e^{-\frac{1}{2}}$, тогда:

$$\Pr\left(\Lambda(\Delta X, \Delta Y) = 2^n\right) = \frac{2^{n-1}!\,2^{2^{n-1}}}{2^n!} \cdot e^{-\frac{1}{2}} = 2{,}97\cdot 10^{-7}..$$

Для полного набора ячеек таблицы (исключая нулевой столбец и нулевую строку) имеем

$$2{,}97\cdot 10^{-7}\cdot(2^4-1)^2 = 0{,}000067,$$

т.е. вероятность получить вырожденную полубайтовую подстановку путём отбора получается менее семи десятитысячных.

Для байтовой подстановки соответственно получаем

$$\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2^8\right) = 9\cdot 10^{-254}$$

и тогда

$$9\cdot 10^{-254}\cdot(2^8-1)^2 = 5{,}85\cdot 10^{-249}.$$

В табл. 7 представлены результаты вычисления значений ″хвостов″ интегрального закона распределения для распределения вероятностей (2), т.е. считалась сумма $\sum_{k=k^*+1}^{2^{n-1}}\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k)$ как функции размера битового входа подстановки $n$ и максимального половинного значения дифференциала $k^*$.

Таблица 7

| $n$ | $k^*$ | $\sum_{k=k^*+1}^{2^{n-1}}\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k)$ |
|---|---|---|
| 4 | 3 | 0,00245 (0,55) |
| 6 | 5 | 0,000015 (0,06) |
| 8 | 6 | 0,000001 (0,065) |
| 10 | 7 | 0,00000006 (0,062) |
| 12 | 8 | 0,0000000034 (0,0057) |

Видно, что даже в ″нормированном″ варианте доля сумм ″хвостов″ оказывается незначительной (а вырожденные подстановки попадают именно в хвосты). В скобках строчек табл. 7 приведены результаты умножения ″хвостов″ на общее число ″ненулевых″ ячеек таблицы $(2^n-1)^2$.

О подстановке под номером 6. В качестве эксперимента взяли хорошую подстановку шифра baby Rijndael [12] и с помощью двух транспозиций воспроизвели в ней переходы 2→4, 3→6 и 4→8 (последний переход уже был в исходной подстановке), имеющиеся в подстановке под номером 6. Полученная в результате этого подстановка повторила по свойствам свойства подстановки под номером 6 (пришла к асимптотическому значению максимума дифференциала, равному 24), т.е. стала вырожденной. В то же время одна транспозиция в подстановке под номером 6 в цикле, не содержащем отмеченные выше переходы, сделала подстановку невырожденной. Нам не удалось найти признаков, по которым можно делить подстановки на вырожденные и невырожденные, однако нам не удалось найти невырожденных подстановок среди наиболее вероятного множества подстановок, приближающихся по линейным и дифференциальным показателям к показателям случайной подстановки, определяемой законами распределения вероятностей (1) и (2).

Представленные примеры вырожденных подстановок ярко свидетельствуют, что S-блоки в шифрах играют важную роль. Существуют подстановки (вырожденного типа), с которыми построить хорошее криптографическое преобразование нельзя. С другой стороны, подстановки являются одним из важных элементов шифрующего преобразования. Они реализуют один из важных для шифра механизмов – механизм нелинейного перемешивания (перестановки) битов блоков данных, с помощью которого удаётся наиболее просто добиться эффекта хаотичности в преобразовании битов.

**Выводы**

К вырожденным S-блокам мы отнесли подстановочные конструкции с дифференциальными и линейными показателями (максимумами XOR таблиц и смещений таблиц линейных аппроксимаций) близкими к предельно возможным.

Результатами работы подтверждено, что получение вырожденных S-блоков при случайном порождении подстановок является маловероятным событием. Особенно это относится к байтовым S-блокам. Для этих S-блоков получение подстановок с максимумами XOR таблиц и смещений таблиц линейных аппроксимаций, близкими к предельно достижимым, является практически невозможным событием. Реальные наиболее вероятные значения максимумов, которые удаётся получить в экспериментах (34 для ЛАТ и 10-12 для ТР) оказываются далёкими от значений $2^{8-1}=128$ (для ЛАТ) и $2^8=256$ (для ТР). При этом с увеличением значений максимумов линейных и дифференциальных показателей вероятности отбора подстановок с такими значениями очень быстро уменьшаются. Таким образом, доля вырожденных подстановок в общем множестве подстановок симметрической группы оказывается незначительной.

Это значит, что положение, сформулированное в начале работы, состоящее в том, что все шифры независимо от используемых в них S-блоков после небольшого начального числа циклов шифрования становятся случайными подстановками, выполняется с высоким уровнем доверия. Порождение вырожденных S-блоков является маловероятным событием, и самое главное – они всегда могут быть обнаружены и исключены на основе результатов экспериментов.

**Список литературы:** 1. *Лисицкая, И.В.* Методология оценки стойкости блочных симметричных шифров / И.В. Лисицкая // Автоматизированные системы управления и приборы автоматики. – 2011. – № 163. – С. 123-133. 2. *Лисицкая, И.В.* Большие шифры – случайные подстановки / И.В. Лисицкая, А.А. Настенко // Радиотехника. – 2011. – Вып. 166. – С. 50-55.6. 3. *Лисицкая, И.В.* Дифференциальные свойства шифра FOX / И.В. Лисицкая, Д. С. Кайдалов // Прикладная радиоэлектроника. – 2011. – Т.10, №2. – С. 122-126. 4. *Markku-Juhani O. Saarinen* Cryptographic Analysis of All 4×4-Bit S-Boxes // IACR Cryptology ePrint Archive Vol. 2011 (2011), p. 218. 5. *Токарева, Н. Н.* Квадратичные аппроксимации специального вида для четырёхразрядных подстановок в S-блока // Прикладная дискретная математика. – 2008. – Т. 1, N 1. – С. 50-54. 6. *H. M. Heys.* A Tutorial on Linear and Differential Cryptanalysis, CRYPTOLOGIA, v 26, N 3, 2002, p 189-221. 7. *Лисицкая, И.В.* Об участии S-блоков в формировании максимальных значений линейных вероятностей блочных симметричных шифров / И.В. Лисицкая, В.В. Ковтун // Радиотехника. – 2011. – Вып. 166. – С. 17-25. 8. *Лисицкая, И.В.* Об участии S-блоков в формировании максимальных значений дифференциальных вероятностей блочных симметричных шифров / Лисицкая И.В., Казимиров А.В. // Proceedings International Conference SAIT 2011, Kyiv, Ukraine, May 23-28. – 2011. – С. 459. 9. *Долгов, В.И.* Свойства таблиц линейных аппроксимаций случайных подстановок / В.И. Долгов, И.В. Лисицкая, О.И. Олешко // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 334-340. 10. *Joan Daemen.* Probability distributions of Correlation and Differentials in Block Ciphers / Joan Daemen, Vincent Rijmen // April 13, 2006, pp. 1–38. 11. *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. 12. *Долгов, В.И.* Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров / В.И. Долгов, А.А. Кузнецов и др. // Прикладная радиоэлектроника. – 2009. – Т. 8, № 3. – С. 268-277.

*Харьковский национальный*
*университет радиоэлектроники*

*Поступила в редколлегию 17.09.2012*