УДК 621. 391:519.2:519.7

ДИФФЕРЕНЦИАЛЬНЫЕ СВОЙСТВА ПОДСТАНОВОК

Р.В. ОЛЕЙНИКОВ, О.И. ОЛЕШКО, К.Е. ЛИСИЦКИЙ, А.Д. ТЕВЯШЕВ

Выводятся расчетные соотношения для определения среднего значения максимумов XOR таблиц случайных подстановок. Показывается, что дифференциальные свойства 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 полных дифференциалов.

Ключевые слова: симметричный блочный шифр, дифференциальный криптоанализ, случайная перестановка.

ВВЕДЕНИЕ

В наших предыдущих работах [1, 2] мы представляли результаты вычислительных экспериментов по исследованию дифференциальных свойств случайных таблиц подстановок. В частности, было установлено, что среднее значение максимумов таблиц XOR разностей является специфическим показателем S-блоков фиксированного порядка, не зависящим от циклового класса, к которому принадлежат подстановки.

Дальнейшие исследования [3, 4] показали, что это свойство является характерным и для шифрующих преобразований, выполняемых современными блочными симметричными шифрами, в то время как многие из подходов к оценке дифференциальных свойств шифров строятся на основе изучения свойств входящих в шифр подстановочных преобразований (S-блоков), а не шифров в целом как подстановок.

Учитывая жесткую связь дифференциальных свойств шифрующих преобразований с показателями их стойкости к атакам дифференциального криптоанализа, возникает желание более глубокого изучения накопленных фактов и осмысления имеющихся результатов.

В этой работе ставится задача теоретического обоснования полученных экспериментально дифференциальных показателей случайных подстановок, в качестве которых рассматриваются и блочные симметричные шифры.

Напомним, что в процессе экспериментов мы интересовались средним значением максимумов таблиц XOR разностей подстановок. Соответствующий показатель теперь необходимо определить расчетным путем.

1. ВЫВОД РАСЧЕТНЫХ СООТНОШЕНИЙ

Отметим сразу, что решение близкой по постановке задачи нам удалось найти в работе Luka O'Connor-a [5] 1994-го года. Однако манера представления материала Luka O'Connor-ом, особенно в части выполнения доказательств и интерпретации конечных результатов, нас не удовлетворила и сделала целесообразной изложение собственной позиции по этому вопросу.

Следуя работе [5], положим, что $\pi: Z_2^m \to Z_2^m$ является биективным m-битным отображением и пусть S_{2^m} будет множеством всех таких отображений, известное в математической литературе как симметрическая группа. Пусть $\Lambda_\pi(\Delta X, \Delta Y)$ будет значением XOR таблицы (её ячейки) для пары значений разностей входов и выходов ΔX, $\Delta Y \in Z_2^m$, $\Delta X = X + X'$, $\Delta Y = \pi(X) + \pi(X')$ подстановки $\pi \in S_{2^m}$.

Напомним, что XOR таблица представляет собой $2^m \times 2^m$ матрицу, у которой $XOR_\pi(i,j) = \Lambda_\pi(i,j)$, $0 \le i, j \le 2^{m-1}$.

Для m-битной подстановки π XOR таблица имеет следующую общую форму

$$XOR_\pi = \begin{vmatrix} 2^m & 0 & 0 & \cdots & 0 \\ 0 & a_{1,1} & a_{1,2} & \cdots & a_{1,2^{m-1}} \\ 0 & a_{2,1} & a_{2,2} & \cdots & a_{2,2^{m-1}} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & a_{2^{m-1},1} & a_{2^{m-1},2} & \cdots & a_{2^{m-1},2^{m-1}} \end{vmatrix} \overset{def}{=}$$

$$\overset{def}{=} \begin{vmatrix} 2^m & 0 \\ 0 & A_\pi \end{vmatrix}.$$

Мы будем интересоваться свойствами $2^{m-1} \times 2^{m-1}$ подматрицы $A_\pi = \left| a_{i,j} \right|$, $1 \le i, j \le 2^{m-1}$, которая соответствует части XOR таблицы с входами (ячейками), приписываемыми к ненулевым характеристикам.

Рассмотрим задачу определения вероятности события, заключающегося в том, что значение дифференциальной таблицы случайно взятой подстановки π порядка 2^m для перехода входной разности ΔX в соответствующую выходную разность ΔY будет равно $2k$ (значения ячеек XOR таблицы всегда четное). Как и в [5] эту вероятность обозначим $\Pr(\Lambda_\pi(\Delta X, \Delta Y) = 2k)$.

В [5] приводится теорема 2.1, определяющая эту вероятность в виде:

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

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

где функция $\Phi(d)$ определяется выражением

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

Как уже отмечалось выше, в [5] доказательства этих результатов приведены схематично (не полностью) и трудно понимаемы, а главное они не приведены к нужному нам виду. Мы здесь предлагаем более простую и более прозрачную версию доказательства этой и других теорем с последующей своей интерпретацией получающихся результатов.

Доказательство. Заметим сначала, что при операции вычисления разностей XOR входов подстановки π они попарно переходят друг в друга ($\Delta X = X\oplus X' = X'\oplus X$). Поэтому в дифференциальной таблице число переходов входной разности ΔX в выходную разность ΔY (значение ячейки таблицы дифференциальных разностей) всегда четное, и к тому же входы (и соответствующие выходы) подстановки распределяются по парам, так что для одной и той же разности ΔX мы имеем дело с 2^{m-1}-ой парами входов. Одновременно становится понятным, что для заданного сочетания входов и выходов подстановки π каждое конкретное значение входной разности может переходить не во все возможные значения выходных разностей, и что разные пары входов с одной и той же разностью ΔX могут переходить в одну и ту же выходную разность ΔY.

Для подстановок, выбираемых равновероятно из множества S_2^m, под искомой вероятностью, очевидно, следует понимать отношение числа подстановок $\pi\in S_2^m$, обладающих желаемым свойством (реализующих необходимое число $(2k)$ раз заданный переход $\Delta X\to\Delta Y$), к общему числу подстановок симметрической группы S_2^m:

$$\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)=\frac{\#\left\{\Lambda_\pi(\Delta X,\Delta Y)=2k\right\}}{2^m!}. \quad (3)$$

Выполним подсчет числа подстановок $\#\left\{\Lambda_\pi(\Delta X,\Delta Y)=2k\right\}$ с обусловленным количеством переходов входных разностей ΔX в выходную разность ΔY. Очевидно, что в это число будут входить подстановки, отличающиеся конфигурациями (сочетаниями) входов и выходов, участвующих в реализации желаемого свойства (реализующих необходимое число $(2k)$ раз заданный переход $\Delta X\to\Delta Y$).

Поскольку k пар переходов любой подстановки, участвующих в реализации необходимого свойства $\Delta X\to\Delta Y$, и $2^{m-1}-k$ оставшихся из общего числа 2^{m-1} пар переходов со свойством $\Delta X\to\Delta Y$ (обозначение из работы Эли Бихама и Ади Шамира [6]) компонуются в произвольном сочетании (переходы каждой из этих двух групп входов и выходов подстановки формируются независимо друг от друга), то интересующее нас число включает две компоненты (два сомножителя):

– первый сомножитель определяется числом различных подстановок π, у которых k пар входов из имеющегося в подстановке 2^{m-1} числа таких пар реализуют заданный переход $\Delta X\to\Delta Y$ (независимо от остальных $2^{m-1}-k$ пар входов каждой из подстановок);

– второй сомножитель определяется дополнительным расширением множества подстановок, у которых k пар входов реализуют заданный переход $\Delta X\to\Delta Y$, за счет многообразия вариантов выбора $2^{m-1}-k$ оставшихся пар входов каждой из подстановок, которые заданного перехода не реализуют, т.е. для которых $\Delta X\to\Delta Y$.

Рассчитаем сначала число вариантов подстановок, определяющих первый сомножитель.

Начнем с того, что в соответствии с комбинаторными соображениями для фиксированного набора из k пар входов, имеющих разность ΔX, которые имеют заданную выходную разность ΔY, возможно $k!$ вариантов различных перестановок k пар выходов по заданному набору входов (подстановки нормализованного вида отличаются расстановкой пар выходных значений по парам входных).

Очередной возможностью расширения множества подстановок, которые имеют заданное число k переходов входной разности ΔX в выходную разность ΔY, является варьирование наборами входов и выходов подстановки, участвующими в формировании переходов входной разности ΔX в выходную разность ΔY. Из общего числа 2^{m-1} пар входов, имеющих разность ΔX, в формировании интересующих нас переходов участвует только k пар входов. Очевидно, что они могут быть выбраны из общего числа 2^{m-1} пар входов $C_{2^{m-1}}^k$ способами. Аналогичное положение характерно и для множества пар выходов, имеющих разность ΔY. Поскольку компоновка входных и выходных пар осуществляется независимо, то приходим к общему числу $\left(C_{2^{m-1}}^k\right)^2$ вариантов подстановок с интересующим нас свойством.

Наконец, имеется еще одна степень свободы в построении подстановок с заданным числом переходов входной разности ΔX в выходную разность ΔY. Одна и та же пара входов с разностью ΔX может реализовать два варианта переходов в выходную разность ΔY (входы подстановки, входящие в пару, можно поменять местами). Но тогда множество возможных подстановок с фиксированным переходом входной разности ΔX в выходную разность ΔY дополнительно увеличится ещё в 2^k раз.

В результате мы действительно для вероятности того, что значение дифференциальной таблицы случайно взятой подстановки π порядка 2^m с переходом входной разности ΔX в соответствующую выходную разность ΔY будет равно числу $2k$, приходим к соотношению (1), в котором роль второго сомножителя, о котором шла речь выше, играет функция $\Phi(2^{m-1}-k)$.

Остается учесть варианты расширения множества подстановок интересующего нас вида за счет второго сомножителя. В работе [5], чтобы определить второй сомножитель, выводится расчетное соотношение для функции $\Phi(d)$ в виде соотношения (2).

Для получения этого расчетного соотношения в [5] использована «Спаривающая теорема», краткое доказательство которой без разъяснений, приводит автор. Мы здесь предлагаем свой вариант вывода расчетного соотношения для функции $\Phi(d)$, являющегося по существу следствием доказанного выше соотношения (1).

Действительно, будем теперь интересоваться «хвостом» из $2^{m-1}-k$ пар входов и выходов, которые в предыдущем рассмотрении не учитывались (считались фиксированными). По оговоренному условию это пары, которые не имеют заданного перехода $\Delta X \to \Delta Y$. Множество этих пар можно рассматривать как отдельную подстановку порядка 2^m-2k. Тогда для определения числа подстановок порядка 2^m-2k, не имеющих заданного перехода $\Delta X \to \Delta Y$, очевидно можно просто из общего числа подстановок такого порядка вычесть число подстановок, имеющих заданный переход. Подстановки порядка 2^m-2k с обусловленным переходом могут содержать одну пару с таким переходом, две пары, и так до 2^m-2k пар переходов.

В результате в терминах функции $\Phi(d)$ выражение для расчета второго сомножителя можно представить в виде

$$\Phi(d)=(2d)!-\sum_{i=1}^{d} i!\cdot 2^i\binom{d}{i}^2\Phi(d-i). \qquad (4)$$

Остается показать, что представления (2) и (4) эквивалентны.

Это легко устанавливается последовательной подстановкой в (4) значений функции $\Phi(d-i)$, $i=1,2,\ldots,d$ и использованием очевидных соотношений

$$1!\cdot 2^1\cdot\binom{d}{1}^2\cdot 1!\cdot 2^1\cdot\binom{d-1}{1}^2-2!\cdot 2^1\cdot\binom{d}{2}^2=$$

$$=2!\cdot 2^2\cdot\binom{d}{2}^2$$

для коэффициента при функции $\Phi(d-2)$ после подстановки в (4) явного вида функции $\Phi(d-1)$;

$$-\left[1!\cdot 2^1\cdot\binom{d}{1}^2\cdot 1!\cdot 2^1\cdot\binom{d-1}{1}^2-2!\cdot 2^2\cdot\binom{d}{2}^2\right]\times$$

$$\times\left[1!\cdot 2^1\cdot\binom{d-2}{1}^2\right]+$$

$$+\left[1!\cdot 2^1\cdot\binom{d}{1}^2\cdot 2!\cdot 2^2\cdot\binom{d-1}{2}^2-3!\cdot 2^3\cdot\binom{d}{3}^2\right]=$$

$$=-3!\cdot 2^3\cdot\binom{d}{3}^2$$

для коэффициента при функции $\Phi(d-3)$ после подстановки в (4) явного вида функции $\Phi(d-2)$ и так до свертывания коэффициентов при всех последующих функциях $\Phi(d-i)$, $i=4,5,\ldots,d$. В результате приходим к выражению (2). Утверждение доказано.

Далее, как и в [5] обозначим ожидаемое число ненулевых характеристик ΔX, ΔY, для которых $\Lambda_\pi(\Delta X,\Delta Y)=2k$ как $\Lambda_{m,2k}$.

При выводе выражения (1) мы не фиксировали значений пары разностей $\Delta X, \Delta Y \in Z_2^m$, для которых оно получено. Это значит, что соотношение (1) справедливо для произвольных сочетаний разностей на входе и выходе подстановок. Мы уже отмечали ранее, что результаты, полученные для ансамбля подстановок, считаются справедливыми и для отдельной подстановки π, т.е. полученные формулы можно трактовать как закон распределения ненулевых характеристик для каждой подстановки.

Выражение (1) определяет вероятность того, что в XOR таблице случайно взятой подстановке число переходов входной разности $\Delta X \in Z_2^m$ в выходную разность $\Delta Y \in Z_2^m$ будет равно $2k$.

Но тогда становится понятным, что выражение для числа $\Lambda_{m,2k}$ переходов таблицы дифференциальных разностей подстановки порядка 2^m обусловленного типа, – а именно для среднего значения числа ненулевых характеристик $\Delta X \to \Delta Y$, таких, что $\Lambda_\pi(\Delta X,\Delta Y)=2k$, – может быть получено путем умножения выражения (1) на число ячеек подматрицы $A_\pi=\left|a_{i,j}\right|$ таблицы XOR_π равное $(2^m-1)^2$:

$$\Lambda_{m,2k}=\frac{(2^m-1)^2}{2^m!}\cdot\binom{2^{m-1}}{k}^2\cdot k!\cdot 2^k\cdot\Phi(2^{m-1}-k). \qquad (6)$$

Это выражение и есть то, которое нам нужно.

2. СРАВНЕНИЕ РАСЧЕТНЫХ И ЭКСПЕРИМЕНТАЛЬНЫХ РЕЗУЛЬТАТОВ

Нас теперь будет интересовать среднее значение максимума таблицы XOR разностей. Оно находится из соотношения (6) просто путем определения максимального значения k, при котором результат расчетов по этому выражению при-

водит к наименьшему целому значению. Другими словами, нам нужно найти решение уравнения

$$\frac{(2^m-1)^2}{2^m!}\cdot\left(\begin{array}{c}2^{m-1}\\ k\end{array}\right)^2\cdot k!\cdot 2^k\cdot\Phi(2^{m-1}-k)\approx 1. \qquad (7)$$

Это решение можно искать переборным методом, ориентируясь при этом на экспериментальные данные.

Полезной аппроксимацией для выполнения расчетов может стать и еще один результат, также приведенный в работе [5]. Имеется в виду замечание о том, что в знакопеременной сумме в выражении (2) первый терм (при $i=0$) является доминирующим, и что

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

Остается заметить, что $e^{-\frac{1}{2}}=0{,}6065$.

Например, для $m=4$, $k=3$ получим

$$\Lambda_{4,6}=\frac{(2^4-1)^2}{2^4!}\cdot\left(\begin{array}{c}2^{4-1}\\ 3\end{array}\right)^2\cdot 3!\cdot 2^3\cdot\Phi(2^{4-1}-3).$$

С учетом того, что $\Phi(5)=2088960$ в итоге приходим к результату

$$\Lambda_{4,6}=\frac{15^2}{2^4!}56^2\cdot 3!\cdot 2^3\cdot 2088960=3{,}379.$$

Мы получили ожидаемое среднее значение максимума таблицы дифференциальных разностей для значения $m=4$ несколько большее $2k=6$, что хорошо согласуется с результатами наших экспериментов.

Для других значений m расчеты, выполненные в соответствии с соотношениями (1), (2) и (7), представлены в табл. 1.

Таблица 1

Сравнение расчетных и экспериментальных результатов

m	$\Lambda_\pi(\Delta X,\Delta Y)=2k$	$2k$	Эксперимент
4	3,379 0,459	6 8	6,7 $\le(m+3)$
5	3,08 1,708	6 8	7,94 $\le(m+3)$
6	6,6 0,675	8 10	9,1 $\le(m+4)$
7	2,641 0,221	10 12	10,3 $\le(m+4)$
8	0,8748	12	11,4
9	3,474 0,248	12 14	12,5 $\le(m+4)$
10	13,8495 0,99	12 14	13,4 $\le(m+4)$
11	3,952 0,247	14 16	14,5 $\le(m+4)$
12	15,787 0,987	14 16	15,3 $\le(m+4)$

Таблица 2 иллюстрирует результаты вычислительного эксперимента, полученные нами ра-

Таблица 2

Результаты вычислительного эксперимента

Степень подстановки / Число циклов подстановки	23 = 8	24 = 16	25 = 32	26 = 64	27 = 128	28 = 256	29 = 512	210 = 1024	211 = 2048	212 = 4096
1	4.8014	6.69454	7.94398	9.11202	10.2827	11.4222	12.0	13.75	15.3333	14.0
2	4.2591	6.71003	7.94526	9.11991	10.2921	11.3765	12.3467	13.6429	14.1538	15.0
3	4.7807	6.68965	7.94006	9.11311	10.3022	11.4241	12.3697	13.2647	14.3947	15.68
4	4.2616	6.71753	7.94177	9.11112	10.3097	11.3012	12.5144	13.4481	14.5745	15.3235
5	4.9487	6.6881	7.94223	9.10677	10.3043	11.3252	12.4528	13.4565	14.3969	15.4066
6	4.5187	6.71281	7.95425	9.11403	10.3178	11.3645	12.4948	13.3743	14.529	15.3509
7	8.0	6.72067	7.94278	9.11009	10.3157	11.3144	12.4095	13.4121	14.3967	15.37
8	8.0	6.84496	7.94878	9.11502	10.3248	11.3216	12.4316	13.4607	14.5284	15.4055
9		7.0137	7.95743	9.11899	10.3165	11.2887	12.4122	13.3596	14.5089	15.4027
10		6.91892	7.98563	9.1015	10.3071	11.3538	12.5669	13.4009	14.4336	15.4268
11		8.0	8.03191	9.15496	10.3183	11.359	12.4249	13.3284	14.4715	15.368
12			7.6	9.0	10.2954	11.3429	12.3457	13.2179	14.4822	15.3313
13			8.0	9.42222	10.2264	11.0667	12.7111	13.55	14.4785	15.2735
14				9.0	10.5882	11.0	12.7619	13.125	14.3939	15.625
15				10.0	9.33333	11.0	12.0	13.4667	14.1935	15.4333
16					10.0	12.0	12.0	13.5	14.4	15.5333
17					10.0			13.0	14.0	15.7143
18								14.0	14.05.09	15.6
19									-	16.5
Число подстановок	1000000	1000000	1000000	500000	100000	10000	5000	5000	5000	5000

нее и приведенные в работе [1] (здесь они даны в более полном объеме).

Расчеты, выполненные в соответствии с выражением (6), для 16-битной подстановки представлены также в левой колонке табл. 3. В правой колонке этой таблицы представлены соответствующие результаты для 16-битного шифра по Хейсу [7] с линейным преобразованием, подобным операции MixColumn в шифре Rijendael.

Таблица 3

Распределение парных разностей для SPN шифра с умножением на матрицу

Расчет		Эксперимент	
#2.	1302484861	#2.	1302551726
#4.	325626184	#4.	325625709
#6.	54271858	#6.	54253870
#8.	6784085	#8.	6781574
#10.	678418	#10.	677785
#12	56535	#12	56793
#14.	4038	#14.	3974
#16.	252	#16.	272
#18.	14	#18.	17
#20.	1	#20.	0

Сопоставление результатов таблиц 1 и 2, а также таблицы 3 свидетельствует о хорошем согласовании полученных ранее и следующих из теоретических рассуждений результатов.

Интересно отметить, что для закона распределения (1) с большой точностью выполняется соотношение

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

и, следовательно, справедливо равенство

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

В свою очередь легко убедиться, что

$$\frac{\left(2^{m-1}\right)^2-2^m}{(2^{m-1}-1)^2}=\frac{2^{m-1}\cdot\left(2^{m-1}-2\right)}{(2^{m-1}-1)^2}=$$

$$=\frac{1}{1-2^{-m+1}}\cdot\frac{1-2^{-m+2}}{1-2^{-m+1}}\approx 1.$$

Это означает, что для выражения (1) с большой точностью выполняется условие нормировки

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

Здесь k^* представляет собой половину от максимального значения числа переходов XOR таблицы случайной подстановки.

Таким образом, формула (1) может рассматриваться как закон распределения числа ненулевых (по входу) переходов $\Delta X\to\Delta Y$ для отдельной подстановки, т.е. набор значений переходов $\Lambda_\pi(\Delta X,\Delta Y)=2k$, $k=0,1,\ldots,k^*$ представляет практически полную группу событий. Мы фактически и воспользовались этим, выполняя вычисления по выражению (6).

В табл. 4 представлены результаты вычисления значений «хвостов» формулы (1), т.е. $\sum_{k=k^*+1}^{2^{m-1}}\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$ как функции размера битового входа подстановки m (в скобках представлены значения этих же сумм «хвостов», умноженных на число ячеек подматрицы A_π XOR таблицы). Видно, что даже в «нормированном» варианте доля сумм «хвостов» оказывается незначительной.

Таблица 4

Результаты расчетов хвостов распределений

m	k^*	$\sum_{k=k^*+1}^{2^{m-1}}\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$
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)

Этим подтверждается высказанная в начале статьи установка, что свойства отдельной случайной подстановки однозначно выражаются через свойства ансамбля случайных подстановок.

Вместе с тем, мы хотим еще раз обратить здесь внимание читателей на то, что отмеченные выше результаты характерны не только для случайных подстановок, но и для многоцикловых шифрующих преобразований, свойственных 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 него оказываются справедливыми расчетные соотношения, представленные в этой работе.

Соответствующие идеи в этом направлении высказываются и в цитируемой нами работе [5]. Однако Luka O'Connor связывает свои результаты только с шифрами, использующими случайные подстановки, и как во многих известных работах, посвященных оценке стойкости БСШ к атакам дифференциального криптоанализа, показатели стойкости шифров связываются с дифференциальными свойствами подстановочных преобразований, использованных при их построении. 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 [3]. 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. А это означает, что на основе полученных в работе соотношений действительно может строиться методика оценки стойкости шифров к атакам дифференциального криптоанализа.

Мы здесь в определенном смысле повторяем рассуждения Luka O'Connor-а, но в более корректной, как нам кажется, форме (некоторые рассуждения и соотношения раздела в [5], посвященного формированию оценок стойкости к атакам дифференциального криптоанализа, нам представляются не совсем корректными).

Luka O'Connor, поднимая вопрос о связи дифференциальных показателей случайных подстановок с устойчивостью к атакам дифференциального криптоанализа, рассматривает отображение G, базирующееся на m-битных подстановках выбранных равновероятно из S_{2^m}. Отображение G, в частности, считается состоящим из S-блоков, являющихся m-битными подстановками $\pi_1, \pi_2, \ldots, \pi_s$ такими, что $G: Z_2^{m \cdot s} \to Z_2^{m \cdot s}$, где π_1 – первый блок из s битов, π_2 операция второго блока из s битов и т.д. Далее он говорит о вероятности самой вероятной характеристики (probability of the most likely characteristic), покрывающей весь шифр, выражая ее через соответствующую вероятность одноцикловой характеристики p^{Ω}. Он считает, что для любой r-цикловой характеристики выполняется условие $p^{\Omega_r} \le \left(\frac{\Lambda_m^*}{2^{m-1}} \right)^r$, где Λ_m^* определяется соотношением

$$2^m p^{\Omega} \le \Lambda_m^* \stackrel{def}{=} \max_{\substack{\pi \in (\pi_1, \pi_2, \ldots, \pi_s) \\ \Delta X, \Delta Y \in Z_2^m \\ w(\Delta X), w(\Delta Y) > 0}} \Lambda_\pi(\Delta X, \Delta Y).$$

И если с понятием и определением самой вероятной характеристики можно согласиться, то дальнейшее рассмотрение задачи определения общей границы для значения самой вероятной характеристики нам представляется не совсем аккуратным (хотя бы из-за того, что вероятности входят в неравенства равноправно с числом ненулевых характеристик: $\Pr(\Lambda_m^* = 2k) < \Pr(\Lambda_\pi = 2k) \le \Lambda_{m,2k}$, где $\Lambda_{m,2k}$ определяется формулой (6)). Тем не менее, окончательный результат, сформированный Luka O'Connor-ом в виде Утверждения 3.1, о том, что для больших m и предположении равномерного распределения подстановок на множестве S_{2^m} ожидаемая вероятность самой правдоподобной (вероятной) ненулевой дифференциальной характеристики ограничена значением $\frac{m}{2^{m-1}}$, оказывается, как мы увидим далее, близким к истине. Однако это утверждение строится Luka O'Connor-ом на результатах, полученных эмпирическим путем, и никак не связано со свойствами шифрующих преобразований.

Наша позиция состоит в том, что результирующие дифференциальные свойства блочных симметричных шифров (по крайней мере, Rijendael-подобных шифров) не связаны со свойствами S-блоков шифра, а являются общим свойством шифра как случайной подстановки. Особенностью шифрующего преобразования в виде БСШ, рассматриваемого как подстановка, является существенно меньшее множество реализуемых им подстановок. БСШ реализует только 2^m (по числу ключей) подстановок из общего их числа $2^m!$, причем, несмотря на такое существенное уменьшение допустимого множества подстановок, оно продолжает сохранять свойства, характерные для множества случайных подстановок [3, 4, 9] (по инверсиям, возрастаниям, циклам, дифференциальным и линейным характеристикам).

И если, определяя среднее значение максимума таблицы дифференциальной разности (полного дифференциала шифра-подстановки) для произвольной случайной подстановки, мы можем говорить о том, что существует, хотя и очень мало вероятное, значение максимума, превышающее (может быть даже существенно) среднее значение максимума, то для шифра таких мало вероятных значений, сколько-нибудь заметно отличающихся от среднего значения максимума нет. Наши эксперименты с малыми моделями шифров показывают, что среднее значение максимума для полного дифференциала шифра практически как раз и является наиболее вероятным (граничным) значением.

Опираясь на экспериментальные данные, для определения реальной границы максимума полного дифференциала (таблицы XOR разностей для всего шифра), можно рассмотреть отношение $\frac{\Lambda_{m,2k}}{k}$, из которого можно определить граничное значение k, при котором оно становится меньшим единице. Полученное значение k_{max} и следует принять в качестве максимально вероятного значения дифференциала. Но именно эта задача и решалась при построении таблицы 1. Как следует из данных расчетов и экспериментов, максимально возможное значение дифференциала для подстановки порядка 2^m оказывается близким к $m + 4$, что укладывается в границы, оговоренные Luka O'Connor-ом, и, следовательно, утверждение 3.1 из работы [5], опираясь на наши эмпирические

данные, применительно к блочным симметричным шифрам (что выходит за рамки, оговоренные Luka O'Connor-ом) можно перефразировать так:

Утверждение. *Для шифрующих преобразований, определяемых многоцикловыми процедурами перестановочно-подстановочных биективных отображений, свойственными современным блочным симметричным шифрам, ожидаемая вероятность самой правдоподобной ненулевой дифференциальной характеристики ограничена значением* $\frac{m+4}{2^m}$.

Таким образом, дифференциальные 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 (неразличимыми). Все они реализуют наибольшую вероятность максимума полного дифференциала (для 128 битных версий) близкую к 2^{-120}. Кстати, эти же характеристики стойкости к атакам дифференциального криптоанализа демонстрирует при соответствующем числе циклов (например, при 10 как в шифре Rijendael) и классическая SPN структура, рассмотренная в 1973 г. в работе Х. Фейстеля [8] (16-битная конструкция этого типа детально исследована проф. Н. Хеусом [7]).

На основе полученных результатов можно, тем не менее, предложить подход к сравнению эффективности решений по построению алгоритмов шифрования (при прочих равных условиях) в виде минимального числа циклов алгоритма, при котором реализуется асимптотический показатель среднего значения максимума полных дифференциалов.

По этому показателю, как свидетельствует анализ уменьшенных версий рассмотренных шифров, преимущество следует отдать шифру Лабиринт, который выходит на асимптотическое значение показателя уже при двух итерациях (за счет мощного начального преобразования), далее следует Rijendael и решения, представленные на украинский конкурс (4-е цикла), и затем уже идет SPN шифр Х. Фейстеля (6-ть циклов).

Другой важный вывод, который напрашивается по результатам экспериментов, состоит в том, что при мощном (доцикловом) преобразовании и другие известные решения по построению блочных шифров, в том числе и обобщенная SPN структура Х. Фейстеля (с существенно худшим по эффективности чем примененное в шифре Rijendael линейным преобразованием) обеспечивает дифференциальные свойства (максимальную вероятность полного дифференциала), не уступающие шифру Rijendael и по скорости достижения асимптотических показателей. Использование в таких структурах случайных S-блоков обеспечит и повышенную по сравнению с шифром Rijendael устойчивость к алгебраическим атакам.

Литература

[1] *Олейников Р. В., Лисицкий К. Е.* Исследование дифференциальных свойств подстановок различных цикловых классов. Двенадцатая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах», 19-20 МАЯ 2009 г., Тезисы докладов. – К.: ЧП "ЕКМО", НИЦ "ТЕЗИС" НТУУ "КПИ", 2009. – С. 24-25.

[2] *Олейников Р.В., Лисицкая И.В., Широков А.В., Лисицкий К.Е.* Исследование дифференциальных свойств подстановок. Сборник трудов Первой Международной научно-технической конференции «Компьютерные науки и технологии», 8-10 октября 2009 г., Белгород, Ч. I, С. 59-63.

[3] *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.

[4] *Долгов В.И., Лисицкая И.В., Киянчук Р.И.* Rijndael – это новое или хорошо забытое старое? Сборник трудов Первой Международной научно-технической конференции «Компьютерные науки и технологии», 8-10 октября 2009 г., Белгород, Ч. II, С. 32-35.

[5] *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. Helleseth ed., Springer-Verlag, pages 360-370, 1994.

[6] *E. Biham and A. Shamir.* Differential cryptanalysis of the full 16-round DES. Technical Report 708. Technion, Israel Institute of Technology, Haifa, 1991.

[7] *H.M. Heys.* A Tutorial on Linear and Differential Cryptanalysis, CRYPTOLOGIA, v. 26, N 3, 2002, p. 189-221.

[8] *H. Feistel,* Cryptography and computer privacy. Scientific American, 228(5): 15-23,1973.

[9] *Долгов В.И., Лисицкая И.В., Руженцев В.И.* Анализ циклических свойств блочных шифров // Прикладная радиоэлектроника: научн.-техн. журнал. – 2007. – Т. 6, № 2 – С. 257-263.

Поступила в редколлегию 25.06.2010.

Олейников Роман Васильевич, кандидат технических наук, докторант кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.

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

Лисицкий Константин Евгеньевич, студент 1-го курса кафедры БИТ ХНУРЭ. Область научных интересов: криптографическая защита информации.

Тевяшев Андрей Дмитриевич, доктор технических наук, профессор, заведующий кафедрой прикладной математики. Область научных интересов: криптографическая защита информации.

УДК 621. 391:519.2:519.7

Диференційні властивості підстановок / Р.В. Олійников, О.І. Олешко, К.Є. Лисицький, А.Д. Тевяшев // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 326-333.

Виводяться розрахункові відношення для визначення середнього значення максимумів XOR таблиць випадкових підстановок. Показується. що диференційні властивості сучасних блокових симетричних шифрів (при заявленому числі циклів перетворення) являються одним із проявів властивостей випадкових підстановок. Пропонується підхід до порівняння ефективності рішень по побудові алгоритмів шифрування у вигляді мінімальної кількості циклів алгоритму, при якій реалізується асимптотичний показник середнього значення максимуму повних диференціалів.

Ключові слова: симетричний блоковий шифр, диференційний криптоаналіз, випадкова перестановка.

Табл. 04. Бібліогр.: 09 найм.

UDC 621. 391:519.2:519.7

Differential properties of substitutions / R.V. Oleinykov, O.I. Oleshko, K.E. Lisitskiy, A.D. Tevyashev // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 326-333.

Computational relations for determining the overage of maximum values of XOR tables of random substitutions are derived. It is shown that differential properties of present-day block symmetric ciphers (with the declared number of transformation cycles) are one of the manifestations of properties of random substitutions. 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 is suggested, which implements an asymptotic index of the average maximum value of full differentials.

Key words: symmetric block cipher, differential cryptanalysis, random substitution.

Tab. 04. Ref.: 09 items.