УДК 681.3.06

ОЦЕНКА ЧИСЛА СЛУЧАЙНЫХ ПОДСТАНОВОК С ЗАДАННЫМ РАСПРЕДЕЛЕНИЕМ ПЕРЕХОДОВ XOR ТАБЛИЦ И СМЕЩЕНИЙ ТАБЛИЦ ЛИНЕЙНЫХ АППРОКСИМАЦИЙ

И.В. ЛИСИЦКАЯ, А.В. ШИРОКОВ, Е.Д. МЕЛЬНИЧУК, К.Е. ЛИСИЦКИЙ

Определяются значения показателей отбора (% прохождения) подстановок, обладающих теоретическими значениями законов распределения переходов из XOR таблиц и смещений таблиц линейных аппроксимаций. Приводятся результаты экспериментальной проверки теоретически обоснованных значений показателей отбора.

Ключевые слова: случайная подстановка, таблица XOR разностей подстановки, таблица линейных аппроксимаций подстановки, критерии отбора случайных подстановок, закон распределения переходов таблиц XOR разностей случайной подстановки, закон распределения смещений таблицы линейных аппроксимаций случайной подстановки.

ВВЕДЕНИЕ

В этой работе мы продолжим обсуждение введенных в наших предыдущих работах [1,2] двух новых (дополнительных) критерия отбора случайных подстановок. Здесь обосновываются окончательные (предлагаемые для практического использования) граничные значения параметров b и c в критериях отбора (по Колмогорову) и приводятся примеры практического применения этих критериев для отбора подстановок с ожидаемыми улучшенными криптографическими показателями.

1. ЗАКОНЫ РАСПРЕДЕЛЕНИЯ ПЕРЕХОДОВ ТАБЛИЦ XOR РАЗНОСТЕЙ СЛУЧАЙНЫХ ПОДСТАНОВОК И СМЕЩЕНИЙ ТАБЛИЦЫ ЛИНЕЙНЫХ АППРОКСИМАЦИЙ ПОДСТАНОВКИ

Нас будут интересовать сначала подстановки, таблицы XOR разностей которых имеют заданное распределение парных разностей (переходов входных разностей ΔX в соответствующие выходные разности ΔY).

В обозначениях работы [3] пусть $\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$ будет вероятностью того, что значение ячейки дифференциальной таблицы случайно взятой подстановки π порядка 2^n для перехода входной разности ΔX в соответствующую выходную разность ΔY будет равно $2k$. Эта вероятность определяется теоремой [3].

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

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

где функция $\Phi(d)$ определяется выражением

$$\Phi(d)=\sum_{i=0}^{d}(-1)^i \cdot \left(\begin{array}{c}d\\ i\end{array}\right)^2 \cdot 2^i \cdot i! \cdot (2d-2i)!. \quad (2)$$

В [3] также получено соотношение для среднего значения числа ненулевых характеристик отдельного S-блока с переходами $\Delta X \to \Delta Y$, такими, что $\Lambda_\pi(\Delta X,\Delta Y)=2k$:

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

Предыдущим обозначениям в (3) соответствует $m=n$.

Для иллюстрации в табл. 1 представлены результаты расчетов, выполненных по этому выражению, для подстановки 16-той степени ($m=4$).

Таблица 1

Распределение парных разностей для XOR таблицы подстановки порядка 2^4 (расчёт)

$2k$	Число ячеек	Вероятность
0	132,165	0,587399
2	70, 1592	0,311819
4	18,7723	0,0834326
6	3,381	0,0150289
8	0,4662	0,002072

В табл. 2 представлены результаты расчетов для подстановок порядка 2^8 [2].

Аналогичные соотношения в работах [1, 2] были рассмотрены для законов распределения переходов таблиц линейных аппроксимаций – ЛАТ (законов распределения вероятностей линейных корпусов).

Таблица 2

Распределение парных разностей для XOR таблицы подстановки порядка 2^8 (расчёты с округлением в сторону ближайшего целого)

$2k$	Число ячеек	Вероятность
0	39363	0,605345
2	19758	0,303855
4	4959	0,0762627
6	830	0,0127609
8	104	0,001599
10	10	0,00015378
12	1	0,000015378

В работе [1] было предложено использовать вычисленные таким образом законы распределения парных разностей и смещений ЛАТ подстановок различного порядка для построения новых (дополнительных) критериев отбора случайных подстановок. В последующей работе [2] были рассмотрены вопросы установления границ при использовании критерия Колмогорова для оценки близости законов распределения переходов дифференциальных и линейных таблиц подстановок теоретическим (мы их назвали ″эталонными″), на основе результатов которых принимается решение можно ли отнести проверяемую подстановку к случайной или нет. В этой работе нас будут интересовать вопросы практической реализуемости подстановок с ″предельными″ показателями, т.е. показателями, соответствующими ″эталонным″.

Отметим здесь, что новые критерии построены на идее подчинения свойств подстановок свойствам шифрующих преобразований. Заметим также, что для шифрующих преобразований, рассматриваемых как подстановки, законы распределения переходов дифференциальных и линейных таблиц, если переходить на терминологию работы [4], представляют собой законы распределения полных дифференциалов и линейных корпусов.

2. ТЕОРЕТИЧЕСКАЯ ОЦЕНКА ОЖИДАЕМОГО ЧИСЛА ПОДСТАНОВОК С ЗАДАННЫМИ ЗАКОНАМИ РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ ПЕРЕХОДОВ ДИФФЕРЕНЦИАЛЬНЫХ И ЛИНЕЙНЫХ ТАБЛИЦ

Будем интересоваться теоретически ожидаемым числом подстановок из общего их множества $2^n!$, которые соответствуют ″эталонному″ закону распределения вероятностей. Эти результаты одновременно станут теоретическим обоснованием экспериментальных результатов, приведенных в работе [2].

Здесь определяющим для последующих шагов может стать достаточно очевидное соображение, заключающееся в том, что подстановками с требуемыми свойствами будут те, которые имеют непременно переход с максимальным значением полного дифференциала k_D^* (присутствующим в эталонном распределении).

Но k_D^* – это значение, при котором выражение (3) (см. [3]) принимает значение близкое к единице (Для ЛАТ k_L^* – это значение, при котором уравнение аналогичное (3) (см. [4]) принимает значение близкое к единице).

В соответствии с логикой получения выражения (1) его числитель определяет число подстановок, имеющих значение ячейки XOR таблицы для перехода ΔX в ΔY равное $2k$. Следовательно, вычислив значение этого соотношения при $k = k_D^*$, мы можем найти теоретическое значение вероятности получения (формирования) при случайном выборе подстановки, имеющей переход XOR таблицы равный $2k_D^*$, т. е. вероятность, обозначенную в предыдущей нашей работе [3] $Pr\left(\Lambda_\pi(\Delta X,\Delta Y) = 2k_D^*\right)$.

Этот переход (единственный в подстановке переход с максимальным значением) может присутствовать (появиться) на любой позиции (в любой ячейке) подстановки (в любой строке таблицы).

Учитывая, что каждая подстановка имеет $2^n - 1$ ненулевых строк (столбцов), приходим к выводу, что вероятность получить отдельную подстановку с необходимым для нас переходом (с максимальным значением) на любой из $2^n - 1$ возможных позиций (строк или столбцов) равна сумме вероятностей $2^n - 1$ независимых равновероятных событий, т. е.

$$Pr\Big(\Lambda_\pi(\Delta X_1,\Delta Y_1) = 2k_D^*, \Lambda_\pi(\Delta X_2,\Delta Y_2) = 2k_D^*,$$
$$\ldots, \Lambda_\pi(\Delta X_{2^{n-1}},\Delta Y_{2^{n-1}}) = 2k_D^*\Big) =$$
$$= (2^n - 1)\cdot Pr\left(\Lambda_\pi(\Delta X,\Delta Y) = 2k_D^*\right).$$

Это и есть тот результат, который нам нужен и с помощью которого мы можем получить интересующие нас оценки для вероятностей получения подстановок с дифференциальными и линейными таблицами, повторяющими расчетные распределения таблицы 1 и соответствующих таблиц для переходов линейных таблиц аппроксимаций случайных подстановок.

Остается заметить, что если учесть также то, что умножение вероятности $Pr\left(\Lambda_\pi(\Delta X,\Delta Y) = 2k_D^*\right)$ еще раз на число $2^n - 1$ приводит в соответствии с соображениями [3] к результату:

$$(2^n - 1)^2 \cdot Pr\left(\Lambda_\pi(\Delta X,\Delta Y) = 2k_D^*\right) \approx 1,$$

т.е. мы имеем дело с полной группой событий, что отражает тот очевидный факт, что каждая таблица имеет хотя бы одну ячейку со значением k_D^* (сумма вероятностей $Pr\left(\Lambda_\pi(\Delta X,\Delta Y) = 2k_D^*\right)$ для всех ячеек подматрицы A_π таблицы XOR разностей).

В результате для определения вероятности интересующего нас события – выбора подстановки с заданным законом распределения вероятностей переходов) можно получить оценочное выражение в виде:

$$Pr\Big(\Lambda_\pi(\Delta X_0,\Delta Y_0) = 0, \Lambda_\pi(\Delta X_1,\Delta Y_1) = 2,$$
$$\Lambda_\pi(\Delta X_2,\Delta Y_2) = 4, \ldots, \Lambda_\pi(\Delta X_s,\Delta Y_s) = 2k_D^*\Big) \le \frac{1}{2^n - 1},$$

и при этом

$$\#(\Delta X_0,\Delta Y_0) + \#(\Delta X_1,\Delta Y_1) + \#(\Delta X_2,\Delta Y_2) + \ldots +$$
$$+ \#(\Delta X_s,\Delta Y_s) = (2^n - 1)^2,\ s = k_D^*,$$

которое и предлагается использовать для дальнейших расчетов.

Очевидно, что совершенно аналогичное выражение может быть получено и для оценки вероятности случайного выбора подстановки с таблицей линейных аппроксимаций, повторяющей "эталонную":

$$Pr\left(\Lambda_\pi(\alpha_0,\beta_0)=0,\Lambda_\pi(\alpha_1,\beta_1)=2,\right.$$

$$\left.\Lambda_\pi(\alpha_2,\beta_2)=4,\ldots,\Lambda_\pi(\alpha_s,\beta_s)=2k_L^*\right)\le\frac{1}{2^n-1}.$$

Здесь уже

$$\#(\alpha_0,\beta_0)+\#(\alpha_1,\beta_1)+\#(\alpha_2,\beta_2)+\ldots+$$

$$+\#(\alpha_s,\beta_s)=(2^n-1)^2,\ s=k_L^*.$$

В итоге для практически интересных ситуаций использования в шифрах S-блоков размерами битовых входов равными $n=4$ и $n=8$ для вероятностей получения (генерации) S-блоков случайного типа с параметрами таблиц XOR разностей и линейных аппроксимаций, повторяющих теоретические распределения таблиц 1-4, приходим к значениям:

$$n=4\ \rightarrow\ 2^4-1=15\ \rightarrow$$

$$\rightarrow\ Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=8)\right)=\frac{1}{15}=0{,}06(6);$$

$$n=8\ \rightarrow\ 2^8-1=255\ \rightarrow$$

$$\rightarrow\ Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=12)\right)=\frac{1}{155}=0{,}004.$$

Совершенно аналогичные результаты получаются и для подстановок с соответствующими таблицами линейных аппроксимаций.

Считая теперь, что дифференциальные и линейные показатели подстановок независимы, для вероятности получить при случайном выборе подстановку, обладающую одновременно максимальными значениями ячеек таблиц XOR разностей и линейных аппроксимаций равными k_D^* и k_L^*, приходим к результату (в худшем случае):

$$n=4\ \rightarrow\ 2^4-1=15\ \rightarrow$$

$$\rightarrow Pr\left(\Lambda_\pi\{(\Delta X,\Delta Y)=k_D^*),(\alpha,\beta\right)=k_L^*\}=$$

$$=(0{,}06(6))^2\approx 0{,}004.$$

$$n=8\ \rightarrow\ 2^8-1=255\ \rightarrow$$

$$\rightarrow Pr\left(\Lambda_\pi\{(\Delta X,\Delta Y)=k_D^*),(\alpha,\beta\right)=k_L^*\}=$$

$$=(0{,}004)^2\approx 0{,}000016.$$

В соответствии с этими результатами (полученными теоретическим путем) выходит, что из общего числа 16! подстановок порядка $2^4=16$

– около 7% подстановок имеют дифференциальные или линейные свойства, повторяющие теоретические распределения, свойственные случайным подстановкам, из них ожидается, что одновременно имеют интересующие нас дифференциальные и линейные показатели примерно 0,4% всех подстановок.

Для подстановок порядка $2^8=256$ соответствующие показатели прохода (удовлетворения) критериев случайности имеют значения:

0,04% при раздельной фильтрации по дифференциальным или линейным показателям и

0,0016% при одновременном удовлетворении дифференциальных и линейных показателей отбора.

Приведенные цифры свидетельствуют, что реализация соответствующих параметров отбора для подстановок рассмотренного порядка вполне осуществима.

В итоге для отбора подстановок, удовлетворяющих новым критериям случайности, теоретически можно использовать самые жесткие ограничения (нулевые значения параметров b и c).

Результаты экспериментов с отбором случайных подстановок в целом подтвердили теоретически полученные значения вероятностей и по дифференциальным и по линейным показателям.

Эксперименты, однако, также показали, что подстановок, удовлетворяющих одновременно двум показателям случайности (одновременно и дифференциальным и линейным показателям) найти не удалось. Поэтому в процессе экспериментов были определены возможности минимального изменения границ отбора, при которых удалось достигнуть одновременного выполнения двух предлагаемых критериев. Опять-таки экспериментальным путем установлено, что достаточно, оказалось, ввести допустимые расхождения между эталонными и реальными значениями ворот отклонений от эталонных целочисленных значений в пределах ±2 единиц. В итоге, в пересчете на значения параметров b и c мы пришли к граничным значениям параметров отбора случайных подстановок.

Для подстановок порядка $2^4=16$:

$$b=c=\frac{2}{15^2}=0{,}008(8).$$

Для подстановок порядка $2^8=256$:

$$b=c=\frac{2}{255^2}=0{,}00003.$$

Примеры подстановок, отобранных с помощью представленных уточненных критериев, представлены в таблицах 3-4.

Таблица 3

Подстановки порядка 2^4 прошедшие отбор с параметрами критериев случайности $a=1$, $b=c=0{,}00889$

	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
S_1	2 8 14 5 7 9 1 13 12 11 15 4 6 0 10 3
S_2	0 6 9 5 15 13 8 7 4 3 14 1 11 12 10 2
S_3	9 5 11 4 6 14 10 8 2 15 12 13 0 1 7 3
S_4	2 8 14 5 7 9 1 13 12 11 15 4 6 0 10 3
S_5	10 15 12 1 8 2 14 0 9 11 3 13 6 4 7 5
S_6	9 5 11 4 6 14 10 8 2 15 12 13 0 1 7 3

В этом эксперименте из 1000 сгенерированных подстановок удовлетворили установленным критериям 8-мь подстановок (0,8%).

1000 подстановок такого порядка на компьютере с процессором AMD Sempron 2500+BOX требует порядка 30 минут времени. Это значит, что для проверки выборки объемом 1000000 потребуется 30 000 минут, что приводит к общему времени анализа ≈ 20 дней. Поэтому мы здесь приведем пример формирования (отбора) подстановки порядка 2^8 не с предельными показателями.

На рис. 1 представлен пример такой подстановки вместе с ее характеристиками.

Таблица 4

Пример подстановки порядка 2^8, прошедшей критерии отбора: $a > 1$, $b = 0{,}0002153$, $c = 0{,}00035417$

67	7e	4c	86	6	66	2d	dd	ee	c1	21	6b	bd	7d	26	fd
9d	7c	C9	2	3	f4	79	e	a0	2c	a9	8f	c5	74	b7	3d
68	72	af	3b	43	1a	63	3a	88	fb	C4	70	7b	5a	76	B8
5c	1e	39	41	8e	96	e9	b1	5	42	e7	de	c3	a4	17	7f
b	e5	0	4d	d2	ec	bc	87	18	94	85	a	34	d	9b	46
bb	f3	2f	aa	3e	7a	ba	dc	91	3c	37	4	33	93	83	e4
e6	4f	64	9f	5d	29	ea	78	65	c2	28	f9	12	e1	47	fa
b2	ac	25	d0	71	77	44	9e	2e	24	cb	a1	b6	c0	52	97
14	a7	22	ef	ad	ff	e3	90	10	bf	48	84	51	ca	d4	ae
F8	3f	56	92	5f	b4	6c	6a	c	d7	60	32	62	53	ce	b3
6d	a3	eb	6e	cc	50	54	b5	cf	9c	cd	c7	2a	c8	38	69
78	15	9a	80	59	d5	1f	5b	23	c6	ed	db	99	b0	1b	d1
F6	8d	f	b1	e0	4b	f1	a2	f0	98	d8	d3	f5	a5	27	35
73	fc	da	31	a6	36	2b	8c	57	61	1d	7	5e	81	11	9
6f	1	d9	a8	ab	8a	8b	fe	1c	f2	82	be	e8	45	4a	55
49	89	20	b9	df	e2	8	58	19	30	16	40	13	f7	95	d6

Cycles: 9
Inversions: 15321
Increasings: 131

Max DT: 12
Number of max DT: 1
MaxLAT: 34
Number of max LAT: 1

Elements DT:

0	39363
2	19758
4	4959
6	830
8	102
10	11
12	1
14	0
16	0
18	0
20	0
22	0
24	0
26	0
28	0
30	0
32	0
34	0

Max diversion: 0,0002153 (±14)

Elements LAT:

0	6465
2	12536
4	11404
6	9817
8	7839
10	5967
12	4255
14	2816
16	1778
18	1003
20	581
22	306
24	153
26	57
28	31
30	8
32	6
34	1

Max diversion: 0,00035417 (±23)

ЗАКЛЮЧЕНИЕ

Таким образом, мы показали, что существует достаточно большое число подстановок, имеющих законы распределения вероятностей переходов XOR разностей и смещений таблиц линейных аппроксимаций, повторяющие соответствующие законы распределения вероятностей случайных подстановок, полученные теоретическим путем.

Для подстановок порядка $2^4 = 16$ около 7% всех подстановок симметрической группы имеют дифференциальные или линейные свойства, повторяющие теоретические распределения, свойственные случайным подстановкам, из них ожидается, что одновременно имеют интересующие нас дифференциальные и линейные показатели

примерно 0,4% всех подстановок (отдельный эксперимент дал значение 0,8%).

Выполнение критериев случайности для инверсий, возрастаний и циклов приводит к дополнительному уменьшению допустимого множества на 50%.

Для подстановок порядка $2^8 = 256$ соответствующие показатели прохода (удовлетворения) критериев случайности имеют значение 0,0016% при одновременном удовлетворении дифференциальных и линейных показателей отбора.

Приведенные цифры свидетельствуют, что реализация соответствующих параметров отбора для подстановок рассмотренного порядка вполне осуществима.

И еще!

Можно сделать также вывод о том, что работоспособными оказываются намного более жесткие критерии отбора случайных подстановок, которые могут оказаться полезными при поиске подстановок с высокими криптографическими показателями.

По крайней мере, в разрешенное множество вошли подстановки, которые по своим свойствам повторяют свойства шифрующих преобразований.

Представляется, что с помощью таких подстановок удастся реализовать предельные показатели по скорости перехода шифрующих преобразований к асимптотическому режиму, определяемому с точки (момента), когда шифрующее преобразование приобретает свойства случайной подстановки. Найти убедительные аргументы в пользу плодотворности предлагаемого подхода станет задачей наших дальнейших исследований.

Литература

[1] *Лисицкая И.В., Лисицкий К.Е. Широков А.В., Мельничук Е.Д.* Случайные подстановки в криптографии // Радіоелектронні та комп'ютерні системи, 2010, № 5 (46), С. 79-84.

[2] *Горбенко И.Д., Лисицкая И.В.* Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 28147-89 // Радиотехника. Всеукр. межвед. науч.-техн. сб. – 1997. Вып 103. – С. 121–130.

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

[4] *Долгов В.И., Лисицкая И.В., Олешко О.И.* Свойства таблиц линейных аппроксимаций случайных подстановок // Прикладная радиоэлектроника: научн.-техн. журнал. – 2010. Т. 9, № 3. – С. 334-340.

Поступила в редколлегию 29.06.2010.

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

Широков Алексей Викторович, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: криптоанализ.

Мельничук Евгений Дмитриевич, магистрант кафедры БИТ ХНУРЭ. Область научных интересов: криптографическая защита информации.

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

УДК 681.3.06

Оцінка числа випадкових підстановок із заданим розподілом переходів XOR таблиць і зміщенням таблиць лінійних апроксимацій / І.В. Лисицька, О.В. Широков, Є.Д. Мельничук, К.Є. Лисицький // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 341-345.

Визначаються значення показників відбору (% проходження) підстановок, що володіють теоретичними значеннями законів розподілу переходів їх XOR таблиць і зсувів таблиць лінійних апроксимацій. Наводяться результати експериментальної перевірки теоретично обгрунтованих значень показників відбору.

Ключові слова: випадкова підстановка, таблиця XOR різниць підстановки, таблиця лінійних апроксимацій підстановки, критерії відбору випадкових підстановок, закон розподілу переходів таблиць XOR різниць випадкової підстановки, закон розподіленості зміщень таблиці лінійних апроксимацій випадкової підстановки.

Табл. 04. Бібліогр.: 04 найм.

UDC 681.3.06

Estimating the number of random substitutions with a given distribution of transitions of XOR tables and shifts of tables of linear approximations / I.V. Lisitskaya, A.V. Shirokov, E.D. Melnichuk, K.E. Lisitskiy // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 341-345.

Values of indices of selecting (% of passing) substitutions having theoretical values of distribution laws of transitions of their XOR tables and shifts of tables of linear approximations are determined. The results of experimental verification of theoretically substantiated values of the indices of selection are given.

Key words: random substitution, XOR substitution difference table, linear approximations of substitution table, criteria for selection of random substitutions, law of distributing transitions of random substitution XOR difference tables, law of distributing shifts of the random substitution linear approximations table.

Tab. 04. Ref.: 04 items.