УДК 621. 3.06

ИССЛЕДОВАНИЕ СООТВЕТСТВИЯ НОВЫМ КРИТЕРИЯМ ОТБОРА ПОДСТАНОВОЧНЫХ КОНСТРУКЦИЙ СОВРЕМЕННЫХ БСШ

Е.Д. МЕЛЬНИЧУК

Рассматриваются показатели случайности S-блоков ряда современных шифров.

Ключевые слова: подстановка, линейные показатели стойкости, дифференциальные показатели стойкости.

ВВЕДЕНИЕ

Многочисленными экспериментами [1, 3, 4] показано, что все современные шифры после небольшого начального числа циклов зашифрования становятся случайными подстановками (для шифра DES требуется 16 циклов, для остальных 3–4). Здесь имеются в виду повторение шифрами законов распределения вероятностей для числа циклов, инверсий, возрастаний, а также законов распределения вероятностей переходов XOR таблиц и смещения таблиц линейных аппроксимаций соответствующих законов распределения вероятностей случайных подстановок.

Этот факт вызвал интерес к изучению случайных подстановок и исследованию методов их генерации [1, 10] не только как шифрующих преобразований, но и как подстановочных (нелинейных) преобразований, используемых при построении шифров. Выполнен ряд работ по математическому описанию законов распределения вероятностей случайных подстановок [1] и их использованию для построения дополнительных критериев отбора подстановок.

Возникли закономерные вопросы о криптографической значимости подстановок случайного вида: насколько применимы в шифрах подстановки, отобранные по критериям случайности; позволяют ли они улучшить криптографические показатели шифров? Целью этой статьи является изучение ответов на первый вопрос.

В первой части статьи мы кратко излагаем методику оценки показателей случайности подстановок, а во второй мы приводим результаты анализа S-блоков ряда современных шифров на предмет оценки близости их показателей случайности показателям случайных подстановок.

Оценке криптографической пригодности случайных подстановок посвящена наша отдельная работа [1].

1. МЕТОДИКА ОЦЕНКИ ПОКАЗАТЕЛЕЙ СЛУЧАЙНОСТИ ПОДСТАНОВОК

В этой работе мы изучим показатели случайности S-блоков ряда современных шифров. Все S-блоки имеют размер 8×8 (байтовые входы и байтовые выходы). Нас будут интересовать следующие показатели случайности:

- показатели комбинаторной группы критериев (число инверсий, число циклов, число возрастаний);
- линейные и дифференциальные показатели;
- закон распределения переходов таблиц дифференциальных разностей;
- закон распределения переходов таблиц линейных аппроксимаций;
- максимальное расхождение интегральных законов распределения переходов таблиц дифференциальных разностей и таблиц линейных аппроксимаций.
- значение максимума XOR таблицы и число таких максимумов (δ -равномерность);
- значение максимума таблицы ЛАТ и число таких максимумов.

2. КРИТЕРИИ СЛУЧАЙНОСТИ ПОДСТАНОВКИ

Начнем с определения случайной подстановки и критериев случайности подстановки. В частности, в работе [1] введено новое определение случайной подстановки, которое сформулировано в следующем виде:

Подстановка является *случайной*, если вместе с выполнением критериев случайности 1–3 для заполнений ячеек её XOR таблицы и таблицы линейных аппроксимаций выполняются законы распределения вероятностей (критерий случайности 4 и критерий случайности 5).

Критерий 1. Число инверсий η_n в подстановке степени n приблизительно равно числу “антиинверсий”, а практически, если

$$\left|\eta_n - \frac{n(n-1)}{4}\right| \le a\sigma_\eta,\ \sigma_\eta = \frac{n^{3/2}}{6}.$$

Критерий 2. Число циклов ξ_n в подстановке степени n близко к $\ln n$, а практически, если

$$\left|\xi_n - \ln n\right| \le a\sigma_\xi,\quad \sigma_\xi = \sqrt{\ln n}\,.$$

Критерий 3. Подстановка удовлетворяет критерию случайности 3, если число возрастаний θ_n в подстановке степени n приблизительно равно числу убываний, а практически, если

$$\left|\theta_n - \frac{n}{2}\right| \le a\sigma_\theta,\ \ \sigma_\theta = \sqrt{n/12}\,.$$

В этих соотношениях a – параметр, выбираемый в значительной степени из субъективных соображений (по крайней мере, из условия, что множество допустимых подстановок не станет меньше некоторого заданного числа).

Критерий 4. Подстановка удовлетворяет критерию случайности 4, если закон распределения однотипных переходов

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

её таблицы XOR разностей для входов, приписываемых к ненулевым характеристикам, соответствует по критерию согласия Колмогорова теоретическому закону распределения переходов (3.2), т.е. наибольшее значение модуля разности теоретического и эмпирического законов распределения вероятностей удовлетворяет условию $|F_T(x_k)-F(x_k)|\le b$.

Критерий 5. Подстановка удовлетворяет критерию случайности 5, если закон распределения однотипных переходов $Pr(\lambda^*(\alpha,\beta)=2k)$, $k=0,1,\ldots,k^*$ её таблицы линейных аппроксимаций соответствует по критерию согласия Колмогорова теоретическому закону распределения (3.6), т.е. наибольшее значение модуля разности теоретического и эмпирического законов распределения вероятностей удовлетворяет условию $|F_T(x_k)-F(x_k)|\le c$.

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

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

где функция $\Phi(d)$ определяется выражением

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

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 (3.2) на число ячеек подматрицы $A_\pi=|a_{i,j}|$ таблицы XOR_π равное $(2^m-1)^2$:

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

Утверждение 5. 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 α,β не нулевые. Тогда смещения $\lambda^*(\alpha,\beta)$ принимают только четные значения и для $|k|\le 2^{n-2}$

$$Pr\left(\lambda^*(\alpha,\beta)=|2k|\right)=\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}-|k|}^2.$$

В результате мы можем получить выражение для вычисления $E[\lambda(\pi,2k)]$ как простое умножение формулы (3.10) на общее число ячеек таблицы подстановки, исключая первую строку и первый столбец

$$E[\lambda(\pi,2k)]=\frac{(2^n-1)^2\cdot\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+|k|}^2.$$

3. РЕЗУЛЬТАТЫ АНАЛИЗА S-БЛОКОВ ДЛЯ РЯДА СОВРЕМЕННЫХ ШИФРОВ

Для выполнения такого рода исследований на кафедре БИТ ХНУРЭ был разработан программный комплекс, позволяющий получить все интересующие нас оценки.

Результаты вычислительных экспериментов иллюстрируют таблица 1 – таблица 4. На каждой из таких таблиц представлен сам S-блок в общепринятой в литературе системе представлений (вход в таблицу состоит из двух полубайтов – один является входом по строкам, а другой – входом по столбцам, а на пересечении соответствующей строки и столбца читается значение байта в шестнадцатеричном представлении на выходе S-блока).

Как следует из содержания таблиц, на них представлены показатели случайности S-блоков шифров Rijndael, Лабиринт, Мухомор (Калина), Iceberg, ADE, Камелия, GrandCry и Anubis (Khazad).

Таблица 1

S-блок шифра ADE (один из набора)

63	E3	B8	0E	15	AA	D5	41	58	7D	1C	A7	A3	EB	E9	24
65	A1	F7	7F	DC	1D	01	1B	98	79	BC	96	BD	CD	5B	A2
FB	31	99	8D	29	7C	F6	14	27	51	5C	87	C9	CF	C4	A6
9E	4F	6E	30	8C	7A	02	CC	0C	4B	AF	B1	E4	11	18	B6
B4	3D	4A	82	1E	49	8F	B2	46	03	77	84	A9	2D	D8	D0
DA	9A	E1	95	FC	AD	8A	13	36	F9	AE	0D	2B	5A	81	86
06	9B	75	40	7E	C6	CA	4C	0F	4E	EF	71	48	EE	2F	7B
D4	20	EC	8B	05	21	91	F8	A0	67	C1	60	45	3F	89	08
88	57	D7	09	6C	E6	93	A8	DD	5F	ED	72	8E	62	10	C7
F1	33	C8	B0	F2	3B	0B	66	9D	07	DF	3A	BE	F0	BA	5D
BF	56	9F	26	B9	90	83	FE	AC	94	04	FF	97	E8	C0	00
52	6B	B5	DB	85	E5	54	E7	47	39	64	78	12	92	0A	28
D1	9C	1F	44	F3	C3	69	D3	76	2C	2A	61	B7	3C	F4	68
55	E0	F5	80	25	73	6A	59	6D	BB	A5	43	DE	3E	6F	B3
23	D2	C2	D9	A4	53	17	74	50	FD	42	EA	1A	AB	35	22
19	2E	FA	CB	32	CE	E2	38	70	5E	D6	C5	16	37	4D	34

Таблица 2

Показатели случайности S-блока ADE (один из набора)

Количество циклов	3
Количество инверсий	16179
Количество возрастаний	130
Максимум таблицы XOR	4
Количество максимумов XOR	255
Максимальное отклонение XOR	0,103391
Максимум таблицы LAT	16
Количество максимумов LAT	1275
Максимальное отклонение LAT	0, 0757866

Таблица 3

Закон распределения элементов таблиц XOR и таблицы LAT S-блока ADE (один из набора)

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	32640	4080
2	32130	12240
4	255	9180
6	0	10200
8	0	8670
10	0	6120
12	0	9180
14	0	4080
16	0	1275

Таблица 4

S-блок шифра ADE (второй из набора)

63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Таблица 5

Показатели случайности S-блока ADE (второй из набора)

Количество циклов	9
Количество инверсий	15821
Количество возрастаний	125
Максимум таблицы XOR	4
Количество максимумов XOR	255
Максимальное отклонение XOR	0,103391
Максимум таблицы LAT	16
Количество максимумов LAT	1275
Максимальное отклонение LAT	0, 0757866

Таблица 6

Закон распределения элементов таблиц XOR и таблицы LAT S-блока ADE (второй из набора)

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	32640	4080
2	32130	12240
4	255	9180
6	0	10200
8	0	8670
10	0	6120
12	0	9180
14	0	4080
16	0	1275

Таблица 7

S-блок шифра AES, GrandCru

63	7C	77	7B	F2	6B	6F	C5	30	1	67	2B	FE	D7	AB	76
CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
4	C7	23	C3	18	96	5	9A	7	12	80	E2	EB	27	B2	75
9	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
53	D1	0	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
D0	EF	AA	FB	43	4D	33	85	45	F9	2	7F	50	3C	9F	A8
51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
CD	C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	B	DB
E0	32	3A	A	49	6	24	5C	C2	D3	AC	62	91	95	E4	79
E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	8
BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
70	3E	B5	66	48	3	F6	E	61	35	57	B9	86	C1	1D	9E
E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
8C	A1	89	D	BF	E6	42	68	41	99	2D	F	B0	54	BB	16

Таблица 8

Показатели случайности S-блока AES, GrandCru

Количество циклов	5
Количество инверсий	16753
Количество возрастаний	126
Максимум таблицы XOR	4
Количество максимумов XOR	255
Максимальное отклонение XOR	0,103391
Максимум таблицы LAT	16
Количество максимумов LAT	1275
Максимальное отклонение LAT	0, 0757866

Таблица 9

Закон распределения элементов таблиц XOR и таблицы LAT S-блока AES, GrandCru

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	32640	4080
2	32130	12240
4	255	9180
6	0	10200
8	0	8670
10	0	6120
12	0	9180
14	0	4080
16	0	1275

Таблица 10

S-блок шифра Fox

5D	DE	0	B7	D3	CA	3C	D	C3	F8	CB	8D	76	89	AA	12
88	22	4F	DB	6D	47	E4	4C	78	9A	49	93	C4	C0	86	13
A9	20	53	1C	4E	CF	35	39	B4	A1	54	64	3	C7	85	5C
5B	CD	D8	72	96	42	B8	E1	A2	60	EF	BD	2	AF	8C	73
7C	7F	5E	F9	65	E6	EB	AD	5A	A5	79	8E	15	30	EC	A4
C2	3E	E0	74	51	FB	2D	6E	94	4D	55	34	AE	52	7E	9D
4A	F7	80	F0	D0	90	A7	E8	9F	50	D5	D1	98	CC	A0	17
F4	B6	C1	28	5F	26	1	AB	25	38	82	7D	48	FC	1B	CE
3F	6B	E2	67	66	43	59	19	84	3D	F5	2F	C9	BC	D9	95
29	41	DA	1A	B0	E9	69	D2	7B	D7	11	9B	33	8A	23	9
D4	71	44	68	6F	F2	E	DF	87	DC	83	18	6A	EE	99	81
62	36	2E	7A	FE	45	9C	75	91	C	F	E7	F6	14	63	1D
B	8B	B3	F3	B2	3B	8	4B	10	A6	32	B9	A8	92	F1	56
DD	21	BF	4	BE	D6	FD	77	EA	3A	C8	8F	57	1E	FA	2B
58	C5	27	AC	E3	ED	97	BB	46	5	40	31	E5	37	2C	9E
A	B1	B5	6	6C	1F	A3	2A	70	FF	BA	7	24	16	C6	61

Таблица 11

Показатели случайности S-блока Fox

Количество циклов	8
Количество инверсий	17056
Количество возрастаний	126
Максимум таблицы XOR	16
Количество максимумов XOR	70
Максимальное отклонение XOR	0,046105
Максимум таблицы LAT	32
Количество максимумов LAT	219
Максимальное отклонение LAT	0,187922

Таблица 12

Закон распределения элементов таблиц XOR и таблицы LAT S-блока Fox

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	42361	18686
2	15377	18171
4	5758	15888
6	680	6405
8	754	4280
10	19	983
12	6	352
14	0	41
16	70	219

Таблица 13

S-блок шифра Мухомор (один из набора)

F9	CA	14	61	E4	1C	43	20	4E	54	58	A0	FC	DB	C0	72
22	74	FE	B5	65	A8	25	ED	69	33	F1	B1	36	9	6	9A
8E	90	CF	F6	EA	27	BC	7	7F	D7	3C	7C	44	45	21	6B
1A	52	62	29	13	9B	CC	99	4B	42	B6	1D	C7	91	76	16
92	4F	47	70	98	66	C2	48	96	B	2F	C9	C6	38	8C	63
10	F2	A9	37	A7	D3	55	3D	2C	7A	AF	EE	3E	F5	67	C
77	84	C1	C5	DE	A4	DD	B4	E3	B3	EF	49	E2	71	4C	AD
DF	3	12	19	9C	D9	D2	78	50	DC	AA	15	4	39	9D	D1
2D	11	24	2E	F7	59	FA	1E	68	3A	7E	CB	AE	D6	A5	FD
5F	5	F	6A	A6	E7	EC	30	5C	6F	83	CD	B2	BB	EB	2
28	73	4D	18	A3	86	9F	5B	3F	81	AB	75	1B	6C	E	53
64	FB	26	40	7D	E1	95	34	BF	A	BD	31	2B	B0	F4	8D
E0	1	87	56	CE	FF	5D	6D	A2	6E	88	9E	94	89	46	35
4A	B9	DA	C3	F3	5E	8F	97	B7	D4	51	60	D5	23	57	D0
79	3B	17	C4	B8	C8	7B	2A	D	8B	D8	0	E8	BA	E6	F8
41	85	32	F0	80	93	8	E5	82	BE	E9	1F	A1	8A	AC	5A

Таблица 14

Показатели случайности S-блока Мухомор (один из набора)

Количество циклов	5
Количество инверсий	15601
Количество возрастаний	135
Максимум таблицы XOR	8
Количество максимумов XOR	90
Максимальное отклонение XOR	0, 0045059
Максимум таблицы LAT	30
Количество максимумов LAT	8
Максимальное отклонение LAT	0,0034077

Таблица 15

Закон распределения элементов таблиц XOR и таблицы LAT S-блока Мухомор (один из набора)

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	39070	6434
2	20244	12644
4	4827	11330
6	794	9667
8	90	7786
10	0	6067
12	0	4321
14	0	2859
16	0	1785
18	0	1033
20	0	564
22	0	303
24	0	146
26	0	59
28	0	17
30	0	8

Таблица 16

S-блок шифра Мухомор (второй из набора)

C	68	DE	9F	42	C0	AA	55	CC	1B	24	16	27	C9	21	AC
97	A9	A5	7C	FC	4	D7	E1	BC	C3	51	D9	F1	B6	D1	74
2F	A	6A	3E	83	71	9A	6D	D0	DB	25	2	A6	8A	DC	B3
FB	9D	E4	4A	69	89	7F	E0	B9	F2	A0	A8	D3	77	10	57
AD	54	6C	C7	11	C5	86	B5	36	0	14	E3	BF	5C	52	18
92	33	D2	8C	E5	1A	34	50	56	87	F3	78	29	22	9E	D8
FA	2E	75	2D	E9	C1	B2	AB	C2	DF	D5	7D	FD	A1	CD	31
AF	F	D6	F7	88	BE	5F	4E	5A	7B	C6	67	6E	5	1E	40
70	B0	F4	60	98	76	7	E	19	F5	8D	28	95	2A	44	32
23	1C	2C	D4	E8	6	91	6B	ED	66	94	93	BD	20	BB	BA
1F	E7	82	3C	EB	FE	CA	30	80	EE	5B	46	8E	9B	7A	F9
17	61	DA	E2	A3	EA	58	9C	B7	99	3A	73	35	FF	CE	B4
8F	CB	90	4C	5D	A7	62	DD	64	F6	37	8B	E6	15	D	4D
2B	AE	53	1D	3B	85	F0	39	81	48	84	F8	45	59	13	38
8	63	6F	EF	1	A2	96	B8	43	79	A4	C8	B	C4	5E	4F
3D	3F	EC	12	7E	49	4B	47	9	72	3	41	B1	26	65	CF

Таблица 17

Показатели случайности S-блока Мухомор (второй из набора)

Количество циклов	5
Количество инверсий	17467
Количество возрастаний	134
Максимум таблицы XOR	8
Количество максимумов XOR	80
Максимальное отклонение XOR	0,004090
Максимум таблицы LAT	30
Количество максимумов LAT	6
Максимальное отклонение LAT	0,002807

Таблица 18

Закон распределения элементов таблиц XOR и таблицы LAT S-блока Мухомор (второй из набора)

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	39097	6420
2	20140	12438
4	4944	11420
6	754	9811
8	80	7811
10	0	6141
12	0	4228
14	0	2524
16	0	1763
18	0	1052
20	0	585
22	0	319
24	0	125
26	0	49
28	0	31
30	0	6

Таблица 19

S-блок шифра Iceberg

24	C1	38	30	E7	57	DF	20	3E	99	1A	34	CA	D6	52	FD
40	6C	D3	3D	4A	59	F8	77	FB	61	A	56	B9	D2	FC	F1
7	F5	93	CD	0	B6	62	A7	63	FE	44	BD	5F	92	6B	68
3	4E	A2	97	B	60	83	A3	2	E5	45	67	F4	13	8	8B
10	CE	BE	B4	2A	3A	96	84	C8	9F	14	C0	C4	6F	31	D9
AB	AE	E	64	7C	DA	1B	5	A8	15	A5	90	94	85	71	2C
35	19	26	28	53	E2	7F	3B	2F	A9	CC	2E	11	76	ED	4D
87	5E	C2	C7	80	B0	6D	17	B2	FF	E4	B7	54	9D	B8	66
74	9C	DB	36	47	5D	DE	70	D5	91	AA	3F	C9	D8	F3	F2
5B	89	2D	22	5C	E1	46	33	E6	9	BC	E8	81	7D	E9	49
E0	B1	32	37	EA	5A	F6	27	58	69	8A	50	BA	DD	51	F9
75	A1	78	D0	43	F7	25	7B	7E	1C	AC	D4	9A	2B	42	E3
4B	1	72	D7	4C	FA	EB	73	48	8C	C	F0	6A	23	41	EC
B3	EF	1D	12	BB	88	D	C3	8D	4F	55	82	EE	AD	86	6
A0	95	65	BF	7A	39	98	4	9B	9E	A4	C6	CF	6E	DC	D1
CB	1F	8F	8E	3C	21	A6	B5	16	AF	C5	18	1E	F	29	79

Таблица 20

Показатели случайности S-блока Iceberg (близкие показатели у шифра Anubis (Khazad))

Количество циклов	128
Количество инверсий	16108
Количество возрастаний	133
Максимум таблицы XOR	8
Количество максимумов XOR	102
Максимальное отклонение XOR	0,001353
Максимум таблицы LAT	32
Количество максимумов LAT	5
Максимальное отклонение LAT	0,001934

Таблица 21

Закон распределения элементов таблиц XOR и таблицы LAT S-блока Iceberg (близкие показатели у шифра Anubis (Khazad))

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	39275	6419
2	19875	12610
4	4962	11291
6	811	9774
8	102	7881
10	0	6060
12	0	4166
14	0	2892
16	0	1887
18	0	940
20	0	566
22	0	288
24	0	137
26	0	62
28	0	33
30	0	14
32	0	5

Таблица 22

S-блок шифра Лабиринт

E6	F4	73	BE	7	6A	42	F7	41	4C	5	EA	DC	76	D8	6C
74	87	A5	8B	1A	9C	4E	6B	B	24	91	34	4A	2E	F3	E8
DA	64	7A	8F	EF	D4	93	AF	66	13	CF	82	59	D7	31	4F
C4	65	3	BF	D9	68	C5	E2	84	A6	23	99	C7	B0	5B	62
A0	12	83	ED	8C	0	57	DD	22	FF	9A	A4	F5	F9	3D	6D
FA	5C	49	39	43	5E	86	F	B7	67	52	CA	14	38	DB	25
3A	70	E4	1E	4	55	72	DE	56	47	CD	B6	8D	85	88	D6
A9	F0	5F	AE	9	8A	81	53	21	B5	F6	4B	4D	5D	44	2F
2B	F8	D2	D5	35	A2	3F	C6	BB	C2	A3	F1	9F	6F	1D	E1
60	7E	E0	7F	2D	AC	E3	D	BC	9D	C0	FE	3B	D1	1B	C3
80	63	C9	46	79	E7	89	E9	1C	AB	17	97	5A	20	30	EC
71	B8	B2	2	6	F2	E5	FD	28	D3	3E	3C	D0	BA	CE	29
10	B9	50	8	A1	A8	7D	40	1	15	7C	78	33	69	EB	E
6E	7B	77	54	92	58	95	C1	98	EE	1F	9B	96	51	26	61
2A	CC	B4	C	DF	A7	27	9E	32	37	B3	FC	A	AD	2C	19
B1	11	C8	AA	90	18	45	36	75	94	8E	CB	16	BD	FB	48

Таблица 23

Показатели случайности S-блока Лабиринт

Количество циклов	5
Количество инверсий	17043
Количество возрастаний	127
Максимум таблицы XOR	4
Количество максимумов XOR	255
Максимальное отклонение XOR	0,103391
Максимум таблицы LAT	16
Количество максимумов LAT	1275
Максимальное отклонение LAT	0,075786

Таблица 24

Закон распределения элементов таблиц XOR и таблицы LAT S-блока Лабиринт

Элемент	Плотность элемента в таблицах	
	XOR	LAT
0	32640	4080
2	32130	12240
4	255	9180
6	0	10200
8	0	8670
10	0	6120
12	0	9180
14	0	4080
16	0	1275

В таблице 25 и таблице 26 представлены для сравнения показатели совершенных по рассматриваемым критериям подстановок.

Таблица 25

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	0,00160149
10	10	0,000160795
12	1	0,000013454

В работе [9] для проверки соответствия эмпирического распределения теоретическому распределению предлагается воспользоваться критерием согласия Колмогорова [10], который позволяет решить поставленные задачи путем сравнения теоретического интегрального закона распределения вероятностей $F(x)$ (с известными параметрами) с эмпирическим законом распределения вероятностей $F_n(x)$, полученным на входе вычислительного эксперимента.

Статистический критерий согласия Колмогорова, как известно, применяется для проверки простой и параметризованной гипотезы H_0, соответственно которой одинаково распределенные случайные величины X_1, X_2, ..., X_n имеют заданную непрерывную функцию распределения $F(x)$, причем альтернативная гипотеза H_1 предполагается двухсторонней:

$$| EF_n(x) - F(x) | > 0,$$

где EF_n – математическое ожидание функции эмпирического распределения $F_n(x)$. Критическое множество критерия Колмогорова выражается неравенством:

$$D_n = \underset{|x|<\infty}{Sup} |F_n(x) - F(x)| > \lambda_n .$$

В случае справедливости гипотезы H_0 распределение статистики D_n не зависит от функции $F(x)$, причем, если $n \to \infty$, то

$$P\{\sqrt{n} D_n < \lambda\} \to K(\lambda), \quad \lambda > 0.$$

Здесь $K(x)$ – функция распределения Колмогорова, табличная.

Соответственно критерию Колмогорова гипотезу H_0 с уровнем значимости α, $0 < \alpha < 0{,}5$ стоит отбросить, если $D_n \ge \lambda_n(\alpha)$, где $\lambda_n(\alpha)$ – критическое значение критерия Колмогорова, которое соответствует заданному уровню значимости α и есть корнем уравнения $\{D_n \ge \lambda\} = \alpha$.

Для подстановок порядка 2^8 (параметр критерия Колмогорова $n = 255^2$) имеем

$$\frac{\lambda_0}{\sqrt{n}} = \frac{1{,}23}{255} = 0{,}00482 .$$

Таблица 26

Распределение переходов таблицы LAT для подстановки порядка 2^8

$\lvert 2k \rvert$	Число ячеек	Вероятность
0	6502	0,100097
2	12508	0,192818
4	11196	0,1756863
6	9982	0,1535101
8	7872	0,121061
10	5952	0,091534
12	4228	0,065021
14	2822	0,0433987
16	1768	0,0271895
18	1040	0,0159938
20	574	0,00882737
22	298	0,00229178
24	146	0,00458285
26	66	0,00101499
28	28	0,00043060
30	10	0,00015378
32	4	0,00006151
34	2	0,000030757

ВЫВОДЫ

Представленные в таблицах 2–25 результаты свидетельствуют, что практически все рассмотренные S-блоки, используемые в современных шифрах, не укладываются в рамки S-блоков случайного типа.

S-блоки шифров AES (GrandCru), ADE, Fox и Лабиринт не входят даже в допустимые границы (3.8). В эти границы укладываются показатели только S-блоки шифров Мухомор, Iceberg и близкие к ним по показателям S-блоки шифра Anubis (Khazad). Мы уже не говорим здесь о других показателях, которые получаются далекими от показателей совершенных подстановок. В результате удается ввести намного более жесткие, и вместе с тем практически реализуемые критерии отбора случайных подстановок, которые мы посчитали сначала полезными при поиске подстановок с высокими криптографическими показателями. Подстановки, удовлетворяющие самым жестким критериям случайности (и по комбинаторным показателям и по дифференциальным и линейным) предложено называть совершенными.

Мы надеялись, 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.

Однако проверка степени соответствия новым критериям отбора подстановочных конструкций некоторых известных современных шифров [5–7] показала, что практически все рассмотренные S-блоки, используемые в современных шифрах (S-блоки шифров Rijndael, Лабиринт, Мухомор (Калина), Iceberg, ADE, Камелия, GrandCry и Anubis (Khazad)и др.), не укладываются в рамки S-блоков случайного типа. S-блоки шифров AES (GrandCru), ADE, Fox и Лабиринт не входят даже в допустимые границы. В эти границы укладываются показатели только S-блоки шифров Мухомор, Iceberg и близкие к ним по показателям S-блоки шифра Anubis (Khazad). Мы уже не говорим здесь о других показателях, которые получаются далекими от показателей совершенных подстановок. Более того оказалось, что для обеспечения высоких криптографических показателей шифров совсем не требуются S-блоки со специальными свойствами.

С другой стороны, как показали исследования, свойства подстановок, совершенных по комбинаторным показателям и одновременно совершенным по дифференциальным и линейным показателям, оказались выполненными асимптотически практически для всех известных итеративных шифров.

Литература

[1] Долгов В.И. S-блоки для современных шифров / В.И. Долгов, Е.Д. Мельничук // Науково-технічний журнал «Радіоелектронні та комп'ютерні системи». – Х., 2012. – Вип. 171. – С. 121-133.

[2] Спецификация алгоритма шифрования «Калина-2», версия от 17.08.2012.

[3] Lisitskaya I.V. Importance of S-Blocks in Modern Block Ciphers / I.V. Lisitskaya, E.D. Melnichuk, K.E. Lisitsky // Internet Journal «Computer Network and Information Securuty». – Delhi., – 2012., – Vol. 10, P. 1–12.

[4] Лисицкая И.В. Большие шифры – случайные подстановки / И.В. Лисицкая, А.А. Настенко // Межведомственный научн. технический сборник. Радиотехника. – 2011. – Вып. 166. – С. 50–55.

[5] Лисицкая И.В. Дифференциальные свойства шифра FOX. / И.В. Лисицкая, Д. С. Кайдалов // Прикладная радиоэлектроника. – 2011. – Т. 10, № 2. – С. 122–126.

[6] Горбенко І.Д. Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікації. / І.Д. Горбенко, В.І. Долгов, и др.// Прикладна радіоелектроніка. – 2007. – Т.6. – № 2. – С. 195–208.

[7] Горбенко І.Д. Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація / І.Д. Горбенко, М.Ф. Бондаренко, В.І. Долгов, и др. // Прикладная радиоэлектроника. – 2007. – Том. 6, №2. – С. 147–157.

[8] Головашич С.А. Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. – Том. 6, №2. – С. 230–240.

[9] Олейников Р.В. Результаты анализа алгоритма шифрования ADE. /Р.В. Олейников, В.И. Руженцев, М.С. Михайленко, А.Б. Небывайлов // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2008. – Том. 7, № 3. – С. 210–214.

[10] Долгов В.И. Случайные подстановки в криптографии / В.И. Долгов, И.В. Лисицкая, К.Е. Лисицкий // Радиоэлектронные и компьютерные системы. – Харьков, НАУ ХАИ, 2010. – № 5(46). – С. 79–84 .

[11] Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся вузов. – М.: Наука, 1980. – 976 с.

Поступила в редколлегию 28.03.2013

Мельничук Евгений Дмитриевич, аспирант кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники. Научные интересы: криптография, методы криптоанализа.

УДК 621.3.06

Дослідження відповідності новим критеріям відбору підставних конструкцій сучасних БСШ / Є.Д. Мельничук // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 240–246.

Метою статті є вивчення питання про криптографічні значущості підстановок випадкового виду: наскільки застосовні в шифрах підстановки, відібрані за критеріями випадковості; чи дозволяють вони поліпшити криптографічні показники шифрів. Стисло викладається методика оцінки показників випадковості підстановок, наводяться результати аналізу S-блоків ряду сучасних шифрів на предмет оцінки близькості їх показників випадковості показниками випадкових підстановок.

Ключові слова: підстановка, лінійні показники стійкості, диференціальні показники.

Табл.: 26. Бібліогр.: 10 найм.

UDC 621.3.06

Research of correlation between the new selection criteria and substitutions of modern block ciphers / E.D. Melnichuk // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 240–246.

The purpose of this paper is to study the question of the significance of cryptographic random permutations of a new type: to what extent substitutions selected by randomness criteria are applicable to ciphers; whether the said substitutions allow to improve the performance of cryptographic ciphers. The paper briefly presents the methodology of performance assessment of random permutations and provides the results of analyzing S-blocks of a number of modern ciphers with respect to assessing the similarity of their performance randomness and the corresponding indicators of random permutations.

Keywords: substitution, linear stability indicators, differential resistance indices.

Tab.: 26. Ref: 10 items.