УДК 004:37

Белецкий А.Я.
Национальный авиационный университет, Киев, Украина

ТАБЛИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ ПРИМИТИВЫ НЕЛИНЕЙНОЙ ПОДСТАНОВКИ

DOI: 10.14308/ite000517

Классические примитивы нелинейной подстановки осуществляют простую замену каждого символа шифруемого текста на некоторый фиксированный символ того же самого алфавита, фактически реализуя преобразования одноалфавитного шифра простой замены. И как следствие – энтропия зашифрованного текста совпадает с энтропией исходного текста. В работе рассмотрены различные варианты рандомизации примитивов нелинейной подстановки, в результате которых достигается существенное повышение энтропии выходного текста, при этом шифрограмма приобретает свойства, близкие к свойствам белого шума.

Ключевые слова: *криптографический примитив, нелинейная подстановка, рандомизация.*

Введение и постановка задачи

Современные алгоритмы криптографической защиты информации (шифрование) представляют собою математические преобразования сообщений (входных текстов), рассматриваемых как определенным образом упорядоченные совокупности бинарных чисел (байтов), представленных в памяти компьютера с произвольным расширением [1]. Криптографическими преобразованиями «осмысленные сообщения» (входной или открытый текст) отображается в область «бессмысленных сообщений» (выходной или шифротекст, шифрограмма). С позиций теории сигналов зашифрование исходного (коррелированного, избыточного, сжимаемого) текста состоит в его «отбеливании». Процесс отбеливания сообщения заключается в обращении шифруемого текста в некоррелированную последовательность (0, 1)-элементов шифрограммы (практически несжимаемой) с плотностью распределения элементов выходного алфавита максимально близкой к равномерному распределению.

Для целей отбеливания сообщения прибегают к итерационным многораундовым преобразованиям исходного текста совокупностью криптографических примитивов, как это осуществляется, например, в блочных симметричных шифрах. Использование нескольких раундов обусловлено необходимостью обеспечения алгоритмам шифрования перемешивающих свойств.

К настоящему времени устоявшимся является положение, согласно которому криптографически стойкие алгоритмы шифрования должны включать, по крайней мере, хотя бы один примитив нелинейной подстановки, именуемый также как узел нелинейной замены или S-блок (S-box от Substitution-box). Если шифрование сводится к преобразованию исходного текста произвольным числом только линейных примитивов, то все они могут быть представлены одним эквивалентным оператором линейного преобразования, что существенно упрощает задачу взлома шифрограммы и снижает криптостойкость алгоритма.

Нередко именно примитивы нелинейной подстановки (ПНП) оказываются единственными примитивами, определяющими нелинейность шифрующего преобразования и уровень стойкости современных блочных алгоритмов (Rijndael [2], Camellia [3], DES [4] и др.) к разнообразным криптоаналитическим атакам.

Существует множество разнообразных критериев оптимальности S-блоков, таких, например, как: критерии нелинейности и распространения, максимума спектра автокорреляции, корреляционного и алгебраического иммунитета, строгого лавинного эффекта и др. [5, 6]. Кстати, отметим, что S-блок AES шифра не удовлетворяет большинство из перечисленных выше критериев оптимальности [7]. И, тем не менее, это не вызывает каких-либо сомнений относительно криптостойкости данного ПНП, как и шифра в целом.

Произвольные нелинейные подстановки (НП) могут быть отображены, по крайней мере, в трех различных формах: алгебраической нормальной форме, над полем $GF(2)$ и в виде таблицы замены [5]. Узлы нелинейной замены в современных блочных шифрах строят, как правило, на основе именно табличного представления. Обоснованием такого подхода к построению ПНП служат не только простота описания алгоритма преобразования, но и практически подтвержденная криптографическая стойкость табличного S-блока, используемого, например, в самом популярном симметричном блочном шифре XXI века – AES шифре.

Одним из актуальных и перспективных направлений развития современной криптографии является разработка алгоритмов шифрования на основе так называемого *динамического хаоса* (*dynamic chaos*) [8-10]. Суть динамического хаоса состоит в таком явлении, при котором поведение нелинейной системы выглядит случайным, несмотря на то, что оно определяется детерминистическими законами [11]. В криптографии, например, таковыми могут быть S-блоки. Детерминизм хаоса гарантирует обратимость преобразований, обязательных для алгоритмов шифрования информации, а его случайность придает криптографической системе повышение стойкости к взлому.

Компьютерная реализация табличных форм S-блоков предполагает, во-первых, что таблица замен содержит $N = 2^m$ элементов ($m-$битных чисел), принимающих значение в интервале от 0 до $N-1$, причем $m-$натуральное число, совпадающее с числом двоичных разрядов, посредством которых задается адрес расположения в таблице нелинейно преобразованных входных данных. В частности, для AES шифра $m = 8$, т.е. осуществляется подстановка типа «байт в байт». И, во-вторых, S-блок выполняет *биективное* (взаимно-однозначное) отображение множества N входных целых чисел $x = \{0,1,\ldots,N-1\}$ во множество N выходных чисел $y \in \overline{0, N-1}$. Из второго свойства следует, что в такой форме S-преобразование не приводит к изменению энтропии Шеннона-Колмогорова выходной последовательности H_{out} по сравнению с энтропией входной последовательности H_{in}, т.е. соблюдается равенство $H_{\text{out}} = H_{\text{in}}$.

Основная задача, которая ставится в данной статье, состоит в разработке таких способов формирования AES-подобных (табличных, по схеме 8x8) примитивов нелинейной подстановки, которые за счет рандомизации, являющейся разновидность динамического хаоса, вызывают увеличение энтропии преобразуемого сообщения, т.е. обеспечивают неравенство $H_{\text{out}} > H_{\text{in}}$.

1. Понятийно-терминологические определения и базовые характеристики S-блоков Уточним, прежде всего, понятие «рандомизированного примитива НП».

Определение 1. *Рандомизированным примитивом нелинейной подстановки будем называть такой примитив, в котором один или несколько шагов вычислений основаны на случайном выборе правила выполнения примитива.*

Предлагаемое определение рандомизированного примитива опирается на определение *рандомизированного алгоритма* (*randomized algorithm*), приведенное в [12].

Одним из важнейших показателей качества преобразования $y = f(x)$ в примитивах НП является корреляционная зависимость (корреляция), отображающая статистическую взаимосвязь величин x и y. Принято считать, что чем меньше эта зависимость, тем лучшими свойствами перемешивания (битов, байтов или других конструктивов входного текста) обладает примитив.

Для графического представления корреляционной связи можно использовать прямоугольную систему координат с осями, которые соответствуют обеим переменным. Каждая пара значений переменных x, y маркируется при помощи определённого символа (точки). Такой график называется *диаграммой рассеяния* (ДиР) или *диаграммой разброса, точечной диаграммой, полем корреляции* (*scatterplot*) [13]. Диаграмма рассеяния ПНП алгоритма Rijndael приведена на рис. 1.

Математической мерой корреляции величин x и y диаграммы рассеяния ПНП служит коэффициент корреляции (*correlation coefficient*) r, определяемый соотношением

$$r = \sum_{i=0}^{255} \dot{x}_i \cdot \dot{y}_i \Bigg/ \sqrt{\sum_{i=0}^{255} \dot{x}_i^2 \cdot \sum_{i=0}^{255} \dot{y}_i^2}\,, \qquad (1)$$

где $\dot{x}_i$ – центрированные и нормированные независимые переменные x диаграммы (рис. 1), т.е.

$$\dot{x}_i = (x_i - 127.5)/255, \quad i = \overline{0, N-1}.$$

Аналогичным образом вычисляются также переменные $\dot{y}_i$.

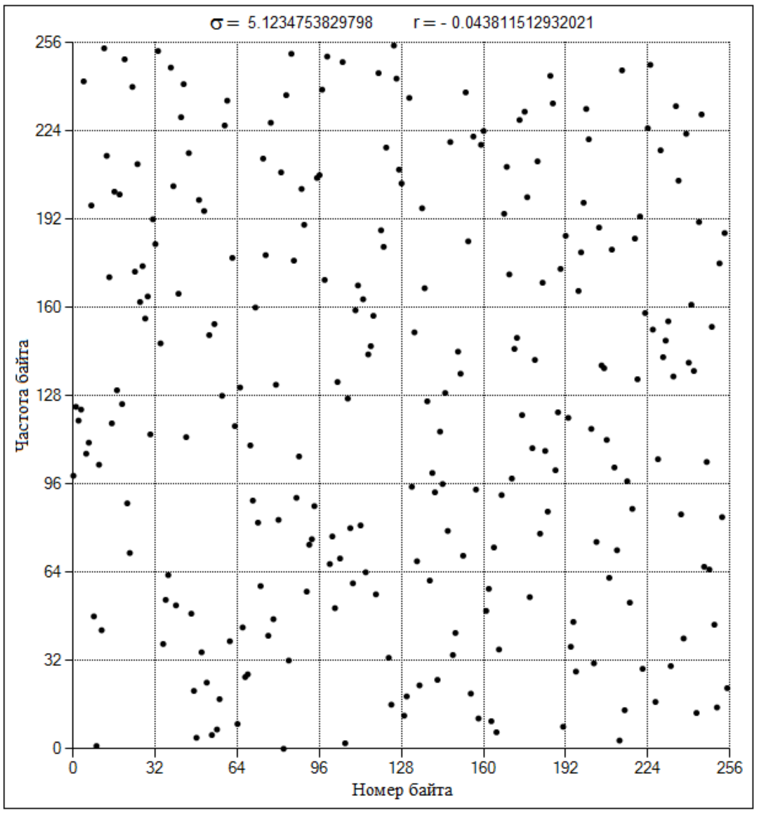

Рис. 1. Диаграмма рассеяния примитива нелинейной подстановки алгоритма Rijndael

Рассчитанный по формуле (1) коэффициент корреляции параметров x и y диаграммы рассеяния ПНП оказался достаточно малым, равным -0.0438, что дает возможность вынести заключение о слабой корреляционной зависимости этих дискретных величин.

Из визуального осмотра точечной диаграммы можно вынести качественное суждение о равномерности распределения точек x, y на плоскости рассевания. Введем оценку количественной меры равномерности рассеяния. С этой целью разобьем всю поверхность диаграммы на 64 квадрата, как это показано на рис. 1. Подсчитаем число $n_{i,j}$, $i, j = \overline{0,7}$, точек, попавших в квадраты. Если точка x, y расположена на нижней или левой стороне квадрата, то она считается принадлежащей этому квадрату, и в противном случае – не принадлежащей данному квадрату. «Идеально равномерным» будет такое распределение, когда в каждый квадрат диаграммы рассеяния попадает по четыре точки.

В качестве математической меры равномерности рассеяния σ примем нормированное среднеквадратическое отклонение (СКО) значений случайной величины $n_{i,j}$ относительно её математического ожидания, равного четырем, т.е.

$$\sigma = \frac{1}{8}\sqrt{\sum_{i=0}^{7}\sum_{j=0}^{7}\left(n_{i,j}-4\right)^2}\,. \tag{2}$$

В идеальном варианте r и σ равны нулю. Для примитива алгоритма Rijndael $r = -0.0438$ и $\sigma = 5.1235$ (приведены сверху ДиР на рис. 1).

2. Базовые аналоги примитива

В качестве базовых аналогов примитивов нелинейной подстановки будем рассматривать AES-подобные примитивы [14]. S-блок AES шифра реализует преобразование

$$y = x_f^{-1} \cdot A + \beta\,, \tag{3}$$

в котором $f = 100011011$ неприводимый полином восьмой степени; $A -$ циркулянтная матрица восьмого порядка

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix};$$

и байт $\beta = 01100011 -$ аддитивная компонента.

Логика работы S-блока отражена в 16-ричной табл. 1, в которой байт x соотношения (3) определяется конкатенацией старшего x_2 и младшего x_1 полубайтов.

Таблица 1.

Таблица замен S-блока алгоритма Rijndael

$x_2 \downarrow$ / $x_1 \rightarrow$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Тестовым входным файла выбран словарь В. Даля [15], объем которого составляет 17'390'588 байт. Распределение частот значений байтов словаря представлено в табл. 2.

Таблица 2

Распределение частот исходного текстового файла

dec	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]
[0]	283173	13	1730	227	2	0	799674	19768	49575	67	3378	162	0	1162	18283	608120
[16]	0	212	21429	9903	24	131	281	0	39396	333	458	0	0	0	25285	22816
[32]	4170	5767	0	31459	0	426	121	519707	9516	35416	0	513899	958	0	3955	41356
[48]	0	0	208541	8263	2149	0	16	0	0	0	474181	452	0	10294	0	39790
[64]	0	0	46996	442332	0	0	20	0	0	0	131333	54	1608	296	751	999510
[80]	182	202	0	27480	0	1259379	465	864	4	0	85	3722	0	4448	2	0
[96]	0	375153	1036	0	0	3515	0	0	0	31935	221466	0	0	9370	380	367499
[112]	6778	0	926351	0	0	150	0	4	0	0	2173	0	64076	207	0	0
[128]	7431	0	0	0	16796	101069	0	695	5261	0	0	2964826	0	0	2166	144
[144]	11416	6060	683	0	775052	0	331	962	0	0	0	0	0	0	19464	0
[160]	0	15535	40	56955	0	1280	254886	0	37489	0	0	327611	101	216	0	0
[176]	72	24	197818	0	0	0	0	389	0	687016	119	0	181844	164	49865	6252
[192]	32	6	0	13	5582	85	0	0	0	0	742	88	0	9440	0	237411
[208]	89	154	212	184	1645	536169	0	10821	247	5178	103752	0	368932	0	0	5324
[224]	1983	0	0	0	0	1031	318183	1401	42142	6490	0	643472	673	1251	1	0
[240]	48921	224	0	0	201909	19099	0	52474	254886	21503	7118	1854	3903	0	0	68

$\rightarrow x_1$

$\downarrow x_2$

Десятичное значение d байта (dec) определяется суммой чисел, находящихся в квадратных скобках строки x_2 (левая колонка табл. 2) и столбца x_1 (верхняя строка таблицы), т.е. $d=[x_2]+[x_1]$. Частота байта $p_d = p_{x_2+x_1}$ вписана в ячейку таблицы, расположенной на пересечении ее строки x_2 и столбца x_1. Например, $p_{101} = p_{96+5} = 3515$.

S-преобразование (3) осуществляет простую замену символа исходного алфавита на другой символ из того же самого алфавита. Это означает, в частности, что некоторый символ a, в какой бы области исходного текста он не находился, заменяется символом, например b, но при этом частота p_b символа b остается равной частоте p_a символа a. Как следствие подобной замены, приходим к известному результату, состоящему в том, что классическое S-преобразование сохраняет энтропию входного текста.

Энтропии входного текста и шифрограммы рассчитывались по формулам Шеннона-Колмогорова

$$H_1 = -\sum_{k=0}^{255} p_k \cdot \log_2 p_k \,, \tag{4}$$

– для файлов, рассматриваемых как последовательность байтов, и

$$H_2 = -\sum_{k=0}^{65535} p_k \cdot \log_2 p_k \,, \tag{5}$$

– для файлов, рассматриваемых как последовательность слов (двух байтных кодов), причем p_k в (4) есть относительная частота значений байтов, а в (5) – 16-битных слов; в обоих случаях эти значения (байтов или слов) определяются индексом при частоте p_k.

В табл. 3 сведены частоты байтов выходного текста (шифрограммы) при 16-битном S-преобразовании исходного (входного) текста.

Таблица 3

Распределение частот выходного текста при 16-битном S-преобразовании

→ x_1

dec	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]
[0]	13587	34068	86126	101397	104280	50235	59836	247377	26059	42375	5279	34074	10149	77774	97261	39146
[16]	64728	5528	60578	37095	47762	26323	62020	128462	3147	46344	54970	77340	82691	75320	68318	54813
[32]	12430	30254	120480	148131	59343	248088	139837	100700	9532	55856	3650	113649	86399	66485	57698	19800
[48]	44434	85218	13916	40710	21491	50078	84708	50007	80596	61344	39338	70559	13535	93114	44629	115230
[64]	79442	99983	17783	6517	41445	22590	21815	123513	65935	16393	20317	158162	58334	207919	8321	65245
[80]	33786	21469	386249	12532	104448	21415	4465	14217	483505	150315	109771	69773	22992	26578	34925	81001
[96]	55369	20607	33270	44612	88735	114600	56116	16750	46114	32052	26592	121592	10457	40624	34759	45746
[112]	9230	20090	10423	85820	45853	38473	11007	49123	20187	128959	94271	197092	21661	71989	120910	155348
[128]	82782	3843	74396	37164	16650	96276	48091	94146	74395	89180	51412	25927	16109	28999	102903	21158
[144]	69539	164731	69153	43389	131093	91937	16361	30307	21234	28477	152049	10049	53264	535132	101400	35393
[160]	15548	26423	52663	104863	25063	100992	12885	188788	110071	144968	80047	45922	71551	46303	59379	84120
[176]	42274	84386	76595	74114	57772	32423	43570	99130	23051	198720	3520	67200	57556	50694	12983	31700
[192]	31988	53905	64125	83555	99071	37596	77427	53759	48318	26378	31596	47779	67432	261540	5769	39612
[208]	11588	97382	69006	129874	193197	83616	15308	13371	25234	108250	13574	85981	82716	75878	124051	100528
[224]	49564	60326	34214	103950	78417	184098	26399	65285	101130	29105	71845	31027	39527	43487	46194	82465
[240]	13533	34073	116718	75222	140098	83630	89038	25960	24403	27031	28528	101721	70108	3925	113631	29032

↓ x_2

На основании данных, приведенных в табл. 3, приходим к таким заключениям. Во-первых, преобразования 16-битных слов исходного текста 16-битным S-блоком не приводит к изменению энтропии шифрограммы, что отвечает, как об этом было сказано выше, сути классического
S-преобразования. Во-вторых, переход от восьми битного S-блока, сохранявшего энтропию входного текста, равную 4.878793, к 16-битному S-блоку привел к увеличению энтропии шифрограммы, которая достигла значения 7.540047.

Данный эффект увеличения энтропии, наглядно прослеживаемый по табл. 2, может быть пояснен следующим образом. Предположим, что некоторое 16-битное слово c составлено конкатенацией двух байтов a и b, т.е. $c = a\square b$. Если входной текст преобразуется восьмибитным S-блоком, то каждому байту a и b ставятся в соответствие, например, байты a' и b'. При этом $H_{\text{out}} = H_{\text{in}}$. В том случае, когда исходный текст преобразуется 16-битным S-блоком, то слово c трансформируется в некоторое слово $c'' = a''\square b''$, причем байты a'' и b'', как правило, не совпадают с байтами a' и b'. Следствием 16-битного преобразования открытого текста является увеличение числа различных символов в шифрограмме, по сравнением с числом символов в открытом тексте, что и обуславливает рост энтропии шифрограммы, т.е. $H_{\text{out}} > H_{\text{in}}$.

3. Синтез обобщенных нелинейных подстановок

В статье [16], как и в монографии [14], высказано сомнение относительно того, что параметры f, A и β классического S-преобразования (3) являются оптимальными, полученными в результате тщательной и скрупулезной оптимизации. Подтверждением данному предположению может служить тот факт, что рассевающие свойства AES-подобных S-блоков, оцениваемые, по крайней мере, энтропией формируемых ими шифрограмм (или коэффициентом корреляции вход /выходных переменных блоков), оказываются не чувствительными к параметрам преобразования. Но для шифраторов специального назначения эти параметры, будучи переведенными в группу секретных параметров, могут выступать в качестве долговременных ключей, расширяя общую длину ключа шифрования, как это, например, принято частично в российском симметричном блочном шифре ГОСТ 28147-89 [17].

На основании визуального анализа диаграммы рассеивания ПНП алгоритма Rijndael (рис. 1) и таблицы замен S-блока этого алгоритма (табл. 1) выдвинем гипотезу о том, что совсем не обязательно при формировании таблиц замен придерживаться правила (3), или ему подобных, как, например, предложенному в [16], согласно которому

$$y = (x+\alpha)_f^{-1} \cdot A_{\omega,\varphi} + \beta, \tag{6}$$

где α и β – аддитивные компоненты, являющиеся произвольными двоичными векторами восьмого порядка; f и φ – неприводимые полиномы восьмой степени; и A – невырожденная матрица Галуа восьмого порядка, порождаемая образующим элементом ω и НП φ [18].

Суть гипотезы состоит в следующем.

Гипотеза. *В качестве таблицы T_S нелинейной подстановки S двоично-рационального порядка $N = 2^n$, где n – натуральное число, без ущерба для стойкости шифра может быть выбрана произвольная стохастическая таблица T, удовлетворяющая выбранным граничным условиям.*

Определение 2. *Стохастической будем называть таблицу T, составленную из $N = 2^n$ случайным образом переставленных $n-$битных чисел, первичная совокупность которых упорядочена в порядке возрастания от $00\ldots0$ до $11\ldots1$.*

Порядок N таблицы замен T_S, как и стохастической таблицы T, совпадает с числом элементов ($n-$битных векторов) таблицы. Таблицы T_S могут быть представлены в двух формах: в виде одномерного, или двумерного массивов. Алгоритм синтеза таблицы T_S соответствует одной из простейших моделей теории вероятности – *урновой схеме* проведения эксперимента (испытаний) с извлечением шаров *без возвращения*.

Приведем описание урновой схемы: рассматривается некоторая урна, содержащая N шаров, перенумерованных от 0 до $N-1$. После перемешивания из урны наугад извлекается один из N шаров и его номер $n-$битным кодом записывается в нулевую ячейку T_S таблицы. Затем одним из $N-1$ способов из урны извлекается второй шар, номер которого записывается в очередную ячейку таблицы. По окончании испытаний все N ячеек таблицы T_S оказываются заполненными в случайном порядке $n-$битными числами от 0 до $N-1$. Общее количество выборок (перестановок) L_N в схеме урн без возвращения определяется формулой $L_N = N!$

Естественно, что в результате машинного синтеза могут быть получены *слабые стохастические* таблицы T. К «слабым» будем относить, например, таблицы, в ячейках которых числа размещены строго в порядке возрастания или убывания, т.е. на диаграмме рассеивания точки размещаются на главной или вспомогательной диагоналях диаграммы. Существует большое число и других слабых стохастических таблиц.

Для того чтобы иметь возможность отсеять слабые таблицы T необходимо ввести математические критерии (параметры), на основании которых можно осуществлять фильтрацию стохастических таблиц. В качестве таких параметров выберем коэффициент корреляции $r_{\text{т}}$ и СКО $\sigma_{\text{т}}$, рассчитываемые для диаграммы рассеивания ПНП по формулам (1) и (2) соответственны. Примем значения $\hat{r} = 0.0438$ и $\hat{\sigma} = 5.1235$, ранее вычисленные для S-блока Rijndael шифра, в качестве граничных значений.

Для того чтобы таблица T могла быть принята в качестве таблицы нелинейной подстановки T_S, необходимо и достаточно совместного выполнения двух граничных условий:

$$|r_T| \le \hat{r} \quad \text{и} \quad \sigma_T \le \hat{\sigma} \tag{7}$$

Если хотя бы одно условие (7) не выполняется, то таблица T отбраковывается.

На рис. 2 приведен пример диаграммы рассеяния одного из приемлемого варианта 256-байтного S-блока табличного ПНП, синтезированного на компьютере по критериям (7).

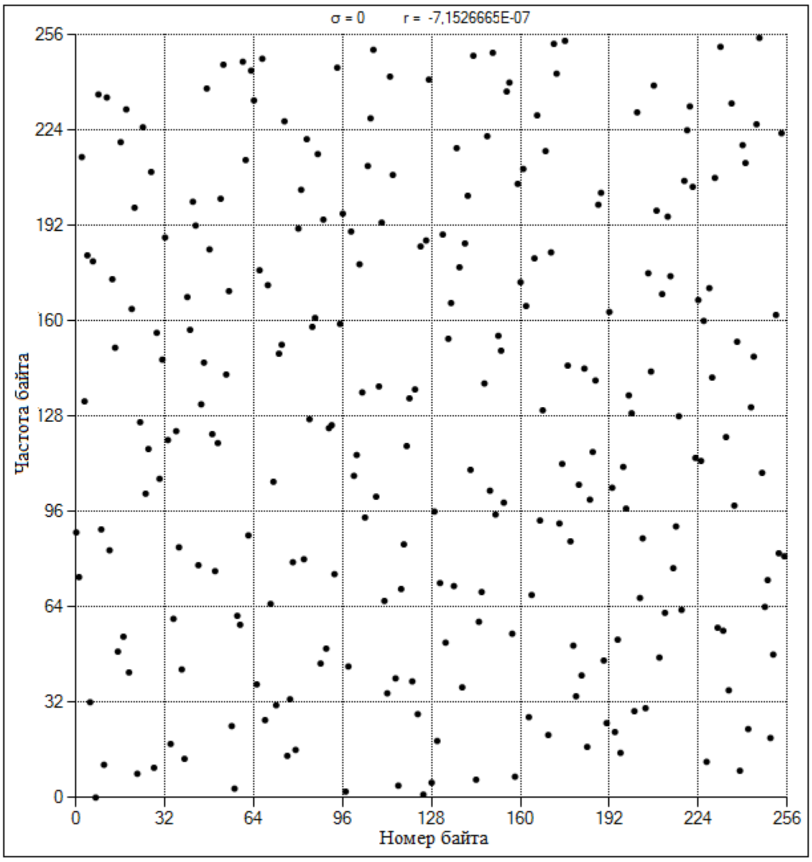

Рис. 2. Диаграмма рассеяния синтезированного примитива нелинейной подстановки

Как следует из рис. 2 в каждой клетке диаграммы оказалось ровно по четыре точки, обеспечивая СКО $\sigma = 0$, к тому же коэффициент корреляции $r = -7.156665E-07$ является достаточно малым, что свидетельствует о хороших свойствах рассеивания, доставляемых синтезированным табличным примитивом нелинейной подстановки.

4. Обобщенный алгоритм рандомизации ПНП

Основная идея рандомизации восьмибитных AES-подобных табличных примитивов НП состоит в следующем. Пусть $x -$ входной байт, которому соотношениями (3) или (6) ставится в соответствие байт y, извлекаемый из таблицы S-блока по адресу x.

Отобразим данное нелинейное преобразование соотношением

$$y = S(x), \tag{8}$$

в котором $S -$ оператор табличного отображения x в y.

Обобщенный алгоритм рандомизации ПНП представим в таком виде

$$y = S\left(\langle x + c \rangle\right), \tag{9}$$

где $c -$ управляемое по тому или иному закону смещение адреса x, а $\langle z \rangle = z (\bmod 256)$.

В штатном режиме (8) если в пределах одного или нескольких блоков шифруемого текста входной байт x сохраняет свое значение, то при каждом обращении к S-блоку последний вырабатывает одно и то же значение отклика y. И, как следствие однозначности преобразования, энтропия шифрограммы H_{out} оказывается равной энтропии H_{in} входного текста.

Картина существенно меняется в режиме рандомизации (9). В самом деле, рассмотрим некоторый входной байт x_k равный x, т.е. $x_k = x$, а соответствующее ему смещение $c = c_k$. По адресу $A_k = x_k + c_k = x + c_k$ из таблицы S-блока извлекается байт $y_k = S(x + c_k)$. Предположим далее, что $l-$й входной байт x_l также оказался равным байту x_k, т.е. $x_l = x$, тогда как смещение $c_l \neq c_k$. Теперь уже адресом $A_l = x_l + c_l = x + c_l$ из таблицы S-блока извлекается байт $y_l = S(x + c_l)$, не совпадающий с байтом y_k.

В предлагаемой схеме ПНП возрастает мощность (число различных символов) алфавита шифрограммы по сравнению с мощностью алфавита входного текста, что и приводит к росту энтропии шифрограммы, образуемой рандомизированным ПНП. В этом и состоит основная суть рандомизации примитива НП.

5. Равномерно линейная рандомизация

Идея базового метода *равномерно линейной рандомизации* (РЛР) табличного примитива НП (условно обозначим модель РЛР символом B) достаточна простая.

Пусть схема преобразования (9) организована так, что при каждом обращении к S-блоку смещение c увеличивается на 1. Тем самым обеспечивается подстановка

$$y_k = S(x_k + k), \quad k = 0,1,2,... \tag{10}$$

в которой смещение $c = k$.

Схема замен РЛР (10) обладает такой особенностью: при повторном обращении к S-блоку одним и тем же входным байтом x из таблицы извлекается байт y', отличный от байта y, являющийся откликом S-блока на первое обращение x.

Пусть стартовое смещение и входной байт равны c_0 и x соответственно. Обращаясь к таблице S-блока по адресу $A_0 = x + c_0$, извлекаем из нее значение $y_0 = S(A_0) = b0$. Затем увеличиваем смещение c на 1, вычисляя $c_1 = c_0 + 1$. Предположим, что и на этом шаге преобразования входной байт остался прежним и равным x, но теперь уже обращаемся к S-таблице по адресу $A_1 = x + c_1$ и извлекаем из нее другое значение $y_1 = S(A_1) = b1$. Видим, что одно и то же значение входного байта x заменено разными значениями отклика S-блока y.

Возможны два варианта построения базовой рандомизации блочных шифров. Пусть, для примера, длина блока шифра составляет 128 бит. Обозначим условно через C1: 0, 1,…, 15 – смещения в 1-м 128-битном блоке (16 байт), через C2 – смещения во 2-м блоке и т.д.

Вариант 1 ($B1$): C2 = C3 = C4 =…= C1;

Вариант 2 ($B2$): C2 = 16, 17, …, 31; C3 = 32, 33, …, 47 и т.д.

Назовем вариант $B1$ вариантом *автономного формирования смещения* адресов обращения к таблице S-блока табличного ПНП ($A-$смещением), а $B2$ – вариантом формирования смещения с *накоплением* ($H-$смещением).

Сопоставим таблицы распределения частот шифрограммы словаря В. Даля объемом 17'390'588 байт, сформированных вариантами рандомизации $B1$ и $B2$ ПНП (табл. 4 и 5 соответственно), полагая, что размер шифруемых блоков составляет 128 бит.

Из сопоставления табл. 4 и 5 следует, что вариант $H-$смещения доставляет большую равномерность рассеивания частот символов, чем $A-$смещение, что вполне очевидно.

В табл. 6 приведены оценки энтропии H и среднеквадратического отклонения σ распределения частот байтов шифрограмм словаря, образованных перечисленными в табл. 3 и 4 вариантами S-преобразования. Согласно приведенным параметрам шифрограмм следует, что вариант рандомизации $B2$, которому фактически соответствует размер блока шифрования, совпадающий с размером входного файла, доставляет как максимум энтропии выходного файла, так и минимум СКО распределения частот шифрограммы.

Таблица 4

Распределение частот шифрограммы словаря В. Даля
(вариант В1 рандомизированного S-преобразования)

dec	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]
[0]	143607	2627	0	15429	2593	11378	244	2353	66601	0	17362	1002	150	363990	215	10
[16]	0	20491	3209	4491	65614	143970	2917	366498	17	486361	63919	5550	11322	111	321875	25000
[32]	6	0	104	0	144372	11125	4466	7	0	360383	32584	1991	3258	206659	6424	66788
[48]	11229	0	14965	64612	4589	22697	275392	60137	4476	246513	142808	3825	163	1993	18187	2691
[64]	4783	458541	202392	0	11186	82180	226425	832	113	66712	16	730	24937	179	0	4637
[80]	85875	271	316269	3208	65852	408471	34105	0	1349	20643	0	13100	27350	837	113	9
[96]	408225	143756	485365	4687	8	67106	0	113958	0	27718	162639	151	19695	0	13407	5
[112]	11305	67238	4135	3	3222	1605	67125	84461	26325	144	837	112938	1511	24749	0	0
[128]	11275	513815	5586	12	4117	4047	285756	11015	0	795	19909	11128	0	11	3010	180507
[144]	9925	144153	15	183605	347650	64036	0	4562	0	4572	225	716	146510	379319	2626	2719
[160]	2557	2776	416052	0	11105	2547	463006	2011	0	3142	511464	225	177	22347	24019	67592
[176]	0	92216	510142	210545	4564	66556	12	0	0	11	205	210679	3025	7093	0	3613
[192]	4622	92501	11276	143952	0	12631	0	4609	241016	4674	264	2557	9799	73220	3354	70076
[208]	26926	230	4097	17	143238	148429	147156	2764	0	110	2497	145185	530191	3299	109	16402
[224]	99	4204	214259	26180	10	240	173	2498	29119	206	26035	2573	66563	0	537124	4850
[240]	2931	743	8364	22800	50449	11110	457780	31644	126	1262	146608	3358	5484	0	105	126027

$\rightarrow x_1$

$\downarrow x_2$

Таблица 5

Распределение частот шифрограммы словаря В. Даля
(вариант В2 рандомизированного S-преобразования)

dec	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]
[0]	64080	63929	63604	64315	63860	64398	63922	64190	63909	63964	63715	63897	64033	64112	64184	63878
[16]	64080	63964	63918	64280	64284	64015	64227	63691	64151	63829	64061	63755	64052	63722	64090	64406
[32]	63605	64084	64118	63970	63682	63990	64280	63639	64096	63594	64017	63972	63915	63589	63954	63592
[48]	64068	64043	63860	63986	63928	63642	63995	63528	64103	64037	64300	63766	63824	63942	64375	64207
[64]	63921	64033	63452	64345	64257	63933	63956	64106	64720	63986	63577	63810	64214	64295	64380	64102
[80]	63958	63950	63752	64040	64075	63569	63969	64431	64038	63681	63760	63646	64172	64024	64116	64012
[96]	64344	63808	64500	64244	63854	64023	64207	64081	63723	63889	63950	63825	63904	63805	64019	64163
[112]	63818	64328	63861	63633	63671	64089	64095	64057	64314	63806	64283	63560	64576	63837	63811	63895
[128]	64024	63965	63567	64039	64344	64044	64107	63860	64020	64042	63926	64290	64071	63883	64041	63713
[144]	64150	64197	63556	64421	64242	64345	64102	63911	64277	63712	63785	63978	63876	64603	63697	64439
[160]	63858	63922	63508	63756	63999	63906	63887	64170	64229	64281	64244	63982	63978	64280	63570	63894
[176]	63864	63791	64632	64273	64249	64133	63707	63932	63792	64052	64248	64148	63776	63960	63678	64268
[192]	64262	63930	64288	64269	64116	64150	63690	64136	63834	64209	64034	63920	63593	64210	63994	64077
[208]	63938	64019	64058	64052	63815	63656	64059	63855	63805	64026	63662	64191	63705	63950	64251	63978
[224]	63881	63987	64038	63668	64019	63558	64225	63989	63814	64071	63541	64360	63640	63915	63839	64572
[240]	63858	64391	63959	64033	63698	63901	63845	63933	64027	64000	64275	64126	64133	64100	63701	63713

$\rightarrow x_1$

$\downarrow x_2$

Таблица 6

Параметры шифрограмм

Вариант	Энтропия (H)	СКО (σ)
$B1$	6.195878	486.2178
$B2$	7.999990	0.9362

6. Однотабличная рандомизация

В дополнении к базовым алгоритмам рандомизации ПНП, обозначенным в разделе 5, как варианты $B1$ и $B2$, рассмотрим альтернативный способ однотабличной рандомизации (ОТР).

Суть альтернативного метода рандомизации ПНП (модель алгоритма рандомизации обозначим символом T) состоит в следующем. В любом блочном алгоритме, например, в шифре Rijndael, кроме таблицы замен прямого S-блока (табл. 1) присутствует таблица замен инверсного S-блока, которую обозначим $\bar{\mathrm{S}}$ (табл. 7).

Таблица 7

Таблица замен инверсного S-блока шифра Rijndael

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

$\rightarrow y_1$

$\downarrow y_2$

Воспользуемся табл. 7 для формирования смещения s адресов обращения к S-блоку, представленному табл. 1, следующим образом. Пусть $\bar{S}(k)-$ содержимое $k-$й ячейки инверсного S-блока (табл. 7). Нелинейное преобразование входных байтов x_k может выполняться по одной из двух схем:

$$y_k = \begin{cases} S\left(\Box x_k + \bar{S}(k)\Box\right); & (11) \\ S\left(x_k \oplus \bar{S}(k)\right), & (12) \end{cases} \quad k = 0,1,2,\ldots$$

где $\oplus-$ оператор поразрядного сложения байтов по $\bmod 2$ (операция XOR).

Преобразование (11) назовем арифметическим табличным рандомизированным преобразованием и обозначим символом ${}^{+}T$, а (12) – логическим табличным преобразованием, обозначив его символом ${}^{\oplus}T$.

Подобно блочным шифрам с базовыми рандомизированными ПНП, шифры с табличными подстановками ${}^{+}T$ и ${}^{\oplus}T$ также могут быть реализованы двумя способами: в виде вариантов с автономной рандомизацией ${}^{+}T1$ и ${}^{\oplus}T1$ ($A-$рандомизация), или вариантов рандомизации с накоплением ${}^{+}T2$ и ${}^{\oplus}T2$ ($H-$рандомизация).

Результаты компьютерной оценки энтропии H и среднеквадратического отклонения σ распределения байтов шифрограмм словаря В. Даля для всех перечисленных выше вариантов рандомизации табличных примитивов НП T приведены в табл. 8.

Таблица 8

Параметры шифрограмм

Вариант	Энтропия (H)	СКО (σ)
${}^{+}T1$	7.549561	205.87
${}^{\oplus}T1$	7.589824	194.84
${}^{+}T2$	7.999988	1.0375
${}^{\oplus}T2$	7.999989	0.9681

Как и для РЛР в схеме однотабличной рандомизации примитива нелинейной подстановки вариант организации смещения с накоплением обеспечивает более высокие показатели, как для энтропии шифрограмм, так и СКО распределений их частот по сравнению с соответствующими показателями автономного смещения.

7. Мультитабличная рандомизация

Суть мультитабличной рандомизации (МТР) состоит в том, что смещение c адреса A обращения к таблице S-блока в (10) определяется или арифметической суммой, или поразрядным сложением по $\bmod 2$ байтов, выбираемых из q, $q \ge 2$, различных таблиц подстановки U_1, U_2, …, U_q.

Обозначим условно модель мультитабличной рандомизации примитива нелинейной подстановки символом M_q, где индекс q указывает на число 256-байтных таблиц, которые задействуются в процессе вычисления смещения c. В частности, для варианта арифметического смещения имеем

$$c = \left[\sum_{i=1}^{q} U_i \right],$$

тогда как для варианта логического смещения

$$c = U^{[q]}\left(A\right) = \bigoplus_{i=1}^{q} U_i\left(A_i\right),$$

где $U^{[q]}$ – композиция из q таблиц подстановок и A – конкатенация восьмибитных адресов $A^{(i)}$,

$$A = A^{(q)} \,\|\, A^{(q-1)} \,\|\, \cdots \,\|\, A^{(2)} \,\|\, A^{(1)}, \tag{13}$$

которыми из таблиц U_i, $i = \overline{1, q}$, извлекаются компоненты $c^{(i)}$ смещения

$$c = c^{(q)} \oplus c^{(q-1)} \oplus \cdots \oplus c^{(2)} \oplus c^{(1)}. \tag{14}$$

Пусть A_0 – начальное значение $8q$ – битного адреса, которое может быть заполнено или нулями, или случайным набором бинарных чисел. На k – м шаге рандомизации адрес A_k переопределяется по формуле

$$A_k = \left[A_0 + k\right]_q, \quad [z]_q = z\,(\mathrm{mod}\ 2^{8q});$$

затем A_k разбивается на байты $A_k^{(i)}$, посредством которых из таблиц U_i извлекаются компоненты $c_k^{(i)}$ смещения

$$c_k = c_k^{(q)} \oplus c_k^{(q-1)} \oplus \cdots \oplus c_k^{(2)} \oplus c_k^{(1)}. \tag{15}$$

Как и в модели ОТР входные байты x_k могут быть преобразованы одним из двух способов

$$y_k = \begin{cases} S\left(\ x_k + c_k\ \right); & (16) \\ S\left(x_k \oplus c_k\right), & (17) \end{cases} \quad k = 0, 1, 2, \ldots,$$

в которых c_k определяются выражением (15).

Преобразование (16) назовем *арифметическим* МТР преобразованием и обозначим символом ${}^{+}M_q$, а (17) – *логическим* МТР преобразованием, обозначив его символом ${}^{\oplus}M_q$.

Подобно блочным шифрам с однотабличными рандомизированными ПНП, шифры с мультитабличными подстановками ${}^{+}M_q$ и ${}^{\oplus}M_q$ также могут быть реализованы двумя способами: в виде вариантов с автономной рандомизацией ${}^{+}M_q1$ и ${}^{\oplus}M_q1$, или вариантов рандомизации с накоплением ${}^{+}M_q2$ и ${}^{\oplus}M_q2$.

Частным вариантом МТР является *мультициклическая* $q-$табличная подстановка (МЦТП), которая сводится к таким преобразованиям. Обозначим модель мультициклической табличной подстановки символом MC_q. Пусть $q=2$ и $T1$, $T2-$ две различные 256-байтные таблицы подстановок, сформированные для варианта MC_2. В таком случае все нечетные байты входного текста преобразуются с помощью таблицы $T1$, а четные – с помощью таблицы $T2$. Предположим, что некоторый входной символ, например символ a, впервые появился в нечетной группе символов. Это означает, что он будет преобразован таблицей $T1$, порождая символ b. Очередной символ a совсем не обязательно окажется в нечетной группе. И если он принадлежит четной группе символов, то таблицей $T2$ будет преобразован в символ c. Следовательно, каждый символ входного текста подстановкой MC_2 приводит к появлению двух символов шифрограммы и, как следствие, подстановка MC_2 сопровождается увеличением энтропии выходного текста по сравнению с энтропией входного текста.

Результаты компьютерной оценки энтропии H и среднеквадратического отклонения σ распределения байтов шифрограмм словаря В. Даля для всех перечисленных выше вариантов M_q, MC_q и $N=128$ рандомизации мультитабличных примитивов НП значения H и σ приведены в табл. 9.

Таблица 9

Показатели шифрограмм

Вариант	$q=2$		$q=3$		$q=4$	
	H	σ	H	σ	H	σ
${}^{+}M_q1$	7.6144	195.50	7.5694	208.43	7.5781	199.26
${}^{\oplus}M_q1$	7.6582	180.06	7.5709	208.31	7.5928	202.10
${}^{+}M_q2$	7.9999	0.9927	7.9999	1.0586	7.9999	0.9436
${}^{\oplus}M_q2$	7.9999	0.9332	7.9999	1.0322	7.9999	0.9956
MC_q	5.7738	614.80	6.1804	512.45	6.5087	430.71

Из сопоставления показателей шифрограмм следует, что оба варианта способов формирования смещения (автономного или с накоплением) в МТР алгоритмах достаточно близки по статистическим характеристикам подстановок, тогда как МТЦП значимо уступает по аналогичным характеристикам алгоритмам МТР.

Отметим дополнительно такие особенности модели МТР. Во-первых, как следует из выражений (13) или (14) мультитабличная модель рандомизации ПНП обеспечивает длину цикла L формирования адреса A, как и повторения последовательности байтов смещения c, определяемую соотношением $L=2^{8q}$, в то время как в более простых моделях РЛР и ОТР длина повторения последовательности смещения составляет величину, равную 256. И, во-вторых, модель OTP является частным случаем (и это очевидно) модели MTP, если положить в ней параметр $q = 1$.

Наглядным подтверждением эффективности предлагаемого варианта примитива нелинейной подстановки может служить статистический портрет, построенный пакетом NIST STS v. 2.1.2 [19] на основании шифрограммы словаря В. Даля (рис. 3), для таких параметров мультитабличной рандомизации: число таблиц, задействованных для определения смещения – 4; режим смещения – с накоплением.

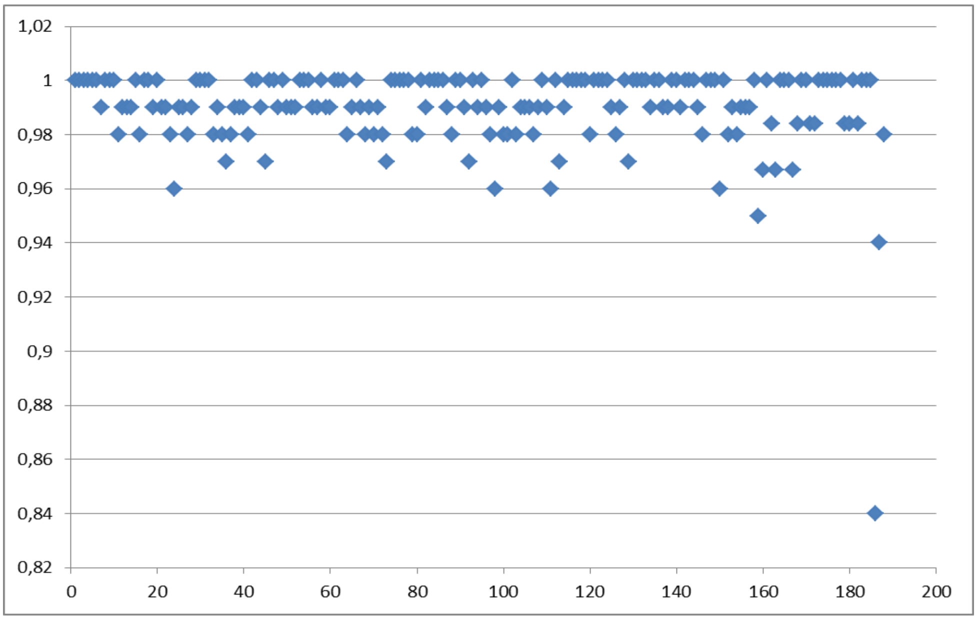

Рис. 3. Статистический портрет шифрограммы, образованной ПНП

Энтропия шифрограммы достигла значения $H = 7.9999888$, что является подтверждением достаточно высокого качества отбеливания входного текста.

Заключение

Проведенные исследования дают возможность сформулировать такие основные научные результаты. Во-первых, предложен новый способ формирования криптографических примитивов нелинейной подстановки, принципиально отличающийся от способа, который использован в самом популярном симметричном блочном AES шифре, основанном на алгоритме Rijndael. Суть предлагаемого способа построения S-блоков сводится к непосредственному стохастическому синтезу таблиц подстановки, диаграммы рассеяния которых обладают свойствами, максимально приближенными к свойствам «идеального» равномерного рассеяния. И, во-вторых, за счет достаточно простых методов рандомизации ПНП достигается эффект существенного увеличения энтропии текста на выходе рандомизированных примитивов по сравнению с энтропией входного текста и, как следствие, – увеличение криптостойкости шифра.

Отмеченное свойство, касающееся роста энтропии шифрограмм, порождаемых рандомизированными примитивами нелинейной подстановки, практически отсутствует во всех классических шифрах с табличными S-блоками. Примерами таких шифров могут служить шифры AES, ГОСТ и другие.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Харин Ю. С. Математические и компьютерные основы криптологии: Учебное пособие / Ю.С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич. – Мн.: Новое знание, 2003. – 382 с.
2. Daemen J., Rijmen V. The design of Rijndael. The AES – Advanced Encryption Standard. Springer-Verlag, Berlin, 2002.

3. Aoki K., Ichikawa T., Kanda M. at all. Camellia: A-128 Bit Block Cipher Suitable for Multiple Platforms. Nessie. September 26, 2000. – Режим доступа: http://www.cryptonessie.org
4. FIPS-46.3. Data Encryption Standards (DES). National Bureau of Standard, USA, 1993. – Режим доступа: csrc.nist.gov/publications/fips/fips46-3/ fips46-3.pdf
5. Казимиров А. В. Метод построения нелинейных узлов замены на основе градиентного спуска. / А. В. Казимиров, Р. В. Олейников // Радиотехника: Всеукр. межвед. научно техн. сб. – 2013. – Вып. 172: Информ. безопасность. – С. 104-108.
6. Логачев О. А. Булевы функции в теории кодирования и криптологии. / О. А. Логачев, А. А. Сальников, В. В. Ященко – М.: МЦМНО, 2004. – 470 с.
7. Olijnykov R. An Impact of S-box Boolean Function Properties to Strength of Modern Symmetric Block Ciphers / R. Olijnykov, O. Kazymyrov // Радиотехника, 2011. Вып. 116. – С. 11-17.
8. Kocarev L. Chaos-based cryptography: a brief overview // Circuits and Systems Magazine, IEEE. – 2001. Vol. 1. # 3. pp. 6-21.
9. Дмитриев А. А. Кодирование и передача информации на основе хаотических динамических систем с дискретным временем: Дис. на соиск. уч. степ. канд. физ.-мат. наук: 01.04.03: Москва, 2003. – 153 с. – Режим доступа: http: // www.dslib.net/radiofizika/kodirovanie-i-peredacha-informacii-na-osnove-haoticheskih-dinamicheskih-sistem-s.html#463251
10. Сидоренко А. В. Шифрование данных на основе дискретных хаотических систем и отображений. / А. В. Сидоренко, К. С. Мулярчик // Минск, Доклады Белорусского гос. ун-та информатики и радиоэлектроники, № 1 (71), 2013. – С. 61-67.
11. Динамический хаос. – Режим доступа: https://www.google.ru/?gws_rd=ssl#newwindow= 1&q =теория+динамического+хаоса+
12. Граничин О. Н. Рандомизированные алгоритмы в задачах обработки данных и принятия решений. / О. Н. Гаранин // Системное программирование. Вып. 6, 2012. – С. 141-162. – Режим доступа: http://www.math.spbu.ru/user/gran/ papers/10580575.pdf
13. [Электронный ресурс] – Режим доступа: http://vizualdata.ru/?go=all/chot-takoe-diagram-maras seivaniya-ili-scatterplot/
14. Зензин О. С. Стандарт криптографической защиты – AES. Конечные поля. / О. С. Зензин, М. А. Иванов. Под ред. М. А. Иванова. – М.: КУДИЦ-ОБРАЗ, 2002. – 176 с.
15. Даль В. И. Толковый словарь живого великорусского языка. [Электр. ресурс] – Режим доступа:http://royallib.com/book/dal_vladimir/tolkoviy_slovar_givogo_velikorussrogo_yazika
16. Белецкий А. Я. Программно-моделирующий комплекс криптографических AES-подобных примитивов нелинейной подстановки. / А. А. Белецкий, А. Я. Белецкий, Д. А. Навроцкий, А. И. Семенюк. // Захист інформації. Том 16, № 1. – 2004. – С. 12-22.
17. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – Режим доступа: http://protect.gost.ru/v.aspx?control 7=&id=139177
18. Белецкий А. Я. Примитивные матрицы Галуа в криптографических приложениях. / А. Я. Белецкий. // Захист інформації. Том 16, № 4. – 2004. – С. 274-283.
19. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications: SP800–22, Rev. 1a. National Institute of Standards and Technology, 2010. – 131 p. http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf

Стаття надійшла до редакції 06.03.15

Anatoly Beletsky
National Aviation University, Kiyv, Ukraine

THE TABULAR OF CRYPTOGRAPHIC PRIMITIVES OF NONLINEAR SUBSTITUTIONS

Classic primitives nonlinear substitution is a simple replacing each character encrypted text on a fixed symbol of the same alphabet, actually realizing the transformation one alphabet simple substitution cipher. And as a consequence - the entropy cipher text coincides with the entropy of the source text. The paper discusses the various options for randomization primitives nonlinear substitution in the results, those who achieved a significant increase in the entropy of the output text, with the cryptograms acquires properties similar to those of white noise.

Keywords: cryptographic primitive, non-linear substitution, randomization.

Білецький А. Я.
Національний авіаційний університет, Київ, Україна

ТАБЛИЧНІ КРИПТОГРАФІЧНИ ПРИМІТИВИ НЕЛІНІЙНОЇ ПІДСТАНОВКИ

Класичні примітиви нелінійної підстановки здійснюють просту заміну кожного символу тексту, що шифрується, на деякий фіксований символ того ж самого алфавіту, фактично реалізуючи перетворення одноалфавитного шифру простої заміни. І як наслідок - ентропія зашифрованого тексту збігається з ентропією вихідного тексту. В роботі розглянуті різні варіанти рандомізації примітивів нелінійної підстановки, в результаті яких досягається суттєве підвищення ентропії вихідного тексту, при цьому шифрограма набуває властивостей, близьких до властивостей білого шуму.

Ключові слова: криптографічний примітив, нелінійна підстановка, рандомізація.