УДК 681.3.06: 519.248.681

И.В. ЛИСИЦКАЯ, канд. техн. наук, А.С. КОРЯК

УТОЧНЕННЫЕ КРИТЕРИИ ОТБОРА ТАБЛИЦ ПОДСТАНОВОК С ЗАДАННЫМИ ХАРАКТЕРИСТИКАМИ СЛУЧАЙНОСТИ

В работах [1,2] предложены критерии отбора случайных таблиц подстановок, решающих задачу построения долговременных ключей для алгоритма шифрования ГОСТ 28147-89. Использование числовых конструкций типа подстановок характерно и для ряда других симметричных шифров. Конечно, при рассмотрении других шифров возникает необходимость вводить дополнительные ограничения и правила проверки [3]. Вместе с тем, по мере накопления опыта по применению, развиваемого в отмеченных работах подхода, появились дополнительные соображения и аргументы по обоснованию и уточнению некоторых параметров и правил отбора случайных таблиц подстановок, введенных ранее. В этой работе мы изложим ряд из сформулированных в [1] положений в новой редакции и с большей детализацией, а также приведем результаты статистического моделирования предлагаемых процедур отбора.

Напомним прежде всего, что под случайными здесь понимаются подстановки и таблицы подстановок, относящиеся к множеству наиболее вероятных случайных подстановок и случайных таблиц подстановок, и процедура проверки заключается в отбраковке подстановок и таблиц подстановок не входящих в это множество. Результаты анализа и статистических экспериментов по использованию критериев отбора, сформулированных в [1], говорят, однако, о том, что рассматриваемое в [1] множество допустимых подстановок и таблиц подстановок может быть расширено. Так в [4] показано (утверждается), что вполне приемлемыми характеристиками статистической безопасности обладают одно-цикловые подстановки и таблицы, составленные из одно-цикловых подстановок. Совершенно неоправданно исключать из рассмотрения и множество подстановок противоречивого типа [5]. Действительно, противоречивые подстановки, т.е. подстановки, не имеющие совпадающих элементов, должны считаться при составлении таблиц подстановок наиболее предпочтительными, так как они полностью исключают тождественные переходы (ситуации, когда подстановка как бы не участвует в криптографическом преобразовании). Более того, таблиц, составленных только из одно-цикловых или противоречивых подстановок, оказывается вполне достаточно, чтобы удовлетворить требованиям их использования в качестве секретных параметров шифров, как это требуется, например, для алгоритма ГОСТ 28147-89. Результаты проверки таких таблиц по критериям статистической безопасности [6] также полностью подтверждают эффективность их применения в алгоритмах симметричного шифрования. Отмеченное и побудило выполнить коррекцию введенных в [1] критериев отбора таким образом, чтобы расширить допустимое множество подстановок и таблиц подстановок за счет включения в него одно-цикловых, противоречивых и близких к ним подстановок. В этой работе излагается такая уточненная система критериев отбора случайных таблиц подстановок, рассматриваются расчетные соотношения, лежащие в их основе, и приводятся результаты статистической проверки случайных таблиц подстановок, полученных с помощью разработанного программного комплекса генерации долговременных ключей для шифра ГОСТ 28147-89.

Прежде всего, кратко напомним основные идеи подхода, развиваемого в [1].

Система (набор) из m различных подстановок n-ой степени $S_{n,m}$ (таблица подстановок) в дальнейшем записывается в виде расширения традиционного представления подстановки за счет добавления новых строк, т.е. в виде матрицы

$$S_{m,n} = \begin{bmatrix} 1 & 2 & 3 & \dots & n \\ i_{11} & i_{12} & i_{13} & \dots & i_{1n} \\ i_{21} & i_{22} & i_{23} & \dots & i_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ i_{m1} & i_{m2} & i_{m3} & \dots & i_{mn} \end{bmatrix} \qquad (1)$$

Верхняя строка называется нулевой, а остальные нумеруются от 1-ой до m-ой. Рассматривается задача построения некоторого заданного числа таких таблиц подстановок, которые удовлетворяют определенным критериям отбора (для шифра ГОСТ 28147-89 – $n = 16$, $m = 8$).

Предлагается использовать показатели и критерии проверки случайности трех уровней. На первом уровне проверяется соответствие показателей "случайности" отдельно взятой подстановки свойствам случайной равновероятной подстановки. Подстановки, прошедшие первый уровень проверки считаются уже подстановками случайного типа.

На втором уровне проверки оценивается соответствие характеристик случайности системы подстановок, попавших в таблицу, свойствам среднестатистической таблицы случайных подстановок. Таблицы подстановок, прошедших первые два уровня проверки, считаются случайными таблицами подстановок.

На третьем уровне осуществляется оценка степени подобия различных таблиц подстановок, из которых отбираются уже таблицы, выступающие в качестве системы (набора) долговременных ключей.

Соответствующие критерии отбора подстановок, таблиц подстановок и множеств таблиц подстановок названы критериями отбора первого, второго и третьего уровней.

Сущность уточненных правил, с помощью которых предлагается осуществлять отбор случайных таблиц подстановок, состоит в следующем.

Критерии отбора подстановок первого уровня, т.е. критерии отбора подстановок по индивидуальным характеристикам случайности формулируются, как и ранее в виде трех требований.

Требование 1.1. Число инверсий η_n в подстановке степени n должно удовлетворять условиям

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

Требование 1.2. Число циклов ξ_n в подстановке степени n должно удовлетворять условиям

$$\xi_n \le \ln n + a\sigma_\xi, \sigma_\xi = \sqrt{\ln n} .$$

Требование 1.3. Число возрастаний θ_n в подстановке степени n должно удовлетворять условиям

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

Здесь изменения коснулись только требования, определяющего допустимое число циклов. Двухстороннее ограничение в этом требовании заменено односторонним, что позволило включить в допустимое множество подстановок и одно-цикловые подстановки.

При формировании критериев отбора подстановок на втором уровне рассматриваются таблицы, составленные из подстановок, которые прошли первый уровень проверки. Предлагаемая методика строится на основе понятия противоречивости подстановок (числа несовпадений элементов).

Практически для каждой таблицы из m подстановок n-й степени формируется двумерный метрический "портрет", т.е. таблица определяется двумя "векторами".

В первом случае определяется конфигурация $(t_0, t_1, t_3, \ldots, t_n)$ совпадений элементов в $N_k = m \cdot (m-1)/2$ попарных декомпозициях строк этой таблицы подстановок. Элемент конфигурации t_i, $i = 1, 2, \ldots, n$ представляет собой число пар строк среди общего их числа N_k, которые имеют совпадающих элементов, так что $\sum_{i=0}^{n} t_i = N_k$. На множестве возможных исходов $\{t_0, t_1, \ldots, t_n\}$ определяется закон распределения вероятностей $P(t = i)$ для числа i совпадений элементов в паре равновероятных подстановок n-ой степени, $i = 0, 1, 2, \ldots, n$.

Во втором случае определяется конфигурация $(\varsigma_0, \varsigma_1, \varsigma_2, \ldots, \varsigma_{\lfloor m/2 \rfloor})$ совпадений элементов в столбцах таблицы. Здесь элемент конфигурации ς_s, $s = 0, 2, \ldots, \lfloor m/2 \rfloor$ – это число столбцов с s повторениями (в том числе и многократными) элементов столбца, при этом $\sum_{s=0}^{\lfloor m/2 \rfloor} \varsigma_s = n$. Затем на множестве возможных исходов $\left\{\varsigma_0, \varsigma_1, \varsigma_2, \ldots, \varsigma_{\lfloor m/2 \rfloor}\right\}$ определяется закон распределения вероятностей $P(\varsigma = s)$

для s повторений (в том числе многократных) различных элементов в столбце таблицы подстановок, $s = 0, 1, 2, \ldots, \lfloor m/2 \rfloor$. Здесь и ранее $\lfloor x \rfloor$ обозначает наибольшее целое число x, не превосходящее x.

На основе полученных законов распределения вероятностей для числа совпадений элементов по строкам и столбцам таблиц подстановок строится эталонный портрет случайной среднестатистической таблицы подстановок, и в дальнейшем осуществляется отбор таблиц подстановок по степени их близости к эталону (для ГОСТ эталонный метрический портрет имеет вид (2, 7, 6, 1, 0), (9, 11, 6, 2, 0, . . . , 0); для DES – это конфигурация (11, 5, 0) по столбцам и конфигурация (2, 3, 1, 0, . . ., 0) по совпадениям в парах строк).

Изменения для критериев для отбора таблиц подстановок на втором уровне коснулись некоторого уточнения самих правил проверки. Остановимся в связи с этим более подробно на идеях построения решающих правил, использованных ранее.

Напомним, что в работах [1,2] при построении правил отбора на втором уровне для оценки степени близости конфигурации совпадений в столбцах и строках проверяемой таблицы к эталонной был взят двухсторонний критерий Пирсона, основанный на использовании таблиц χ^2 распределения Стьюдента, для применения которого необходимо выполнить требования в отношении значений ожидаемых частот (они должны быть большими 10). Анализ показывает, что такие условия строго не выполняются для рассматриваемых в этой работе шифров. В этом случае, как отмечено в [7], предельное распределение χ^2, приведенное в соответствующих таблицах, как правило, не дает надежных результатов т.е. таблицами пользоваться не следует. Тем не менее, в [3] были приведены аргументы в пользу возможности применения в рассматриваемом случае критерия Пирсона и требования 5 и 6 в работе [1] построены именно на использовании критерия χ^2 в чистом виде.

В рассматриваемом случае предлагается отойти от применения критерия χ^2. Во первых, предлагается воспользоваться вместо двухстороннего критерия односторонним. Во вторых, – оценку близости конфигураций совпадений в строках и столбцах проверяемой таблицы подстановок к эталонной предлагается проводить не путем вычисления и сравнения величины χ^2 с граничным значением, а на основе непосредственного сопоставления числа совпадений элементов по отдельным их типам (разновидностям) в проверяемой таблице подстановок с модифицированной эталонной. При этом для включения в число допустимых таблиц подстановок предельного случая – латинских прямоугольников (таблиц, составленных из противоречивых подстановок) в обоих случаях разрешается максимально возможное число несовпадений.

В итоге требования по отбору таблиц подстановок на втором уровне проверки предлагается сформулировать в следующем виде:

Требование 2.1. (не обязательное) В таблицу подстановок должны входить подстановки, не имеющие совпадений с нулевой строкой (не имеющие циклов нулевой длины).

Требование 2.2. Подстановки, вошедшие в таблицу, должны по конфигурации $(t_0, t_1, t_3, \ldots, t_n)$ совпадений элементов в N_k попарных декомпозициях строк таблиц подстановок удовлетворять критерию $t_0 \le N_k$, $t_1 \le t'_1$, $t_2 \le t'_2$, . . . , $t_n \le t'_n$, где элементы конфигурации t_i, $i = 1, 2, \ldots, n$ представляет собой число пар строк из общего их числа N_k, которые имеют i совпадающих элементов (для ГОСТ 28147-89 модифицированный эталон – $(t'_0, t'_1, t'_3, \ldots, t'_n) = (28, 11, 6, 2, 0, \ldots, 0)$), при этом $\sum_{i=0}^{n} t_i = N_k$.

Требование 2.3. Подстановки, вошедшие в таблицу, должны по конфигурации $(\varsigma_0, \varsigma_1, \varsigma_2, \ldots, \varsigma_{\lfloor m/2 \rfloor})$ совпадений элементов в столбцах таблицы подстановок, удовлетворять критерию $\varsigma_0 \le n$, $\varsigma_1 \le \varsigma'_1$, . . . , $\varsigma_{\lfloor m/2 \rfloor} \le \varsigma_{\lfloor m/2 \rfloor}$, где элементы конфигурации ς_s, $s = 0, 2, \ldots, \lfloor m/2 \rfloor$ – это числа столбцов с s повторениями (в том числе и многократными) элементов столбца (для ГОСТ 28147-89 модифицированный эталон – $(\varsigma'_0, \varsigma'_1, \varsigma'_2, \varsigma'_3, \varsigma'_4) = (16, 7, 6, 1, 0)$), удовлетворяющие ограничению $\sum_{s=0}^{\lfloor m/2 \rfloor} \varsigma_s = n$.

При формировании критериев отбора таблиц на третьем уровне проверки используется идея наложения таблиц и подсчета числа совпадающих элементов. Для этого случая также рассчитан

теоретический закон распределения вероятностей для числа совпадений элементов в паре наложенных таблиц подстановок и определены его числовые характеристики.

В результате требования по отбору таблиц подстановок на третьем уровне проверки сформулированы следующим образом.

Требование 3.1. Множество таблиц подстановок, используемых в качестве долговременных ключей, должно при всех попарных наложениях таблиц давать число совпадающих элементов q удовлетворяющее условиям $q \le m + \sqrt{m}$.

При формулировке этого требования в отличие от [1] также использовано одностороннее ограничение по максимуму.

Требование 3.2. Можно запретить и совпадение строк, стоящих на различных позициях таблиц если потребовать в записанном выше правиле, что для каждой пары таблиц процедура наложения выполняется со всеми циклическими подстановками строк одной из них.

Приведем основные расчетные соотношения, определяющие правила и показатели отбора случайных таблиц подстановок на втором и третьем уровнях проверки.

Закон распределения вероятностей $P(t = i)$ совпадений i элементов в паре равновероятных подстановок n-ой степени (в паре наложенных строк таблицы подстановок), используемый в формулировке требования 2.2, выражается через известное в комбинаторике [8] число беспорядков D_{ni} в виде

$$P(t = i) = 1 - \frac{D_{ni}}{n!} = 1 - \frac{1}{i!}\sum_{k=0}^{n-i}(-1)^k \frac{1}{k!}, i = 1,2,...,n \qquad (2$$

и оказывается близким к биномиальному.

Расчеты, выполненные по формуле (2), при $n = 16$, $m = 8$ иллюстрирует таблица 1.

Таблица 1

Число совпадений t	Вероятность $P(t = i)$
0	0,3316
1	$3{,}79 \cdot 10^{-1}$
2	$2 \cdot 10^{-1}$
3	$6{,}76 \cdot 10^{-2}$
4	$1{,}57 \cdot 10^{-2}$
5	$2{,}69 \cdot 10^{-3}$
6	$3{,}53 \cdot 10^{-4}$
7	$3{,}59 \cdot 10^{-5}$
8	$2{,}9 \cdot 10^{-6}$
9	$1{,}77 \cdot 10^{-7}$
⋮	⋮

Итоговое выражение для определения вероятности $P(\varsigma = s)$ числа s различных повторяющихся (в том числе и многократно) элементов в столбце таблицы (1) получено в [2]. Мы здесь его напомним

$$P(\varsigma = s) = \sum_{k_1=0}^{\left\lfloor \frac{m-2s}{s} \right\rfloor} \sum_{k_2=0}^{\left\lfloor \frac{m-s(k_1+2)}{s-1} \right\rfloor} \sum_{\cdots} \cdots \sum_{k_s=0}^{m-s(k_1+2)-(s-1)k_2-(s-2)k_3-\ldots-2k_{s-1}} P_{2+k_1,2+k_1+k_2,\ldots,2+k_1+k_2+\ldots+k_s} \qquad (3$$

В этом выражении $P_{i,j,\ldots,l}$ – вероятности композиций совпадений по $i,j,\ldots,l$ различных элементов. Например, расчетное соотношение для вероятности $P_{i,j,\ldots,l}$ в случае $i = 2 + k_1, j = 2 + k_1 + k_2$ $l = 2 + k_1 + k_2$, имеет вид

$$P_{2+k_1,2+k_1+k_2,2+k_1+k_2} = \frac{C_m^{2+k_1} C_{m-2-k_1}^{2+k_1+k_2} C_{m-4-2k_1-k_2}^{2+k_1+k_2} (n-1)_{m-3k_1-3-2k_2}}{2!\cdot(n-1)^m}, \tag{4}$$

$$k_1 = 0,1,\ldots,\left\lfloor \frac{m-6}{3} \right\rfloor k_2 = 1,2,3,\ldots,\left\lfloor \frac{m-3(2+k_1)}{2} \right\rfloor.$$

Здесь $(n-1)_m$ – m-размещение из $n-1$ элементов

$$(n-1)_m = \begin{cases} (n-1)\ (n-2)\cdots(n-m-2), m \le n-1 \\ 0, m > n-1 \end{cases} \tag{5}$$

В таблице 2 представлен закон распределения вероятностей $P(\varsigma = s)$ для значений $n = 16$, $m = 8$, рассчитанный по формулам (2)-(4).

Таблица 2

Число повторений s	Вероятность $P(\varsigma = s)$
0	0,1012
1	0,4433
2	0,3843
3	0,0698
4	0,0014

Этот закон, как показывает анализ, достаточно точно аппроксимируется в дискретных точках отсчетами функции нормального распределения.

Комбинаторные соображения позволяют представить записать и итоговое выражение для вероятности $P_k^{(n,m)}$ совпадения k элементов в m строках пары наложенных друг на друга таблиц типа (1)

$$P_k^{(n,m)} = \sum_{\substack{\sum_{i=1}^{m} k_i = k \\ \sum_{j=1}^{s} l_j = m}} C_m(l_1, l_2, \ldots, l_s) \prod_{i=1}^{m} P(t = k_i). \tag{6}$$

В этом выражении k_i, – число совпадающих элементов в i-той (i = 1, 2, . . . , m) паре строк рассматриваемой таблицы (композиции $(k_1, k_2, \ldots, k_8)$); l_{ij}, – число одинаковых k_i j-го типа, т.е. значений k_i, имеющих одно и то же число совпадений j = 1, . . . , s, s – число различающихся наборов совпадающих значений k_i, ($s \le m$).

В (6) использовано также обозначение $C_m(l_1, l_2, \ldots, l_s)$ – полиномиальный коэффициент, который определяется следующим образом [9]:

$$C_m(l_1, l_2, \ldots, l_s) = \frac{m!}{l_1! l_2! \ldots l_s!}.$$

Очевидно, что для вероятностей $P_k^{(n,m)}$, $k = 0,1,\ldots,nm$ должно выполняться условие

$$\sum_{k=0}^{mn} P_k^{(m)} = 1.$$

Расчеты, выполненные по формулам (6) и (2), иллюстрируют таблица 3 и таблица 4. Вторая таблица отличается от первой тем, что при ее построении учитывалось выполнение требования 2.1 (в таблицу подстановок не должны входить подстановки, элементы которых совпадают с соответствующими элементами нулевой строки).

Изложенные выше подходы к формированию методов и критериев отбора случайных подстановок были положены в основу разработки программного комплекса генерации и сертификации долговременных ключей для алгоритма ГОСТ-28147-89.

Таблица 3

Число совпадений k	Вероятность $P_k^{(16,8)}$
0	0,000258
1	0,002205
2	0,009335
3	0,026139
4	0,054455
5	0.090033
6	0,123045
7	0,142967
8	0,144158
9	0,128141
10	0,101658
11	0,072701
12	0,047256
13	0,0288111
14	0,015394
15	0,007800
16	0,003672
17	0,001613
18	0,000663
19	0,000256
20	0,000093
21	0,000032
22	0,000010
23	0,000003
24	0,000001
25	0,000000
⋮	⋮
сумма	1,000000

Таблица 4

Число совпадений k	Вероятность $P_k^{(16,8)}$
0	0,000146
1	0,001336
2	0,006059
3	0,018178
4	0,040577
5	0,071879
6	0,105251
7	0,131027
8	0,141556
9	0,134815
10	0,114593
11	0,087805
12	0,061150
13	0,038975
14	0,022868
15	0,012414
16	0,006262
17	0,002947
18	0,001298
19	0,000537
20	0,000209
21	0,000077
22	0,000027
23	0,000009
24	0,000003
25	0,000001
⋮	⋮
Сумма	1,000000

Некоторые результаты статистической проверки процедур отбора случайных подстановок и случайных таблиц подстановок с заданными характеристиками случайности представлены в таблицах 5÷8.

В таблице 5, приводится пример обработки файла статистики при отбраковке подстановок на первом уровне проверки. Численные значения показателей случайности подстановок установлены соответственно равными: для инверсий – 49-71, для возрастаний – 7-9, для циклов – 1-5. В правой колонке таблицы приводится количество подстановок в процентах от их общего числа, попавших в установленные границы.

Таблица 5

Проверяемый показатель случайности	Попало в интервал в %
инверсий	66%
возрастаний	77%
циклов	99%
инверсий и возрастаний	53%
инверсий и циклов	66%
возрастаний и циклов	76%
инверсий, возрастаний и циклов	53%

Теоретическая оценка числа случайных подстановок для шифра ГОСТ 28147-89, прошедших границы, установленные в [1], выполнялась для асимптотически нормальных законов распределения вероятностей соответствующих параметров.

Напомним, что для вероятности события, заключающегося в том, что случайная величина x, распределенная по нормальному закону $p(x)$ с параметрами $m_x = 0$ и $\sigma_x^2 = 1$, попадет в интервал $|x| \le a$, справедливо соотношение

$$P(|x| \le a) = \int_{-\infty}^{\infty} p(x)dx = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{x^2}{2}} dx = 2\Phi(a) - 1.$$

Тогда, при $a = 1$ (для границ, установленных в эксперименте) имеем результат $P(|x| \le 1) = 0{,}6826$.

Если считать, что все три рассматриваемые случайные величины η_n, ξ_n и θ_n статистически независимы, то для вероятности порождения случайной подстановки, удовлетворяющей одновременно трем критериям случайности, можно получить оценку

$$P(\eta'_n \le 1,\ \xi'_n \le 1,\ \theta'_n \le 1) = (P(|x| < 1))^3 = 0{,}318.$$

Полученное расчетное значение достаточно близко повторяет результат таблицы 5. Заметим здесь, что более тщательные вычисления (уточнение пределов интегрирования, и др.), позволяют добиться еще более близкого подтверждения результатов эксперимента.

Что касается второго и третьего уровней проверки, то здесь представляет интерес задача определения потенциально возможного числа различных случайных таблиц подстановок (например, числа различных долговременных ключей для алгоритма ГОСТ 28147-89), которые можно сформировать при заданных значениях n и m.

Оценим сначала число таблиц подстановок, удовлетворяющих требованию 2.3.

Комбинаторные соображения позволяют для фиксированного "эталона" $(\varsigma'_0, \varsigma'_1, \varsigma'_2, \varsigma'_3, \varsigma'_4)$, записать формулу для общего числа различных допустимых по требованию 2.3. конфигураций совпадений элементов в таблицах подстановок по столбцам, в виде

$$N^{(n,\square)}\left(\varsigma'_0, \varsigma'_1, \ldots, \varsigma'_{\lfloor m/2 \rfloor}\right) = \sum_{\substack{\sum_{i=0}^{\lfloor m/2 \rfloor} k_i = n,\, k_i \le \varsigma'_i}} C_n\left(k_0, k_1, \ldots, k_{\lfloor m/2 \rfloor}\right).$$

Здесь уже k_i – число столбцов с i повторениями элементов в таблице подстановок, функция $C_n(k_0, k_1, \ldots, k_r)$ – это опять полиномиальный коэффициент, т.е. при $\sum_{i=1}^{r} k_i = n$

$$C_n(k_0, k_1, \ldots, k_r) = \frac{n!}{k_0! k_1! \cdots k_r!}. \qquad (7)$$

Если интересоваться только числом разрешенных конфигураций совпадений элементов в столбцах таблицы подстановок $\left(\varsigma_0, \varsigma_1, \varsigma_2, \ldots, \varsigma_{\lfloor m/2 \rfloor}\right)$, удовлетворяющих ограничениям $\varsigma_0 \le n$, $\varsigma_1 \le \varsigma'_1$, $\ldots$, $\varsigma_{\lfloor m/2 \rfloor} \le \varsigma'_{\lfloor m/2 \rfloor}$, то можно ввести вспомогательную числовую функцию

$$\psi_n(k_0, k_1, \ldots, k_r) = \begin{cases} 1, \text{ при } \sum_{i=0}^{r} k_i = n,\ k_i \le \varsigma'_i, \\ 0 \text{ в остальных случаях.} \end{cases}$$

Тогда формулу для определения размерности множества допустимых конфигураций совпадений элементов в столбцах таблицы подстановок можно представить в виде

$$N^{(n,m)}_{\left(\varsigma'_0, \varsigma'_1, \ldots, \varsigma'_{\lfloor m/2 \rfloor}\right)} = \sum_{\sum_{i=0}^{\lfloor m/2 \rfloor} k_i = n} \psi\left(k_0, k_1, \ldots, k_{\lfloor m/2 \rfloor}\right).$$

Для шифра ГОСТ 28147-89 (n = 16, m = 8) и модифицированного эталона $(\varsigma'_0,\varsigma'_1,\varsigma'_2,\varsigma'_3,\varsigma'_4)$ = (16 7, 6, 1, 0) вычисления с помощью ЭВМ приводят к результату

$$N^{(16,8)}_{(k_0,k_1,..,k_4)} = 112.$$

Заметим, что общее число возможных для заданных значений n и m различных вариантов совпадений элементов в столбцах таблицы подстановок можно получить, воспользовавшись свойствами полиномиальных коэффициентов [9],

$$\sum_{k_0+k_1+\ldots+k_r=n} C_n(k_0,k_1,\ldots,k_r) = (r+1)^n.$$

Так, при $r = \lfloor m/2 \rfloor = 4$ и $n = 16$ всего возможно $5^{16} \approx 1{,}53\cdot10^{11}$ различных вариантов конфигураций совпадений, из которых допустимыми являются только 112.

Для вероятности того, что произвольно взятая таблица удовлетворит оговоренным правилам проверки (требованию 2.3), соответственно можно записать выражение

$$P_c^{(m,n)} = \sum_{\substack{\sum_{i=0}^{\lfloor m/2 \rfloor} k_i = n,\, k_i \le \varsigma'_i}} C_n\left(k_0,k_1,\ldots k_{\lfloor m/2 \rfloor}\right) \prod_{s=0}^{\lfloor m/2 \rfloor} \left(P(\varsigma = s)\right)^{k_s}.$$

Расчеты, выполненные по этой формуле для параметров ГОСТ 28147-89, приводят к результату $P_c^{(m,n)} = 0{,}0781$, т.е. требованию 2.3 удовлетворяют около 10% всех таблиц подстановок (заметим, что в принципе можно получить более 10^{82} различных таблиц в пределах только одной конфигурации (2, 7, 6, 1, 0)).

Будем теперь интересоваться числом таблиц подстановок, удовлетворяющих требованию 2.2.

Выполним оценку ожидаемого числа таблиц подстановок, прошедших проверку по совпадениям элементов в парах строк. Как и в предыдущем случае, рассмотрим модифицированную эталонную конфигурацию $(t'_0,t'_1,t'_3,\ldots,t'_n)$ = (28, 11, 6, 2, 0, . . . , 0). Для общего числа возможных вариантов выбора таблицы с конфигурацией совпадений, удовлетворяющих требованию 2.2, можем записать выражение

$$N^{(n,m)}\left(t'_0,t'_1,\ldots t'_{\lfloor \frac{m}{2} \rfloor}\right) = \sum_{\substack{\sum_{i=0}^{n} q_i = \frac{m(m-1)}{2},\, q_i \le t'_i}} C_{\frac{m(m-1)}{2}}\left(q_0,q_1,\ldots,q_{\lfloor m/2 \rfloor}\right).$$

Расчеты общего числа различных конфигураций совпадений, выполненные по аналогии с предыдущим случаем, приводят к результату $N^{(16,8)}_{(t'_0,t'_1,..t'_4)} = 144$.

Для вероятности получения таблицы с конфигурацией совпадений в парах строк, удовлетворяющей требованию 2.2, здесь в рамках введенных выше обозначений можем записать выражение

$$P_s^{(m,n)} = \sum_{\substack{\sum_{i=0}^{\lfloor m/2 \rfloor} q_i = \frac{m(m-1)}{2},\, q_i \le t'_i}} C_{\frac{m(m-1)}{2}}\left(q_0,q_1,\ldots,q_{\lfloor m/2 \rfloor}\right) \prod_{i=0}^{\lfloor m/2 \rfloor} \left(P(t = i)\right)^{q_i}.$$

В этом случае для параметров ГОСТ 28147-89 приходим к результату $P_s^{(m,n)} = 0{,}0081$, т.е. требованию 2.2 удовлетворяют около 1% всех таблиц подстановок. Оценить реальные показатели отбраковки подстановок на втором уровне проверки позволяют также результаты статистического моделирования этого этапа проверки, представленные в таблице 6.

Таблица 6

Сгенерировано 132 таблицы, из них:	Число (%)
принято алгоритмом	10 (7.6%)
отброшено по совпадениям в столбцах	73 (55.3%)
отброшено по совпадениям в парах строк	111 (84.1%)

Из приведенных данных следует, что после второго уровня проверки остается $\sim 0(10^{82})$ различных таблиц, из которых на третьем уровне проверки будут уже отбираться варианты для реализации нужного количества долговременных ключей.

Результаты экспериментальных исследований по отбору таблиц подстановок на третьем уровне проверки приведены в таблице 7.

Сопоставление результатов таблицы 3 и таблицы 7 свидетельствуют о достаточно высоком совпадении экспериментальных результатов с расчетными.

Проверка статистической безопасности шифра ГОСТ 28147-89, выполненная по методике, изложенной в [6], практически повторила ранее полученные результаты и выводы.

Таблица 7

Количество k совпадений элементов в парах наложенных таблиц подстановок	Количество (%) пар таблиц из общего их числа 338182, имеющих k совпадений элементов	Эмпирический закон распределения вероятностей числа k совпадений элементов
0	101 (0%)	0,0003
1	770 (0%)	0,0023
2	3199 (1%)	0,0095
3	8826 (3%)	0,0261
4	17963 (5%)	0,0531
5	29237 (9%)	0,0864
6	39552 (12%)	0,1169
7	46215 (14%)	0,1455
8	46908 (14%)	0,1387
9	42706 (13%)	0,1263
10	34609 (10%)	0,1023
11	25928 (8%)	0,0767
12	17632 (5%)	0,0521
13	11134 (3%)	0,0329
14	6452 (2%)	0,0190
15	3568 (1%)	0,0105
...	...	...

В таблице 8 представлен пример долговременного ключа для шифра ГОСТ 28147-89, построенного с помощью предлагаемой методики. В нижних строках этой таблицы представлены значения числа совпадений в столбцах таблицы подстановок.

Таблица 8

№	Инв.	Возр.	Цикл.	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	50	8	2	4	2	7	5	9	1	0	8	E	3	B	C	D	7	A	6
2	76	6	2	C	9	F	E	8	1	3	A	2	7	4	D	6	0	B	5
3	75	8	3	D	8	E	C	7	3	9	A	1	5	2	4	6	F	0	B
4	70	7	1	E	9	B	2	5	F	7	1	0	D	C	6	A	4	3	8
5	59	7	1	3	E	5	9	6	8	0	D	A	B	7	C	2	1	F	4
6	71	9	3	8	6	F	B	1	9	C	5	D	3	7	A	0	E	2	4
7	55	10	3	9	B	C	0	3	6	7	5	4	8	E	F	1	A	2	D
8	59	7	3	C	6	5	2	B	0	9	D	3	E	7	A	F	4	1	8
Ср.	64,37	7,75	2,25	1	2	2	1	0	1	3	3	0	1	1	2	1	1	1	2

Представляется, что изложенные результаты могут стать основой разработки общей методики построения таблиц подстановок, которые используются в симметричных шифрах.

Список литературы: **1.** *Горбенко И.Д., Лисицкая И.В.* Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 2847-89 // Радиотехника. Всеукр. межвед. науч.-техн. сб. 1997. Вып. 103. С. 121–130. **2.** *Бильчук В.М., Лисицкая И.В.* Информационно-управляющие системы на железнодорожном транспорте. 1998. № 1. С. 10–17. **3.** *Лисицкая И.В., Головашич С.А., Олешко О.И., Олейников Р.В., Коряк А.С.* Построение таблиц подстановок для стандарта шифрования данных // Проблемы бионики. 1999. Вып. 50. С. 185-194. **4.** *Кононова И.В.* Оценка и анализ подмножества одно-цикловых подстановок // Информационные системы: Сб. научн. тр. - Харьков: НАНУ, ПАНУ, ХВУ, 1994. С. 37–46. **5.** *Кононова И.В.* Противоречивые подстановки в алгоритме ГОСТ 28147-89 // Информационные системы: Сб. научн. тр. Харьков: НАНУ, ПАНУ, ХВУ. 1995. С. 70–77. **6.** *Горбенко И.Д., Лисицкая И.В., Коряк А.С.* Анализ стойкости алгоритма ГОСТ 28147-89 при использовании подстановок случайного типа. // Радиоэлектроника и информатика. 1998. №1 (02). С. 39–43. **7.** *Крамер Г.* Математические методы статистики: Пер. с англ. - М.: ГИИЛ, 1948. - 631 с. **8.** *Математическая* энциклопедия: В 5 т. / Гл. ред. Виноградов И.М. - М.: Советская энциклопедия, 1979. - Т.2: Д-КОО. - 278 с. **9.** *Бронштейн И.Н. Семендяев К.А.* Справочник по математике для инженеров и учащихся Втузов, - М.: Наука, 1980. - 976 с.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 15.03.2000