УДК 621. 3.06

О ПРИХОДЕ ИТЕРАТИВНЫХ ШИФРОВ К СТАЦИОНАРНОМУ СОСТОЯНИЮ, СВОЙСТВЕННОМУ СЛУЧАЙНОЙ ПОДСТАНОВКЕ

И.В. ЛИСИЦКАЯ, К.Е. ЛИСИЦКИЙ

В статье обосновывается положение о том, что произведение цикловых шифрующих преобразований с ростом их числа приходит к случайной подстановке.

Ключевые слова: случайная подстановка, произведение подстановочных преобразований, механизм случайного перемешивания.

ВВЕДЕНИЕ

Одним из ключевых моментов развиваемой новой идеологии оценки показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа является положение, в соответствии с которым практически все известные итеративные шифры после небольшого начального числа циклов шифрования приходят к стационарному состоянию, свойственному случайной подстановке соответствующей степени [1]. Заметим, что для Фейстель-подобных шифров DES, ГОСТ и некоторых других переход к стационарному состоянию оказывается более затянутым по сравнению с другими итеративными шифрами.

Сегодня эти результаты подтверждены уже большим числом экспериментов, как с малыми, так и большими версиями современных шифров и опубликованы нами в ряде работ [2–5 и мн. др.].

До сих пор мы не смогли найти теоретического обоснования этому свойству. Удалось лишь показать [1], что после достижения стационарного распределения на выходе итеративного шифра при дальнейшем наращивании числа его циклов это стационарное распределение сохраняется. В этой работе мы представляем дополнительные результаты исследований по обоснованию правомерности приведенного утверждения.

В первой части работы изучаются свойства произведений подстановочных преобразований. Во второй её части представляются соображения по теоретическому обоснованию показателей случайности произведения подстановок. В заключении приводится обсуждение полученных теоретических и экспериментальных результатов.

1. СВОЙСТВА ПРОИЗВЕДЕНИЯ ПОДСТАНОВОЧНЫХ ПРЕОБРАЗОВАНИЙ

Напомним, что в работе [6] было показано, что все известные итеративные шифры являются Марковскими шифрами (первого или второго порядка). Воспользуемся результатом из работы [3], в соответствии с которым для Марковского шифра первого порядка формирование матрицы переходных вероятностей всего шифра (здесь под матрицей переходных вероятностей понимается дифференциальная таблица, связывающая разности текстов на входе шифра с соответствующими разностями на его выходе) сводится к последовательному выполнению r однотипных (одноцикловых) преобразований входного блока данных.

По результатам экспериментов в работе [6] сделан вывод о том, что *произведение одноцикловых преобразований после небольшого начального числа их повторений приобретает свойства случайной подстановки соответствующей степени независимо от показателей случайности исходного одноциклового преобразования.*

Для подтверждения этих слов в [6] были приведены результаты вычислительного эксперимента с подстановками 256-й степени ($n = 8$). В таблице 1 мы воспроизводим результаты вычислительного эксперимента по определению максимумов XOR таблиц последовательности подстановочных преобразований для двух байтовых подстановок. Одна подстановка взята с показателем δ-равномерности равным 4-м, а вторая с показателем δ-равномерности равным 8-ми. Видно, что обе подстановки (их произведение) уже на втором цикле приходят к максимуму дифференциала равному 10–12, характерному для случайной подстановки степени 2^8 [7].

Интересно отметить, что результат не зависит от ключевых значений, если их ввести после каждого подстановочного преобразования.

Конечно, по законам комбинаторики этот процесс должен быть периодическим, но для интересующих нас значений мы, как правило, оказываемся очень далеко от циклового периода подстановки.

Таблица 1

Распределение максимумов XOR таблиц последовательности подстановочных преобразований байтовой подстановки

Число циклов (повторов)	1	2	3	4	5	6	7	8	9	10	11
Значение максимума XOR таблицы для AES S-блока	4	12	12	10	12	12	10	12	12	12	12
Значение максимума XOR таблицы для S-блока шифра Мухомор	8	10	10	12	10	14	12	12	10	12	10

В этой работе нас будет интересовать сам процесс формирования значений переходов произведения подстановочных преобразований.

Рассмотрим две подстановки (не обязательно разные), для которых заданы (определены) их таблицы дифференциальных разностей, которые будем представлять в виде матриц $A=\{a_{ij}\}$ и $B=\{b_{lk}\}$.

Произведение матриц $C=AB$ мы бы выполняли по правилам $c_{ik}=\sum_{l=1}^{2^n} a_{il}b_{lk}$, где 2^n – степень подстановки (размер таблицы дифференциальных разностей по строкам или столбцам). Но умножение подстановок есть последовательное их выполнение одна за другой, т.е. для произведения подстановочных преобразований мы будем иметь для каждой ячейки результата сумму, но не произведений переходов, а значений последовательной реализации переходов для первой и второй подстановок, которые, как мы убедимся, формируются случайным образом.

Поясним это на примере. Пусть мы рассматриваем произведение самого на себя подстановочного преобразования (10 2 0 6 15 1 12 4 14 11 7 13 9 5 3 8) (произведение одинаковых полубайтовых подстановочных преобразований). Здесь для упрощения рассуждений мы взяли подстановку степени 16 ($n=4$) Очевидно, что

$$(10\ 2\ 0\ 6\ 15\ 1\ 12\ 4\ 14\ 11\ 7\ 13\ 9\ 5\ 3\ 8)\times$$
$$\times(10\ 2\ 0\ 6\ 15\ 1\ 12\ 4\ 14\ 11\ 7\ 13\ 9\ 5\ 3\ 8)=$$
$$=(7\ 0\ 10\ 12\ 8\ 2\ 9\ 15\ 3\ 13\ 4\ 5\ 11\ 1\ 6\ 14).$$

Дифференциальная таблица для подстановки (10 2 0 6 15 1 12 4 14 11 7 13 9 5 3 8) имеет вид (это одна из подстановок, сконструированных регулярными методами [8]):

16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	2	2	0	4	0	2	2	2	0	2	0
0	0	0	2	2	2	2	0	0	2	4	0	0	2	0	0
0	2	2	2	0	0	2	0	0	0	**0**	2	4	2	0	0
0	0	2	2	2	4	0	2	0	0	0	0	2	0	2	0
0	0	2	0	2	0	0	0	0	0	2	4	0	2	2	2
0	**0**	0	2	0	0	4	2	2	0	0	0	0	2	2	2
0	2	2	0	2	0	2	0	2	2	0	0	0	0	4	0
0	0	0	0	4	0	2	2	0	2	0	2	2	0	0	2
0	4	0	0	2	0	0	2	2	0	2	**0**	2	2	0	0
0	2	0	0	0	2	0	0	0	2	0	0	2	4	2	2
0	0	2	0	0	2	0	4	2	2	0	2	0	2	0	0
0	2	**0**	4	0	0	0	2	0	2	2	2	0	0	2	0
0	2	0	2	2	2	0	0	2	0	0	2	0	0	0	4
0	0	2	2	0	0	0	0	2	4	2	0	2	0	0	2
0	2	4	0	0	2	2	2	0	0	2	0	**0**	0	0	2

Произведение рассматриваемой подстановки саму на себя будет иметь дифференциальную таблицу:

16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	2	0	0	0	**0**	0	4	2	2	0	4	0	0	0	2	0
0	2	0	0	0	0	0	2	2	0	0	0	2	6	0	2
0	0	0	0	0	2	2	4	0	2	2	4	0	0	0	0
0	0	4	4	0	0	0	0	2	0	0	2	2	0	0	**2**
0	0	2	2	0	6	2	0	2	0	2	0	0	0	0	0
0	0	2	2	2	2	0	0	0	0	0	0	0	0	4	4
0	0	0	0	2	2	0	**0**	4	2	0	2	0	2	2	0
0	2	0	4	2	0	0	0	0	2	0	0	0	2	2	2
0	0	0	2	0	0	0	2	2	6	2	0	0	0	0	2
0	2	2	2	0	2	0	0	0	2	0	0	2	0	4	0
0	0	2	0	6	0	2	2	2	0	0	0	0	0	0	2
0	2	2	0	0	0	0	0	0	0	0	2	2	4	2	0	2
0	2	0	0	2	2	2	0	0	0	**2**	4	2	0	0	0
0	4	2	0	0	0	0	2	0	0	2	0	2	2	2	0
0	0	0	0	2	0	4	2	0	2	0	2	2	2	0	0

Когда строится таблица произведения подстановок, необходимо для фиксированного входа исходной подстановки рассматривать все возможные пары входов с фиксированной разностью. Для всего этого набора входов получаются входы во вторую подстановку как весь набор значений выходов (строки дифференциальной таблицы) для соответствующей фиксированной разности входа. В результате для заданного значения разности на выходе произведения подстановок необходимо просмотреть и просуммировать все значения переходов, которые формируются каждым из входов во вторую подстановку (значениями пар, формирующих выходные разности строки таблицы дифференциальных разностей первой подстановки), в заданную выходную разность, определяемую элементами соответствующего столбца дифференциальной таблицы второй подстановки. Действительно получается, что в формировании интересующего нас перехода участвуют элементы дифференциальных таблиц, фигурирующих в произведении матриц. Но в нашем случае результат взаимодействия переходов, фигурирующих в «произведении», определяется возможностью реализации перехода произведения подстановок, а именно согласованием пар текстов, формирующих выходные разности первой подстановки с допустимыми парами входов, формирующих заданную выходную разность второй подстановки, а этот процесс оказывается случайным.

Рассмотрим, например, процесс формирования переходов $c_{ik}=\Lambda_\pi(\Delta X=1,\Delta Z=6)=4$ и $c_{ik}=\Lambda_\pi(\Delta X=1,\Delta Z=2)=0$ для дифференциальной таблицы произведения подстановок.

Выпишем значения строки и столбца таблицы разностей, участвующих в формировании этих переходов, в две колонки:

$c_{ik} = \Lambda_\pi(\Delta X = 1, \Delta Z = 6) = 4$ $c_{ik} = \Lambda_\pi(\Delta X = 1, \Delta Z = 2) = 0$

0	0	0	0
0	4	0	0
0	0	0	0
0	2	0	2
0	0	0	2
2	2	2	2
2	0	2	0
0	0	0	2
4	0	4	0
0	0	0	0
2	0	2	0
2	2	2	2
2	0	2	0
0	2	0	0
2	0	2	2
0	4	0	4

Видно, что в первом случае в формировании интересующего нас перехода произведения участвуют два перехода исходной подстановки, причём первый переход $\Delta X = 1 \to \Delta Y = 6$ равный 2-м формируется одной и той же разностью входов (одной и той же парой входов) и далее при проходе второй подстановки $\Delta Y = 6 \to \Delta Z = 6$ пара выходов первой подстановки повторила пару текстов (входов во вторую подстановку), формирующих выходную разность $\Delta Y = 6$. Совершенно аналогичная ситуация состоялась и для второго перехода. В результате эти два перехода дали результирующее значение ячейки дифференциальной таблицы произведения подстановок равное 4-м.

Во втором случае из трёх ненулевых пар переходов, входящих в сумму ни один не оказался согласованным по парам текстов, формирующих разности на выходе первой подстановки с парами текстов, формирующих переход во второй подстановке в выходную разность $\Delta Z = 2$. Здесь результатом (значением ячейки дифференциальной таблицы произведения подстановок) является 0.

Как мы видим процесс формирования переходов действительно оказывается случайным. Чтобы состоялся ненулевой переход входной разности $\Delta X \neq 0$ в выходную разность произведения подстановок $\Delta Z \neq 0$ необходимо:

1) чтобы состоялись ненулевые переходы исходной входной разности ΔX в промежуточные ненулевые выходные разности ΔY первой подстановки, для которых имеются ненулевые переходы в выходную разность ΔZ второй подстановки;

2) чтобы промежуточные выходные разности первой подстановки оказались бы согласованными с входами во вторую подстановку (совпадали бы пары выходов первой подстановки с ненулевыми парами входов во вторую подстановку, имеющими выбранную выходную разность).

В результате мы приходим к случайному механизму формирования переходов подстановки-произведения (даже для подстановки, построенной с помощью регулярных методов, результирующая подстановка получается случайной).

Далее мы будем представлять процедуру формирования значений переходов произведения подстановок в виде

$$c^*_{ik} = \sum_{l=1}^{2^n} a_{il} \circ b_{lk}, \quad (1)$$

$$i,k = 1,2,\ldots,2^n.$$

В этой формуле символ $\circ$ будет обозначать результат осуществления операции последовательного перехода (прохода) a_{il} -го элемента дифференциальной таблицы первой подстановки «через» b_{lk} -й элемент второй.

Отметим, что при увеличении степени подстановок число случайных слагаемых в суммах (1) быстро увеличивается. Для байтовой подстановки это число для ненулевых переходов подстановок, входящих в произведения, будет уже достигать значения близкого к 25.

Таким образом, представленные результаты свидетельствуют о том, что при умножении подстановок связь входов с выходами этого преобразования формируется на основе механизма случайного взаимодействия полного набора выходов первой подстановки с соответствующим набором входов второй подстановки. Поэтому подстановку-произведение можно действительно рассматривать как случайное преобразование (случайную булеву векторную функцию). Далее в связи с отмеченным обстоятельством предлагается краткая подборка материалов, связанных с математическим описанием свойств случайных булевых векторных функций, одним из известных представлений которых являются подстановки.

2. ЭЛЕМЕНТЫ ТЕОРИИ СЛУЧАЙНЫХ ПОДСТАНОВОК. ПРОИЗВЕДЕНИЕ ПОДСТАНОВОК — СЛУЧАЙНАЯ ПОДСТАНОВКА

Напомним некоторые математические факты, изложенные в работе [9], имеющие отношение к случайным преобразованиям. В этой работе рассматриваются дифференциальные свойства n-разрядных m-битных векторных булевых функций.

Мы здесь воспользуемся более общепринятым определением дифференциальной вероятности, отличающимся от соответствующего определения, приведенного в работе [9] тем, что здесь учитывается удвоение значений дифференциального перехода для каждой разности, возникающего при побитном сложении (XOR) входов для одной и той же пары текстов, взятых в разном порядке и то, что множество из 2^n входов для заданной разности образует 2^n пар.

В соответствии с [9] дифференциал над векторной булевой функцией α состоит из входной разности a и выходной разности b и обозначается (a,b). Дифференциальная вероятность (DP)

дифференциала (a,b) определяется числом пар, которые имеют входную разность a и выходную разность b, поделенным на общее число пар с входной разностью a:

$$DP(a,b) = \#\{\{v,u\} \mid v \oplus u = a \;\&\; \alpha(v) \oplus \alpha(u) = b\} / 2^n$$

(в [9] понятие дифференциала связывается с половинным значением ячеек дифференциальной таблицы и соответственно нормировка выполняется по 2^{n-1} ненулевым значениям входной разности). В [9] далее доказывается теорема:

Теорема 1. *Для случайной n-разрядной m-битной векторной булевой функции, мощность $N(a,b)$ данного дифференциала (a,b) является стохастической переменной с биномиальным распределением:*

$$\Pr\big(N(a,b) = 2i\big) = (2^{-m})^i (1-2^{-m})^{2^{n-1}-i} \cdot \binom{2^{n-1}}{i}.$$

Мы здесь опять при записи формулы тоже внесли поправку (учли то, что заполнениями ячеек дифференциальной таблицы являются чётные числа).

Доказательство очень простое: случайная векторная булева функция отображает 2^n различных входных значений v в независимые выходные значения $\alpha(v)$ и, следовательно, она отображает переходы разности пар входов $\{v, u\}$, в независимые выходные разности. Данный дифференциал (a,b), принимающий пару с входной разностью a, является исходом случайного эксперимента, который считается успешным, если выходная разность равна b. Число экспериментов (число различных пар входов преобразования) равно 2^{n-1} и вероятность успеха есть 2^m. Пусть из общего числа 2^{n-1} возможных различных входных пар i пар имеют заданный переход (являются успешными исходами) в выходную разность, а остальные $2^{n-1} - i$ не дают заданного перехода. Тогда число успехов при независимых исходах имеет биномиальное распределение представленного выше вида.

Приведём также следствие из теоремы 1, приведенное в [9] (с нашей коррекцией).

Следствие 1. При $n \geq 5$ и небольшом значении $n - m$, мы имеем:

$$\Pr\big(N(a,b) = 2i\big) \approx e^{-2^{n-m-1}} \frac{2^{(n-m-1)i}}{i!} = \\ = Puasson(i, 2^{n-m-1}).$$

Справедливость следствия вытекает из того, что при $n \geq 5$ и малом значении разности $n - m$, биномиальное распределение близко (хорошо) аппроксимируется распределением Пуассона с параметром $\lambda = 2^{n-m-1}$ [9]. И ещё одно следствие из этой работы.

Следствие 2. *Для случайного векторного Булева преобразования мы имеем*

$$\Pr\big(N(a,b) = 2i\big) \approx Puasson\left(i, \frac{1}{2}\right) = \frac{e^{-\frac{1}{2}}}{i! \cdot 2^i}. \qquad (2)$$

Приведенный результат следует из следствия 1 при $m = n$ и тогда $\lambda = 1/2$ (в работе [9] следствия 1 и 2 представлены под номерами 2 и 4, а теорема 1 представлена под номером 2).

Далее полученные результаты переносятся на случайную подстановку. Отмечается, что в случайной подстановке, входы в определении её таблицы не являются независимыми друг от друга.

Так, для суммы элементов дифференциальной таблицы подстановки-произведения справедливы очевидные соотношения:

$$\sum_{i=1}^{2^n} c^*_{ik} = \sum_{i=1}^{2^n} \sum_{l=1}^{2^n} a_{il} \circ b_{lk} = 2^n,$$

а также

$$\sum_{k=1}^{2^n} c^*_{ik} = \sum_{k=1}^{2^n} \sum_{l=1}^{2^n} a_{il} \circ b_{lk} = 2^n.$$

В серии из 2^{n-1} экспериментов применения пар с заданной входной разностью и наблюдаемой выходной разностью видно, что пары выходов для всех 2^n возможных значений появляются точно один раз. Это ограничение сильно усложняет анализ. К счастью, как отмечается в работе [9], случай подстановок был подробно изучен и описан в работах [10, 11]. За исключением того, что дифференциалы вида (a, 0) с $a \neq 0$ невозможны, получается, что рассмотренная выше вероятность того, что пара с заданной входной разностью отображается в данную выходную разность, заметно не меняется от того факта, что преобразование является подстановкой. Отсюда следует, что при расчете распределения достаточно заменить вероятность успеха в полученном выше соотношении на $1/(2^n - 1)$ для ненулевого выходного различия b и 0 для $b = 0$. При больших n эта замена оказывает незначительное влияние на мощность дифференциалов (a,b) с $b \neq 0$ и, следовательно, следствие 4 для случайных преобразований справедливо и для случайных подстановок.

Мы здесь можем напомнить и результаты нашей работы [12], в которой доказано, что для закона распределения переходов дифференциальной таблицы случайной подстановки действительно справедлива аппроксимация (2).

Так, для рассмотренного выше примера с байтовыми подстановками ($n = 2^8$) из соотношения для определения заполнений XOR таблицы $(2^n - 1)^2 \cdot \Pr\big(N(a,b) = 2i\big)$, следующего из закона распределения вероятностей (2), получим для $i = 5$ результат 10,24, в то время как для $i = 6$ имеем 0,854, т.е. значения максимумов дифференциалов для случайной подстановки степени 2^8 как раз получаются равными 10-ти или 8-ми, как в нашем эксперименте.

В заключение отметим, что совершенно аналогичные выводы в отношении показателей случайности произведения подстановок будут справедливы и для линейных характеристик этого преобразования. И в этом случае значения

переходов, связывающие маски входов и выходов произведения подстановок, будут формироваться с использованием отмеченного случайного механизма взаимодействия переходов подстановок-сомножителей. Только теперь необходимо будет рассматривать взаимодействие элементов строк и столбцов линейных аппроксимационных таблиц подстановок. Как и в случае дифференциальных переходов произведения подстановок и в этом случае значения слагаемых соотношения вида (1) для каждого из переходов произведения не могут быть больше меньшего из значений переходов подстановок-сомножителей.

Для линейных аппроксимационных таблиц в формуле (1) a_{il} (i,l)-й элемент таблицы первой подстановки для пары масок входа и выхода (α_i,β_l), а b_{lk} – (l,k)-й элемент таблицы второй подстановки для пары масок входа и выхода (ξ_l,θ_k), участвующих в рассматриваемом переходе. Символ $\circ$ теперь будет обозначать результат осуществления операции последовательного перехода (прохода) a_{il}-го элемента линейной таблицы первой подстановки «через» b_{lk}-й элемент второй. В этом случае должны сшиваться наборы выходных равенств четности первой подстановки с соответствующими наборами равенств четности второй.

Таким образом, действительно *произведение* (*последовательность*) *подстановочных преобразований нетривиального типа* (*а не только шифров*) *является с большой вероятностью случайной подстановкой, независимо от свойств подстановок, участвующих в формировании этого преобразования*.

Мы посчитали, что это утверждение является неким «законом природы», который выполняется независимо от нашего желания.

Конечно, здесь речь идёт не о вырожденных подстановках, к которым мы отнесли подстановки с дифференциальными и линейными показателями, выходящими далеко за рамки среднестатистических показателей случайных подстановок [13].

Одновременно становится понятным, что использование разных (отличающихся) S-блоков в шифрах не будет приносить сколько-нибудь ощутимых преимуществ.

ВЫВОДЫ

В работе представлено обоснование замечательного свойства произведения подстановочных преобразований, которое заключается в том, что результатом произведения является подстановка случайного типа.

Итеративные шифры являются произведением подстановочных преобразований. Даже без введения в циклы случайных подключей шифр после некоторого числа начальных цикловых преобразований становится случайной подстановкой. Для шифров с сильным линейным преобразованием (с байтовыми подстановками) этот процесс является достаточно кратковременным (до трёх–четырёх циклов). Для шифров со слабым линейным преобразованием (с полубайтовыми подстановками) этот процесс перехода шифра к случайной подстановке может затягиваться до 7–10 и более циклов. Переходный период прихода к случайной подстановке, характерный для шифров, связан с тем, что при малом числе циклов шифрования булевы векторные функции, описывающие цикловые преобразования, ещё не связаны со всеми битами входа в цикловое преобразование. Необходимо, чтобы сработал механизм перемешивания выходных битов подстановок, входящих в шифр, реализуемый с помощью соответствующих линейных преобразований.

Одновременно представленные результаты подтверждают новую точку зрения по вопросу оценки безопасности блочных шифров к атакам дифференциального и линейного криптоанализа [14, 15], состоящую в том, что максимумы средних вероятностей дифференциалов и линейных корпусов полноцикловых версий шифров от свойств используемых в них S-блоков (исключая вырожденные их конструкции) не зависят (за исключением шифра DES, допускающего построение итеративных характеристик обнуляющего типа).

Конечно, изложенные выше соображения не могут претендовать на высокую математическую строгость, но приведенные аргументы и примеры, на наш взгляд, можно рассматривать как достаточно убедительное свидетельство правомерности положения, лежащего в основе новой методологии оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа [1], в соответствии с которым итеративные шифры в результате применения последовательности подстановочных преобразований становятся случайными подстановками.

Литература

[1] Лисицкая И.В. Методология оценки стойкости блочных симметричных шифров. / И.В. Лисицкая // Автоматизированные системы управления и приборы автоматики. – 2011. – № 163. – С. 123–133.

[2] Долгов В.И. Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс. / В.И. Долгов, А.А. Кузнецов, С.А. Исаев. // Электронное моделирование. – 2011.– Т 33, № 6. – С. 81–99.

[3] Кузнецов А.А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс. / А.А. Кузнецов, И.В. Лисицкая, С.А. Исаев // Прикладная радиоэлектроника. – 2011. – Т. 10, № 2 – С. 135–140.

[4] Лисицкая И.В. Большие шифры – случайные подстановки. Сравнение показателей статистической безопасности блочных симметричных шифров, представленных на украинский конкурс / И.В. Ли-

сицкая, А.А. Настенко, К.Е. Лисицкий // Східно-Європейський журнал передових технологій. – 2012. – Т. 6, № 9 (60). – С. 11–21.

[5] Лисицкая И.В. Большие шифры – случайные подстановки. Сравнение дифференциальных и линейных свойств шифров, представленных на украинский конкурс и их уменьшенных моделей. / И.В. Лисицкая, А.А. Настенко, К.Е. Лисицкий // Автоматизированные системы управления и приборы автоматики. – 2012. – Вып. 159. – С. 31–39.

[6] Лисицкая И.В. Оценки максимальных значений дифференциалов и линейных корпусов Марковских шифров. / И.В. Лисицкая., В.И. Долгов, А.А. Настенко // Прикладная радиоэлектроника. – 2012. – Т. 11, № 2 – С. 144–151.

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

[8] A Description of Baby Rijndael, ISU CprE/Math 533; NTU ST765-U, February 19, 2003.

[9] Joan Daemen, Vincent Rijmen Probability distributions of Correlation and Differentials in Block Ciphers. / Joan Daemen, Vincent Rijmen // April 13, 2006, pp. 1–38.

[10] L. O'Connor, "On the Distribution of Characteristics in Bijective Mappings," Advances in Cryptology, Proceedings of Eurocrypt '93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1993, pp. 360–370.

[11] P. Hawkes and L O'Connor, "XOR and Non-XOR Differential Probabilities," Advances in Cryptology, Proceedings of Eurocrypt '99, LNCS 1592, J. Stern, Ed., Springer-Verlag, 1999, pp. 272–285.

[12] Лисицкая И.В. Свойства законов распределения XOR таблиц и таблиц линейных аппроксимаций случайных подстановок. / И.В. Лисицкая // Вісник Харківського національного університету імені В.Н. Каразіна. – 2011. – № 960. Вип.16. – С. 196–206.

[13] Лисицкая И.В. Вырожденные подстановки. / И.В. Лисицкая // Радиотехника. – 2012. – Вып. 171. – С. 41–49.

[14] Лисицкая И.В. Об участии S-блоков в формировании максимальных значений дифференциальных и линейных вероятностей блочных симметричных шифров / И.В. Лисицкая // Спеціальні телекомунікаційні системи та захист інформації. Вип. 7 (21) – Київ.– 2012. – С. 71–84.

[15] Lisitskaya I.V. Importance of S-Blocks in Modern Block Ciphers. / I.V. Lisitskaya, E.D. Melnychuk, K.E. Lysytskiy // Computer Network and Information Security, 2012, 10, 1-12 ISSN: 2074-9104.

Поступила в редколлегию 19.03.2013

Лисицкая Ирина Викторовна, доктор технических наук, доцент кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники. Научные интересы: криптография, методы криптоанализа.

Лисицкий Константин Евгеньевич, студент Харьковского национального университета радиоэлектроники. Научные интересы: криптография, методы криптоанализа.

УДК 621. 3.06

Про прихід ітеративних шифрів до стаціонарного стану, властивому випадковій підстановці / І.В. Лисицька, К.Є. Лисицький // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. № 2. – С. 230–235.

У статті обгрунтовується положення про те, що добуток циклових шифруючих перетворень із зростанням їх числа приходить до випадкової підстановки.

Ключові слова: випадкова підстановка, добуток підстановних перетворень, механізм випадкового перемішування.

Таб. 1. Бібліогр.: 15 найм.

UDC 621. 3.06

On the reaching by iterative ciphers of a steady state characteristic of a random permutation / I.V. Lisitskaya, K.E. Lisitsky // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 230–235.

The paper substantiates the thesis that the product of cycle encrypting transformations with the growth of their number results in a random substitution.

Keywords: random substitution, product of substitution transformations, mechanism of accidental mixing.

Tab.: 4. Ref.: 15 items.