УДК 681.3.06 **DOI:10.30837/rt.2020.3.202.12**

К.Е. ЛИСИЦКИЙ, И.В. ЛИСИЦКАЯ, канд. техн. наук

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СЛУЧАЙНОЙ ПОДСТАНОВКИ

Введение

Самые современные традиционные ключевые криптосистемы базируются на идее произведения (product) шифров, которые представляют класс криптосистем, многократно повторяющих сложную операцию, отображающую преобразование плайнтекста в шифртекст. Каждое такое повторение (итерация) известно как цикл шифра. Сложная (составная) операция, выполняющаяся в каждом цикле, является обычно комбинацией из набора примитивных операций, таких как сдвиг, линейное преобразование, модульное сложение и подстановка. В частности, комбинация перестановочных и подстановочных операций может привести к криптографически сильному нелинейному преобразованию, если оно применяется достаточное число раз. Подстановочные операции во многих шифрах выступают при этом как основной нелинейный элемент циклового преобразования (нелинейный элемент замены). Поэтому значительные усилия исследователей направлены на изучение подходов к построению подстановок с высокими криптографическими показателями [1 – 6] и многие другие.

Наиболее разработанным и наиболее популярным математическим аппаратом оценки криптографических свойств нелинейных элементов замены (S-блоков) стал аппарат линейной алгебры и, в частности, аппарат булевых функций. Его развитию и применению посвящено большое число публикаций [7 – 10 и др.]. Предложено и используется множество критериев и показателей оценки свойств как самих булевых (компонентных) функций S-блоков, так и критериев и показателей криптографических свойств S-блоков в целом. В их числе такие: сбалансированность булевой функции, нелинейность N_f, корреляционный иммунитет, критерий распространения (строгий лавинный критерий) $KP(k)$, алгебраическая степень булевой функции $\deg(f)$, а также соответствующие характеристики S-блоков – критерий битовой независимости (*BIC*), критерий нелинейности, максимальный порядок строгого лавинного критерия (*MOSAC*), максимальное значение линейной аппроксимационной таблицы, δ-гладкость (δ-равномерность) XOR-таблицы S-блока [11 и др.].

Следует отметить также предложенный в свое время подход к отбору подстановок [12 – 14], строящийся на основе оценки показателей их случайности (значений числа циклов, возрастаний и инверсий), дополненных ограничениями на максимально допустимые значения таблиц дифференциальных разностей и линейных аппроксимаций. Здесь и в дальнейшем будут сделаны ссылки в основном на наши публикации, так как это направление не привлекло внимание зарубежных исследователей. Можно лишь отметить работы, посвященные использованию подстановок для построения ключей шифрования [15 и др.].

Отмеченный подход нашел продолжение в работах [15, 16 и др.], выполненных, с участием авторов этой работы. Основное внимание в этих публикациях сосредоточено на разработке дополнительных критериев отбора случайных подстановок, построенных на использовании законов распределения переходов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок. Было предложено два (дополнительных к комбинаторным) критерия отбора, основанных на оценке близости дифференциальных и линейных законов распределения вероятностей подстановок к теоретически полученным законам [16]. Напомним здесь кратко их суть, следуя [16].

Критерий 4. *Подстановка удовлетворяет критерию случайности* 4*, если закон распределения однотипных переходов* $\Pr(\Lambda_\pi(\Delta X,\Delta Y)) = 2k,\ k = 0,1,...,k*$*, ее таблицы XOR разностей для входов, приписываемых к ненулевым характеристикам, соответствует по критерию согласия Колмогорова теоретическому закону распределения переходов случайной подста-*

новки, т.е. наибольшее значение модуля разности теоретического и эмпирического законов распределения вероятностей удовлетворяет условию $|F_{\mathrm{T}}(x_k) - F(x_k)| \le b$.

Здесь граничный параметр b подлежит уточнению по результатам экспериментов.

Критерий 5. *Подстановка удовлетворяет критерию случайности* 5*, если закон распределения однотипных переходов* $\Pr(\lambda^*(\alpha,\beta)) = 2k),\ k = 0,1,...,k^*$*, ее таблица линейных аппроксимаций соответствует по критерию согласия Колмогорова теоретическому закону распределения переходов случайной подстановки, т.е. наибольшее значение модуля разности теоретического и эмпирического законов распределения вероятностей удовлетворяет условию* $|F_{\mathrm{T}}(x_k) - F(x_k)| \le c$.

Здесь параметр c также подлежит уточнению по результатам экспериментов.

В последующей работе [17] рассмотрено установление границ (значений параметров b и c) при использовании критерия Колмогорова для оценки близости законов распределения переходов дифференциальных и линейных таблиц подстановок теоретическим (мы их назвали ″эталонными″), на основе результатов которых принимается решение, можно ли отнести проверяемую подстановку к случайной или нет.

Ожидалось, что подстановки, отобранные по предлагаемой системе критериев, будут более предпочтительными, чем известные конструкции. Однако, с одной стороны, формируемые в этом случае подстановки, как показал анализ, не имеют заметных преимуществ в сравнении с известными. С другой – применение представленных выше критериев для практического отбора случайных подстановок встретило определенные затруднения, так как неясной стала сама стратегия применения этих критериев. Вроде бы мы порождаем случайные подстановки, а потом начинаем их фильтровать. Не ясно, какие же показатели отбора являются предпочтительными.

В этой работе мы хотим изменить позицию к определению показателей случайности. Мы хотим ответить на вопросы, а какими свойствами будет обладать выборка случайно порождаемых подстановок? С какими подстановками в этом случае реально мы имеем дело? Как они соотносятся с приведенными критериями отбора?

В работе будут изучаться показатели последовательности байтовых подстановок, порождаемых случайным генератором. Итогом их изучения станет усовершенствованная модель случайной подстановки, отличающаяся от известных использованием свойств выборки случайных подстановок, что позволило существенно упростить правила отбора случайных подстановок (а практически использовать подстановки, порождаемые генератором случайных подстановок без каких-либо ограничений). Для недоверчивых можно лишь выполнять проверку поцикловых значений максимумов таблиц XOR разностей и смещений таблиц линейных аппроксимаций.

Задача практически сводится к определению законов распределения выборки, составленной из максимумов таблиц XOR разностей и максимумов смещений таблиц линейных аппроксимаций случайных подстановок.

Математические аспекты этой задачи рассмотрены в приложении работы [18]. В ней изучаются случаи, когда все значения выборки имеют одно и то же распределение и их плотности уменьшаются с ростом переменной x экспоненциально. Но это как раз и есть наши случаи.

Далее приведем краткое изложение сути этой методики с нашими исправлениями [19], затем применим ее для построения законов распределения максимумов переходов таблиц XOR разностей и максимумов смещений таблиц ЛАТ байтовых подстановок.

Суть методики определения законов распределения максимумов для больших по объему выборок независимых одинаково распределенных случайных величин

Нас будут интересовать два случая.

1-й случай, когда выборка состоит из случайных значений переходов XOR таблиц случайных подстановок. Как известно [20], в этом случае распределение вероятностей переходов подчиняется пуассоновскому закону:

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

Здесь $\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$ – вероятность, что значение дифференциальной таблицы случайно взятой подстановки π порядка 2^n для перехода входной разности ΔX в соответствующую выходную разность ΔY будет равна $2k$.

2-й случай, когда выборка состоит из случайных значений, являющихся смещениями таблиц линейных аппроксимаций случайных подстановок, подчиняющихся нормальному закону распределения. Как показано в [18], в этом случае справедливо утверждение.

Утверждение. *Для случайной n-битовой подстановки, с* $n \geq 5$ *дисбаланс* Imb(v,*u*) *аппроксимации является случайным значением с распределением, которое может быть аппроксимировано в виде*

$$\Pr(\mathrm{Imb}(v,u)=z)\approx 2Z\left(\frac{z}{2^{(n-2)/2}}\right) \tag{2}$$

для z четного и ноль – для z нечетного.

В наших обозначениях дисбаланс Imb(*v*, u) = *z* при $z = 2k$ как раз соответствует значению смещения таблицы линейных аппроксимаций.

В работе [18] отмечается, что распределение максимумов больших по объему выборок независимых одинаково распределенных случайных величин хорошо изучено в теории вероятностей и описывается распределением экстремальных значений Фишера – Типпета или log-Вейбула в виде

$$D_{\max}(X)\approx e^{-e^{\frac{a-X}{b}}}.$$

Это распределение имеет математическое ожидание $\mu(X) = a + b\gamma$ с $\gamma \approx 0{,}58$ и среднеквадратическое отклонение $\frac{\pi}{\sqrt{6}}b \approx 1{,}3b$. Параметр *a* является решением уравнения

$$\ln(2)Y=-\ln f(X), \tag{3}$$

а *b* является единицей, деленной на производную функции – ln*f*(*x*) в точке *a* (здесь используется линейная аппроксимация функции – ln*f*(*x*) в точке *a*).

В работе [18] также показано, что решение уравнения (3) для выборки из 2^Y случайных значений, распределенных по пуассоновскому закону, имеет вид

$$i=\frac{\ln(2)y-\frac{1}{2}\ln(2\pi i)-\lambda}{\ln\left(\frac{i}{\lambda}\right)-1}. \tag{4}$$

Это уравнение может быть решено итеративно. Производная – ln*f*(*x*) определяется по формуле

$$\ln\left(\frac{i}{\lambda}\right)+\frac{1}{2i}. \tag{5}$$

Определив *a* и используя условие $a >> \lambda$, имеем

$$b=\frac{1}{\ln\left(\frac{a}{\lambda}\right)}.$$

Для нормального распределения (2) параметр a_s (подстрочный индекс *s* для стандарта) является решением уравнения

$$a_s = \sqrt{2\ln(2)y - \ln(2\pi) - 2\ln(a_s)}, \tag{6}$$

которое может быть найдено итеративным путем, без учета правого члена в первой итерации. Производная $f(x)$ определяется по формуле

$$x + \frac{1}{x}, \tag{7}$$

и, следовательно,

$$b_s = \frac{a_s}{a_s^2 + 1} \approx \frac{1}{a_s}. \tag{8}$$

Грубо говоря, максимум имеет распределение со средним значением $1{,}17\sqrt{y}$ и стандартным отклонением $1{,}11/\sqrt{y}$. Авторы работы [7] отмечают, что можно найти значения *a* и *b* для любого нормального распределения со средним значением $\mu(X)$ и стандартным отклонением σ заменив *x* на $\frac{X - \mu(X)}{\sigma}$. Это дает

$$\begin{aligned} a &= \sigma a_s - \mu(X), \\ b &= \sigma b_s \end{aligned} \tag{9}$$

Распределение максимумов XOR таблиц и смещений таблиц линейных аппроксимаций выборки из байтовых подстановок

Мы здесь будем рассматривать выборку размера 2^n, $n = 8$. Для $n = 8$ из (4) имеем:

Таблица 1

i	$\frac{\ln(2)\cdot 16 - \frac{1}{2}\ln(2\pi i) - \frac{1}{2}}{\ln(2i) - 1}$
5	6,8
5,5	6,3
5,9	5,98
6	5.9
7	5,3

И, следовательно, решением уравнения (4) является значение $i = a$ близкое к числу 6. Соответственно $b = \frac{1}{\ln(12)} = 0{,}4$. Но заметим здесь, что формула (4), по которой мы определяли значение *a*, работает с половинным значением перехода дифференциальной таблицы. Поэтому при подсчете действительного среднего значения мы должны полученный результат удвоить.

И тогда

$$\mu(X) = 2\cdot 6 + 2\cdot 0{,}4\cdot 0{,}58 = 12{,}4.$$

Если ориентироваться на результаты реального эксперимента, то среднее значение максимума должно быть близким к 11,55. Поэтому мы скорректируем наше значение до $a = 5$.

Это значение хорошо согласуется с результатами расчетов и экспериментов, представленными в работах [21 и др.].

Выше отмечалось, что поскольку распределение максимумов дискретное, то малая величина стандартного отклонения $b = \frac{1}{\ln(12)} = 0{,}4$ приводит к тому, что распределение сосредоточено в двух целочисленных значениях вблизи $\mu(X) \approx 2a$. В наших экспериментах с байтовыми подстановками это два значения 10 и 12.

Расчет далее предлагается вести для распределения

$$D_{\max}(X) \approx e^{-e^{\frac{10-2\cdot X}{0{,}87}}}, \qquad (10)$$

где использовано значение $a = 5$ (формула записана с учетом реального удвоения значений переходов XOR таблицы).

В табл. 2 приведено распределение значений максимумов для 256-битовых подстановок, рассчитанных по выражению (10), и результаты эксперимента.

Решение уравнения (6) способом подбора для байтовой подстановки приведено в табл. 3. Для ориентировочного выбора начальных значений, используемых в переборе, вполне можно опираться на результаты расчетов и экспериментов, приведенные в [21].

Таблица 2

k^* (X_1,X_2)	Pr(k^*)	Расчетное значение	Эксперимент
8	0,00004	0,01	0
10 (10,8)	0,368 – 0,00004 = 0,368	94	92
12 (12,10)	0,905 – 0,368 = 0,537	137	147
14 (14, 12)	0,9901 – 0,905 = 0,008	22	14
16 (16,14)	0,9967 – 0,9901 = 0,0066	1,71	3
18 (18,16)	0,9999– 0,9967 = 0,0032	0,819	0

Таблица 3

a_S	$\sqrt{\ln(2)32 - \ln(2\pi) - 2\ln(a_s)}$
4	4,19
5	4.13
6	4,09
8	4

Мы и в этом случае сделали небольшую коррекцию результата, ориентируясь на данные экспериментов. В качестве значения a_S рассматривалось значение $a_S = 4$ и соответственно

$$b_s = \frac{a_s}{a_s^2 + 1} \approx \frac{1}{a_s} = \frac{1}{4} = 0{,}25 \qquad (11)$$

(здесь уже учитываем результаты выполненных экспериментов, представленных в табл. 3). Для подстановок степени 2^8 имеем $\sigma = 2^{\frac{8-4}{2}} = 2^2$ и тогда $a = \sigma a_s + \mu(X) = 4\cdot 4 + 0 = 16$ и в соответствии с (21)

$$b = 4\cdot 0{,}25 = 1$$

и приходим к интегральному закону распределения максимумов полных дифференциалов уменьшенной 16-битной модели шифра в виде

$$D_{\max}(X) \approx e^{-e^{\frac{16-X}{1}}}, \quad (12)$$

или с учетом реального удвоения результатов смещений таблицы линейных аппроксимаций:

$$D_{\max}(X) \approx e^{-e^{\frac{32-X}{2}}}. \quad (13)$$

В табл. 4 представлены результаты расчетов по определению распределения значений максимумов линейных корпусов на основе интегрального закона распределения вероятностей (13).

Заметим, что по результатам ранее выполненной теоретической и экспериментальной оценки значения максимума смещения линейной аппроксимационной таблицы случайной подстановки степени $_2{}^8$ равны 32 (расчет) и 34 (эксперимент) [22].

Видно, что и в этом случае результаты экспериментов практически повторяют результаты расчетов.

Таблица 4

$k^*(X_1,X_2)$	Pr(k^*)	Число значений	Эксперимент
< 26	$3.41\ 10^{-7}$	0	0
28 (28,26)	$5{,}6\ 10^{-4} - 3{,}4110^{-7} = 5{,}6\ 10^{-4}$	0,14	0
30 (30,28)	$0{,}064 - 5{,}6\ 10^{-4} = 0{,}0638$	16	10
32 (32,30)	0,368–0,064 = 0,304	78	86
34 (34,32)	0,692 – 0,304 = 0,388	99	98
36 (36,34)	0,874 – 0,692 = 0,181	46	46
38(38,36)	0,9518 – 0,874 = 0,078	19	10
40 (40,38)	0,9821 – 0,9518 = 0,03	8	6
42 (42,40)	0,9933 – 0,9821 = 0,011	3	0
44 (44,42)	0,9975 – 0,9973 = 0,00028	0,07	0

Из расчетов следует, что вероятность получить подстановку со смещением равным 30 уже менее шести сотых, а получить значение, большее 38, – меньше семи сотых, т.е. с большой вероятностью случайно взятая байтовая подстановка будет иметь значение смещения, близкое к 34 (чаще всего встречаемое).

Таким образом, значения дифференциальных и линейных переходов (смещений) соответствующих таблиц байтовых случайных подстановок имеют ярко выраженные прогнозируемые максимумы, которые в два раза больше предельных значений (таких, например, как у AES-x S-блоков).

Подводя итог, можно в соответствии с представленными результатами ввести и более практичное определение случайной подстановки.

В частности, байтовая подстановка является случайной, если:

1) значение максимума ее XOR таблицы принимает значения 10,12;

2) значения максимумов смещений ее таблицы линейных аппроксимаций имеют значения в диапазоне 32 – 38.

Этими определениями мы уточняем критерии 4 и 5, введенные ранее. Уточнение касается наложения (выполнения) ограничений лишь на максимальные значения переходов XOR таблиц и смещений таблиц линейных аппроксимаций.

На самом деле, поскольку случайные подстановки с большой вероятностью будут давать максимальные значения дифференциальных и линейных вероятностей, то приведенные ограничения можно рассматривать лишь как проверочные.

И если для 128-битного шифра Rijndael с родными S-блоками минимальное число активизируемых S-блоков для прихода шифра к состоянию случайной подстановки по дифференциальным показателям равно 21, то для шифра со случайными подстановками потребуется активизировать минимум 32 S-блоков [23].

Это значит, что 128-битный шифр Rijndael с родными S-блоками приходит к состоянию случайной подстановки за три цикла, а шифр со случайными подстановками – за четыре [23].

256-битный шифр Rijndael приходит к состоянию случайной постановки с родными S-блоками по дифференциальным показателям при активизации минимум 42 S-блоков, а шифр со случайными S-блоками требует для прихода к случайной подстановке при активизации минимум 48 S-блоков [23].

256-битный шифр с родными S-блоками приходит к состоянию случайной подстановки по линейным показателям при активизации минимум 50 S-блоков, а шифр со случайными S-блоками требует для прихода к случайной подстановке активизации минимум 65 S-блоков [23].

Это значит, что 256-битный Rijndael приходит к состоянию случайной подстановки по линейным показателям за четыре цикла, а шифр со случайными подстановками – за пять [23].

По линейным показателям 128-битный шифр Rijndael с родными S-блоками приходит к состоянию случайной подстановки за три цикла, а шифр со случайными подстановками – за четыре [23].

Таким образом, использование случайных S-блоков увеличивает на один цикл минимальное число циклов прихода шифра к состоянию случайной подстановки.

Но, как показали эксперименты, именно случайные подстановки, сформированные без всяких ограничений, с очень большой вероятностью оказались подходящими, с точки зрения криптографических приложений, в предложенных новых конструкциях блочных симметричных шифров [23], цикловые функции которых строятся с использованием управляемых подстановок. Использование цикловых функций с управляемыми подстановками (по крайней мере, на первых циклах шифрования) позволяет увеличить минимальное число активизируемых S-блоков на этих циклах, что дает возможность реализовать динамические показатели выхода шифров к асимптотическим показателям случайных подстановок, не уступающие считающимся лучшими (отобранными по специальным методикам) S-блокам практически всех современных шифров [11 – 23].

Выводы

Таким образом, результатом выполненных исследований является уточненное определение случайной подстановки (уточненная математическая модель случайной подстановки), строящееся на свойствах выборки случайных подстановок. Теперь появилось полное понимание о том, с какими подстановками мы имеем дело при их случайном формировании. Как оказалось, с очень большой вероятностью будут получаться подстановки, для которых значения максимумов дифференциальных таблиц и значения максимумов смещений таблиц линейных аппроксимаций принимают существенно ограниченное число возможных значений. Все они концентрируются вокруг теоретических значений максимумов случайных подстановок соответствующей степени.

Как показывают эксперименты [24], случайные подстановки, взятые с выхода генератора случайных подстановок без всяких ограничений, вполне могут конкурировать с лучшими

известными конструкциями S-блоков, используемыми в современных шифрах. Увеличенные по сравнению с предельными значениями максимумов, к которым стремятся авторы большинства работ по поиску S-блоков с улучшенными показателями, могут быть компенсированы использованием в шифрах цикловых функций с увеличенным числом активизируемых S-блоков на первых циклах [24].

Список литературы:

1. Adams C. M. and Tavares S.E. The Structured design of cryptographically good S-boxes // Journal of Cryptology**,** 3(1): 27-41, 1990.

2. Forré R. Methods and instruments for designing S-boxes // Journal of Cryptology, 2(3): 115-130, 1990.

3. Nyberg K. Perfect nonlinear S-boxes // Advances in cryptology -EUROCRYPT91, volume 547, Lecture Notes in Computer Science, pp. 378-386. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

4. Nyberg K. On the construction of highly nonlinear permutations // Advances in cryptology – Proceedings of EUROCRYPT'92 (1993) vol. 740, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 92-98.

5. Nyberg K. Differentially uniform mappings for cryptography // Advances in cryptology – Proceedings of EUROCRYPT'93 (1994) vol. 765, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York, pp. 55-65.

6. Claudia Peerez Ruisanchez A NEW ALGORITHM TO CONSTRUCT S-BOXES WITH HIGH DIFFUSION // International Journal of Soft Computing, Mathematics and Control (IJSCMC). Vol. 4, No. 3, August 2015. DOI : 10.14810/ijscmc.2015.4303 41.

7**.** Seberry J., Zhang X.-S. and Zheng Y. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions // Inforsation and Cosputation. Vol. 119, No 1, pp. 1-13, 1995.

8. Pasalic E., Johansson T., Saitra S., Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity // Workshop of Coding and Cryptography, Electronic Notes in Discrete Mathematics. Elsevier, January 2001.

9. Xiao G-Z and Massey J.L. A Spectral Characterization of Correlation-Immune Combining Functions // IEEE Transaction on Information Theory. Vol. 34, №.3 (1988), pp. 569-571.

10. Clark J., Jacob J., Stepney S., Saitra S. and Sillan W. Evolving of Boolean functions satisfying sultiple criteria", proceedings of INDOCRYPT'02, LNCS vol 2551, pages 246-259, Springer, 2002.

11. Yücel M.D. IAM501-Introduction to Cryptography. Institute of Applied Mathematics METU, Ankara, Turkey (9700501), 2002, p. 1-28.

12. Лисицкая И.В. К вопросу построения долговременных ключей для алгоритма ГОСТ 28147-89 // Информационно-управляющие системы на железнодорожном транспорте. 1997. № 3. С. 54–57.

13. Lysytska I.V., Koriak A.S., Golovashich S.A., Oleshko O.I., Oleinik R.V. The selection criteria of random substitution tables for symmetric enciphering algorithms // Abstracts of XXVIth General Assembly. Toronto, Ontario Canada, August 13-21, 1999. P. 204.

14. Горбенко И.Д., Лисицкая И.В. Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 28147-89 //. Радиотехника. 1997. Вып 103. С. 121–130.

15. Лисицкая И.В. Оценка числа случайных подстановок с заданным распределением парных разностей XOR таблиц и смещений таблиц линейных аппроксимаций / И.В. Лисицкая, А.В. Широков, Е.Д. Мельничук, К.Е. Лисицкий // Прикладная радиоэлектроника. Харьков : ХНУРЭ, 2010. Т. 9, № 3. С. 341-345.

16. Долгов В.И. Случайные подстановки в криптографии / В.И. Долгов, И.В. Лисицкая, К.Е. Лисицкий // Радіоелектронні та комп'ютерні системи. 2010. № 5 (46). С. 79-85.

17. Лисицька І.В. Экспериментальная проверка работоспособности новых критериев отбора случайных подстановок / І.В. Лисицька, К.Є. Лисицкий, А.В. Широков, Е.Д. Мельничук // Радіоелектронні та комп'ютерні системи. 2010. № 6 (47). С. 87-93.

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

19. Лисицкий К.Е. О методике оценки законов распределения вероятностей максимумов полных дифференциалов и смещений линейных оболочек блочных симметричных шифров // Прикладная радиоэлектроника. Харьков : ХНУРЭ, 2015. Т. 14, № 4. С. 335-338.

20. Лисицкая И.В. Свойства законов распределения XOR таблиц и таблиц линейных аппроксимаций случайных подстановок // Вісник Харк. нац. ун-ту ім. В.Н. Каразіна. 2011. №960, Вип.16. С. 196-206.

21. 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.

22. Долгов В.И. Свойства таблиц линейных аппроксимаций случайных подстановок / В.И. Долгов, И.В. Лисицкая, О.И. Олешко // Прикладная радиоэлектроника. Харьков : ХНУРЭ, 2010. Т. 9, № 3. С. 334-340.

23. Долгов В.И. S-блоки для современных шифров. / В.И. Долгов, Е.В. Мельничук // Радиотехника. 2012. Вып.171. С. 121-133.

24. Dolgov V.I. The new concept of block symmetric ciphers design / V.I. Dolgov, I.V. Lisitska, K.Ye. Lisitskyi // Telecom RadEng. v. 76, 2017, i. 2. pages 157-184. DOI: 10.1615.

Поступила в редколлегию 08.09.2020

Сведения об авторах:

Лисицкий Константин Евгеньевич – Харьковский национальный университет имени В.Н. Каразина, аспирант кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Украина, e-mail: konstantin.lisickiy@mail.ru

Лисицкая Ирина Викторовна – канд. техн. наук, Харьковский национальный университет имени В.Н. Каразина, профессор кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Украина, e-mail: konstantin.lisickiy@mail.ru