УДК 681.3.06

И.В. ЛИСИЦКАЯ, К.Е. ЛИСИЦКИЙ, А.В. ШИРОКОВ, Е.Д. МЕЛЬНИЧУК

Харьковский национальный университет радиоэлектроники, Украина

ЭКСПЕРИМЕНТАЛЬНАЯ ПРОВЕРКА РАБОТОСПОСОБНОСТИ НОВЫХ КРИТЕРИЕВ ОТБОРА СЛУЧАЙНЫХ ПОДСТАНОВОК

Излагается сущность новых критериев отбора случайных подстановок, строящихся на основе оценки близости интегральных законов распределения вероятностей переходов таблиц XOR разностей и таблиц линейных аппроксимаций проверяемых подстановок теоретическим распределениям, формируемым расчетным путем. Приводятся результаты экспериментальной оценки влияния на показатели отбора (на число подстановок, прошедших установленные границы) граничных значений критериев как отдельно каждого из новых двух правил, так и при их совместном использовании. Эксперименты распространяются и на совместное использование новых правил отбора и правил, предложенных для использования авторами ранее. Экспериментами подтверждается более высокий (жесткий) уровень прохождения новых критериев отбора. Отмечаются направления дальнейшего разворачивания работ по проверке эффективности предлагаемой методики.

***Ключевые слова**: случайная подстановка, таблица XOR разностей подстановки, таблица линейных аппроксимаций подстановки, критерии отбора случайных подстановок.*

Введение

В нашей предыдущей работе [1] были сформулированы два новых критерия отбора случайных подстановок, один, – строящийся с использованием закона распределения однотипных переходов $\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$, $k=0,1,\ldots,k^*$ таблицы XOR разностей входов $\Delta X,\Delta Y\in Z_2^n$ подстановки, приписываемых к ненулевым характеристикам, и второй, строящийся с использованием закона распределения $\Pr\left(\lambda^*(\alpha,\beta)=2k\right)$, $k=0,1,\ldots,k^*$ однотипных переходов для пар масок $\alpha,\beta\in Z_2^n$, $\alpha,\beta\neq 0$ таблицы линейных аппроксимаций подстановки. Напомним, что значение k* представляет собой половину от максимального числа переходов XOR таблицы и максимального смещения линейной аппроксимационной таблицы (*LAT*) случайной подстановки соответственно. Они были сформулированы в дополнение к трем ранее введенным критериям отбора случайных подстановок, которые в свое время были нами предложены в работе [2] как некий эквивалент известным критериям случайности двоичных последовательностей (критерий уравновешенности, критерий серий и критерий корреляций).

Основная идея построения этих критериев заключается в том, чтобы перенести свойства криптографических преобразований, свойственных блочным симметричным шифрам, рассматриваемым как подстановки, на подстановочные конструкции в целом, т.е. была поставлена задача расширить критерии отбора случайных подстановок за счет дополнительных критериев случайности, характерных именно для шифров.

Цель этих поисков и исследований – найти более совершенную методику построения подстановок с хорошими криптографическими свойствами, являющуюся альтернативой известных далеко не совершенных подходов.

1. Сущность новых критериев отбора случайных подстановок

Напомним сначала сущность предлагаемых критериев отбора. В работе [1] они были сформулированы в виде четвертого и пятого критериев так:

Подстановка удовлетворяет критерию случайности 4, *если закон распределения переходов*

$$\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right),\ \Delta X,\Delta Y\in Z_2^n,\ k=0,1,\ldots,k^*$$

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

Подстановка удовлетворяет критерию случайности 5, *если закон распределения однотипных переходов* $\Pr\left(\lambda^*(\alpha,\beta)=2k\right)$, $k=0,1,\ldots,k^*$, *для масок входа и выхода* $\alpha,\beta\neq 0$, $\alpha,\beta\in Z_2^n$ *её таблицы*

линейных аппроксимаций соответствует по критерию согласия Колмогорова теоретическому закону распределения линейных аппроксимаций случайных подстановок, т.е. наибольшее значение модуля разности теоретического и эмпирического законов распределения вероятностей удовлетворяет условию $\left|F_T(x_k) - F(x_k)\right| \le c$.

Здесь k* половинные значения максимумов полных дифференциалов XOR таблицы и смещения LAT случайной подстановки соответственно.

Значения граничных параметров b и c были определены как подлежащие уточнению по результатам экспериментов.

Напомним также определения соответствующих законов распределения вероятностей, которые фигурируют в приведенных критериях отбора.

Следуя работе [2], пусть $\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right)$ будет вероятностью того, что значение ячейки $\Lambda_\pi(\Delta X, \Delta Y)$ дифференциальной таблицы случайно взятой подстановки π порядка 2^n для перехода входной разности ΔX в соответствующую выходную разность ΔY будет равно $2k$. Эта вероятность определяется теоремой.

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

$$\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right) = \\ = \begin{pmatrix} 2^{n-1} \\ k \end{pmatrix}^2 \cdot \frac{k! \cdot 2^k \cdot \Phi(2^{n-1} - k)}{2^n!}, \qquad (1)$$

где функция $\Phi(d)$ *определяется выражением*

$$\Phi(d) = \sum_{i=0}^{d} (-1)^i \cdot \begin{pmatrix} d \\ i \end{pmatrix}^2 \cdot 2^i \cdot i! \cdot (2d - 2i)!. \qquad (2)$$

Здесь $\Lambda_\pi(\Delta X, \Delta Y)$ – значение XOR таблицы подстановки $\pi \in S_2^n$ (её ячейки) для пары значений разностей её входов и выходов ΔX, $\Delta Y \in Z_2^n$, $\Delta X = X \oplus X'$, $\Delta Y = \pi(X) \oplus \pi(X')$ (для соответствующего перехода $\Delta X \to \Delta Y$):

$$\Lambda_\pi(\Delta X, \Delta Y) \overset{\text{def}}{=} \\ \overset{\text{def}}{=} \#\left\{\Delta X = X \oplus X' / \Delta X \in Z_2^n, \Delta Y = \pi(X) \oplus \pi(X')\right\},$$

$\oplus$ – операция побитного сложения n-битных векторов.

Закон распределения вероятностей (1) получен для полного множества подстановок. Однако замечательным его свойством является то, что он оказывается справедливым и для усеченного (причем, существенно) множества подстановок, формируемых симметричными шифрами, так как такие преобразования, осуществляемые на различных ключах зашифрования, формируют множество подстановок случайного типа.

Также закон распределения (1), (2), полученный на основе анализа всего множества $2^n!$ равновероятных подстановок, является справедливым и для множества ячеек таблицы XOR разностей каждой отдельно взятой случайной подстановки степени 2^n. В частности для рассматриваемого закона распределения вероятностей, примененного к отдельной подстановке, с большой точностью выполняется условие нормировки

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

Здесь k* представляет собой половину от максимального значения числа переходов XOR таблицы случайной подстановки.

Аналогичное по содержанию утверждение получено для вероятности значений линейных аппроксимационных таблиц $LAT_\pi^*(\alpha, \beta)$ случайных подстановок.

Утверждение 2. *Пусть* $\lambda^*(\alpha, \beta)$ *будет случайным значением распределения* $LAT_\pi^*(\alpha, \beta) = \left|LAT_\pi(\alpha, \beta) - 2^{n-1}\right|$, *когда подстановка* π *выбрана равновероятно из множества* 2^n *и маски* α, β *не нулевые. Тогда* $\lambda^*(\alpha, \beta)$ *принимает только четные значения и*

$$\Pr\left(\lambda^*(\alpha, \beta) = 2k\right) = \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ 2^{n-2} - k \end{pmatrix}^2 \qquad (3)$$

для $|k| \le 2^{n-2}$.

Здесь линейная аппроксимационная таблица LAT_π подстановки π с элементами $LAT_\pi(\alpha, \beta)$, определяется для каждой пары $\alpha, \beta \in Z_2^n$ соотношением

$$LAT_\pi(\alpha, \beta) \overset{\text{def}}{=} \\ \overset{\text{def}}{=} \#\left\{X / X \in Z_2^n, \bigoplus_{i=1}^{n} X[i] \cdot \alpha[i] = \bigoplus_{i=1}^{n} \pi\left(X[i]\right) \cdot \beta[i]\right\},$$

X_i обозначает i-й бит n-битного вектора $X \in Z_2^n$, а $'\cdot'$ обозначает операцию побитного логического ИЛИ.

И для этого распределения с высокой точностью справедлива нормировка

$$\sum_{k=0}^{k^*} \Pr\left(\lambda^*(\alpha,\beta) = 2k^*\right) = 1 . \qquad (4)$$

Здесь k* – половинное значение максимума смещения таблицы $\mathrm{LAT}_\pi^*(\alpha,\beta)$.

На основе полученных результатов в [1] и было предложено новое (или уточненное) определение случайной подстановки.

Определение 2. *Подстановка является случайной, если вместе с выполнением критериев случайности* 1–3 *для ячеек её XOR таблицы и таблицы линейных аппроксимаций выполняются законы распределения вероятностей* (1) *и* (4).

Правила проверки соответствия закону распределения вероятностей переходов таблиц дифференциальных разностей названы в работе [1] *критерием случайности* 4, а правила проверки соответствия закону распределения переходов таблиц линейных аппроксимаций определены в [1] как *критерий случайности* 5

Наша ближайшая задача выполнить проверку работоспособности и эффективности дополнительных критериев 4 и 5.

2. Выбор значений параметров b и c для новых критериев отбора

В качестве объекта исследований этого раздела станут подстановки порядка 2^4 и 2^8, являющиеся наиболее популярными при конструировании современных шифров.

В соответствии с методикой применения критерия Колмогорова, изложенной в работе [1], необходимо иметь ″эталонные портреты″ проверяемых подстановок.

Результаты расчетов, выполненных по формулам (1), (2) и (3), представлены в табл. 1 – 4.

Таблица 1

Распределение парных разностей для XOR таблицы подстановки порядка 2^4 (расчёт)

$2k$	Число ячеек	Вероятность
0	132,165	0,587399
2	70, 1592	0,311819
4	18,7723	0,0834326
6	3,381	0,0150289
8	0,4662	0,002072

Здесь представлены расчетные значения для числа ячеек одного и того же типа без округления в сторону ближайшего целого, так как в дальнейших вычислениях (при определении интегрального закона распределения вероятностей) можно использовать и дробные значения, – это не мешает последующему сравнению результатов с пороговыми.

Нам также понадобятся расчетные соотношения для граничных значений параметров b и c, которые мы будем уточнять в процессе экспериментов. В соответствии с [1] для подстановок порядка 2^4 (в критерии Колмогорова используется параметр n = 225) имеем

$$\frac{\lambda_0}{\sqrt{n}} = \frac{1,23}{15} = 0,082 .$$

Соответственно для подстановок порядка 2^8 (параметр критерия Колмогорова $n = 255^2$) имеем соответственно $\frac{\lambda_0}{\sqrt{n}} = \frac{1,23}{255} = 0,00482$.

Эти граничные значения и расчетные данные из приведенных выше таблиц были использованы при разработке и настройке программного комплекса, реализующего изложенную в [1] методику отбора случайных подстановок.

Таблица 2

Распределение парных разностей для XOR таблицы подстановки порядка 2^8 (расчёты с округлением в сторону ближайшего целого)

$2k$	Число ячеек	Вероятность
0	39363	0,605345
2	19758	0,303855
4	4959	0,0762627
6	830	0,0127609
8	104	0,00160149
10	10	0,000160795
12	1	0,000013454

Таблица 3

Распределение переходов LAT таблицы подстановки порядка 2^4

$\lvert 2k \rvert$	Число ячеек	Вероятность
0	85,6643	0,38073
2	109,6504	0,487335
4	27,4126	0,12183
6	2,23776	0,00994
8	0,03494	0,0001755

Таблица 4

Распределение переходов для LAT таблицы подстановки порядка 2^8

$\|2k\|$	Число ячеек	Вероятность
0	6466	0,0994438
2	12538	0,192818
4	11424	0,1756863
6	9982	0,1535101
8	7872	0,121061
10	5952	0,091534
12	4228	0,065021
14	2822	0,0433987
16	1768	0,0271895
18	1040	0,0159938
20	574	0,00882737
22	298	0,00229178
24	146	0,00458285
26	66	0,00101499
28	28	0,00043060
30	10	0,00015378
32	4	0,00006151
34	2	0,000030757

Результаты экспериментов, выполненных с применением разработанного программного комплекса, представлены в табл. 5 – 8, в которых обобщаются результаты оценки эффективности отбора (фильтрации) случайных подстановок (ДТ – дифференциальных таблиц и LAT – таблиц линейных аппроксимаций) при использовании критериев с различными граничными значениями параметров b и c.

Примечательно, что в обоих случаях (как для XOR таблиц, так и для LAT) расчетные значения параметров критерия Колмогорова оказались весьма мягкими (допускается разница теоретического и расчетного значений интегральных законов распределения в абсолютном исчислении равная 18 – это, по-видимому, очень много).

Таблица 5

Прохождение подстановок порядка 2^4 при использовании критерия отбора 4 (ДТ)

Значение параметра *b* в критерии 4	Процент подстановок, прошедших критерий из 100000
0,082	98,0527
0,041	88,113
0,02	51,974
0,01	22,931
0,005	2,4841
0,0049	2,4767
0,00487333334	2,4635
0,00487333333	0

Таблица 6

Прохождение подстановок порядка 2^8 при использовании критерия отбора 4 (ДТ)

Значение параметра *c* в критерии 5	Процент подстановок, прошедших критерий из 100000
0,005	99,95
0,004	99,04
0,003	95,33
0,002	81,57
0,001	46,66
0,0005	17,00
0,0003	6,82
0,0001	0,028
0,00005	0,003
0,00001	0

Таблица 7

Прохождение подстановок порядка 2^4 при использовании критерия отбора 5 (LAT)

Значение параметра *b* в критерии 4	Процент подстановок, прошедших критерий из 100000
0,082	93,861
0,041	75,992
0,02	37,697
0,01	8,897
0,009	7,011
0,008	6,095
0,007	5,893
0,006	2,832
0,005	0

Таблица 8

Прохождение подстановок порядка 2^8 при использовании критерия отбора 5 (*LAT*)

Значение параметра *c* в критерии 5	Число подстановок, прошедших критерий из 100
0,01	100
0,005	79
0,004	54
0,003	24
0,002	7
0,001	0

И в первом и во втором случае установленные границы проходят почти 100% подстановок. По мере уменьшения пороговых значений b и c число подстановок прошедших ″ворота″ быстро падает. По-видимому, целесообразно будет выбрать более жесткие границы отбора подстановок, что можно будет уточнить при анализе свойств отобранных подстановок, например, с использованием известных алгебраических методов.

Дальнейшие усилия были направлены на оценку показателей совместного использования нескольких критериев отбора.

Результаты экспериментов этого этапа иллюстрируют таблицы 9 – 11.

Сначала были оценены показатели отбора только при использовании 4-го и 5-го критериев отбора каждого отдельно и обоих критериев одновременно (табл. 9). На втором этапе были подключены для анализа и первые три критерия отбора (табл. 10).

Таблица 9

Данные отбора подстановок порядка 2^4

Критерий	Параметры критериев *b* и *c*	Прошло, в % (из 100000)
ТД	0,00518	2,524
ЛАТ	0,006	2,837
Оба критерия		1,883

Приведем здесь примеры подстановок, прошедших оба критерия (нижние строки нормализованной матрицы – подстановки):

(10 13 4 8 5 2 15 1 7 6 14 3 12 9 0 11),
(5 0 9 13 15 10 14 12 4 11 3 6 1 7 2 8).

Таблица 10

Данные отбора подстановок порядка 2^4

Критерий	Параметры критерия	Прошло
Инверсии	60-70	5709/10000
Возрастания	6-10	
Циклы	2-6	
ТД	0,00518	1,605
ЛАТ	0,006	0,0163
Все критерии		0,0025

Как следует из представленных результатов, все критерии отбора ″работают независимо″ (ни один из них не подменяет другой).

Примечательно, что подстановки, прошедшие рассматриваемую группу критериев, содержат фиксированные точки.

Но это не должно быть странным, так как при изучении циклических свойств уменьшенных моделей многих шифров (Rijndael, Камелия, ADE, Лабиринт и др. [3 – 6] и др.) было установлено, что практически для каждого ключа зашифрования существуют не шифруемые тексты (это принципиальное свойство многоцикловых процедур зашифрования симметричных шифров).

Отметим также, что в работе [4] приведена теорема о фиксированных точках случайных подстановок, в соответствии с которой для подстановки π, взятой случайно из множества S_2^n, вероятность, что π имеет с фиксированных точек есть $1/c!e$.

Как следует из этого результата, вероятность получить подстановку с фиксированными точками получается достаточно большой (в самом общем случае каждая третья подстановка имеет фиксированную точку).

В таблицах 10 – 14 представлены результаты применения критериев отбора для подстановок порядка 2^8.

Следует заметить, что объем вычислений существенно возрастает с увеличением порядка постановок (в основном за счет вычисления таблиц линейных аппроксимаций).

Поэтому выборки, на которых строился анализ подстановок порядка 2^8, взяты по объему на порядок меньше, чем для подстановок порядка 2^4.

Таблица 10

Данные отбора подстановок порядка 2^8

Критерий	Параметры критериев	Прошло
ТД	0,002	82/100
ЛАТ	0,005	79/100
Оба критерия		66/100
Цикл. Инв. Возр.	a =1	41476/100000
Все критерии		22/100

Таблица 11

Данные отбора подстановок порядка 2^8

Критерий	Параметры критериев	Прошло
ТД	0,001	42/100
ЛАТ	0,004	54/100
Оба критерия		29/100
Цикл. Инв. Возр.	a =1	41476/100000
Все критерии		13/100

Как следует из приведенных результатов, для подстановок порядка 2^8 допускаются значения расхождений эмпирических и теоретических распределений существенно (на порядок и более) меньшие, чем для подстановок порядка 2^4.

Таблица 12

Данные отбора подстановок порядка 2^8

Критерий	Параметры критериев	Прошло
ТД	0,001	42/100
ЛАТ	0,003	24/100
Оба критерия		12/100
Цикл. Инв. Возр.	a =1	41476/100000
Все критерии		5/100

Таблица 13

Данные отбора подстановок порядка 2^8

Критерий	Параметры критериев	Прошло
ТД	0,002	82/100
ЛАТ	0,003	24/100
Оба критерия		22/100
Цикл. Инв. Возр.	a =1	41476/100000
Все критерии		6/100

Таблица 14

Данные отбора подстановок порядка 2^8

Критерий	Параметры критериев	Прошло
ТД	0,002	82/100
ЛАТ	0,002	7/100
Оба критерия		5/100
Цикл. Инв. Возр.	a =1	41476/100000
Все критерии		1/100

Заключение

Результаты исследований, выполненных в данной работе, позволяют сделать следующие выводы:

1. В целом подтверждена работоспособность предложенных в работе [1] дополнительных критериев отбора.

2. Критерии случайности 4 и 5 являются в значительной степени независимыми, каждый из критериев вносит свою долю в отсев подстановок исключаемых из кандидатов на случайные подстановки.

3. Граничные значения параметров отбора (допустимых расхождений эмпирического и теоретического законов распределения вероятностей) существенно зависят от порядка исследуемых подстановок. С увеличением порядка подстановки минимально достижимая степень расхождения распределений быстро уменьшается.

4. Критерии отбора по дифференциальным и линейным свойствам являются более жесткими. При уменьшении значения допустимого расхождения распределений число подстановок прошедших проверку по всем критериям быстро уменьшается.

5. Предлагаемая система критериев представляется достаточно гибкой и может рассматриваться как конструктивный подход к отбору подстановок, приближающихся по своим свойствам к шифрующим многоцикловым преобразованиям.

Представляется целесообразным продолжить исследование рассмотренного в работе подхода для окончательной оценки его перспективности.

Так, в число задач дальнейших исследований можно выделить:

– проверку свойств отобранных по рассмотренным критериям подстановок с помощью алгебраических методов, о которых упоминалось во введении к работе. В их числе такие как: сбалансированность булевых функций, корреляционный иммунитет, критерий распространения (строгий лавинный критерий) $KP(k)$, алгебраические степени булевых функции $\deg(f)$, а также соответствующие характеристики S-блоков – критерий битовой независимости (*BIC*), максимальный порядок строгого лавинного критерия (*MOSAC*) и многие другие;

– уточнение параметров отбора, использованных при построении рассмотренных критериев с учетом более детальных данных изучения алгебраических показателей булевых функций соответствующих S-блоку.

– исследование влияния на результирующие показатели стойкости шифров применения при их реализации конструкций S-блоков, полученных с помощью рассмотренных в работе методов.

Литература

1. Лисицкая И.В. Случайные подстановки в криптографии / И.В. Лисицкая, К.Е. Лисицкий // Радиоэлектронные и компьютерные системы. – 2010. – № 5 (46). – С. 79–85.

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

3. Долгов В.И. Анализ циклических свойств блочных шифров / В.И. Долгов, И.В. Лисицкая, В.И. Руженцев // Прикладная радиоэлектроника – 2007. – Т.6, №2 – С. 257-263.

4. O'Connor L.J. On the Distribution of Characteristics in Bijective Mappings / L.J. O'Connor // Advances in Cryptology. EUROCRIPT 93, Lecture Notes in Computer Science, T. Helleseth ed., Springer-Verlag, , 1994. – V. 795. – P. 360–370.

5. Luke O'Connor. Properties of Linear Approximation Tables. Email: oconnor@dsts. Edu. au, 1995.

6. Courtois Nicolas T. Statistics of Random Permutations and the Cryptanalysis Of Periodic Block Ciphers / Nicolas T. Courtois, Gregory V. Bard, Shaun V. Ault.// J. Math. Crypt. 2, 2008. – P. 1–20.

Поступила в редакцию 15.01. 2010

Рецензент: д-р техн. наук, проф., декан факультета компьютерных наук Л.С. Сорока, Харьковский национальный университет им. В.Н. Каразина, Харьков.

ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ ТА ЕФЕКТИВНОСТІ НОВИХ КРИТЕРІЇВ ВІДБОРУ ВИПАДКОВИХ ПІДСТАНОВОК

І.В. Лисицька, К.Є Лисицький, О.В. Широков, Є.Д. Мельничук

Викладається сутність критеріїв відбору випадкових підстановок, що будуються на основі оцінки близькості інтегральних законів розподілів ймовірностей переходів таблиць XOR різниць та таблиць лінійних апроксимацій підстановок, що перевіряються, теоретичним розподілам, сформованим розрахунковим шляхом. Наводяться результати експериментальної оцінки впливу на показники відбору (на число підстановок, що проходять встановлені межі) граничних значень критеріїв як окремо кожного з нових двох правил, так і за їх сумісному застосуванні. Експерименти поширюються й на сумісне використання нових правил відбору й правил, запропонованих для використання авторами раніше. Експериментами підтверджується більш високий (жорсткий) рівень проходження нових критеріїв відбору. Відмічаються напрямки подальшого розгортання робіт за перевіркою ефективності запропонованої методики.

Ключові слова: випадкова підстановка, таблиця XOR різниць підстановки, таблиця лінійних апроксимацій підстановки, критерії відбору випадкових підстановок.

EXPERIMENTAL VERIFICATION OF CAPACITY AND EFFICIENCY OF NEW CRITERIA OF SELECTION OF RANDOM SUBSTITUTIONS

I.V. Lysytska, K.E. Lysytskay, A.V. Shurokov, E.D. Melnichuk

The essence of selection criteria of random substitutions built on the estimation of integral distribution laws similarity of transition probabilities distributions of difference distribution and linear approximation tables verified by theoretical distribution formed by computational way is discussed. There are given the results of experimental estimation of the influence to selection indexes (to the number of substitutions passed the given thresholds) of criteria border values for separate application of each of new proposed rules, as for their common application. Experiments are also expanded to common application of both new rules and rules proposed by authors earlier. A higher (stronger) passing level for the new selection criteria is also approved by experiments. There are shown further research directions for effectiveness verification of proposed method.

Key words: random permutation, difference distribution table, linear approximations table, the criteria for random permutations selection.

Лисицкая Ирина Викторовна – канд. техн. наук, доцент, доцент кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники, Харьков, e-mail: dolgovvi@mail.ru.

Лисицкий Константин Евгеньевич – ученик лицея № 89, Харьков, e-mail: dolgovvi@mail.ru.

Широков Алексей Викторович – аспирант Харьковского национального университета радиоэлектроники, Харьков, Украина, e-mail: alexey.cpp@gmail.com.

Мельничук Евгений Дмитриевич – студент факультета компьютерной инженерии Харьковского национального университета радиоэлектроники, Харьков, Украина, e-mail: timeslip@rambler.ru.