УДК 681.3.06

В.И. ДОЛГОВ, И.В. ЛИСИЦКАЯ, К.Е. ЛИСИЦКИЙ

Харьковский национальный университет радиоэлектроники, Украина

СЛУЧАЙНЫЕ ПОДСТАНОВКИ В КРИПТОГРАФИИ

Обсуждаются известные подходы к конструированию подстановок (S-блоков) с высокими криптографическими показателями. Выделяется подход к построению (отбору) S-блоков, развитый в свое время в работах авторов, строящийся на основе проверки показателей случайности подстановок (числа их инверсий, возрастаний и циклов). В качестве дальнейшего развития этого подхода предлагается новое определение случайной подстановки, которое связывается с дополнительной проверкой близости законов распределения переходов таблиц разностей и таблиц линейных аппроксимаций S-блоков теоретическим распределениям, найденным в последних работах авторов. Приводится само правило оценки близости теоретических и эмпирических законов распределения вероятностей, строящиеся с помощью критерия согласия Колмогорова. Формулируется задача по выполнению более тщательной проверки подстановок, прошедших предложенные критерии случайности, на соответствие их криптографических показателей другим известным критериям, в частности, строящимся с использованием и алгебраических методов.

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

Введение

Интерес и внимание к исследованию и разработке процедур генерации криптографически стойких подстановочных преобразований (S-блоков) возник в начале 90-х годов прошедшего столетия [1 – 6 и др.]. Он стал закономерным исходом изучения и исследования специалистами надежности американского стандарта симметричного шифрования DES, завоевавшим к тому времени мировой авторитет и признание (ставшим фактически всемирным стандартом).

К этому же времени относится появление работы израильских ученых-криптографов Бихама и Шамира [7], предложивших атаку дифференциального криптоанализа на шифр DES, а двумя годами позже работы Мацуи [8], посвященной линейному криптоанализу – второму новому типу криптонападения на DES.

Эти работы стали заметным стимулом дальнейшего разворачивания работ, посвященных исследованию и анализу S-блоковых конструкций и алгоритмов [9 – 16 и мн. другие], может быть часто не опирающиеся прямо на S-блоки, но, тем не менее, имеющие к ним самое непосредственное отношение.

Сегодня эти работы, конечно уже вышли далеко за рамки шифра DES. Появилось множество новых решений по построению алгоритмов шифрования. На смену самого шифра DES в США не так уж и давно принят новый стандарт шифрования AES (FIPS–197). Естественно, что параллельно с развитием техники конструирования шифров происходило и совершенствование методов криптоанализа, направленных на преодоление показателей стойкости, закладываемых в шифр его разработчиками.

Остается отметить, что и сегодня вопросы построения более совершенных процедур шифрования и алгоритмов криптографической защиты информации в целом не потеряли своей актуальности и в центре внимания криптографов и математиков продолжают оставаться методы и алгоритмы конструирования новых шифров и в том числе методы (генерации) более совершенных S-блоковых конструкций.

Мы уже обращались в наших работах к обсуждению подходов к конструированию S-блоков с высокими криптографическими показателями [17, 18].

Отмечалось, что к сегодняшнему дню уже можно насчитать огромное число публикаций, посвященных этой проблеме.

Наиболее плодотворным рассматривается подход, основанный на алгебраических методах описания S-блоков с помощью аппарата булевых функций.

Наш анализ, однако, показывает, что, несмотря на красивый математический аппарат, позволяющий выполнить строгое обоснование свойств конструируемых S-блоков, предлагаемые подходы либо дают решения, ориентированные на определенные классы шифров (например, DES-подобные), часто не лишенные слабостей, либо оказыва-

ются достаточно сложными для практического применения, не говоря уже о присущих им ограничениях (например, метод работает только для S-блоков нечетного порядка или для несимметричных S-блоков).

Было отмечено [18], что более прогрессивным выглядит использование для построения S-блоков отдельных предложений, имеющихся в отмеченных разработках, в частности, предложений (соображений) К. Ниберг. Именно они нашли дальнейшее развитие и практическое применение в конструкциях S-блоков, построенных в процессе создания новых блочных симметричных шифров.

Мы хотим здесь напомнить и другой подход к построению (отбору) подходящих S-блоков, развитый в свое время в наших работах [19, 20] и др. Он строится на основе изучения (определения) показателей случайности блоков подстановок и последующего отбора ″хороших″ S-блоков с помощью проверки их показателей случайности (инверсий, возрастаний и циклов).

Последние наши исследования шифрующих преобразований как случайных подстановок [21 и др.], показали, что этот подход заслуживает дальнейшего развития.

Возникла идея перенести свойства криптографических преобразований, рассматриваемых как подстановки и на подстановочные конструкции в целом, т.е. расширить критерии отбора случайных подстановок за счет дополнительных критериев случайности, характерных именно для шифров.

Работа посвящена разработке и исследованию перспективности этой идеи.

1. Известный подход к определению случайных подстановок и его усовершенствование

Напомним, что ранее в нашей работе [20] понятие случайной подстановки было определено следующим образом.

Определение 3. *Случайной подстановкой считается подстановка, которая удовлетворяет одновременно трем критериям случайности:*

1. *Число инверсий* η_n *в подстановке степени n приблизительно равно числу "антиинверсий", а практически находится в границах*

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

2. *Число циклов* ξ_n *в подстановке степени n близко к* $\ln n$*, а практически*

$$\left|\xi_n - \ln n\right| \le a\sigma_\xi, \quad \sigma_\xi = \sqrt{\ln n}.$$

3. *Число возрастаний* θ_n *в подстановке степени n приблизительно равно числу убываний, а практически*

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

В этих соотношениях a – параметр, выбираемый в значительной степени из субъективных соображений. В наших предложениях использовалось значение a = 1.

Дальнейшее внимание сосредотачивается на последних наших публикациях [21, 22], посвященных исследованию дифференциальных и линейных свойств случайных подстановок и подстановочных преобразований, развивающих результаты работ Luka O'Connora [23 – 25].

В этих работах мы приводим свои варианты доказательства двух утверждений, сформулированных в работах Luka O'Connora, но не доказанных им в полном объеме, которые характеризуют дифференциальные и линейные свойства случайных подстановок. Напомним здесь их, так как они являются важными для дальнейшего.

В обозначениях работы [23] пусть $\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right)$ будет вероятностью того, что значение ячейки 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* $\Delta X, \Delta Y \in Z_2^n$ *в предположении, что подстановка* π *выбрана равновероятно из множества* S_2^n *и* $0 \le k \le 2^{n-1}$,

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

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

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

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.

Такие преобразования, осуществляемые на различных ключах зашифрования, как показывает

практика, формируют множество подстановок случайного типа. Об этом свидетельствуют многочисленные результаты экспериментов. И это еще не все!

Получается, что для множества подстановок, определяемых шифрующими преобразованиями, выполняется свойство, напоминающее эргодическое свойство случайных процессов (среднее по множеству реализаций совпадает со средним по времени для одной достаточно длинной реализации [27]).

Это свойство проявляется в том, что закон распределения (1), 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.

Подтверждением этого факта является то, что для закона распределения вероятностей $\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$, рассматриваемого применительно к отдельной подстановке, с высокой точностью выполняется условие нормировки характерное для полной группы событий

$$\sum_{k=0}^{k^*}\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)=1. \qquad (3)$$

Здесь $\Lambda_\pi(\Delta X,\Delta Y)-$ значение ячейки XOR таблицы для фиксированной пары значений разностей входов и выходов $\Delta X,\Delta Y\in Z_2^n$, $\Delta X=X+X'$, $\Delta Y=\pi(X)+\pi(X')$ подстановки $\pi\in S_2^n$.

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

Выполненные многочисленные проверки подтверждает и это положение.

Совершенно аналогичное по содержанию утверждение справедливо для вероятности значений линейных аппроксимационных таблиц $LAT_\pi^*(\alpha,\beta)$ случайных подстановок [25].

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

$$\Pr\left(\lambda^*(\alpha,\beta)=2k\right)=\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\begin{pmatrix}2^{n-1}\\2^{n-2}+k\end{pmatrix} \qquad (4)$$

для $|k|\le 2^{n-2}$.

И для этого распределения справедлива нормировка

$$\sum_{k=-k^*}^{k^*}\Pr\left(\lambda^*(\alpha,\beta)=2k^*\right)=1. \qquad (5)$$

Здесь k* – половинное значение максимального для таблицы $LAT_\pi^*(\alpha,\beta)$ смещения.

На основе полученных результатов представляется логичным в дополнение к уже известным подходам сформировать (сформулировать) новое (или уточненное) определение случайной подстановки, дополняющее приведенные выше критерии.

Определение 2. *Подстановка является случайной, если вместе с выполнением критериев случайности* 1–3 *для заполнений ячеек её XOR таблицы и таблицы линейных аппроксимаций выполняются законы распределения вероятностей* (1), (2) (*критерий случайности* 4) *и* (4) (*критерий случайности* 5).

Дальнейший материал будет посвящен построению конструктивного правила проверки соответствия отдельно взятой подстановки приведенным выше законам распределения вероятностей.

2. Построение нового правила отбора случайных подстановок

Для проверки соответствия законов распределения дифференциалов и линейных аппроксимаций заданным (эталонным) предлагается воспользоваться идеями работы [20], и ввести в рассмотрение ″метрические портреты″ подстановок различного порядка (эталонных подстановок), в качестве которых рассматривать подстановки, законы распределения вероятностей совпадают с законами распределения вероятностей (1) и (4), полученными расчетным путем.

Остановимся на обосновании этого предложения более детально.

Будем рассматривать задачу проверки соответствия эмпирического распределения (для дифференциалов), полученного для произвольной подстановки ″эталонному″, определяемому формулами (1) и (2) как задачу обработки результатов статистических экспериментов.

Примеры распределений, которые требуется сопоставить представлены в табл. 1. В левой колонке таблицы представлены расчеты, выполненные в соответствии с выражением (1) для подстановки 16-го порядка. В правой колонке этой таблицы представлены соответствующие результаты для 16-битного шифра по Хейсу с линейным преобразованием, подобным операции MixColumn в шифре Rijendael, взятые из работы [26].

Напомним далее, что для обработки результатов статистических экспериментов по проверке выдвигаемых гипотез о соответствии эмпирических распределений теоретическим распределениям к настоящему времени разработано и используется много подходов и критериев (критерий χ^2, критерии Спирмена, Колмогорова, Мизеса и др.) [27 и др.].

Таблица 1

Распределение парных разностей для SPN шифра с умножением на матрицу

Расчет		Эксперимент	
#2.	1302484861	#2.	1302551726
#4.	325626184	#4.	325625709
#6.	54271858	#6.	54253870
#8.	6784085	#8.	6781574
#10.	678418	#10.	677785
#12	56535	#12	56793
#14.	4038	#14.	3974
#16.	252	#16.	272
#18.	14	#18.	17
#20.	1	#20.	0

Мы здесь выполним проверку близости законов распределения для числа парных разностей

$$\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right),$$

представленных в табл. 1. Воспользуемся для этого критерием согласия Колмогорова [27], который позволяет решить поставленную задачу путем сопоставления теоретического интегрального закона распределения вероятностей F(x) (с известными параметрами) с эмпирическим законом распределения вероятностей $F_n(x)$, полученным на основе вычислительного эксперимента.

Статистический критерий Колмогорова, как известно, применяется для проверки простой непараметрической гипотезы H_0, согласно которой независимые одинаково распределенные случайные величины $X_1, X_2, ..., X_n$ имеют заданную непрерывную функцию распределения F(x), причем альтернативная гипотеза H_1 предполагается двухсторонней:

$$\left| EF_n(x) - F(x) \right| > 0,$$

где EF_n – математическое ожидание функции эмпирического распределения $F_n(x)$.

Критическое множество критерия Колмогорова выражается равенством

$$D_n = \operatorname*{Sup}_{|x|<\infty} \left|F_n(x) - F(x)\right| > \lambda_n .$$

В случае справедливости гипотезы H_0 распределение статистики D_n не зависит от функции F(x), причем, если $n \to \infty$, то

$$P\left\{\sqrt{n} D_n < \lambda\right\} \to K(\lambda), \qquad \lambda > 0.$$

Здесь K(x) – функция распределения Колмогорова, которая табулирована.

Согласно критерию Колмогорова гипотезу H_0 с уровнем значимости α, $0 < \alpha < 0{,}5$ следует отвергнуть, если

$$D_n \geq \lambda_n(\alpha),$$

где $\lambda_n(\alpha)$ – критическое значение критерия Колмогорова, соответствующее заданному уровню значимости α и являющееся корнем уравнения $\left\{D_n \geq \lambda\right\} = \alpha$.

Продемонстрируем теперь методику применения этого критерия для сравнения распределений, представленных в табл. 1.

Нам в этом случае необходимы дискретные значения интегрального теоретического закона распределения вероятностей F(x) и интегрального реального (эмпирического) закона распределения вероятностей $F_n(x)$ числа однотипных переходов дифференциальных таблиц подстановок.

Они представлены в табл. 2, построенной в соответствии с расчетами, выполненными по данным из табл. 1.

Из табл. 2 следует, что наибольшее значение разности $D_n = \left| F_n(x_k) - F(x_k) \right|$ равно 0,000013.

Тогда, для $\alpha = 0{,}1$ из таблицы распределения Колмогорова-Смирнова [27] находим

$$Q(\lambda_0) = 1 - \alpha = 1 - 0{,}1 = 0{,}9 \ \to \lambda_0 = 1{,}23.$$

Далее для $n = (2^{15}-1)^2$ имеем

$$\frac{\lambda_0}{\sqrt{n}} = \frac{1{,}23}{2^{16}-1} = 0{,}00001876,$$

и, следовательно,

$$D_n < \frac{\lambda_0}{\sqrt{n}}.$$

Таким образом, гипотеза о том, что эмпирический закон распределения $F_n(x_k)$ соответствует теоретическому закону $F(x_k)$ подтверждается.

В результате можно предложить в качестве 4-го критерия случайности подстановок использовать проверку близости эмпирически полученного закона распределения парных разностей XOR таблицы рассматриваемой подстановки расчетным значениям в следующем виде:

Таблица 2

Теоретический $F(x_k)$, и "эмпирический" $F_т(x_k)$ законы распределения вероятностей и их различие для преобразований табл.1.

	Теоретически рассчитанное распределение		Экспериментально полученное распределение		Расхождение распределений
k	$\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k)$	$F(x_k)$	$\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k)$	$F_n(x_k)$	$\lvert F_n(x_k)- F(x_k)\rvert$
0	0,605345	0,605345	0,605342	0,605342	0,000003
2	0,303267	0,908612	0,303283	0,908625	0,000013
4	0,075818	0,98443	0,0758179	0,9844429	0,0000129
6	0,0126365	0,9970665	0,0126323	0,997077	0,0000105
8	0,0016	0,9986665	0,00158	0.998657	0,0000095
10	0,00016	0,9988265	0,00015784	0,9988148	0,0000117
12	0,0000134	0,9988399	0,000013225	0,998828	0,0000119
14	0,00000096	1,0000	0,0000009257	0,998804	0,000011
16	0,000000058	1,0000	0,00000006338	0,998804	0,000011
18	0,00000000326	1,0000	0,00000000396	0,998805	0,000011
20	0,000000000233	1,0000	0,00000	0,998805	0,000011

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

$$\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k),\ k=0,1,\ldots,k^*$$

её таблицы XOR разностей для входов, приписываемых к ненулевым характеристикам, соответствует по критерию согласия Колмогорова теоретическому закону распределения переходов (1)*, т.е. наибольшее значение модуля разности теоретического и эмпирического законов распределения вероятностей удовлетворяет условию*

$$\lvert F_T(x_k)- F(x_k)\rvert \le b.$$

Здесь граничный параметр b подлежит уточнению по результатам экспериментов.

Совершенно аналогично вводится и критерий случайности на основе оценки свойств ЛАТ подстановки.

5. *Подстановка удовлетворяет критерию случайности* 5*, если закон распределения однотипных переходов* $\Pr(\lambda^*(\alpha,\beta)=2k)$, $k=0,1,\ldots,k^*$ *её таблицы линейных аппроксимаций соответствует по критерию согласия Колмогорова теоретическому закону распределения* (4)*, т.е. наибольшее значение модуля разности теоретического и эмпирического законов распределения вероятностей удовлетворяет условию* $\lvert F_T(x_k)- F(x_k)\rvert \le c$. Здесь параметр *c* также подлежит уточнению по результатам экспериментов.

В этой работе мы ограничимся изложением самой идеи реализации дополнительных критериев отбора, а результаты экспериментальной проверки предложений мы отложим для отдельной публикации.

Заключение

Таким образом, сформулированы дополнительные критерии отбора случайных подстановок, позволяющие перенести свойства криптографических преобразований, рассматриваемых как подстановки, и на подстановочные конструкции в целом.

Естественно предстоит ещё выполнить более тщательную и более полную проверку подстановок, прошедших предложенные критерии случайности на соответствие другим известным критериям, и, в частности, строящимся с использованием и алгебраических методов.

Литература

1. Brickell E.F. Structure in the S-boxes DES / E.F. Brickell, J.H. Moore, M.R. Purtill // Advances in cryptology, CRYPTOZ, Lecture Notes in Computer Science, A.M. Odlyzko ed., Springer-Verlag, 1987. – V. 263. – P. 3-8.

2. Adams C.M. A formal and practical design procedure for Substitution-Permutation network crypto-

system. PhD thesis, Department of Electrical Engineering, Queen's University at Kingston, 1990.

3. Adams CM. The Structured design of cryptographically good S-boxes / C.M. Adams, S.E. Tavares // Journal of Cryptology. – 1990. – № 3(1). – P. 27-41.

4. Forré R. Methods and instruments for designing S-boxes / R. Forré // Journal of Cryptology. – 1990. – № 2(3). – P. 115-130.

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

6. Dawson M.H. A unified framework for substitution box design based on information theory / M.H. Dawson // Vaster's thesis, Queen's University, Kingston, Ontario, Canada, 1991.

7. Biham E. Differential Cryptanalysis of DES-like Cryptosystems / E.Biham, A.Shamir // Journal of Cryptology. – 1991. – Vol. 4. – №.1 – P. 3-72.

8. Matsui M. Linear cryptanalysis method for DES cipher / M. Matsui // In Advances in Cryptology – EUROCRYPT'93, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York. – 1991. – V. 765. – P. 386-397.

9. Nyberg K. Provable security against differential cryptanalysis / K. Nyberg, L.R Knudsen // In Advances in cryptology – EUROCRYPT'92, volume Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, 1992. – P. 566-574.

10. Beth T. On permutations against differential cryptanalysis / T. Beth, C. Ding // In Advances in cryptology – EUROCRYPT'93. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

11. Nyberg K. Differentially uniform mappings for cryptography / K. Nyberg // In Advances in cryptology – Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York. – 1994. – V. 765 – P. 55–65.

12. Seberry J. Pitfalls in Designing Boxes (Extended Abstract) / J. Seberry, X.M. Zhang, Y. Zheng // Copyright © Springer-Verlag, 1998. – P. 383-396.

13. Seberry J. Relationships among nonlinearity criteria / J. Seberry, X.M. Zhang, Y. Zheng // Presented at EUROCRYPTV4, 1994.

14. Zhang X.M. Non-existence of Certain Quadratic S-boxes and Two Bounds on Nonlinear Characteristics of General S-boxes / X.M. Zhang, Y. Zheng, H. Imai // October 1997. – P. 1-18.

15. Nyberg K. On the construction of highly nonlinear permutations / K. Nyberg // In Advances in cryptology – Proceedings of EUROCRYPT'92, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York, 1993. – V. 740. – P. 92-98.

16. Seberry J., Zhang X.M., Zheng Y. Improving the strict avalanche characteristics of cryptographic functions. Information Processing Letters, 50:37-41, 1994.

17. Долгов В.И. Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров / В.И. Долгов, А.А. Кузнецов, И.В. Лисицкая, Р.В. Сергиенко // Прикладная радиоэлектроника. – 2009.– Т.8 – №.3. – С. 268-277.

18. Долгов В.И. Подстановочные конструкции современных блочных симметричных шифров / В.И. Долгов, Р.В. Олейников, И.В. Лисицкая, Р.В. Сергиенко, Е,В. Дроботько , Е.Д. Мельничук // Радиоэлектроника и компьютерные системы. – 2009. – № 6(40). – С. 89-93.

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

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

21. Олейников Р.В. Исследование дифференциальных свойств подстановок различных цикловых классов / Р.В. Олейников, К.Е. Лисицкий // Двенадцатая Международная научно-практическая конференция "Безопасность информации в информационно-телекоммуникационных системах", 19–20 МАЯ 2009 г., Тез. док. – К.: ЧП "ЕКМО", НИЦ "ТЕЗИС" НТУУ "КПИ", 2009. – С. 24-25.

22. Олейников Р.В. Исследование дифференциальных свойств подстановок / Р.В. Олейников, И.В. Лисицкая, А.В. Широков, К.Е. Лисицкий // Сборник трудов Первой Международной научно-технической конференции "Компьютерные науки и технологии", 8-10 октября 2009 г., Белгород. – Ч. I. – С. 59-63.

23. 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.

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

25. Luke O'Connor. On Linear Approximation Tables and Ciphers secure against Linear Cryptanalysis. Email: oconnor@dsts. Edu. au, 1995.

26. Долгов В.И. Rijndael – это новое или хорошо забытое старое / В.И. Долгов, И.В. Лисицкая, Р.И. Киянчук // Сборник трудов Первой Международной научно-технической конференции "Компьютерные науки и технологии", 8-10 окт. 2009 г., Белгород. – Ч. 2. – С. 32-35.

27. Бронштейн И.Н. Справочник по математике для инженеров и учащихся вузов / И.Н. Бронштейн, К.А. Семендяев. – М:. Наука, 1980. – 976 с.

Поступила в редакцию 13.01.2010

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

ВИПАДКОВІ ПІДСТАНОВКИ У КРИПТОГРАФІЇ

В.І. Долгов, І.В. Лисицька, К.Є. Лисицький

Обговорюються відомі підходи до конструювання підстановок (S-блоків) з високими криптографічними показниками. Виділяється підхід до відбору S-блоків, розвинутий у свій час в роботах авторів, що будується на основі перевірки показників випадковості підстановок (кількості їх інверсій, зростань та циклів). У якості подальшого розвитку цього підходу пропонується нове визначення випадкової підстановки, що пов'язується з додатною перевірки близькості законів розподілу переходів таблиць різниць й таблиць лінійних апроксимацій S-блоків теоретичним розподілам, знайденим в останніх роботах авторів. Приводиться само правило оцінки близькості теоретичних та емпіричних законів розподілу ймовірностей, що отримуються за допомогою критерію згоди Колмогорова. Формулюється задача за виконанням більш старанної перевірки підстановок, що пройшли запропоновані критерії випадковості, на відповідність їх криптографічних показників іншим відомим критеріям, зокрема, що будуються з використанням й алгебраїчних методів.

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

RANDOM SUBSTITUTIONS IN THE CRYPTOGRAPHY

V.I. Dolgov, I.V. Lysytskaya, K.E. Lysytskay

Known approaches to S-boxes with good cryptographic indexes construction are discussed. An approach to S-boxes selection developed in the previous papers based on randomness index verification (number of inversions, grownesses and cycles) is selected. As a further development of this approach there is suggested a new definition of random substitution based on additional verification of the distribution law similarity of S-boxes difference distribution and linear approximation tables according to theoretical distributions found in recent authors' papers. The estimation rule for theoretical and empirical similarity of probabilities distribution obtained by Kolmogorov's criterion is given. It is formed a task for a more careful verification of substitutions passed proposed randomness criteria to their cryptographic indexes correspondence to known criteria, particularly, based on know algebraic methods.

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

Долгов Виктор Иванович – д-р техн. наук, проф. кафедры безопасности информационных технологий, Харьковский национальный университет радиоэлектроники "ХНУРЭ", Харьков, Украина.

Лисицкая Ирина Викторовна – канд. техн. наук, доцент, доцент кафедры безопасности информационных технологий, Харьковский национальный университет радиоэлектроники "ХНУРЭ", Харьков, Украина.

Лисицкий Константин Евгеньевич – ученик 11-Б класса, лицей № 89, Харьков, Украина.