УДК 621. 391:519.2:519.7

И.В. ЛИСИЦКАЯ, канд. техн. наук, В.В. КОВТУН

ОБ УЧАСТИИ S-БЛОКОВ В ФОРМИРОВАНИИ МАКСИМАЛЬНЫХ ЗНАЧЕНИЙ ЛИНЕЙНЫХ ВЕРОЯТНОСТЕЙ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Введение

Мы хотим возвратиться к работе [1], в которой приведен краткий обзор ряда публикаций последних лет по вопросам оценки доказуемой стойкости блочных симметричных шифров (БСШ) к атакам дифференциального и линейного криптоанализа.

В этой работе отмечается, что в затронутых публикациях и во многих других работах на эту тематику развивается концепция, в соответствии с которой показатели доказуемой стойкости БСШ к атакам дифференциального и линейного криптоанализа непосредственно связываются с дифференциальными и линейными показателями входящих в шифры S-блоковых конструкций, и излагается новая точка зрения к оценке соответствующих показателей. Эта точка зрения появилась на основе развития нового подхода в теории и методах криптоанализа, родившегося на кафедре БИТ ХНУРЭ [3], о котором уже говорилось в работе [4]. Он ориентирован, как было отмечено, с одной стороны, на использование при определении ожидаемых показателей стойкости больших шифров результатов анализа уменьшенных их версий, а с другой, – сформированной в последнее время новой идеологии определения показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа [1], основывающейся на подтвержденном многочисленными экспериментами с уменьшенными версиями современных шифров (DES, ГОСТ, Rijndael, Лабиринт, Мухомор, Калина, ADE, Камелия, FOX и многих других) положении (факте), состоящем в том, что все эти шифры (и большие и малые их версии) через определенное число циклов (для рассмотренных уменьшенных моделей от трех циклов до семи) независимо от используемых в шифрах S-блоков приобретают свойства случайной подстановки по комбинаторным показателям (числу инверсий, возрастаний и циклов), а также по законам распределения переходов XOR таблиц дифференциальных разностей (полных дифференциалов) и законам распределения смещений таблиц линейных аппроксимаций (линейных корпусов) они повторяют соответствующие показатели случайной подстановки [5 – 7]). Здесь и далее под случайной подстановкой понимается подстановка, удовлетворяющая установленным критериям близости законов распределения циклов, возрастания и инверсий, а также законов распределения переходов их XOR таблиц и смещений таблиц линейных аппроксимаций соответствующим теоретическим (асимптотическим) законам распределения вероятностей [8]. Этот факт зафиксирован в работе [1] в виде утверждения.

Утверждение. *Для каждого блочного симметричного шифра (из числа известных итеративных БСШ) существует вполне определенное число циклов, после которого шифр приобретает свойства случайной подстановки. Дальнейшее наращивание числа циклов не влияет на итоговые дифференциальные и линейные свойства шифра. Это значение является одним и тем же для всех шифрующих преобразований с одинаковым битовым размером входа.*

Конечно, аккуратнее было бы говорить только об уже проверенных шифрах, но, на взгляд авторов работы [1], это свойство должно быть присуще любому сколько-нибудь внушающему доверие шифру.

А это значит, что концепция, разрабатываемая в представленных выше и многих других работах, является неверной. Для подтверждения выдвинутых в работе [1] положений были проведены многочисленные исследования дифференциальных и линейных свойств уменьшенных моделей ряда современных шифров [2, 9 – 12 и др.], а теперь уже и их больших прототипов [13, 14], и экспериментами показано, что и малые и большие конструкции современ-

ных шифров действительно при полном наборе шифрующих операций приобретают свойства случайных подстановок соответствующей степени.

Здесь мы хотим отдельно отметить работу [2], одну из большого числа отмеченных публикаций, посвященную непосредственно исследованию влияния на показатели стойкости шифров характеристик, используемых при их построении S-блоков. В ней были представлены результаты оценки такого влияния на полные дифференциалы уменьшенных моделей ряда современных шифров. В этой работе мы продолжаем излагать результаты исследований в отмеченном направлении и приводим результаты оценки влияния на значения теперь уже максимумов линейных корпусов (оболочек) шифров линейных показателей применяемых при их построении S-блоков.

Понятийный аппарат линейного криптоанализа

Кратко напомним подходы к определению линейных показателей подстановочных преобразований (S-блоков и шифров в целом).

Для характеристики линейных показателей S-блоков воспользуемся определениями работы [15] и ряда других работ. Далее S-блоки рассматриваются как булевы векторные функции.

Определение 1 [16]. Векторной булевой функцией $\mathbf{y} = \mathbf{f}(\mathbf{x})$, $\mathbf{f} = (f_1, f_2, \ldots, f_n)$ называется функция (последовательность функций), отображающая булевой вектор (вектор с битовыми координатами) в другой булевой вектор (здесь и далее такой же размерности, как и исходный вектор):

$$\mathbf{f} : GF(2^n) \to GF(2^n),\ \mathbf{x} \mapsto \mathbf{y} = \mathbf{f}(\mathbf{x}).$$

Очевидно, что одной из математических реализаций булевой векторной функции выступает подстановка.

Аффинность и нелинейность. При использовании математического аппарата булевой алгебры для описания свойств подстановочных преобразований рассматриваются свойства компонентных булевых функций.

Определение 2 [17]. *Аффинной называется функция* $f(\mathbf{x}) : GF(2^n) \to GF(2)$ (здесь рассматривается одна функция из полного их набора $\mathbf{f}$) *над* $GF(2^n)$ *вида*

$$f = a_1 x_1 \oplus \ldots \oplus a_n x_n \oplus c,$$

где $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$.

В обозначениях работы [18]:

$$f = \mathbf{w} \bullet \mathbf{x} \oplus c.$$

Здесь $\mathbf{w} \bullet \mathbf{x}$ обозначает скалярное произведение двух векторов $\mathbf{w}, \mathbf{x} \in GF(2^n)$. Если $c = 0$, то функция f называется *линейной*.

Определение 3 [17]. *Хэммингов весом вектора* $\mathbf{x} \in \mathrm{GF}(2^n)$ *((0,1)-последовательности), обозначаемым как* $W(\mathbf{x})$, *называется число единиц в этом векторе.*

Определение 4 [18]. *Расстоянием Хэмминга* $d_H(f, g)$ *между двумя функциями* f *и* g *является количество позиций, в которых последовательности этих функций различаются.*

Определение 5 [18,19]. *Нелинейность функции* N_f *– это минимальное расстояние Хэмминга между функцией* f *и всеми аффинными функциями линейного пространства* $GF(2^n)$:

$$N_f = \min_{i=1, 2, \ldots, 2^{n+1}} \{d_H(f, \varphi_i)\},$$

где $\varphi_1, \varphi_2, \ldots, \varphi_{2^{n+1}}$ – аффинные функции n мерного линейного пространства над полем $GF(2)$.

В [18] представлено определение нелинейности N_f в виде

$$N_f = \min_{\mathbf{w},c} d_H(f(\mathbf{x}), \mathbf{w} \bullet \mathbf{x} \oplus c).$$

Установлено [17], что для произвольной булевой функции f нелинейность N_f над GF(2^n) может достигать значения

$$N_f \le 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Для сбалансированной функции f над GF(2^n) ($n \ge 3$) нелинейность N_f может достигать значений [17]:

$$N_f \le \begin{cases} 2^{n-1} - 2^{n/2-1} - 2, & n = 2k, \\ \left\lfloor \left\lfloor 2^{n-1} - 2^{n/2-1} \right\rfloor \right\rfloor, & n = 2k+1, \end{cases}$$

где $\lfloor x \rfloor$ – максимальное четное целое, меньшее либо равное x.

Определение 6 (Линейная аппроксимационная таблица – *LAT* для S-блоков) [20]. Для данного S-блока $S(x): GF(2^n) \to GF(2^n)$ (векторной булевой функции) *линейная аппроксимационная таблица*, имеющая вход в w-ю строку и c-ю колонку (в этой работе для обозначения векторов используются прописные символы, которые не выделяются полужирным шрифтом), определяется как

$$\begin{aligned} LAT(w,c) &= \left| x / c \bullet S(x) = w \bullet x \right| - 2^{n-1} = \left| x / f(x) = w \bullet x \right| - 2^{n-1}. \\ &= \left| x \middle| f(x) = l_w(x) \right| - 2^{n-1} \\ &= 2^n - d_H(f, l_w) - 2^{n-1} \\ &= 2^{n-1} - d_H(f, l_w). \end{aligned} \quad (1)$$

В качестве значения ячейки таблицы выступает смещение истинного значения числа выполнения равенств $c \bullet S(x) = w \bullet x$ для заданного значения пары входов в в w-ю строку и c-ю колонку таблицы от значения 2^{n-1} (по предложению автора линейного криптоанализа М. Мацуи).

В этих же обозначениях

Определение 7 (Критерий нелинейности для S-блоков) [18]. *Нелинейность N_s S-блока определяется как худший случай нелинейности:*

$$N_S = \min_f N_f = \min_f \{ N_f / f(x) = c \bullet S(x), c \ne 0 \}, \quad (2)$$

где минимизация ведется по всем возможным выходным битовым комбинациям $f(x) = \oplus_{i=1}^n c_i f(x_i) = c \bullet S(x)$, соответствующим всем ненулевым значениям маскового вектора $c = (c_1, \ldots, c_n)\big|_{1 \times n}$ (по всем компонентным булевым функциям).

Полезно будет также напомнить лемму из работы [18].

Лемма (Соотношение между нелинейностью S-блока и максимальным значением элемента LAT). *Нелинейность S-блока, определяемая из* (2), *может быть представлена в терминах максимального значения элемента LAT как*

$$N_S = \min_f N_f = 2^{n-1} - \max_{w,c \in F_2^n} |LAT(w,c)|, \quad (3)$$

где $f(x) = c \bullet S(x)$, $c \neq 0$ *является любой из выходных линейных комбинаций.*

Далее приведены два определения, относящиеся уже к подстановочному преобразованию в виде ключезависимой функции $f = f[k](x)$ (шифру), заимствованные из работы [15].

Определение 8 (Линейная вероятность): *Линейная вероятность* LP^f *для ключезависимой функции* f *с n-битным входом x и n-битным выходом y* ($x, y \in GF(2)^n$) *есть*

$$LP^f = (\Gamma x \to \Gamma y) = \left(\frac{\#\{x \in GF(2^n / x \cdot \Gamma x = f(x) \cdot \Gamma y)\}}{2^{n-1}} - 1 \right)^2,$$

где Гx *и* Гy *являются входной и выходной масками ключезависимой функции f;* x Гx *обозначает результат скалярного произведения x и* Гx (это практически повторение определения (1) в других обозначениях). Мы несколько модифицируем обозначения работы [15], введя в них зависимость от ключа зашифрования. В работе [16] при рассмотрении случайных блоковых шифров вводится понятие фиксировано-ключевой корреляции $LP[k]$ (в нашем случае мы воспользуемся обозначением $LP^{f[k]}$). Нам оно кажется более уместным.

Определение 9 ($LP_{\max}^{f[k]}$). *Максимальное значение линейной вероятности для ключезависимой функции* f *определяется как*

$$LP_{\max}^{f[k]} = \max_{\Gamma x,\, \Gamma x \neq 0,} LP^{f[k]}(\Gamma x \to \Gamma y). \quad (2)$$

В общем случае ключезависимая функция f является сильной, если значение $LP_{\max}^{f[k]}$ функции f является достаточно малым [15].

Приведем еще одно определение, являющееся нашей модификацией выражения, введенного в работе [15] для *MALHP*.

Определение 10 (*ALHMP*). *Среднее* (*по ключам*) *значение максимальной вероятности линейных корпусов функций* $f[k](x)$ *есть*

$$ALHMP = \operatorname*{ave}_k LP_{\max}^{f[k]}(\Gamma x \to \Gamma y) = \frac{1}{2^h} \sum_{i=1}^{2^h} LP_{\max}^{f[k]}(\Gamma x \to \Gamma y).$$

гое 2^h *– мощность использованного множества ключей зашифрования.*

Результаты вычислительных экспериментов

В этой разделе продемонстрированы результаты исследований по оценке влияния на линейные показатели современных шифров (их малых версий) линейных показателей используемых в шифрах блоков нелинейных замен (S-блоков).

Первая часть экспериментов была связана с генерацией и отбором S-блоков с различными показателями нелинейности. Конкретные примеры подстановок, отобранных в ходе экспериментов этого этапа, иллюстрирует табл. 1.

Представленные в таблице подстановки были использованы в качестве S-блоков во всех исследуемых малых моделях шифров (в каждом шифре использовались S-блоки с одинаковыми показателями нелинейности).

Таблица 1

Полубайтовые подстановки (S-блоки) с различными показателями нелинейности

Нелинейность	S-блок
0	S_1 = {12, 13, 5, 1, 10, 11, 6, 2, 14, 3, 7, 15, 4, 0, 8, 9}
0	S_2 = {5, 0, 13, 6, 4, 8, 2, 3, 9, 1, 15, 10, 12, 14, 7, 11}
2	S_3 = {10, 4, 5, 8, 2, 15, 7, 0, 14, 9, 11, 12, 6, 13, 1, 3}
2	S_4 = {2, 5, 0, 9, 3, 14, 4, 1, 10, 11, 8, 15, 7, 12 ,6, 13}
4	S_5 = {10, 4, 3, 11, 8, 14, 2, 12, 5, 7, 6, 15, 0, 1, 9 ,13}

Вторая (основная) часть исследований и вычислительных экспериментов была посвящена вычислению поцикловых средних значений максимумов смещений линейных корпусов (*ALHMP*) уменьшенных моделей трех шифров из представленных на украинский конкурс (шифры Лабиринт, Мухомор и Калина) и уменьшенной модели шифра Rijndael. Сами конструкции уменьшенных моделей шифров были заимствованы из работ, выполненных на кафедре.

Для каждого шифра с фиксированным числом циклов шифрования выполнялось построение линейных корпусов (таблиц линейных аппроксимаций) для 30 различных ключей зашифрования, сгенерированных случайным образом, определялись максимальные значения смещения для каждой из таблиц, а затем результаты усреднялись. Мы интересовались зависимостью средних значений максимумов смещений линейных корпусов от числа циклов зашифрования.

В табл. 2 – 5 представлены поцикловые значения средних значений максимумов смещений таблиц линейных аппроксимаций (линейных корпусов) для рассмотренных в работе шифров.

Таблица 2

Математическое ожидание максимальных смещений линейных корпусов шифра мини-Лабиринт со значениями среднеквадратического отклонения

Число циклов шифрования r	Показатели нелинейности S-блоков, использованных в шифре				
	0	2	0	2	4
1	10751,6±1934	4385,6±1166	3200±494	4300±1774	3178±777
2	1910,8±460	1182,2±162	1219,6±312	1043,60±252	980±193
3	1032,8±190	839,2±34	864,4±55	831,6±27	825,4±14
4	810±15	813,6±13	822,4±17	811,4±11	825,6±23
5	816,2±17	827,8±16	833,4±25	809±15	817,2±11
6	826,4±24	832±32	814,8±24	828,2±35	824±21
7	817,8±18	812±13	811±17	837,4±22	823,4±30
8	835,4±16	813,6±19	822,6±23	815,4±20	833,6±35
9	819,4±23	812,6±14	815,8±26	820,4±15	824,8±24
10	820,6±20	815,4±22	814,4±20	808±21	819±17

Как следует из представленных результатов, во всех случаях, независимо от значения показателя нелинейности S-блоков, все шифры приходят к одному и тому же среднему значению максимума смещения линейного корпуса, характерному (весьма близкому) случайной подстановке соответствующей степени [6, 7]. По всем рассмотренным шифрам видно, что для перехода к асимптотическому значению смещения требуется 4 – 5 циклов. Видно, что использование S-блоков с высокими показателями нелинейности дает т выигрыш в динамике выхода к асимптотическому значению в пределах одного цикла.

Таблица 3

Математическое ожидание максимальных смещений линейных корпусов шифра мини-Калина со значениями среднеквадратического отклонения для соответствующих S-боксов

Число циклов шифрования r	Показатели нелинейности S-блоков, использованных в шифре				
	0	2	0	2	4
1	21845,3±5565	18090,6±1043	16497,7±2222	11491,5±1825	9671,1±867
2	9557,33±1231	7288,8±758	5432,88±693	3968±307	3370,6±301
3	2823,55±436	1661,22±168	1394,66±219	862,66±50	836,8±15
4	1307,77±216	822,55±30	815,33±17	826,44±23	832,2±21
5	818,88±21	796±20	818,66±11	811,77±12	838,6±21
6	824,22±15	808,66±29	840,44±28	816,88±13	835,5±33
7	810±18	811±30	820,88±32	824,44±23	821,5±22
8	819,77±21	808,88±29	834,66±43	829,33±16	827,3±18
9	808±20	810,66±11	811,33±15	827,77±22	813,3±21
10	836,44±39	821,55±26	816±11	817,33±16	834±28

Таблица 4

Математическое ожидание максимальных смещений линейных корпусов шифра мини-Мухомор со значениями среднеквадратического отклонения для соответствующих S-боксов

Число циклов шифрования r	Показатели нелинейности S-блоков, использованных в шифре				
	0	2	0	2	4
1	32768±0	32768±0	32768±0	32768±0	32768±0
2	16896±2101	15616±1511	14364,4±1372	10951,1±1112	12839,3±1031
3	7082,6±1020	6553,3±663	6599,1±678	6200,8±841	6400±697
4	2190,4±364	2022,6±381	2052,4±395	1663,1±222	1797,6±347
5	1035,7±33	828,8±48	857,5±40	866±47	837,8±47
6	828,6±25	823,1±24	820±34	818,6±15	815,6±24
7	837,5±26	821,7±22	824,4±24	821,7±20	817,2±20
8	849,5±33	810,2±12	830,8±21	834±19	815,8±15
9	810,2±13	815,7±25	825,7±19	806,6±13	815,5±15
10	808,6±8	819,3±21	836,6±27	813,5±18	810±17

В то же время из представленных результатов следует, что значение показателя нелинейности S-блоков не является определяющим. Для S-блоков с одной и той же нелинейностью результаты перехода к асимптотическому значению отличаются на один-два цикла.

В работе [16] рассматриваются корреляции случайных блочных шифров $\mathcal{A}$ (блочных шифров с битовой длиной n и ключевой длиной h, являющихся массивом из 2^h векторных булевых подстановок, оперирующих с n битными векторами). Каждое ключевое значение k определяет векторную булеву подстановку, обозначенную как $\mathcal{A}[k]$. Такой шифр рассматривается как *фиксированно-ключевой (блочный) шифр. Случайный блочный шифр* с блочной длиной n и ключевой длиной h является массивом из 2^h n-битных случайных подстановок: одна случайная n-битная подстановка для каждого ключевого значения.

Таблица 5

Математическое ожидание максимальных смещений линейных корпусов шифра мини-Rijndael со значениями среднеквадратического отклонения для S-блоков с различными показателями нелинейности.

Число циклов шифрования r	Показатели нелинейности S-блоков, использованных в шифре				
	0	2	0	2	4
1	32768±0	24576±0	32768±0	24576±0	16384±0
2	24576±0	7808±0	10368±0	3584±0	2048±0
3	12288±0	2527,1±54	2304±0	1128±107	851,5±48
4	5233,1±58	891,7±58	905,7±29	829,3±22	814,2±14
5	2040,2±103	822,6±24	831,3±29	817,7±11	828,6±20
6	1077,7±35	825,3±19	832,2±21	820,8±23	827,7±31
7	839,7±34	815,7±16	826,4±21	822,6±27	822,2±28
8	821,7±11	810,8±21	822,8±20	819,3±26	803,7±12
9	830±26	811,1±15	821,7±34	830,4±27	810,4±18
10	811,3±18	834,4±29	806,6±11	808,4±14	823,1±27

Эквивалентно, случайный блочный шифр с блочной длиной n и ключевой длиной h является блочным шифром, выбранным случайно из множества $(2^n!)^{2^h}$ возможных блочных шифров той же размерности, где каждый блочный шифр имеет равную вероятность быть выбранным.

Интересно отметить, что в этой работе доказывается теорема о том, что распределение среднего значения LP линейного корпуса над случайным блочным шифром очень близко к нормальному распределению со средним значением 2^{-n} и стандартным отклонением $2^{-n}\,2^{(1-h)/2}$. В табл. 6 приведены данные (и оценки), характеризующие временные затраты на проведение вычислительных экспериментов по определению линейных показателей уменьшенных моделей шифров при использовании базового и ускоренного алгоритмов.

Таблица 6

Время построения ЛАТ

Алгоритм	$T_{1\ строки}$	$T_{1\ таблицы}$	$T_{10\ циклов}$	$T_{30\ ключей}$
Базовый	2,5 мин (2^{32}операций)	272 ч (2^{48}операций)	113 д (2^{51}операций)	3390 дней (2^{56}операций)
Ускоренный	–	2,5 мин (2^{32}операций)	25 мин (2^{35}операций)	12,5 ч (2^{40}операций)

Приведенные результаты свидетельствуют, что концепция оценки доказуемой стойкости, развиваемая в приведенных во введении и многих других работах, ошибочна! Во всех рассмотренных примерах показатели стойкости шифров не зависят от подстановок, использованных при их построении, а зависят только от битового размера входа в шифр. Подстановки влияют лишь на динамику перехода к асимптотическому значению. Этот результат, следующий из большого числа экспериментов со случайными подстановками и малыми моделями шифров, будет сохраняться и для больших версий шифров (и не только для шифров с SPN структурой!).

Заключение

Общий вывод состоит в том, что итоговые асимптотические показатели стойкости шифров к атакам линейного криптоанализа определяются свойствами случайной подстановки соответствующей степени и от свойств S-блоков, используемых в шифре, не зависят. А раз так, то интересующие нас показатели доказуемой стойкости шифров к атакам теперь уже и линейного криптоанализа могут быть определены расчетным путем из соответствующих формул для теоретических законов распределения переходов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок соответствующей степени, полученных в работах [10, 11].

Среднее значение максимального смещения таблицы линейных аппроксимаций (линейных каркасов (оболочек)) для шифров с n-битным значением размера входного блока данных аппроксимируется соотношением $\left(\frac{3}{2}\right)^n$. Для среднего значения максимума вероятности линейного корпуса (*ALHMP*) 128-битного шифра приходим к результату $ALHMP^R = \left(\frac{\left(\frac{3}{2}\right)^{128}}{2^{127}}\right)^2 = 2^{-104}$. Реальное значение может отличаться от приведенного, по нашим предположениям, менее чем в два раза.

Исследованиями установлено, что все рассмотренные шифры после 4 – 5 циклов шифрования становятся случайными подстановками.

Полученными результатами подтверждается концепция оценки стойкости БСШ, развиваемая на кафедре БИТ ХНУРЭ, в соответствии с которой показатели стойкости БСШ к атакам линейного и дифференциального криптоанализа могут быть получены расчетным путе м с использованием значений максимумов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок соответствующей степени.

В отношении сохранения в большом шифре свойств уменьшенной модели можно лишь отметить, что мы говорим о сохранении свойств и показателей случайной подстановки. Представляется, что при увеличении битового размера входа в шифр (с увеличением степени подстановки) ее соответствие асимптотическим законам распределения вероятностей (по инверсиям, возрастаниям и циклам), а также законам распределения вероятностей переходов таблиц полных дифференциалов и таблиц линейных корпусов будет только повышаться, что подтверждается и вычислительными экспериментами с большими версиями шифров.

Список литературы: 1. *Горбенко И.Д.* Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / Горбенко И.Д., Долгов В.И., Лисицкая И.В., Олейников Р.В. // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 212-320. 2. *Лисицкая И.В.* Об участии S-блоков в формировании максимальных значений дифференциальных вероятностей блочных симметричных шифров / Лисицкая И.В., Казимиров А.В. // System Research and Information Technologies. – 2011 (в печати). 3. *Долгов В.И.* Подход к криптоанализу современных шифров / Долгов В.И., Лисицкая И.В., Олейников Р.В. // Материалы второй междунар. конф. "Современные информационные системы. Проблемы и тенденции развития". – Харьков-Туапсе, Украина, 2–5 октября. – 2007. – С. 435-436. 4. *Долгов В.И.* Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс / Долгов В.И., Кузнецов А.А., Исаев С.А. // Представлена к опубликованию. 5. *Lysytska I.V.* The selection criteria of random substitution tables for symmetric enciphering algorithms / Lysytska I.V., Koriak A.S., Golovashich S.A., Oleshko O.I., Oleinik R.V // Abstracts of XXVIth General Assembly. Toronto, Ontario Canada, August 13-21, 1999. – P. 204. 6. *Олейников Р.В.* Дифференциальные свойства подстановок / Олейников Р.В., Олешко О.И., Лисицкий К.Е.,

Тевяшев А.Д. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 326–333. 7. *Долгов В.И.* Свойства таблиц линейных аппроксимаций случайных подстановок / Долгов В.И., Лисицкая И.В., Олешко О.И // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 334–340. 8. *Долгов В.И.* Случайные подстановки в криптографии / Долгов В.И., Лисицкая И.В., Лисицкий К.Е. // Радіоелектронні та комп'ютерні системи. – 2010. – № 5 (46). – С. 79-84. 9. *Долгов В.И.* Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES / Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Олешко О.И. // Прикладная радиоэлектроника. – 2009. – Т.8, № 3 – С. 252-257. 10. *Долгов В.И.* Миниверсия блочного симметричного алгоритма криптографического преобразования информации с динамически управляемыми криптопримитивами (Baby-ADE) / Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Белоковаленко А.Л. // Прикладная радиоэлектроника. – 2008. – Т.7 – № 3. – С. 215-224. 11. *Долгов В.И.* Криптографичекие свойства уменьшенной версии шифра "Калина"/ Долгов В.И. Олейников Р.В. Большаков А.Ю. Григорьев А.В., Дробатько Е.В. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 349–354. 12. *Долгов В.И.* Исследование циклических и дифференциальных свойств уменьшенной модели шифра Лабиринт / Долгов В.И., Лисицкая И.В., Григорьев А.В., Широков А.В. // Прикладная радиоэлектроника. – Харьков : ХТУРЭ. – 2009. – Т. 8 – № 3. – С. 283-295. 13. *Лисицкая И.В.* Большие шифры – случайные подстановки. / Лисицкая И.В., Настенко А. // Прикладная радиоэлектроника. – 2011. (в печати). 14. *Лисицкая И.В.* Дифференциальные свойства шифра FOX / Лисицкая И.В., Кайдалов Д. // Прикладная радиоэлектроника. – 2011. (в печати). 15. *F. Sano, K. Ohkuma, H. Shimizu, S. Kawamura.* On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis/ IEICE Trans. Fundamentals, vol. E86-a, NO.1 January 2003, pp. 37-46. 16. *Joan Daemen.* Vincent Rijmen Probability distributions of Correlation and Differentials in Block Ciphers./ Joan Daemen, Vincent Rijmen // April 13, 2006. 17. *J. Seberry, X. S. Zhang and Y. Zheng.* Relationships among nonlinearity criteria. Presented at EUROCRYPT-94. 1994. 18. *M.D. Yücel* IAM501-Introduction to Cryptography. Institute of Applied Mathematics METU, Ankara, Turkey (9700501), 2002, p. 1-28. 19. *W. Saier, O. Staffelbach.* Nonlinearity criteria for cryptographic functions. In Advances in Cryptology – EUROCRYPT'89, vol.434. Lecture Notes in Cosputer Science. Springer-Verlag, pp.549-562, 1990. 20. *M. Matsui*, "The First Experimental Cryptanalysis of the Data Encryption Standard", Advances in Cryptology – CRYPTO' 94, Lectures in Computer Science no.839, Springer-Verlag, pp. 1-11, 1994.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 05.08.2011