УДК 681.3.06

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ СВОЙСТВ НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕНЫ УМЕНЬШЕННЫХ ВЕРСИЙ НЕКОТОРЫХ ШИФРОВ

В.И. ДОЛГОВ, А.А. КУЗНЕЦОВ, И.В. ЛИСИЦКАЯ, Р.В. СЕРГИЕНКО, О.И. ОЛЕШКО

В работе изучаются свойства S-блоков уменьшенных моделей некоторых современных блочных симметричных шифров, в том числе шифров, представленных на украинский конкурс по выбору нового стандарта шифрования. Делается вывод, что S-блоки рассмотренных уменьшенных моделей, повторяющие конструкции прототипов, практически обладают одинаковыми криптографическими показателями.

The paper studies the properties of S-blocks of the reduced models of some modern block symmetric ciphers, including ones submitted for the Ukrainian contest on the option of a new standard of block symmetric ciphering. A conclusion is made that S-blocks of the considered reduced models, repeating the designs of prototypes, practically possess the same cryptographic factors.

ВВЕДЕНИЕ

Самые современные ключевые криптосистемы базируются на уже ставшей традиционной идее произведения шифров [1], которые представляют собой класс криптосистем, повторяющих сложную операцию, преобразующую плайнтекст в шифртекст. Каждое такое повторение (итерация) известно как цикл шифра [2]. Сложная (составная) операция, выполняющаяся в каждом цикле, является обычно комбинацией набора примитивных операций, таких как сдвиг, линейное преобразование, сложение по модулю и подстановку [3, 4]. В соответствующем сочетании эти преобразования должны реализовать концепцию построения таких шифров, которая, как известно, состоит в том, что комбинация перестановочных и подстановочных операций слабых в отдельности 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. Поэтому значительные усилия исследователей направлены на изучение подходов к изучению свойств и построению подстановок с высокими криптографическими показателями.

Одним из популярных для описания и изучения свойств S-блоков стал математический аппарат линейной алгебры и, в частности, аппарат булевых функций. Этому направлению посвящено большое число работ [5-14 и мн. др.]. Если кратко характеризовать возможности этого подхода, то можно отметить, что его основой является представление S-блока в виде композиции компонентных булевых функций с последующим изучением их свойств. К сегодняшнему дню уже наработан значительный набор подходов и широкий набор критериев оценки свойств компонентных функций. Вместе с тем, несмотря на очевидную результативность и убедительность этого подхода, он представляется все же достаточно сложным как для освоения, так и для практической реализации. С другой стороны, в свое время нами был предложен подход к построению (отбору) S-блоков [15-17], основанный на использовании показателей (критериев) случайности, следующих из общей математической теории подстановок, имеющий на наш взгляд более простую реализационную и теоретическую основу. Правда, к этим критериям пришлось добавить дополнительные ограничения на максимально допустимые значения элементов таблиц дифференциальных разностей и линейных аппроксимаций, которые, однако, присутствуют и при использовании аппарата булевых функций. Возникло естественное желание попытаться установить связи между этими подходами, тем более, что в последнее время активизировалась работа по изучению свойств уменьшенных версий блочных симметричных шифров [18-21], облегчающих в рамках проходящего в Украине конкурса на новый стандарт блочного симметричного шифрования, позволяющих, по крайней мере, выполнить сравнение эффективности различных решений. В этих шифрах большие (байтовые) S-блоки заменяются уменьшенными S-блоками (при стремлении повторить в уменьшенной версии основные преобразования и структуру построения большого алгоритма), анализ которых существенно упрощается в связи с существенным сокращением необходимого объема вычислительных экспериментов. В этой работе выполняется сопоставление (сравнение) двух отмеченных подходов к анализу S-блоков, которое преследует цель: с одной стороны – определить полезность привлечения для оценки и анализа криптографической стойкости S-блоков показателей их случайности (числа циклов, возрастаний и инверсий), а с другой, – найти подтверждения сохранению в уменьшенных моделях шифров (уменьшенных S-блоках) основных показателей (с учетом выполненного масштабирования) больших прототипов.

1. КОНСТРУКЦИИ S-БЛОКОВ МИНИ ВЕРСИЙ ШИФРОВ, ПРЕДСТАВЛЕННЫХ НА КОНКУРС

Основное внимание в работе сосредотачивается на S-блоках уменьшенных моделей шифров, составивших решения, представленные на конкурс по выбору нового стандарта блочного симметричного шифрования Украины, в числе которых шифры КАЛИНА, ADE, МУХОМОР и ЛАБИРИНТ [22-25]. Нас, прежде всего, будет интересовать, как уже отмечалось, возможность сохранения в уменьшенных моделях шифров соотношений криптографических показателей характерных для больших шифров (учет при построении S-блоков принципов, заложенных в исходных алгоритмах). Попутно мы будем интересоваться и показателями S-блоков уже известных уменьшенных моделей шифров mini-AES и Baby-ADE.

S-блоки шифра mini-AES. Как уже отмечалось ранее в нашей работе [18], в шифре mini-AES в качестве подстановки используется первая строка первого S-блока DES – подстановки, сформированной с помощью тщательного отбора [26].

S-блоки шифра baby-Rijndael. В качестве основы построения S-блока шифра Rijndael (AES) его разработчики Даймен и Риджмен взяли отображение $F(x)=x^{-1}$ в конечном поле – конструкцию, предложенную К. Нюберг [27]. Оно обладает высокой нелинейностью, высоким порядком нелинейности, предельной устойчивостью к атакам дифференциального криптоанализа, эффективной конструкцией и хорошей определенностью (вычислимостью). Чтобы повысить дополнительно алгебраическую сложность преобразования, они скомпоновали эту функцию с другой простой функцией, в качестве которой была взята аффинная функция (снова предложение К. Нюберг [27]). В результате процедура подстановки (SubBytes) задается аффинным преобразованием вида

$$b = M \cdot (a)^{-1} + \beta,$$

где M – квадратная невырожденная матрица размером 8×8 с элементами из поля GF(2), a и b – 8-и битные векторы значений входа и выхода преобразования SubBytes соответственно (элементы соответствующих матриц-состояний), а β – фиксированный 8-и битный вектор, являющийся заданным постоянным параметром этого преобразования (т.е. a, b, $\beta \in \mathrm{GF}(2^8)$).

В уменьшенной модели шифра baby-Rijndael [28], найденной в открытой печати, используется S-блок, построенный по представленным выше правилам, но вместо байтовых векторов рассматриваются полубайтовые векторы. Соответственно невырожденная матрица M имеет размеры 4×4. Конструкция и параметры преобразования являются частным случаем построения S-блоков шифра baby-ADE при значении параметра $\gamma = 1$ (4-х битного вектора 0001), которые рассматриваются ниже.

S-блоки шифра baby-ADE. В отличие от AES, в шифре ADE используются изменяемые таблицы блоков замены, формируемые с помощью дополнительно введенного параметра $\gamma \in \mathrm{GF}(2^8)$, который определяется битами расширенного мастер-ключа (предложение по использованию для построения S-блока управляемой цикловыми ключами комбинации инверсного преобразования с линейным или аффинным также можно найти в работе К. Нюберг [27]). Мы повторили идею этого преобразования и в шифре Baby-ADE, только она отмасштабирована соответственно размеру 16-битного состояния [18].

В результате в качестве S-блока выступает изменяемая матрица подстановок, которая строится с помощью вычисления мультипликативно обратного элемента $(a \cdot \gamma)^{-1} \in \mathrm{GF}(2^4)$ с последующим выполнением аффинного преобразования

$$b = M(a \cdot \gamma)^{-1} + \beta.$$

Здесь $a = \{a_0, a_1, a_2, a_3\}$ и $b = \{b_0, b_1, b_2, b_3\}$ – четырехбитные векторы (полубайты матрицы состояний), M – квадратная невырожденная матрица 4×4:

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix},$$

β – 4-х битный вектор ($\beta \in \mathrm{GF}(2^4)$): $\beta^{''} = (1\ \ 0\ \ 1\ \ 0)$. Каждое значение выхода подстановки $b = \{b_0, b_1, b_2, b_3\}$ зависит как от входного состояния $a = \{a_0, a_1, a_2, a_3\}$, так и от случайного вектора $\gamma = \{\gamma_0, \gamma_1, \gamma_2, \gamma_3\}$, который задается значением циклового ключа. В результате осуществляется криптографическое преобразование данных, при котором происходит динамическое изменение S блоков (блоков нелинейных замен), с сохранением показателей их нелинейности.

Так, например, при $\gamma_i = 6 \rightarrow 0110$ функция нелинейного преобразования задается следующей табл. 1 (см. работу [18]).

При $\gamma_i = k_0 = 0 \rightarrow 0000$ параметр γ_i принимается равным значению k_1. Если полубайт k_1 также равен нулю (0000), то $\gamma_i = 3 \rightarrow 0011$.

S-блоки шифра baby-Лабиринт. Как отмечает автор разработки [23], S-блок шифра Лабиринт выбран из множества предельно-нелинейных биективных преобразований. За основу и в этом случае взята конструкция Нюберг-Динга, т.е. преобразование аффинно-эквивалентное функции вычисления обратного элемента в поле GF(2^8). Математически функция, определяющая преобразование S(x), осуществляемое S-блоком шифра Лабиринт, представляется в виде:

$$S(x) = M_Y \times \left\lfloor (M_X \times x \oplus V_X)^E \right\rfloor_B \oplus V_Y,$$

где $x, V_X, V_Y \in GF(2^8)$; $E = 2^8 - 1 - 2^t$, $0 \le t < 8$; $E = 2^8 - 1 - 2^t$, $0 \le t < 8$; B – некоторый базис над

Таблица 1

Таблица подстановок, реализующая S-блок Baby-ADE при $\gamma_i = 6$

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$S(a)$	10	2	0	6	15	1	12	4	14	11	7	13	9	5	3	8

$GF(2^8)$, который определяется образующим (неприводимым) полиномом 8-й степени $f_S(x)$; E – показатель степени; M_X, M_Y – квадратные невырожденные матрицы размера 8×8, с элементами из поля GF(2). В приведенном соотношении, для упрощения записи, вектора, участвующие в матричном умножении, рассматриваются как вектор–столбцы. Более полно с соображениями автора по выбору этого преобразования можно познакомиться в [23].

S-блок, приведенный в спецификации к шифру, был сформирован с использованием следующих параметров:

• Неприводимый (над GF(2)) полином, с помощью которого строится поле, есть

$$f_S(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$$

(в шестнадцатеричном представлении 0x1BD).

• Показатель степени

$$E = 2^8 - 1 - 2^4 = 251.$$

• Матрицы «входного» и «выходного» аффинных преобразований приведены ниже («вес» двоичных разрядов возрастает «сверху вниз» и «слева направо», т.е. элемент M[0,0], находящийся в верхнем левом углу, соответствует самому младшему разряду).

$$M_X = \begin{bmatrix} 10101110 \\ 01011001 \\ 01111001 \\ 00110011 \\ 00110100 \\ 01101000 \\ 01010011 \\ 01000100 \end{bmatrix}; \; V_X = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix};$$

$$M_X = \begin{bmatrix} 11100010 \\ 01100011 \\ 10101001 \\ 11011101 \\ 11011001 \\ 01111001 \\ 01010011 \\ 11010111 \end{bmatrix}; \; V_Y = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

Насколько оправдано такое усложнение процедуры, мы здесь обсуждать не будем. Заметим лишь, что авторы шифра Rijndael постарались выбрать наиболее простую конструкцию, обеспечивающую необходимые показатели стойкости и высокое быстродействие. Они пошли даже на то, что взяли в своем шифре S-блоки одной и той же конструкции (повторяющиеся).

В уменьшенной модели шифра Лабиринт операции выполняются над полубайтами. Поэтому матрицы входного» и «выходного» аффинных преобразований были взяты размером 4×4, а конкретнее:

$$M_X = \begin{bmatrix} 0100 \\ 1000 \\ 0011 \\ 0101 \end{bmatrix}; \quad M_Y = \begin{bmatrix} 1101 \\ 1001 \\ 0011 \\ 1110 \end{bmatrix};$$

$$V_X = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}; \; V_Y = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix},$$

т.е. строки (столбцы) рассматриваются как элементы векторного пространства, образуемому полем $GF(2^4)$. Соответствующий неприводимый полином выбран вида $f_S(x) = x^4 + x + 1$, а параметр E взят равным $E = 2^4 - 1 - 2^2 = 11$. Матричное представление подстановки, вычисленной для этих параметров, имеет вид:

$$\begin{pmatrix} 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15 \\ 9\ 5\ 14\ 7\ 3\ 12\ 13\ 4\ 2\ 1\ 8\ 15\ 10\ 0\ 6\ 11 \end{pmatrix}.$$

Если изменить порядок отсчета разрядов векторов на обратный (в соответствии с указаниями разработчика), то можно прийти также к подстановке

$$\begin{pmatrix} 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15 \\ 9\ 4\ 12\ 7\ 7\ 1\ 11\ 6\ 10\ 8\ 3\ 0\ 14\ 15\ 2\ 13 \end{pmatrix}.$$

S-блоки мини–Калина и мини-Мухомор. В шифре «Калина» [24] используется 8 различных подстановок «байт-в-байт», причем для байтов одной строки текущего состояния шифра используется одна и та же подстановка. В описании шифра готовые таблицы подстановок приведены в приложении. Известно, что они построены с использованием конгруэнтного генератора «случайных» чисел. Для шифра «Мухомор» [25] указывается, что таблицы подстановки совпадают с первыми 4-мя S-блоками алгоритма «Калина». Поэтому при построении уменьшенных моделей этих шифров предложено использовать или набор малых S-блоков (с разными или одинаковыми) параметрами γ шифра baby-ADE, или малые S-блоки шифра Fox [29], обладающие, как утверждают авторы разработки, высокими дифференциальными и линейными характеристиками переходов. Мы в дальнейшем и сосредоточим свое внимание на более детальном изучении крипто-

графических показателей отмеченного семейства малых S-блоков (подстановок 16-го порядка). В табл. 2 представлены построчно варианты подстановок 16-го порядка, которые будут исследованы далее. Для шифра «Лабиринт» приведены оба варианта представления разрядов входных и выходных векторов.

Напомним далее краткую сущность сопоставляемых в работе подходов.

2. МЕТОДИКА ИССЛЕДОВАНИЯ КРИПТОГРАФИЧЕСКИХ СВОЙСТВ S-БЛОКОВ С ПОМОЩЬЮ АППАРАТА БУЛЕВЫХ ФУНКЦИЙ

Что касается первого подхода, то отметим, что любая подстановка S ($n\times m$ S-блоковая конструкция) может быть реализована в виде совокупности операций, осуществляющих переход от n-битного входного блока данных к последовательности m битов на выходе. Функция S при этом допускает моделирование в виде системы уравнений, связывающих биты входа с каждым битом выхода. С этим функциональным представлением имеется возможность оценивать стойкость подстановочного преобразования S, основываясь на свойствах булевых функций (БФ), которые описывают S: f_i^S будет булевой функцией, описывающей i-тый бит S, $1\le i\le m$ такой, что S реализуется как m-типовых m-битных функций $F=[f_1^S, f_2^S, \ldots, f_m^S]$. Исследователи [2, 3, 6, 7, 8] согласились с тем, что каждая булева функция f_i^S должна владеть комбинацией целого набора свойств, среди которых присутствуют нелинейность [8, 10] (согласно некоторой меры нелинейности), строгий лавинный критерий (SAC) [5], корреляционная иммунность (некоторого порядка) [7] или быть бент-функцией [9]. Были введены также и другие показатели, такие как наличие большого числа термов в алгебраической нормальной форме булевой функции [11] и т.д. Наша ближайшая задача воспользоваться основными результатами этого подхода.

В дальнейшем основное внимание будет сосредоточено на S-блоках размера 4×4. Такие S-блоки осуществляют отображение входного 4-битного вектора в выходной вектор такой же размерности, что на языке гомоморфизмов полей обозначает отображение $F(x):GF(2^4)\to GF(2^4)$. Математически такая подстановка представляется в виде матрицы из двух строк (перестановок без повторений) из 16-ти 4-х битных чисел каждая. Обычно рассматриваются подстановки, представленные в каноническом виде (первая строка упорядочена по значениям 4-х битных входов), что в принципе позволяет рассматривать только вторую строку матрицы подстановок. В результате S-блок может быть представлен объединением четырех компонентных булевых функций $f_i(x_1,x_2,x_3,x_4)$, $i=1,2,3,4$ четырех переменных $x_1,x_2,x_3,x_4\in GF(2)$. Табл. 3 иллюстрирует четыре компонентные функции S-блока шифра Baby-Rijndael [28], повторяющего концепцию построения S-блока шифра AES. Жирным шрифтом записана вторая строка матрицы-подстановки (третья строка в табл. 2).

Приведем здесь основные пункты выполнения анализа свойств S-блоков, выполняемого с привлечением математического аппарата булевой алгебры. Воспользуемся методикой, изложенной в нашей работе [30], где рассмотрены свойства S-блоков шифра ГОСТ 28147-89. В качестве объекта исследований будет выступать первая булева функция f_1 S-блока из табл. 3.

В [30] отмечено, что одним из важнейших критериев эффективности булевой функции в криптографическом смысле является ее *сбалансированность*. Сбалансированные функции наиболее стойкие к прямым статистическим атакам. Определить, сбалансирована функция или нет, можно прямым подсчетом единиц и нулей в ее таблице истинности. В данном случае функция $f_1(x)$ имеет равное количество нулей и единиц: по восемь, поэтому она является сбалансированной.

Для определения других криптографических параметров функции (количества термов функции, количества термов, содержащих каждую переменную, алгебраической степени функции, алгебраической степени каждой переменной и др.) необходимо восстановить алгебраическую нормальную форму функции. Напомним, что алгебраической нормальной формой (АНФ) называется представление булевой функции в виде

Таблица 2

S-блоки уменьшенных версий шифров

Шифр	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
MiniA	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
BabyR	10	4	3	11	8	14	2	12	5	7	6	15	0	1	9	13
ADE6	10	2	0	6	15	1	12	4	14	11	7	13	9	5	3	8
ADE7	10	12	9	7	13	5	4	2	1	6	11	8	3	14	0	15
ADE3	10	11	2	14	0	13	6	7	15	5	1	9	12	8	4	3
Лабир. 1	9	5	14	7	3	12	13	4	2	1	8	15	10	0	6	11
Лабир. 2	9	4	12	5	7	1	11	6	10	8	3	0	14	15	2	13
FOX1	2	5	1	9	14	10	12	8	6	4	7	15	13	11	0	3
FOX2	11	4	1	15	0	3	14	13	10	8	7	5	12	2	9	6
FOX3	13	10	11	1	4	3	8	9	5	7	2	12	15	0	6	14

$$f(x_1,\ldots,x_n)=$$

$$=a_0\oplus\bigoplus_{i=1}^{n}a_ix_i\oplus\bigoplus_{1\le i<j\le n}a_{ij}x_ix_j\oplus\ldots\oplus a_{12}x_1x_2\ldots x_n.$$

Коэффициенты $a_i\in GF(2)$, $i=0,1,\ldots,2^n-1$ при каждом терме в приведенном выражении (в рассматриваемом случае $n=4$) находят подстановкой в него значений переменных X_1,X_2,X_3,X_4 и фиксацией значения булевой функции в ее таблице истинности с последующим решением системы уравнений:

$$\sum_{i=0}^{15}a_iT_i=f_i(X_1,X_2,X_3,X_4),$$

где T_i – i-тый одночлен АНФ функции. Соответствующие результаты расчетов для булевой функции $f_1(x)$ приведены в табл. 4.

Найденные значения коэффициентов позволяют записать функцию $f_1(x)$ в необходимом виде:

$$f_1(x)=x_2+x_4+x_2x_3+x_3x_4+x_1x_2x_4+$$
$$+x_1x_3x_4+x_2x_3x_4.$$

Из полученной АНФ функции простым подсчетом можно определить следующие криптографически важные свойства функции:

– количество термов в функции:

$$term(f_1)=7;$$

– количество термов в функции, содержащих определенную переменную:

$$term_{x_1}(f_1)=2,\ term_{x_2}(f_1)=4,$$

$$term_{x_3}(f_1)=4,\ term_{x_4}(f_1)=5;$$

– алгебраическую степень функции (нелинейный порядок функции), $\deg(f_1)=3$;

– алгебраическую степень каждой переменной: $\deg(f_1,x_i)=3$ для всех i.

Аналогичным образом восстанавливается АНФ для остальных компонентных БФ:

$$f_2(x)=1+x_1+x_3+x_4+x_1x_2+x_2x_3+$$
$$+x_2x_4+x_3x_4+x_1x_2x_3+x_1x_3x_4,$$

$$f_3(x)=x_1+x_4+x_1x_2+x_1x_4+$$
$$+x_3x_4+x_1x_2x_3+x_1x_2x_4,$$

$$f_4(x)=1+x_1+x_2+x_4+x_1x_3+x_1x_4+$$
$$+x_2x_4+x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4.$$

Отмеченная группа показателей характеризует стойкость S-блока и шифра в целом к алгебраическим атакам, которые используют недостаточную сложность математического описания шифрующих преобразований.

Очередным важным криптографическим показателем булевой функции является ее *нелинейность*. Нелинейность функции численно определяется минимальным расстоянием Хемминга между данной функцией и всеми аффинными функциями векторного пространства V_n, определяемого полем $GF(2^n)$ [13, 14]:

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

где $\varphi_1,\varphi_2,\ldots,\varphi_{2^{n+1}}$ аффинные функции над V_n.

Для определения этого показателя строятся таблицы истинности всех возможных аффинных функций, и путем сопоставления этих таблиц с таблицами истинности булевой функции определяется значение минимального из расстояний Хемминга между данной функцией и всеми аффинными функциями. Для рассматриваемой булевой функции $f_1(x_1,x_2,x_3,x_4)$, оно равно 4, и, следовательно, значение нелинейности функции есть 4.

Существенным усилением свойства сбалансированности БФ является требование сбалансированности всех частных функций, полученных из исходной функции фиксированием любых ее k или менее переменных. Указанное требование позволяет обеспечить стойкость криптографических преобразований к статистическим атакам при фиксированных значениях битов на входе преобразования. Данное свойство связано с показателем корреляционной иммунности (*КИ*).

Говорят, что функция f обладает *корреляционной иммунностью* порядка k, если последовательность значений функции $y\in Y$ статистически

Таблица 3

Таблицы истинности компонентных БФ S-блока шифра Baby-Rijndael

S	10	4	3	11	8	14	2	12	5	7	6	15	0	1	9	13
f_1	0	0	1	1	0	0	0	0	1	1	0	1	0	1	1	1
f_2	1	0	1	1	0	1	1	0	0	1	1	1	0	0	0	0
f_3	0	1	0	0	0	1	0	1	1	1	1	1	0	0	0	1
f_4	1	0	0	1	1	1	0	1	0	0	0	1	0	0	1	1

Таблица 4

Значения коэффициентов при термах АНФ булевой функции $f_1(x)$

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}
0	0	1	0	1	0	0	0	1	0	1	0	1	1	1	0

не зависит от подмножеств из k координат-аргументов (значений входов) [13]:

$$\forall\ \{x_1, x_2, \ldots, x_m\}$$
$$[P(y \in Y / \{x_1, x_2, \ldots, x_m\} \in X) = P(y \in Y)].$$

Эквивалентное определение корреляционного иммунитета в терминах преобразования Уолша [13]: функция f над полем $GF(2^n)$ имеет корреляционный иммунитет порядка k, $КИ(k)$, если ее преобразование Уолша (ПУ) удовлетворяет равенству $F(\omega) = 0$ для всех $\omega \in V_n$ таких, что $1 \le W(\omega) \le k$:

$$\forall \omega \in V_n, \quad F(\omega) = 0, \quad КИ(f) = k.$$

Напомним, что *преобразование Уолша* $F(\omega)$ функции f над полем $GF(2^n)$ определяется как принимающая действительные значения функция [8]

$$F(\omega) = 2^{-n} \cdot \sum\nolimits_{x \in GF(2^n)} (-1)^{f(x)} (-1)^{\langle \omega, x \rangle},$$

где $\omega \in V_n$, $f(x)$, $\langle \omega, x \rangle \in N$, $\langle \omega, x \rangle$ – скалярное произведение векторов ω и x ($\langle \omega, x \rangle = w_1 \otimes x_1 \oplus \ldots \oplus \oplus w_n \otimes x_n$).

Корреляционно-эффективной является функция, для которой не менее чем для половины векторов веса $1 \le w \le q$ значения компонентов спектра ПУ равны 0.

Определим значения $F(\omega)$ для всех возможных значений ω: $F(1,0,0,0) = 2^{-4} (\sum_x (-1)^{f(x) \oplus x_1}) = 2^{-4}(4) = 1/4$. Таким же образом вычисляем значения ПУ для других ω. Результаты сведены в таблицу 5. Полученные результаты свидетельствуют, что рассматриваемая функция не является корреляционно-иммунной, и даже не является корреляционно-эффективной, так как она имеет всего лишь 5 нулевых значений.

При синтезе БФ, обеспечивающих высокую стойкость к дифференциальному, линейному и корреляционному криптоанализу, большое значение имеет автокорреляционная функция ($АКФ$) БФ. *Автокорреляционная функция* $r_f(s)$ для $s \in 0, \ldots, 2^{n-1}$ определяется как

$$r_f(s) = \sum_{x=0}^{2^n - 1} \hat{f}(x) \hat{f}(x \oplus s)$$

для всех $s \in GF(2^n)$. Здесь используется обозначение $\hat{f}(x) = (-1)^{f(x)}$, с помощью которого обеспечивается преобразование значения $\{0, 1\}$ функции $f(x)$ в значения $\{-1, 1\}$.

Говорят [9], что функция f удовлетворяет *характеристике распространения* m, если для значений s, заключенных в границы $1 \le |s| \le m$, выполняется условие $|r_f(s)| = 0$. Автокорреляция $r_f(s)$ оценивает утечку («просачивание») информационного потока с входа на выход функции.

Аналогично, *автокорреляция* $AC(f)$ функции f определяется как модуль наибольшего значения $r_f(s)$:

$$AC(f) = \max_{s \ne 0} \left| \sum_s \hat{f}(x) \hat{f}(x \oplus s) \right| = \max_{s \ne 0} |r_f(s)|.$$

Она была предложена Цзенгом и Цзангом как глобальная лавинная характеристика [13], поскольку включает все автокорреляции, не только соответствующие s с частными (низкими) весами Хэмминга.

Результаты определения значения $АКФ$ для всех возможных значений s для рассматриваемого примера приведены в табл. 6.

Из таблицы следует, что автокорреляция функции $f_1(x)$ равна 8.

Таблица 5

Расчеты преобразований Уолша для булевой функции $f_1(x)$

ω	<x, ω>	F(ω)	ω	<x,ω>	F(ω)	ω	<x, ω>	F(ω)
(1,0,0,0)	x_1	4	(1,1,0,0)	$x_1 + x_2$	0	(1,1,1,0)	$x_1+x_2+x_3$	-4
(0,1,0,0)	x_2	4	(1,0,1,0)	$x_1 + x_3$	0	(1,1,0,1)	$x_1+x_2+x_4$	0
(0,0,1,0)	x_3	-4	(1,0,0,1)	$x_1 + x_4$	-4	(1,0,1,1)	$x_1+x_3+x_4$	0
(0,0,0,1)	x_4	8	(0,1,1,0)	$x_2 + x_3$	0	(0,1,1,1)	$x_2+x_3+x_4$	8
			(0,1,0,1)	$x_2 + x_4$	4	(1,1,1,1)	$x_1+x_2+x_3+x_4$	4
			(0,0,1,1)	$x_3 + x_4$	-4			

Таблица 6

Расчеты значений $АКФ$ для функции $f_1(x)$

s	АКФ	s	АКФ	s	АКФ
(1,0,0,0)	8	(1,1,0,0)	0	(1,1,1,0)	0
(0,1,0,0)	0	(1,0,1,0)	0	(1,1,0,1)	0
(0,0,1,0)	0	(1,0,0,1)	8	(1,0,1,1)	0
(0,0,0,1)	-8	(0,1,1,0)	-8	(0,1,1,1)	8
		(0,1,0,1)	0	(1,1,1,1)	-8
		(0,0,1,1)	0		

В аналогичном ракурсе определяется и другая глобальная характеристика – сумма квадратов различных автокорреляций, то есть

$$\sigma_f = \sum_s \hat{r}(s)^2.$$

3. МЕТОДИКА ИССЛЕДОВАНИЯ КРИПТОГРАФИЧЕСКИХ СВОЙСТВ S-БЛОКОВ С ПОМОЩЬЮ КРИТЕРИЕВ СЛУЧАЙНОСТИ

Напомним основные положения второго из интересующих нас подходов к оценке криптографических свойств S-блоков. Следуя работе [15], применительно к подстановкам порядка n введем понятие случайной (квазислучайной) подстановки, под которой понимается подстановка, удовлетворяющая трем критериям случайности, включающим выполнение следующих свойств:

Свойство 1. Число инверсий η_n в подстановке степени n удовлетворяет условию

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

Свойство 2. Число циклов ξ_n в подстановке степени n удовлетворяет условию

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

Свойство 3. Число возрастаний θ_n в подстановке степени n удовлетворяет условию

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

В этих соотношениях a – параметр, выбираемый в значительной степени из субъективных соображений (по крайней мере, из условия, что множество допустимых подстановок будет не через чур уж ограниченным).

В этой же работе сделан вывод о возможности использования наиболее жестких из приведенных здесь условий отбора подходящих подстановок, а именно значения $a = 1$. Для $n = 16$ это будут такие ограничения

$$\left|\eta_n - 60\right| \le 10; \quad \left|\xi_n - 3\right| \le 2; \quad \left|\theta_n - 8\right| \le 1.$$

Установлено, что эти границы проходит около 50% всех подстановок, так что «случайных» подстановок оказывается достаточно внушительное число. В итоге, методика отбора подстановок по критериям случайности сводится к проверке числа возрастаний, циклов и инверсий, реализуемых конкретным преобразованием. Например, для рассмотренного ранее S-блока шифра Baby-Rijndael результаты проверки свойств случайности позволили получить: число инверсий в подстановке $\eta_n = 59$; число циклов $\xi_n = 1$; число возрастаний $\theta_n = 8$.

В результате можно заключить, что рассмотренная подстановка является подстановкой случайного типа. Остается учесть дополнительные критерии отбора в отношении значений таблиц дифференциальных разностей и таблиц линейных аппроксимаций. Мы, однако, обсуждение этих ограничений отложим до проведения более полных исследований обоих подходов, так как эти критерии характерны и при использовании аппарата булевых функций.

4. РЕЗУЛЬТАТЫ РАСЧЕТОВ КРИПТОГРАФИЧЕСКИХ СВОЙСТВ КОМПОНЕНТНЫХ ФУНКЦИЙ S-БЛОКОВ НЕКОТОРЫХ ШИФРОВ

В табл. 7 представлены результаты исследования криптографических свойств компонентных булевых функций, составляющих блок замен шифров mini-AES (S-блок шифра DES), Baby-Rijndael, а также всех блоков замен шифра Baby-ADE, сформированные при параметрах $\gamma_1 = 6$, $\gamma_2 = 7$ и $\gamma_3 = 5$ (см. описание шифра Baby-ADE [18]), а в табл. 8 представлены соответствующие результаты для S-блоков шифров мини-Лабиринт и Fox. Полученные результаты свидетельствуют, что практически все компонентные функции блоков замен являются сбалансированными, имеют высокую алгебраическую степень 3, имеют нелинейность 4 (максимально возможную нелинейность сбалансированной функции). Тем не менее, большинство функций (в том числе и все функции S-блока Baby-Rijndael) не имеют корреляционной иммунности и не удовлетворяют строгому лавинному критерию. Нами также были построены таблицы дифференциальных разностей для S-блоков из табл. 2 и оценены максимальные значения достижимых разностей для каждой из таблиц. Эти результаты также представлены в табл. 7 и 8. Видно, что все рассмотренные S-блоки, кроме S-блока шифра mini-AES (DES) обладают высокими показателями (максимальное значение XOR разностей равно 4). У S-блока шифра mini-AES (DES) соответствующее значение равно 6.

С другой стороны видно, что все рассмотренные S-блоки удовлетворяют установленным критериям случайности по числу инверсий, возрастаний и циклов.

Нами был проведен также эксперимент по проверке булевых свойств компонентных функций случайных S-блоков (удовлетворяющих только установленным выше критериям случайности). Эксперимент показал, что большинство (более 50%) из этих случайных подстановок не уступают по своим показателям подстановкам табл. 2, однако среди случайных подстановок имеются подстановки и с ухудшенными криптографическими показателями по сравнению с подстановками табл. 2 (имеются S-блоки с компонентными булевыми функциями, обладающими нелинейностью равной 2; для этих булевых функций параметр AC(f) = 16 и они имеют увеличенное до 33,941 значение сумм квадратов различных корреляций σ_f; имеются даже редкие случаи появления аффинных функций).

Таблица 7

Криптографические свойства компонентных булевых функций блоков замен шифров Baby-Rijndael, mini-AES и Baby-ADE

	S-блок Baby-Rijndael				S-блок mini-AES (DES)				S-блок 6 Baby-ADE				S-блок 7 Baby-ADE				S-блок 3 Baby-ADE			
	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4
Сбалансированность	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Нелинейность N_f	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
Порядок КИ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Корреляц. эф-сть	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Корр. эф-сть 1-го п-ка	–	–	–	–	–	–	–	–	–	–	+	–	+	+	–	+	+	+	–	–
Порядок КР	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1
АС(f)	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
Сумма квадр. кор. σ_f	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6
Кол-во термов	7	10	7	11	5	11	7	8	6	8	6	9	7	9	7	7	6	7	8	8
Кол-во термов с x_1	2	4	5	6	3	5	3	2	3	3	4	5	1	3	5	3	3	4	4	3
Кол-во термов с x_2	4	4	3	5	2	5	3	3	3	4	1	5	3	4	2	4	4	1	6	4
Кол-во термов с x_3	4	5	2	4	1	5	2	5	3	4	3	4	3	5	5	2	2	3	3	4
Кол-во термов с x_4	5	4	4	6	3	5	3	3	4	4	3	3	5	2	3	3	3	3	3	4
Алг. степень deg(f)	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Алг. степень x_1	3	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3
Алг. степень x_2	3	3	3	3	3	2	3	3	3	3	2	3	3	3	3	3	3	2	3	3
Алг. степень x_3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	2	2	3	3	3
Алг. степень x_4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Макс. значение XOR	4(15)				8(1)				4(15)				4(15)				4(15)			
Число инверсий	59				69				57				67				69			
Число возрастаний	8				5				6				6				5			
Число циклов	1				7				1				3				7			

Таблица 8

Криптографические свойства компонентных булевых функций блоков замен шифров Мини-Лабиринт, Мини-Мухомор и Мини-Калина

	S-блок М-Лабиринт1				S-блок 1 FOX				S-блок 2 FOX				S-блок 3 FOX				S-блок М-Лабиринт2			
	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4
Сбалансированность	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Нелинейность N_f	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
Порядок КИ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Корреляц. эф-сть	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Корр. эф-сть 1-го п-ка	–	–	–	–	–	+	–	–	+	–	–	–	–	+	–	–	–	–	–	–
Порядок КР	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1
АС(f)	8	8	8	8	8	8	8	8	8	16	8	8	8	8	8	8	8	8	8	8
Сумма квадр. кор. σ_f	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	27,71	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6	19,6
Кол-во термов	7	7	6	10	11	9	10	4	10	5	7	8	10	5	7	7	9	6	9	8
Кол-во термов с x_1	4	3	3	4	7	5	6	2	5	1	4	3	6	3	4	3	3	3	4	5
Кол-во термов с x_2	2	3	2	5	6	4	4	1	4	2	4	2	4	3	3	3	3	4	3	7
Кол-во термов с x_3	3	3	4	5	6	4	5	3	3	1	3	4	4	3	2	4	4	1	6	4
Кол-во термов с x_4	5	4	3	4	5	3	6	1	5	1	3	3	5	1	3	2	5	3	5	5
Алг. степень deg(f)	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Алг. степень x_1	3	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3
Алг. степень x_2	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	2	3	3
Алг. степень x_3	3	3	3	3	3	2	3	2	3	3	3	3	3	3	3	2	2	3	3	3
Алг. степень x_4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Макс. значение XOR	4(15)				4(18)				4(24)				4(15)				4(15)			
Число инверсий	65				57				64				60				55			
Число возрастаний	7				7				5				9				7			
Число циклов	3				1				2				4				3			

Нами также был проведен эксперимент по проверке достижимых значений дифференциальных разностей случайных S-блоков. Определялся показатель дифференциальной δ-равномерности (максимальное значение таблицы дифференциальных разностей) [31]. Следует заметить, что в рамках сравнительно малого объема выборки (несколько десятков случайных S-блоков) число подходящих (имеющих максимальное значение таблицы дифференциальных XOR разностей) S-блоков составило около 10%. Это говорит о том, что проведение дополнительной фильтрации таких подстановок по допустимым значениям таблиц распределения разностей (XOR) и значениям линейных аппроксимационных таблиц (LAT) позволит для S-блоков 16-го порядка получить S-блоки с необходимыми свойствами. Сохранится ли этот результат для S-блоков большего размера, предстоит выяснить в дальнейших исследованиях.

Из анализа табл. 7 можно также увидеть, что блоки замен шифра Baby-ADE по своим свойствам практически не уступают блоку замен шифра Baby-Rijndael и шифра mini-AES (кроме максимального значения XOR). Во всех исследованных блоках замен Baby-ADE в отличие от блока замен шифра Baby-Rijndael, имеются компонентные функции с корреляционной эффективностью первого порядка, а также в некоторых блоках замен компонентные функции имеют степень распространения 1. В то же время, количество термов в АНФ функций блока замен шифра Baby-Rijndael в среднем на 1-2 больше чем у функций шифров Baby-ADE и mini-AES. Можно посчитать, что это факт может привести к упрощению системы уравнений, описывающих S-блок и шифр Baby-ADE в целом и создать предпосылки для упрощения криптоанализа шифра алгебраическими методами.Однако, блоки замен Baby-ADE зависят от циклового ключа, что приведет скорее к большему усложнению алгебраического описания шифра.

Можно попутно отметить, что по сравнению с рассмотренными блоками нелинейных замен мини и других шифров S-блоки шифра ГОСТ 28147-89 имеют более низкие показатели нелинейности – 2 против 4 для mini-AES, Baby-Rijndael и Baby-ADE [30].

ВЫВОДЫ

Блоки нелинейных замен для рассмотренных мини версий блочных симметричных шифров имеют близкие криптографические показатели, и могут быть построены на основе отбора подстановок по критериям случайности с дополнительной фильтрацией по показателям максимально допустимых значений таблиц дифференциальных разностей и таблиц линейных аппроксимаций.

Результаты показывают, что для всех рассмотренных моделей мини шифров с успехом можно использовать одни и те же S-блоки (S-блоки из табл. 2).

Литература.

[1] *C.E. Shannon*. Communication theory of secrecy systems. *Bell System Technical Journal*, 28: 656-175, 1949.

[2] *L. O'Connor*. An analysis of a class of algorithms for *S*-box construction. Journal of Cryptology, 7 (1): 133-151, 1994.

[3] *H. Feistel. W.A. Notz and J. Lynn Smith*. Some cryptographic techniques for machine-to-machine data communications. *Proceedings of the IEEE*, 63(11):1545-1554. 1975.

[4] *A. Konheim*. Cryptography: a primer. Wiley, 1981.

[5] R. Forrė. The strict avalanche criterion: spectral properties of Booleans functions and an extended definition. *Advances in Cryptology, CRYPTO*'88, *Lecture Notes in Computer Science, vol.* 403, *S. Goldwasser ed., Springer-Verlag,* pages 450-468, 1990.

[6] *J. Piepzyk and G. Finkelstein*. Towards effective nonlinear cryptosystem design. *IEE proceedings,* 135, part E(6): 325-335, 1988.

[7] *Sigenthaler*. Correlation-immunity of nonlinear combining function for cryptographic applications, IEEE Transactions on Information Theory, 30 (5):776-779,1984.

[8] *S.Saitra, E.Pasalic*. Further constructions of resilient Boolean functions with very high nonlinearity. Accepted in SETA, Say, 2001, Norway.

[9] *S. Lloyd*. Counting functions satisfying a higher order strict avalanche criterion, in LNCS 434: *In Advances in Cryptology EUROCRYPT'89*, pp. 63–784. Springer Verlag, 1990.

[10] *W.Saier, O.Staffelbach*. Nonlinearity criteria for cryptographic functions. In Advances in Cryptology – EUROCRYPT'89, vol.434, Lecture Notes in Computer Science, Springer-Verlag, pp.549-562, 1990.

[11] *E. Pasalic, T. Johansson*. Further Results on the Relation Between Nonlinearity and Resiliency for BF. IEEE Trans. on Information Theory, Vol 48, No. 7, July 2002, 1825-1834.

[12] *W. Sillan, A. Clark and E. Dawson,* "Smart Hill Clisbing Finds Better Boolean Functions", Workshop on Selected Areas in Cryptography 1997 (SAC'97), page 50, Workshop Record.

[13] *J. Seberry, X.-S. Zhang and Y.Zheng*. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions // In Information and Computation, Vol. 119, No 1, pp. 1 - 13, 1995.

[14] *W.Saier, O.Staffelbach*. Nonlinearity criteria for cryptographic functions. In Advances in Cryptology – EUROCRYPT'89, vol.434, Lecture Notes in Computer Science, Springer-Verlag, pp.549-562, 1990.

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

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

[17] *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.

[18] *Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Белоковаленко А.Л.* Мини-версия блочного симметричного алгоритма криптографического преобразования информации с динамически управляемыми криптопримитивами (Baby-ADE) // Радиотехника, в печати.

[19] *Долгов В.И., Руженцев И.В., Лисицкая И.В.* Анализ циклических свойств блочных шифров. // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. № 2, С. 257-263.

[21] *Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Белоковаленко А.Л.* Исследование дифференциальных свойств мини-шифра Baby-ADE и Baby-AES // Радиотехника, в печати.

[22] *Кузнецов А.А., Сергиенко Р.В., Наумко А.А.* Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. Том. 6, №2, С. 241-249.

[23] *Головашич С.А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. Том. 6, №2, С. 230-240.

[24] *Горбенко Ю.І., Нейванов А.В.* Принципи побудови та властивості блокового симетричного шифру «Калина» // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. Том. 6, №2, С. 209–216.

[25] *Горбенко І.Д., Бондаренко М.Ф., Долгов В.І., Олійников Р.В., Руженцев В.І., Михайленко М.С., Горбенко Ю.І., Олешко О.І., Кузьміна С.В.* Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. Том. 6, №2, С. 147-157.

[26] *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Пер. с англ.: М.: Издательство ТРИУМФ, 2002. – 816 с.

[27] *K. Nyberg,* "Differentially unifors sappings for cryptography," Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 55-64.

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

[29] *P. Junod and S. Vandenay.* Fox: a new family of block ciphers. To appear in Selected Areas in Cryptography 2004: Waterloo, Canada, August 9-14, 2004.

[30] *Р.В. Сергиенко, И.В. Московченко.* Исследование криптографических свойств нелинейных узлов замен алгоритма симметричного шифрования ГОСТ 28147-89 // Системи обробки інформації, Харків, 2007, випуск 8 (66), С. 91-95.

[31] *Seberry, X.M. Zhang, Y. Zheng.:* Relationships among nonlinearity criteria. Presented at EUROCRYPT-94, 1994.

Поступила в редколлегию 11.09.2009

Долгов Виктор Иванович, доктор технических наук, профессор кафедры «Безопасности информационных технологий» ХНУРЭ. Область научных интересов: математические методы защиты информации.

Кузнецов Александр Александрович, доктор технических наук, профессор. Область научных интересов: алгебраическая теория блоковых кодов, криптография и теория аутентификации, методы обеспечения помехоустойчивости, имитостойкости и скрытности каналов управления и связи.

Лисицкая Ирина Викторовна, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, теория сложности.

Сергиенко Роман Викторович, кандидат технических наук по специальности системы защиты информации. Область научных интересов: алгебраическая теория блоковых кодов, криптографические средства защиты информации.

Олешко Олег Иванович, старший преподаватель кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.