УДК 681.3.06

ЛИНЕЙНЫЕ СВОЙСТВА БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ, ПРЕДСТАВЛЕННЫХ НА УКРАИНСКИЙ КОНКУРС

А.А. КУЗНЕЦОВ, И.В. ЛИСИЦКАЯ, С.А. ИСАЕВ

Развивается новый подход в теории и методах криптоанализа, предложенный на кафедре БИТ ХНУРЭ, основанный на использовании при определении ожидаемых показателей стойкости больших шифров результатов анализа их уменьшенных моделей. Излагается быстрый алгоритм подсчета ЛАТ и новые результаты по изучению линейных свойств уменьшенных моделей шифров, представленных на украинский конкурс, вместе с малой версией шифра Rijndael. Результаты анализа уменьшенных моделей связываются с ожидаемыми показателями стойкости прототипов.

Ключевые слова: блочный симметричный шифр, уменьшенная модель, значение максимума линейного корпуса, доказуемая стойкость.

ВВЕДЕНИЕ

В нашей предыдущей работе [1], была изложена сущность развиваемого нового подхода в теории и методах криптоанализа, предложенного на кафедре БИТ ХНУРЭ [2, 3]. Он основан на использовании при определении ожидаемых показателей стойкости больших шифров результатов анализа их уменьшенных моделей.

Для его обоснования в работе были рассмотрены особенности построения уменьшенных моделей шифров, представленных на открытый конкурс по отбору кандидатов на национальный стандарт блочного симметричного шифрования Украины и приведены обобщенные данные по анализу дифференциальных свойств уменьшенных моделей, а также дополнительные новые результаты по изучению их дифференциальных характеристик.

В заключении к работе отмечается один из центральных её результаты заключающийся в том, что представленные на украинский конкурс шифры Калина, ADE, Мухомор и Лабиринт (их уменьшенные версии) после 4-5 циклов шифрования становятся близкими по дифференциальным свойствам к случайным подстановкам. Результаты работы свидетельствуют о справедливости новой идеологии по оценке показателей стойкости шифров к атакам дифференциального и линейного криптоанализа развиваемой на кафедре БИТ ХНУРЭ [3], основой которой является положение, заключающееся в том, что современные БСШ (при полном наборе цикловых преобразований) являются случайными подстановками (обладают свойствами близкими к свойствам случайных подстановок). Здесь под случайной подстановкой понимается подстановка, у которой законы распределения числа возрастаний, инверсий и циклов, а также законы распределения вероятностей переходов их XOR таблиц и смещений таблиц линейных аппроксимаций совпадают (являются близким) с соответствующими теоретическими законами распределения вероятностей, полученными для случайных подстановок [4-7].

Эта работа продолжает изложение результатов исследований в отмеченном направлении. В дополнение к представленным ранее материалам по исследованию дифференциальных свойств в работе предлагаются результаты экспериментов с малыми моделями шифров, свидетельствующие о том, что и по линейным показателям большие шифры при полном числе циклов шифрования становятся случайными подстановками. До сих пор работы в этом направлении сдерживались существенно увеличивающимся объёмом вычислений, требующимся при построении линейной аппроксимационной таблицы (ЛАТ). Даже для малых версий шифров построение ЛАТ при использовании традиционных методов увеличивало сложность вычислений в 2^{16} раза по сравнению с построением дифференциальной таблицы (для вычисления которой нужно было просчитать значения заполнений 2^{32} её ячеек).

Дело существенно продвинулось вперед в связи с найденным в Интернете описанием быстрого алгоритма просчета ЛАТ [8]. Мы и начнем изложение материала с описания этого алгоритма. На наш взгляд он представляет самостоятельный интерес и заслуживает популяризации.

1. БЫСТРЫЙ АЛГОРИТМ ПОДСЧЕТА ЛАТ

Мы здесь приведем основные результаты, изложенные в недавно обнаруженной работе [8]. У нас были и свои разработки в этом направлении, но автор цитируемой работы оказался более находчивым и оригинальным. В работе [8] они излагаются как быстрый алгоритм вычисления таблицы аппроксимаций *TAf* для случайной функции *f*, определенной в виде $Y = f(X) : \{0,1\}^n \to \{0,1\}^m$. Здесь и далее в подразделе сохранена система обозначений в авторской интерпретации.

Быстрый алгоритм вычисления таблицы аппроксимаций *TAf* состоит из двух шагов. На первом шаге вычисляется начальное значение таблицы *TAf*. Процесс получения начального значения *TAf* включает использование элементарных аппроксимационных таблиц *TP* для всех остаточных функций *f*, зависящих от одной переменой X_0. На втором шаге вычисляется конечное значение *TAf*,

как результат сложения и вычитания этих элементарных таблиц для последовательных значений. Важной особенностью быстрого алгоритма является то, что вычисление таблицы *TAf* может быть выполнено поколоночно, без хранения всей таблицы *TAf* в памяти.

Процедура вычисления начального значения колонки таблицы аппроксимаций *TAf* для *Y′* представлена на рис. 1.

INI-TAC(*TAC, Y′, f, n, m, TP*)
1. for $X' = 0$ to $2^n - 1$ do
2. $TAC[X'] = $ BIT-XOR($f[X']$ and Y', m)
3. for $X' = 0$ to $2^n - 2$ step 2 do
4. ($TAC[X']$, $TAC[X'+1]$) = $TP[TAC[X'], TAC[X'+1]]$
5. Return

Рис. 1. Процедура вычисления начального значения колонки *TAf* для *Y′*

Здесь *X′, Y′* – маски входа и выхода функции *f*, *TAC* (column of approximation table) – колонка аппроксимационной таблицы.

Вспомогательная функция BIT-XOR(*X*, *n*) вычисляет вес Хэмминга *n*-битного вектора *X* (количество единиц в двоичной последовательности).

BIT-XOR(X, n)
1. $w = 0$
2. for $i = 0$ to $n - 1$ do $w = w \oplus X_i$
3. return w

Рис. 2. Процедура вычисления веса Хэмминга *n*-битного вектора

Начальное значение колонки *TAf* для *Y′* вычисляется процедурой INI-TAC(...). В начале (шаги 1-2) для каждой маски *X′* вычисляется значение $Y[Y']$ с использованием вспомогательной функции BIT-XOR(...) рис.2. Затем (шаги 3-4) каждая пара смежных значений заменяется парой, хранящейся в таблице пар *TP*. Сама таблица *TP* представлена в таблице 1:

Таблица 1

Таблица пар TP

ν_0	ν_1	TP[ν_0 , ν_1]
0	0	(1, 0)
0	1	(0, 1)
1	0	(0, –1)
1	1	(–1, 0)

Для каждой функции имеется одна переменная, определяемая значениями ν_0 и ν_1, содержащая пару значений из правой колонки элементарной таблицы аппроксимаций TP.

Процедура вычисления конечного значения колонки *TAf* для *Y′* представлена на рис. 3.

CALC-TAC(TAC, i, j)
1. if $j - i > 2$ then
2. $k = (i + j)$ div 2
3. CALC-TAC(*TAC*, *i*, k)
4. CALC-TAC(*TAC*, *k*+1, *j*)
5. SUMSUB-TAC(*TAC*, *i*, *k*, *k*+1, *j*)
6. return

Рис. 3. Процедура вычисления конечного значения колонки *TAf* для *Y′*, первый вызов функции имеет вид: CALC-TAC(TAC, 0, $2^n - 1$)

Конечное значение колонки *TAf* для *Y′* вычисляется рекурсивной процедурой CALC-TAC(...). В первом вызове процедуры должно быть использовано начальное значение колонки TAf и диапазон строк: i=0, j= $2^n - 1$. Для диапазона большего 2 задача разбивается на две подзадачи (шаги 3-4). Колонка таблицы аппроксимаций вычисляется вспомогательной процедурой SUMSUB-TAC(...).

SUMSUB-TAC(TAC, i_1 , j_1 , i_2 , j_2)
1. for $i = 0$ to $j_1 - i_1$ do
2. (TAC[$i_1 + i$], TAC[$i_2 + i$]) = (TAC[$i_1 + i$] + + TAC[$i_2 + i$], TAC[$i_1 + i$] – TAC[$i_2 + i$])
3. return

Рис. 4. Процедура SUMSUB-TAC(...)

Процедура SUMSUB-TAC(...) для двух частей колонки *TAf* (полученных в результате решения двух подзадач) заменяет первую из них их суммой, а вторую – их разностью.

На рис. 5 представлен быстрый алгоритм вычисления значения *maxTA* для функции *f*:

maxTA(*f*, *n*, *m*)
1. max = 0
2. for $Y' = 0$ to $2^m - 1$ do
3. INI-TAC(*TAC*, *Y′*, *f*, *n*, *m*, *TP*)
4. CALC-TAC(*TAC*, 0, $2^n - 1$)
5. for $X' = 0$ to $2^n - 1$. do
6. if $X' \neq 0$ or $Y' \neq 0$ then
7. if max < $|TAC[X']|$ then max = $|TAC[X']|$
8. return max

Рис. 5. Быстрый алгоритм вычисления значения *maxTA* для функции *f*

Процедуры INI-TAC(...) и CALC-TAC(...) вычисляют колонку *TAf* для *Y′* за линейное время O(*n*+*m*) для одного элемента. Быстрый алгоритм maxTA(...) вычисляет значение maxTA, которое соответствует лучшей ненулевой линейной аппроксимации функции *f*. Вычисление производится поколоночно за время O(*n*+*m*) для одного элемента.

2. ЛИНЕЙНЫЕ СВОЙСТВА СЛУЧАЙНЫХ ПОДСТАНОВОК

В этом подразделе мы сначала кратко напомним результаты изучения линейных свойств случайных подстановок. Пусть $\pi: Z_{2^n} \to Z_{2^n}$ будет биективным *n*-битным отображением и пусть S_{2^n} будет множеством всех таких отображений. Для *n*-битного вектора $X \in Z_{2^n}$ пусть X_i обозначает *i*-тый бит вектора *X*. В соответствии с [5, 7] ли-

нейная аппроксимационная таблица для подстановки π обозначается LAT_π и является таблицей размера $2^n \times 2^n$ с элементами $LAT_\pi(\alpha,\beta)$, определяемыми соотношением

$$LAT_\pi(\alpha,\beta) \overset{def}{=}$$

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

где $\alpha,\beta \in Z_{2^n}$ и $'\cdot'$ обозначает операцию скалярного произведения. Применяется также и более компактная запись скалярных произведений в рассматриваемых равенствах

$$\alpha \cdot X = \beta \cdot \pi(X).$$

В соответствии с приведенным определением, $LAT_\pi(\alpha,\beta)$ представляет собой число равенств четности между линейной комбинацией входных битов (определяемых маской α по входу в LAT_π подстановки по строкам) и линейной комбинацией выходных битов (определяемых маской β по входу в таблицу LAT_π подстановки по столбцам).

Нам будет нужна теорема, сформулированная в [7] и доказанная в работе [5].

Теорема 1: *Пусть* $\lambda(\alpha,\beta)$ *будет случайным числом, соответствующим значению линейной аппроксимационной таблицы подстановки* $LAT_\pi(\alpha,\beta)$, *когда подстановка* π *выбрана равновероятно из множества* S_{2^n} *и маски* α,β *ненулевые. Тогда* $\lambda(\alpha,\beta)$ *для целых значений* k, $0 \le k \le 2^{n-1}$ принимает *только четные значения и вероятность, что* $\lambda(\alpha,\beta) = 2k$ *определяется выражением*

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

На основании (1) в [5,7] получено выражение для вычисления $E\big[\lambda(\pi,2k)\big]$, которым обозначено ожидаемое число ячеек таблицы LAT_π^*, имеющих значение $2k$, как простое умножение формулы (1) на общее число ячеек таблицы подстановки, исключая первую строку и первый столбец

$$E\big[\lambda(\pi,2k)\big] = \frac{(2^n-1)^2 \cdot \left(2^{n-1}!\right)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ 2^{n-2} + |k| \end{pmatrix}^2, \qquad (2)$$

т.е. для положительных и отрицательных значений смещения k результат будет один и тот же.

Выражение (2) имеет тенденцию быстро стремиться к нулю с ростом k. Среднему значению максимума таблицы LAT_π^* подстановки, как следует из сопоставления результатов вычислений с экспериментальными данными, будет соответствовать значение k^*, при котором получается наименьшее значение $E\big[\lambda(\pi,2k)\big]$, превышающее или равное единице, т.е. для определения k^* необходимо найти округленное в сторону увеличения до ближайшего целого решение уравнения

$$\frac{(2^n-1)^2 \cdot \left(2^{n-1}!\right)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ 2^{n-2} + |k^*| \end{pmatrix}^2 = 1. \qquad (3)$$

Варианты решения уравнения (3) (переборным методом, который существенно упрощается при использовании результатов экспериментов), вместе с данными экспериментов иллюстрирует табл. 2.

Таблица 2

Сравнение расчетных и экспериментальных результатов по оценке максимальных значений ЛАТ случайных подстановок

n	$2k^*$	$E\big[\lambda(\pi,2k)\big]$	Эксперимент
4	4	3,89	5,498
	6	1,118	$\left(\frac{3}{2}\right)^8 = 5{,}06$
6	12	9,013	14,48
	14	1,7	$\left(\frac{3}{2}\right)^6 = 11{,}39$
8	32	2,12	34,68
	34	0,7457	$\left(\frac{3}{2}\right)^8 = 25{,}62$
10	74	1,16	78,8
	76	0,64	$\left(\frac{3}{2}\right)^8 = 57{,}66$
12	162	1,129	116,24
	164	0,82	$\left(\frac{3}{2}\right)^8 = 129{,}74$
14	350	1,069	–
	352	0,900	$\left(\frac{3}{2}\right)^{14} = 291$
16	748	1,027	720
	750	0,93	$\left(\frac{3}{2}\right)^{17} = 657$

Из неё хорошо видно, что найденные значения максимумов таблиц линейных аппроксимаций случайных подстановок хорошо согласуются с данными, полученными экспериментальным путем.

Наша задача теперь убедиться в том, что малые версии шифров, представленных на украинский конкурс, вместе с малой версией шифра Rijndael (Mini-AES) асимптотически (т.е. при полном наборе цикловых преобразований) ведут себя как случайные подстановки.

3. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ ЛИНЕЙНЫХ СВОЙСТВ МАЛЫХ ВЕРСИЙ ШИФРОВ

Первые результаты были получены при использовании общепринятого подхода к вычислению ЛАТ [9]. В этих экспериментах использовал-

ся ограниченный объём обработанных данных. Таблица 3 иллюстрирует первые результаты по изучению линейных свойств малых версий шифров. Здесь представлены результаты для полного набора цикловых преобразований и случайного единственного значения ключа. Заметим, однако, что объём выборки в последнем случае взят существенно меньшим, чем в первом. Приведем также ещё один из примеров изучения зависимости значений максимумов линейных корпусов от числа циклов шифрования для шифра Калина(см. табл. 4). Здесь удалось построить полную таблицу ЛАТ, но тоже только для одного значения случайного ключа. Уже на уровне этих первых экспериментов мы убедились, что наши предположения в отношении асимптотического поведения шифров в зависимости от числа циклов шифрования приходят практически к одному и тому же значению максимума ЛАТ, характерному для случайных подстановок целиком и полностью подтверждаются. Как и при изучении дифференциальных свойств, и в этом случае шифры после нескольких начальных циклов преобразований приходят к установившемуся значению, свойственному случайной подстановке соответствующей степени.

Теперь мы приведем результаты применения для построения ЛАТ изложенного выше быстрого алгоритма, с помощью которого удалось более полно исследовать дифференциальные свойства сразу всех интересующих нас шифров. Они представлены в таблицах 5-7. В процессе выполнения экспериментов в каждом случае были выполнены расчеты для множества из 100 случайно сгенерированных ключей шифрования и выполнено последующее усреднение полученных результатов по этому множеству. В табл. 5 представлены математические ожидания максимальных значений смещений линейных корпусов для всего набора исследуемых шифров в зависимости от числа циклов шифрования *r*. Заметим, что для шифра Мини-Лабиринт первые два цикла пропущены. Так мы учли дополнительные начальное и конечное преобразования, которые в шифре Лабиринт по своей структуре каждое реально представляют собой дополнительные циклы этого шифра.

Как следует из представленных результатов, с большим уровнем доверия подтверждается выдвинутое в качестве гипотезы положение, в соответствии с которым блочные симметричные шифры после определенного небольшого числа начальных циклов шифрования по своим линейным свойствам повторяют показатели случайных подстановок соответствующего порядка. Все шифры (кроме шифра Мухомор) после четырех циклов шифрования приходят к установившемуся значению максимума линейного корпуса, характерному для случайных подстановок соответствующей степени. Отличие от расчетного значения (750) оказывается меньшим 25%.

Еще одна серия экспериментов была проведена для определения абсолютных значений максимумов линейных корпусов. Результаты этих экспериментов обобщены в табл. 6.

По всем шифрам, кроме шифра Мухомор можно сделать вывод, что абсолютные значения максимумов линейных корпусов отличаются от средних значений максимумов линейных корпусов менее чем на 15 %. Это означает, что в качест-

Таблица 3

Линейные свойства шифров Лабиринт и Калина

смещение	0	2	100	200	300	400	500	600	720
Линейный корпус шифра Лабиринт.									
количество	81839	163317	120328	48060	10378	1232	82	1	1
Линейный корпус шифра Калина.									
количество	29282	28825	21332	8522	1879	225	15	1	0

Таблица 4

Зависимость значений максимумов линейных корпусов от числа циклов для шифра baby-Калина

Число циклов	1	2	3	4	5	6	7
Максимальное смещение	8192	3584	832	802	860	886	826

Таблица 5

Математические ожидания максимальных смещений линейных корпусов уменьшенных версий шифра Mini-AES и шифров, представленных на украинский конкурс вместе со значениями среднеквадратических отклонений

Шифр *r*	Mini-AES	Mini-ADE	Мини-Лабиринт	Mini-Kalina	Mini-Muhomor
1	16384	16384	-	9349,15±237,02	11602±5424,45
2	9164,8±120,75	9093,10±94,37	-	3545,8±83,93	8499,2±6122,48
3	3658,2±65,8	3509,8±62,37	1069,8 ±38,41	830,55±83,93	7928,7±6134,3
4	827,24±7,25	828,56±7,58	826,36±6,6	820,14±6,96	7605,4±6180,14
5	821,34±6,16	820,52±5,48	820,8±5,44	823,28±4	7660,65 ±6234,62
6	821,68±7	819,92±5,81	822,88 ±7,25	825,04±6,34	7738,65 ±6215,21

Таблица 6

Абсолютные значения максимумов линейных корпусов мини версий шифров, представленных на украинский конкурс

Шифр *r*	Mini-AES	Mini-ADE	Мини-Лабиринт	Мини-Калина	Мини-Мухомор
1	16384	16384	-	12288	12288
2	10240	12288	-	4480	9728
3	4352	4352	1444	936	8396
4	940	932	914	912	8450
5	900	896	902	900	8667
6	922	880	906	912	8696

ве максимальных значений смещений при оценке стойкости шифра можно использовать значение этого показателя, свойственное случайной подстановке 16-ой степени. Для шифра Мини-Мухомор обнаружены максимальные смещения, выходящие за рамки, свойственные другим шифрам. Напомним, что в работе [10], посвященной описанию разработанной уменьшенной модели этого шифра, отмечалось, что не все операции шифра поддаются масштабированию, и при построении уменьшенной модели операция SL преобразования (в большой версии четыре байтовых S-блока с последующим МДР линейным преобразованием) была заменена полубайтовой подстановкой. Может здесь дело и не в этом, а в самой конструкции преобразования. В общем, здесь требуется дополнительная проверка этого результата на большом шифре. Мы сейчас этим занимаемся.

ЗАКЛЮЧЕНИЕ

Здесь мы можем повторить вывод, сделанный в нашей предыдущей работе [1] по отношению к дифференциальным показателям уменьшенных моделей шифров, перенеся теперь его на линейные показатели: если согласиться с правомерностью переноса свойств уменьшенных моделей шифров на их прототипы, то представленные результаты свидетельствуют, что линейные свойства представленных на украинский конкурс шифров Калина, ADE, Мухомор и Лабиринт после 4-5 циклов шифрования повторяют с большой точностью свойства случайных подстановок. Можно сделать общий вывод о том, что современные БСШ (при полном наборе цикловых преобразований) действительно являются случайными подстановками.

Представленными результатами исследований подтверждено ещё раз, что свойства шифрующих преобразований современных блочных симметричных шифров (Rijndael-я и других шифров, представленных на украинский конкурс), являются одним из проявлений свойств случайных подстановок, и в этом смысле шифр Rijendael и шифры, представленные на Украинский конкурс, являются эквивалентными (близкими по стойкости). Все они реализуют в соответствии с приведенным в работе утверждением и расчетным соотношением из работы [3] наибольшую вероятность максимума линейного корпуса (для 128 битных версий) близкую к 2^{-104}. Этот результат следует считать обоснованным и теоретически и практически.

Литература

[1] *Долгов В.И.* Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс. / Долгов В.И., Кузнецов А.А., Исаев С.А. // Представлена к опубликованию в журнале “Электронное моделирование”, Киев, 2011.

[2] *Долгов В.И.* Подход к криптоанализу современных шифров // Материалы второй международной конференции “Современные информационные системы/ Долгов В.И., Лисицкая И.В., Олейников Р.В. Проблемы и тенденции развития”, Харьков-Туапсе, Украина, 2–5 октября. – 2007. – С. 435-436.

[3] *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. 312–320.

[4] *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.

[5] *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.

[6] *O’Connor L.J.* On the Distribution of Characteristics in Bijective Mappings. Advances in Cryptology / L. J. O’Connor // EUROCRIPT 93, Lecture Notes in Computer Science, T. Helleseth ed., Springer-Verlag. – 1994. – vol. 795. – P. 360–370.

[7] *Luke O’Connor.* Properties of Linear Approximation Tables. Email: oconnor@dsts. Edu. au, 1995.

[8] *Krzysztof Chmiel.* On Differential and Linear Approximation of S-box Functions / Biometrics, Computer Security Systems and Artificial Intelligence Applications. / Edited by Khalid Saeed, Jerzy Pejas and Romuald Mosdorf. // Poland, Springer – 2006. – P. 111-120.

[9] *Долгов В.И., Олейников Р.В., Большаков А.Ю., Григорьев А.В., Дробатько Е.В.* Криптографичекие свойства уменьшенной версии шифра “Калина” // Прикладная радиоэлектроника – 2010. – Т.9. – № 3. – С. 349–354.

[10] *Лисицкая И.В.* Криптографические свойства уменьшенной версии шифра “Мухомор”. / Лисицкая И.В., Олешко О.И., Руденко С.Н., Дроботько Е. В, Григорьев А. В. // Збірник наукових праць. – Київ, 2010. С. 31-42.

Поступила в редколлегию 10.05.2011

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

Кузнецов Александр Александрович, доктор технических наук, профессор, профессор кафедры БИТ ХНУРЭ. Область научных интересов: криптография, теория обработки и передачи данных, стеганографические методы защиты информации.

Исаев Сергей Александрович, аспирант Харьковского национального университета им. В.Н. Каразина. Область научных интересов: математические методы защиты информации.

УДК 681.3.06

Лінійні властивості блочних симетричних шифрів, представлених на український конкурс / І.В. Лисицька, О.О. Кузнєцов, С.А. Ісаєв // Прикладна радіоелектроніка: наук.-техн. журнал. – 2011. Том 10. № 2. – С. 135–140.

Розвивається новий підхід в теорії та методах криптоаналізу, запропонований на кафедрі БІТ ХНУРЕ, заснований на використанні при визначенні очікуваних показників стійкості великих шифрів результатів аналізу їх зменшених моделей. Викладається швидкий алгоритм підрахунку ЛАТ і нові результати з вивчення лінійних властивостей зменшених моделей шифрів, представлених на український конкурс, разом з малою версією шифру Rijndael. Результати аналізу зменшених моделей зв'язуються з очікуваними показниками стійкості прототипів.

Ключові слова: блочний симетричний шифр, зменшена модель, значення максимуму лінійного корпусу, доказова стійкість

Табл. 6. Іл. немає. Бібліогр.: 10 найм.

UDC 681.3.06

Linear properties of symmetric block cipher submitted to the Ukrainian contest / I.V.Lisitskaya, E.A. Kuznetsov, S.A. Isaev // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 135–140.

The paper develops a new approach in theory and cryptoanalysis methods suggested at the KNURE Department of Security of Information Technologies and based upon using the results of analyzing the reduced models of big ciphers in determining the expected indeces of the strength of the said ciphers. A fast algorithm of calculating linear approximation table and new results of studying the linear properties of reduced models of ciphers are presented which are submitted to the Ukrainian contest, together with the cipher Rijndael reduced version. Results of analyzing the reduced models are associated with the expected indeces of the strength of prototypes.

Keywords: symmetric block cipher, reduced model, value of maximum linear body, demonstrable strength.

Tab. 6. Fig. no. Ref.: 10 items.