УДК 681.3.06

32-Х БИТНАЯ МИНИ-ВЕРСИЯ БЛОЧНОГО СИММЕТРИЧНОГО АЛГОРИТМА КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ "МУХОМОР". ОЦЕНКА МАКИМАЛЬНОГО ЗНАЧЕНИЯ ПОЛНОГО ДИФФЕРЕНЦИАЛА ШИФРА

И. В. ЛИСИЦКАЯ
И. А. СТАВИЦКИЙ

Харьковский национальный университет радиоэлектроники

e-mail: dolgovvi@mail. ru

Предлагается описание уменьшенной 32-битной версии шифра Мухомор, предложенного на конкурс по выбору национального стандарта Украины. Приводятся результаты оценки максимальных значений дифференциалов, полученных для одной строки дифференциальной таблицы этой уменьшенной версии при различном числе циклов шифрования, которые сравниваются со свойствами случайной подстановки соответствующей степени.

Ключевые слова: шифр Мухомор, малая версия шифра, полный дифференциал, случайная подстановка.

Введение

В этой работе мы продолжаем пропагандировать новый подход в теории и методах криптоанализа, развиваемый на кафедре БИТ ХНУРЭ [1]. Он ориентирован, с одной стороны, на использование при определении ожидаемых показателей стойкости больших шифров результатов анализа уменьшенных их версий, а с другой, – уточнённой в последнее время на основе изучения свойств и показателей случайных подстановок и уменьшенных моделей шифров, рассматриваемых как подстановочные преобразования, концепции (новой идеологии) определения показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа [2]. Шифр "Мухомор" стал последним в серии наших разработок уменьшенных моделей шифров, представленных на украинский конкурс [3]. Мы уже традиционно в первой части работы приводим описание уменьшенной модели этого шифра, а во второй части представляем результаты исследования её дифференциальных свойств.

1. Описание шифра мини Мухомор-32.

В предыдущей работе [4] при построении уменьшенной 16-битной модели шифра Мухомор пришлось столкнуться с ситуацией, когда шифр содержит преобразование, не допускающее прямого масштабирования. К такой операции относится *SL*-преобразование. Она включает слой нелинейных преобразований, реализуемый с помощью 4-х байтовых S-блоков, и последующее МДР преобразование, осуществляющее матричное умножение байтовых выходов 4-х S-блоков (над полем $GF(2^8)$) на квадратную матрицу, размера 4×4 (по существу аналогичное преобразование выполняется в шифре Rijndael с помощью операции MixColumns, только там при умножении используется другой полином). При масштабировании этой операции к 16-ти битной модели она получается 4-х битной (в оригинале она 32-битная). В результате было принято решение заменить эту операцию подстановочной, в каком-то смысле эквивалентной по эффективности. Поскольку в этой работе мы в дальнейшем будем обсуждать дифференциальные показатели уменьшенной модели шифра, то была выполнена оценка дифференциальных свойств (закон распределения переходов таблицы XOR разностей) *SL*-преобразования в виде 16-битной версии, повторяющей оригинальную. В нашем эксперименте для построения *SL*-преобразования были использованы четыре S-блока уменьшенной версии шифра Baby-Rijndael [5]. Результаты вычислительного эксперимента привели к выводу, что для полубайтовых S-блоков выбрать соответствующий разумно обоснованный эквивалент не удаётся (слишком мало степеней свободы в выборе подстановки 16-го порядка). Поэтому было принято решение в качестве

SL-преобразования в малой версии шифра использовать просто полубайтовый S-блок случайного типа, обладающий, как показал анализ, далеко не худшими свойствами. В итоге вопрос о полной адекватности уменьшенной модели прототипу остался открытым (мы улучшили свойства *SL*-преобразования), т.е. мы можем ориентироваться на показатели уменьшенной модели как на границу сверху.

В этой работе мы рассматриваем уже 32-битную уменьшенную модель шифра Мухомор. Здесь вместо функций усложнения М-8 с восьми битными входами уже рассматриваются функции усложнения с шестнадцатибитными входами (М-16) и SL преобразование удается воспроизвести точнее: использовать два полубайтовых S-блока с последующим МДР преобразованием их выходов.

В результате алгоритм шифрования мини-Мухомор-32 практически является результатом более точного масштабирования оригинальной версии к размеру входного блока и ключа равному 32-ум битам. Как и в большом шифре, каждый 32-битный блок входных данных обрабатывается независимо от остальных. В процессе расшифрования используется тот же ключ что и при шифровании. Шифртекст составляется из шифрованных блоков, последовательность которых соответствует очередности блоков открытого текста.

1.1. Процедура зашифрования

Алгоритм шифрования мини-Мухомор поддерживает длину блока 32 бита с использованием ключа шифрования длиной 32 бита. Количество циклов (N_r) – может меняться.

На вход процедуры подается блок открытого текста и масив подключей шифрования (рис. 1). В начале процедуры зашифрования выполняется рандомизация (забеливание) блока открытого текста, после чего полученный блок данных заданное количество раз (N_r) обрабатывается цикловой функцией, т.е. выполняются цикловые преобразования, а в конце выполняется заключительная рандомизация. Полученный в результате зашифрования блок данных является блоком зашифрованных данных (блоком шифртекста).

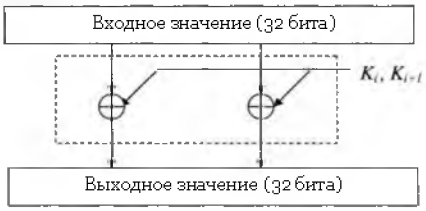

Рис. 1. Процедура рандомизации в шифре мини-Мухомор

1.1.1. Рандомизация. Перед зашифрованием над открытым текстом выполняется операция рандомизации с применением двух подключей шифрования. Эта же операция выполняется после применения всех циклов шифрования, для выполнения финальной рандомизации. Схема рандомизации (начальной и финальной) приведенная на рис. 1.

При выполнении рандомизации блок открытого текста или блок, обработанный цикловой функцией, складывается по модулю 2 с соответствующими подключами.

1.1.2. Цикловое преобразование. Схема циклового преобразования приведена на рис. 2. На вход циклового преобразования шифра мини-Мухомор (рис. 2) подается блок данных, который совпадает по размеру с открытым текстом (32 бита). Входной блок разбивается на 4 равных подблока (по байту каждый), XOR разность (сумма) которых подается на вход функции усложнения М-16 (первый байт складывается со вторым, а третий байт складывается с четвертым). Выходные значения функции усложнения складывается по модулю 2 с входными значениями, после чего первый и третий подблоки подвергаются операции ортоморфного преобразование (О).

Конкатенация подблоков (байтов), прошедших указанные преобразования формируют 32-битный выходной блок данных (выходное значение). В процессе зашифрования выполняется N_r идентичных циклов.

1.1.3. Функция усложнения M-16. Функция усложнения M-16. При размере блока открытого текста 32 бита функция усложнения M-16 принимает очередной 16-и битный подключ K_i, и 2 8-битных значения. Первое из которых вычисляется как разность по модулю.

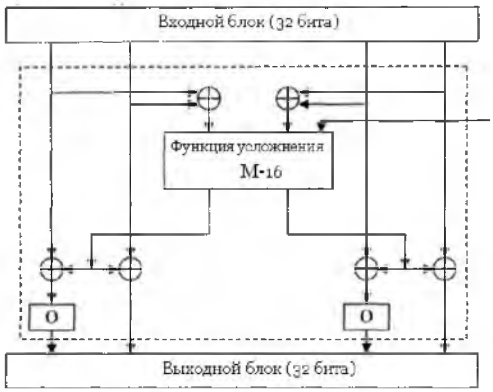

Рис. 2 Цикловое преобразование алгоритма мини-Мухомор

2 между первым и вторым подблоком данных на входе цикла, соответственно второе входное значение – разность по модулю 2 между третьим и четвертым подблоком на входе цикла (см. рис. 2). Схема преобразования M-16 приведена на рис. 3.

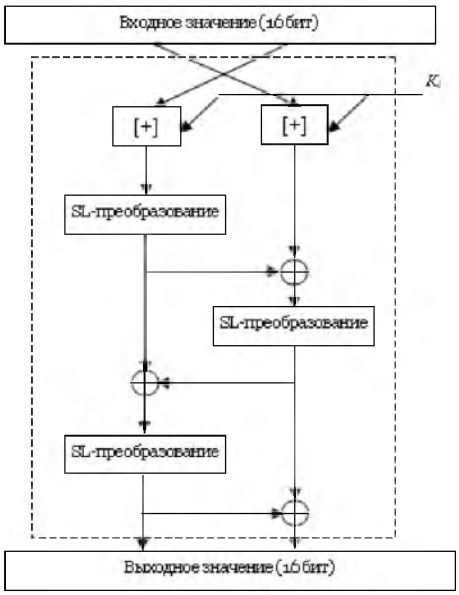

Рис. 3. Функция усложнения M-16

Каждое из 8-битных входных значений функции M-16 складывается по модулю 2^8 с соответствующей половиной следующего подключа, которая подается на вход функции. Потом левая сумма подается на вход первого SL-преобразования, выход которого складывается с правой суммой по модулю 2, и полученный результат подается на второе SL-преобразование. Полученное 8-битное значение складывается по модулю 2 с выходом первого SL-преобразования, результат суммирования поступает на вход 3-го SL-преобразование, выход которого образует левую половину исходного

значения функции усложнения. Правая половина функции М-16 формируется как результат сложения по модулю 2 выходов 2-го и 3-го SL-преобразований.

1.1.3.1. SL-преобразование. Основным в функции усложнения шифра Мухомор является SL-преобразование. В 32-х битной версии шифра SL-функция осуществляет преобразование 8-битных блоков данных. При этом входное 8-битное значение делится на 2 полубайта, и каждый полубайт заменяется в соответствии с заданной таблицей подстановки на новый. В преобразовании используется 2 таблицы подстановки, по одной для каждого полубайта. После замены два полубайта выхода (a_0,a_1) подаются на вход МДР преобразования, которое выполняет матричное умножение следующего вида:

$$\begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} 02 & 03 \\ 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} 02 \cdot a_0 \oplus 03 \cdot a_1 \\ 01 \cdot a_0 \oplus 02 \cdot a_1 \end{bmatrix}$$

Умножение выполняется с использованием неприводимого полинома четвертой степени $x^4 + x + 1$. Выходной 8-битный вектор МДР преобразования (b_0,b_1) является выходным значением SL-преобразования.

Полученная в результате выполнения указанных операций схема SL-преобразования приведена на рис. 4.

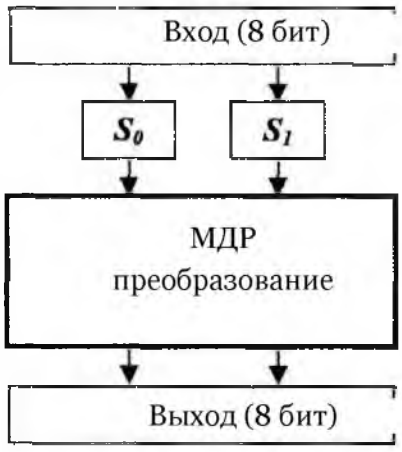

Рис. 4. SL-преобразование

S-блоки, использованные при реализации данной версии шифра, приведены в таблице 1.

Таблица 1

S-блоки, использованные при реализации данной версии

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
S_2	10	4	3	11	8	14	2	12	5	7	6	15	0	1	9	13

1.1.3.2. Ортоморфное преобразование. Ортоморфное преобразование (ОП) выполняется на выходе циклового преобразования для обработки первого и третьего подблоков. Схема ОП приведена на рис. 5. 8-битний блок, который подается на вход ОП, разбивается на две половины, из которых правая на выходе становится левой, а левая на выходе формируется как сумма по модулю 2 левой и правой половин на входе.

1.2. Процедура расшифрования

Процедура расшифрования является обратной к процедуре зашифрования. На вход процедуры подается шифртекст и подключи шифрования. В начале расшифро-

вания выполняется снятие финальной рандомизации шифртекста, после чего полученный блок

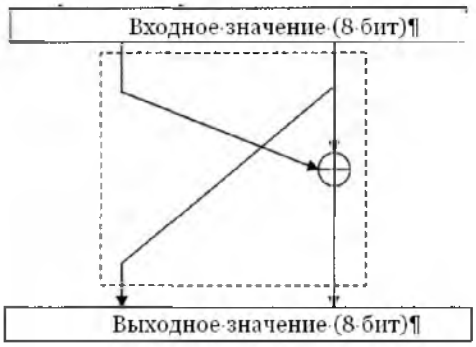

Рис. 5. Ортоморфное преобразование (ОП)

данных соответствующее число раз обрабатывается цикловой функцией, затем выполняется снятие исходной рандомизации открытого текста. Полученный в результате блок данных является открытым текстом.

Схема циклового преобразования при расшифровании показана на рис. 6.

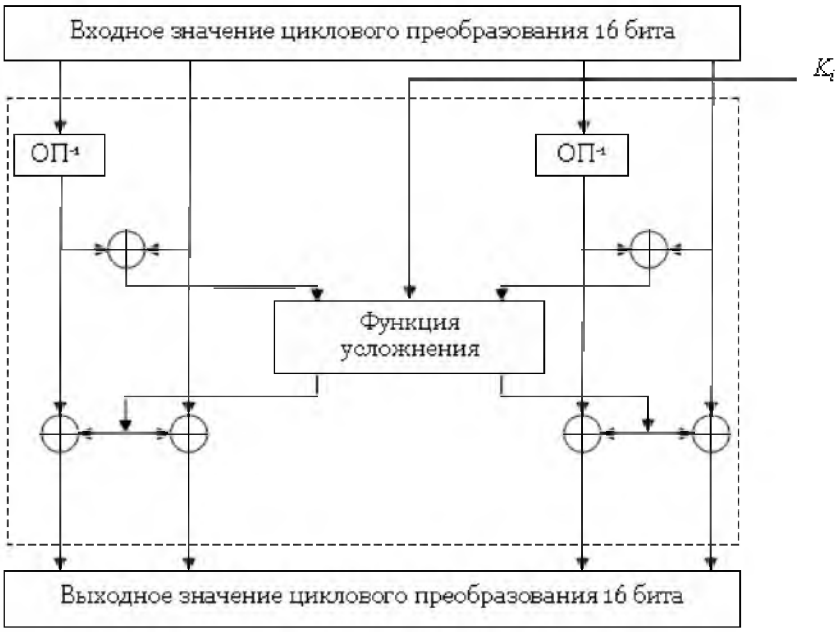

Рис 6. Схема циклового преобразования при расшифровании

Расшифрование совпадает с зашифрованием за исключением следующих деталей:

- подключи (в т.ч. начальной и финальной рандомизации) подаются в обратном порядке;
- вместо операции ортогонального преобразования используется обратная к ней операция ОП$^{-1}$;
- немного изменяется вид циклового преобразования, а именно обратное ортоморфное преобразование выполняется над 1-ым и 3-им блоками перед вычислением разностей соседних блоков и подачей их на функцию усложнения М-8.

1.3. Схема разворачивания ключей.

Для получения цикловых подключей из исходного мастера-ключа используется процедура разворачивания ключей. Для шифрования алгоритма необходимо N_r + 4 подключей, каждый длиной $N_b/2$ бита (N_b – длина блока).

Первые два подключа используются для рандомизации блока открытого текста, последние два подключа применяются для финальной рандомизации.

Процедура формирования подключей использует компоненты функции усложнения для преобразования мастера-ключа и ключевых констант в два и больше подключей шифрования.

Схема разворачивания подключей для длины блока 32 бита и размера ключа 32 бита приведена на рис.8. Очередная ключевая константа C_i (ее левая и правая половины, соответственно) подается на вход функций усложнения М-16, где в качестве подключа используется мастер-ключ (правая половина для правой функции М-16, левая половина ключа для левой функции, рис. 7).

Выходы функций усложнения объединяются в одну строку 8-х битных значений l_0, l_1, r_0, r_1, которые переставляются в следующем порядке: l_0, r_0, l_1, r_1. Результат перестановки снова подается на входы функций усложнения, где в качестве подключа применяется инверсия мастера-ключа (правая половина для правой функции М-16, левая половина ключа для левой функции).

Полученные на выходе значения снова объединяется в одну строку, из младшего байта которой выбираются 4 младших бита, служащие для определения величины байтового циклического сдвига влево этой же строки. Результат сдвига складывается по модулю 2 с мастер-ключом, и полученное значение делится на 2 части, которые образуют подключи K_{2i} и K_{2i+1}.

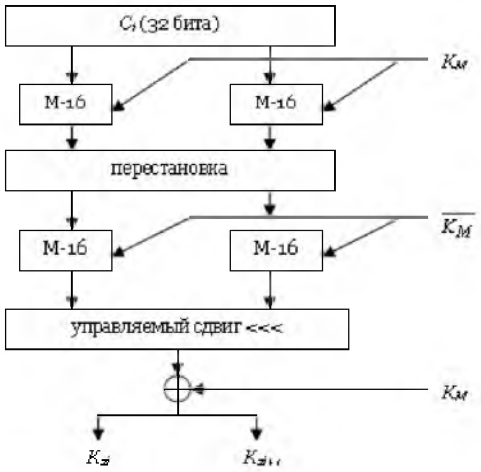

Рис. 7. Схема разворачивания подключей для блока длиной 32 бита и 32-битного ключа

В случае выполнения вычислительного эксперимента с применением меньшего числа циклов шифрования используются подключи, сформированные для 4-х или 8-ми циклов зашифрования.

2. Исследование дифференциальных свойств шифра Мухомор-32

В этом разделе мы выполним оценку максимальных значений полных дифференциалов для шифра мини-Мухомор. В общепринятых обозначениях [7] максимальная дифференциальная вероятность подстановочного преобразования есть

$$DP^f_{\max} = \max_{\Delta x \neq 0,\, \Delta y} DP^f(\Delta x \to \Delta y),$$

где f обозначает функцию преобразования входной разности Δx в выходную разность Δy. Напомним, утверждение из работы [8], определяющее значение $DP^f_{\max}$ для многоциклового шифрующего преобразования.

Утверждение. Для шифрующих преобразований, определяемых многоцикловыми процедурами перестановочно-подстановочных биективных m-битных отобра-

жений, свойственных современным блочным симметричным шифрам, ожидаемая вероятность самой правдоподобной ненулевой дифференциальной характеристики ограничена сверху значением $\frac{m+4}{2^m}$.

Заметим здесь, что в этом утверждении речь идет о полноцикловых БСШ. На самом же деле значение $\frac{m+4}{2^m}$ является асимптотическим в том смысле, что оно устанавливается не сразу, а постепенно по мере увеличения числа цикловых преобразований.

Для 32-х битного шифра значения максимального числа переходов дифференциальной таблицы в соответствии с приведенной формулой равно $m+4 = 36$. Но построение полной таблицы, содержащей $2^{32} \times 2^{32}$ ячеек, нам, конечно, не удастся. Мы далее будем решать задачу вычисления значений числа переходов для отдельной строки дифференциальной таблицы. Теория в этом случае утверждает, что случайная подстановка степени 2^{32} будет иметь построчное распределение переходов таблицы дифференциальной разности совпадающее с распределением переходов полной таблицы дифференциальной разности для случайной подстановки степени 2^{16} [9], т.е. ожидаемое максимальное значение в строке будет ограничено числом 16 + 4 = 20.

Мы сейчас это продемонстрируем на нашей уменьшенной модели. В таблице 2 представлены результаты вычислительного эксперимента по изучению дифференциальных свойств нашей уменьшенной модели шифра Мухомор.

Таблица 2

Поцикловые распределения переходов отдельной строки для дифференциальных таблиц шифра Мухомор-32

Число переходов	Число циклов преобразования			
	2	3	4	5
	Число ячеек таблицы	Число ячеек таблицы	Число ячеек таблицы	Число ячеек таблицы
0	4133321923	2609258697	2605051578	2605031125
2	...	1296391578	1302482284	1302504377
4	16933554	325911215	325628935	325640469
6	3977878	55359859	54279489	54269946
8	42817011	7183143	6785855	6783415
10	798118	770940	678007	677477
12	4815517	75848	56754	56235
14	297646	9085	4125	3988
16	39683069	2943	252	252
18	137153	1009	16	12
20	1389668	646	1	
22	58254	417		
24	8828856	409		
26	34807	180		
...	...	...		
384	146167	2		
...	...			
39936	1			
53568	1			

Как видно из приведенных данных для перехода к асимптотическому (установившемуся) "режиму" для шифра Мухомор оказывается достаточным пяти циклов зашифрования (для шифра baby-Rijndael (baby-AES) достаточно 4-х циклов [9]). Это означает, что шифр Мухомор обладает дифференциальными показателями близкими к показателям малых версий шифра Rijndael и других шифров представленных на украинский конкурс [10,11,12].

Распределение переходов дифференциальной таблицы Мухомор-32 (для ненулевого ключа 240) мы представляем отдельной таблицей 3, так как они не укладываются в общую таблицу 2.

Таблица 3

Распределение переходов дифференциальной таблицы для первого цикла шифра Мухомор-32

Число переходов	Число ячеек таблицы	Число переходов	Число ячеек таблицы
0	4294958702	1966080	2
131072	1477	2097152	164
262144	3160	2228224	7
393216	223	2359296	3
524288	2153	2490368	1
655360	85	2621440	5
786432	250	2752512	1
917504	13	3145728	32
1048576	778	3276800	1
1179648	30	3407872	1
1310720	41	4194304	23
1441792	8	4456448	2
1572864	104	6291456	8
1703936	6	8388608	2
1835008	13	9437184	1

В последнем эксперименте мы построили распределение переходов для одной строки XOR таблицы шифра Мухомор-32 для 14 циклов шифрования.

Количество перебранных пар плайнтекстов в этом случае – 2^{32}. Соответствующие результаты иллюстрирует таблица 4

Таблица 4

Распределение переходов одной строки XOR таблицы шифра Мухомор-32 для 14 циклов шифрования (Среднее значение по 30 ключам)

Расчет		Эксперимент	
#0.	2604969722	#0.	2605041525
#2.	1302484861	#2.	1302509971
#4.	325626184	#4.	325632021,3
#6.	54271858	#6.	54270265,87
#8.	6784085	#8.	6784203,5
#10.	678418	#10.	678442,9333
#12	56535	#12.	56540,3333
#14.	4038	#14.	4055,4
#16.	252	#16.	254,93333
#18.	14	#18.	14,5
#20.	1	#20.	0,8
#22.	0	#22.	0,033333333

В левой колонке табл. 4 представлены результаты полученные расчетным путём из соответствующей формулы для случайной подстановки степени 2^{32}. Хорошее совпадение теоретических и экспериментальны данных видно и без привлечения методов оценки близости распределений.

Заключение

Если согласиться с правомерностью переноса свойств уменьшенных моделей шифров на их прототипы, то представленные результаты свидетельствуют, что дифференциальные свойства шифра Мухомор близки (повторяют) к свойствам шифрующих преобразований современных блочных симметричных шифров (Rijndael и другим шифра представленным на украинский конкурс) Они являются одним из проявлений свойств случайных подстановок, и в этом смысле шифр Rijendael и шифры, представленные на Украинский конкурс, являются эквивалентными (неразличимыми). Все они реализуют в соответствии с приведенным в работе утверждением наибольшую вероятность максимума полного дифференциала (для 128 битных версий) близкую к 2^{-120}.

Литература

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

2. 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.

3. Горбенко І.Д. Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація / 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. // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. Том. 6, №2, С. 147-157.

4. P. Junod. FOX specifications version 1.1. / P. Junod and S. Vaudenay // Technical Report EPFL/IC/2004/75, Ecole Polytechnique F´ed´erale, Lausanne, Switzerland, 2004.

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

6. Олейников Р.В. Дифференциальные свойства случайных подстановок / Олейников Р.В., Олешко О.И., Лисицкий К.Е., Тевяшев Ф.Д. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 326–333.

7. F. Sano, K. Ohkuma, H. Chimisu, and S. Rawamura. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis, IEISE Trans. Fundamentals, VOL. E86-A, No.1, pp. 37–46, Janiary 2003.

8. 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.

9. 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.

10. Олешко О.И. Криптографичекие свойства уменьшенной версии шифра "Калина" / Олешко О.И., Большаков А.Ю., Григорьев А.В., Дроботько Е.В.// Научно-техническая конференция с международным участием «Компьютерное моделирование в наукоемких технологиях» (КМНТ-2010), Харьков, университет им. Каразина.

11. 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.

12. Долгов В.И. Дифферециальные свойства блочных симметричных шифров, представленных на украинский конкурс. / Долгов В.И., Кузнецов А.А., Исаев С.А. // Электронное моделирование – 2011 (в печати).

32-BIT MINI-VERSION OF THE BLOCK SYMMETRIC ALGORITHM OF CRYPTOGRAPHIC DATA TRANSFORMATION "MUCHOMOR". EVALUATION OF THE MAXIMUM FULL DIFFERENTIAL FOR THIS CIPHER

I. V. LYSYTSKAYA
I. A. STAVITSKIY

Kharkov National University of Radio Electronics

e-mail: dolgovvi@mail.ru

We propose the describing of reduced 32-bit Muchomor cipher which was proposed to tender for the selection of the National Ukrainian Standard. In this article were shown the results of evaluation of the maximum values of the differentials which were obtained for a single line of differential table for this smaller version with a different number of encryption rounds. These results were compared with the properties of a random permutation for the appropriate degree.

Key words: Muchomor cipher, smaller version of the cipher, full differential, random permutation.