УДК 621. 3.06

НОВЫЙ ВЗГЛЯД НА ШИФР МУХОМОР

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

Выполняется уточнение динамических показателей прихода шифра Мухомор к состоянию случайной подстановки. Показывается, что шифр Мухомор приходит к состоянию случайной подстановки уже на первом цикле, чего не позволяют все современные шифры. Делается вывод, что шифр Мухомор является на сегодняшний день самым прогрессивным решением по построению блочных симметричных шифров.

Ключевые слова: динамические показатели шифра, случайная подстановка, цикловое преобразование.

ВВЕДЕНИЕ

Мы здесь снова хотим возвратиться к обсуждению конструкторских решений, использованных при построении шифра Мухомор [1], представленного в своё время на украинский конкурс. В свете дальнейшего развития теории и практики построения современных шифров, последних работ по изучению динамических свойств шифров и анализа их цикловых преобразований [2, 3 и др.], появились новые результаты и взгляды, которые позволяют по иному взглянуть на показатели стойкости уже принятых решений, уточнить ранее выполненные оценки и показатели. Это в полной мере относится и к серии шифров Мухомор, хотя и ранее выполненные оценки [1, 4] уже выдвинули его в число лидеров современных методов построения блочных симметричных шифров.

В этой работе мы ещё раз обращаемся к решениям, принятым при построении шифров Мухомор, т. к. сегодня уже стало очевидным, что оценки, выполненные в предыдущих работах [2,3,5], существенно занижены и не раскрывают полностью перспективность использованных при построении этих шифров решений.

1. ДИНАМИЧЕСКИЕ ПОКАЗАТЕЛИ ПРИХОДА ШИФРОВ МУХОМОР К СОСТОЯНИЮ СЛУЧАЙНОЙ ПОДСТАНОВКИ

Дело в том, что при дополнительном анализе преобразований М-64, М-128 и М-256, удалось выявить повышенный запас стойкости шифров серии «Мухомор», который заключался в том, что конструкции цикловых функций этих шифров обеспечивают активизацию большего числа S-блоков, чем мы считали ранее.

Напомним здесь конструкцию цикловой функции М-128. Она представлена на рис. 1.

В соответствии с описанием шифра [1], входные 64-битовые значения функции М-128 меняются местами, затем полученный вектор делится на 4 части по 32 бита каждая. Эти значения складываются по модулю 2^{32} с соответствующей частью очередного подключа, поданного на вход функции. Затем каждое полученное 32-битового слово проходит через SL преобразование, причём результат преобразования складывается по модулю 2 со всеми остальными словами (см. рис. 1). Описанная операция выполнения SL преобразований над четырьмя 32-битовыми блоками выполняется 2 раза. Левое выходное 64-битовое слово формируется как результат конкатенации двух левых 32-битовых слов, правое 64-битовое слово – как результат конкатенации двух правых 32-битовых слов.

Сегодня мы считаем, что в представленных ранее результатах [2, 3] имеются, по крайней мере, две неточности.

1. Обратим здесь внимание на цепочку сложений по модулю 2 выхода самого правого SL преобразования первой и второй линейки SL преобразований цикловой функции со всеми выходами SL преобразований соответствующей линейки (см. рис. 1). Мы пришли к выводу, что эта цепь сложений по модулю два создаёт дополнительные активные S-блоки в каждой из колонок 32-битных слов (SL преобразований), число которых равно количеству активизированных S-блоков последнего в первой и второй линейкаах SL преобразования.

Мы это свойство сформулировали в виде утверждения:

Утверждение. *При сложении по модулю два разностей выходов двух S-блоков результирующая вероятность прохода разностей для двух S-блоков равна произведению вероятностей прохода разностей для каждого из них.*

В соответствии с этим положением динамические показатели прихода цикловой функции к случайной подстановки должны быть улучшены.

Этот момент мы уже учли в нашей работе [5].

Для иллюстрации развиваемого положения мы приведём здесь выдержку из этой работы.

«**Функции усложнения М-128 шифра Мухомор-256** (вход в шифр 256 битов) состоит из восьми SL преобразований. Даже если считать, что на первом цикле задействованными являются минимум 29 S-блоков (точнее 33), формирующими все выходные байты цикла активными, то функция усложнения будет выходить к показателям случайной подстановки для 128-битного входа за один цикл и с показателями δ-равномерности равным 8-ми, 10-ти, 12-ти

и 16-ти (при δ = 16 минимально необходимое число S-блоков есть 30). Эту функцию усложнения также можно применить для построения итеративного128-битного шифра без надстройки Лея-Месси. Такой шифр будет обладать предельными динамическими характеристиками ($r_{min} = 1$)».

Для самого же шифра Мухомор-256 уравнение зашифрования имеет вид ($(2^{-5})^k = 2^{-248}$) и, следовательно, $k_{min} = 49{,}6$. Для этого шифра $r_{min} = 2$. Действительно в представленном здесь результате считается, что первая линейка SL преобразований цикловой функции даёт один активный S-блок (входная разность в цикловую функцию первого цикла – это разность на входе одного из S-блоков последнего SL преобразования первой линейки). Во второй линейке возможен ещё один активный S-блок (МДР преобразование с вероятностью 2^{-59} даёт на выходе один активный байт), остальные МДР преобразования практически все будут да-

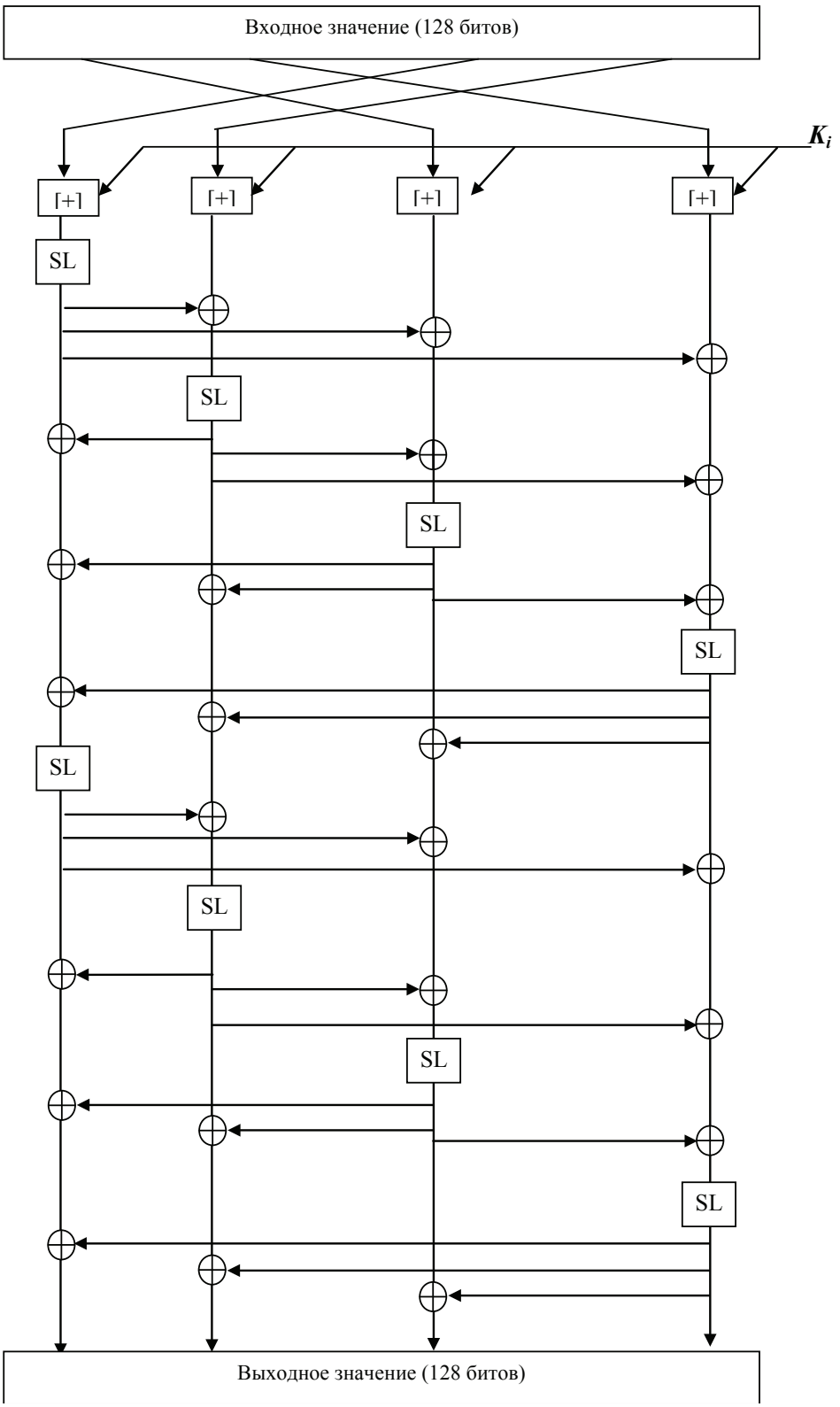

Рис. 1. Функция усложнения М-128

вать четыре активных S-блока. Тогда общее число активных S-блоков циклового преобразования получается на самом деле равным (близким к) $1 \times 4 + 1 + 7 \times 4 = 33$ вместо 29 (в предыдущем результате не учитываются суммирования на входах второй линейки SL преобразований с одноблочным выходом последнего SL преобразования первой линейки). Это действительно означает, что функция усложнения M-128 приходит к случайной подстановке за один цикл! (и по дифференциальным и по линейным показателям).

Но это ещё не всё!

2. Нам представляется, что надстройка шифра Мухомор в виде схемы Лея-Мэсси играет более важную роль в его конструкции, чем мы полагали ранее. Главная её цель, теперь мы считаем, это удвоить число активных S-блоков циклового преобразования шифра (длина блока данных при входе в цикловую функцию после прохода схемы усложнения удваивается). И тогда нужно считать, что в рассмотренном примере минимальное число активизированных S-блоков циклового преобразования шифра Мухомор-256, если исходить из ранее полученных 33-х активных S-блоков функции усложнения, получается равным 66-ти. Это значит, что сам шифр Мухомор-256 с родными S-блокам приходит к случайной подстановке уже на первом цикле. Адекватные выводы можно сделать и по отношению к другим конструкциям шифров серии Мухомор. Приведём далее расчёт динамических свойств шифра, построенного с использованием в качестве циклового преобразования функции усложнения M-256.

2. ПОКАЗАТЕЛИ СЛУЧАЙНОСТИ ШИФРА, ИСПОЛЬЗУЮЩЕГО В КАЧЕСТВЕ ЦИКЛОВОЙ ФУНКЦИИ ПРЕОБРАЗОВАНИЕ M-256

Выше уже было отмечено, что функции усложнения сами (без надстройки Лея-Мэсси) могут быть использованы для построения шифров. В этом параграфе мы приведём результаты оценки ожидаемых параметров перехода шифра, использующего в качестве цикловой функции преобразование M-256, к состоянию случайной подстановки.

В соответствии с идеей развиваемого в [2] подхода необходимо выполнить оценку минимального числа активных (задействованных S-блоков), после прохождения которых шифр становится случайной подстановкой. Это минимальное число определяется дифференциальными и линейными показателями самих S-блоков, применяемых в шифре, конструкциями и свойствами его цикловых преобразований, а также значениями показателей доказуемой стойкости шифра, зависящими от размера его битового входа. В работе [2] эта связь между отмеченными показателями определена в виде двух соотношений:

$$IPS_D = (DP^{\pi}_{\max})^k,\ IPS_L = 2^{k-1} \cdot \left(LP^{\pi}_{\max}\right)^k.$$

Здесь $DP^{\pi}_{\max}$ и $LP^{\pi}_{\max}$ – максимальные значения дифференциальной и линейной вероятностей подстановочных преобразований $\pi(x)$. IPS_D (Differential Indicator of Provable Security) – дифференциальный показатель доказуемой безопасности и IPS_L (Linear Indicator of Provable Security) – линейный показатель доказуемой безопасности, $k = k_{\min}$ – минимальное число активных S-блоков, участвующих в формировании перехода шифра к случайной подстановке.

Пользуясь расчётными соотношениями, установленными в работе [8], можно прийти к выводу, что ожидаемое значение максимума дифференциального перехода для шифра с 256-битным входом оказывается близким к 190, а ожидаемое значение максимума смещения линейного корпуса для шифра с 256-битным входом оказывается близким к 2^{130}. Соответственно получим, что максимальные значения линейной и дифференциальной вероятности для шифра с 256-битным входом получаются близкими друг к другу и равными приблизительно $2^{-248} \div 2^{-250}$ (близкими к сложности атаки полного перебора ключей).

Исходя из приведенных выше соотношений можно сделать вывод, что для шифра с 256-битным входом потребуется для прихода к состоянию случайной подстановки по дифференциальным переходам при использовании S-блоков с предельными показателями δ-равномерности равными $DP^{\pi}_{\max} = 2^{-6}$, (в соответствии с равенством $2^{-248} \approx (2^{-6})^k$) $k_{\min} = 41$ S-блок (для "родных" S-блоков с показателем δ-равномерности равными $DP^{\pi}_{\max} = 2^{-5}$ имеем $k_{\min} = 50$).

Аналогично, для прихода к состоянию случайной подстановки по линейным показателям при использовании S-блоков с предельными показателями нелинейности равными $LP^{\pi}_{\max} = 2^{-6}$ потребуется ($2^{-250} = 2^{k-1} \cdot \left(2^{-6}\right)^k$) $k_{\min} = 50$ S-блоков (для "родных" S-блоков с показателем нелинейности $LP^{\pi}_{\max} = 2^{-5}$ имеем $k_{\min} = 62{,}5$).

Расчёты числа активных S-блоков для этого случая приводят к результату: $1 \times 8 + 1 + 13 \times 4 = 61$. Для прихода к случайной подстановке за один цикл в шифре должны использоваться S-блоки с предельными показателями нелинейности.

3. СЛУЧАЙНЫЕ S-БЛОКИ В ШИФРЕ МУХОМОР

Оценим перспективы использования в шифре Мухомор случайных S-блоков. Будем здесь ориентироваться на функцию усложнения M-256.

Методика выполнения расчётов представлена в работе [3]. В табл. 1 представлены результаты расчётов числа переходов разного типа в 48-ми строках дифференциальной таблицы случайной подстановки. Мы в своих расчётах мето-

Таблица 1

Расчёт числа переходов разного типа в 48-ми строках дифференциальной таблицы случайной подстановки

Значение перехода таблицы	Число переходов дифференциальной таблицы	Число переходов в строке	Число переходов в 48 строках
12	1	0,003906	0,19
10	10	0,039065	1,87
8	104	0,40625	19,5
6	830	3,24218	155,62

дом перебора выбрали сразу такое число активных S-блоков, которое позволяет реализовать приход шифра к случайной подстановке. Для дифференциальных показателей оно равно 48.

Из представленных результатов следует, что для 48 активных S-блоков при выборе в строках максимально вероятных переходов можно ожидать при случайных входах в S-блоки:

– два перехода со значением 10;

– двадцать переходов со значением 8;

– двадцать пять переходов со значением 6.

Всего 48 переходов (48 активных S-блоков). Вычисления в этом случае приводят к нужному результату:

$$\left(\frac{10}{256}\right)^2 \times \left(\frac{8}{256}\right)^{20} \times \left(\frac{6}{256}\right)^{26} = 2^{-250}.$$

Это означает, что использование случайных S-блоков также позволяет прийти шифру к состоянию случайной подстановки за два цикла.

Приведём теперь распределение переходов для смещений линейной аппроксимационной таблицы. В общее число переходов здесь входят и положительные и отрицательные смещения. Пользуясь результатами работы [6], можем рассчитать числа переходов разного типа в 70 строках линейной аппроксимационной таблицы случайной подстановки, итоги расчётов которых представлены в табл. 2.

Опять будем считать, что за счёт введения цикловых подсключей входы в S-блоки будут случайными и статистически не зависимыми. Методика расчётов представлена в работе [3]. В таблице представлены результаты оценки числа переходов и их значений в 70 случайно взятых строках таблицы ЛАТ. Из результатов следует, что для 70 активных S-блоков при использовании максимально вероятных переходов можно ожидать при случайных входах в случайные S-блоки: один переход со значением 32; три перехода со значением 30; восемь переходов со значением 28; восемнадцать переходов со значением 26; тридцать девять переходов со значением 24. Самый первый (один) S-блок взят с максимально возможным значением перехода (34).

Полагая далее, что строки в S-блок выбираются из всего множества 256-ти строк, при этом переходы по S-блокам идут в произвольном порядке и осуществляются по наиболее вероятному пути, можем выполнить оценку вероятности прихода шифра к состоянию случайной подстановки со случайными S-блоками. Вычисления для значения $k = 70$ приводят к результату

$$2^{69} \times \left(\frac{34}{128}\right)^2 \times \left(\frac{32}{128}\right)^2 \left(\left(\frac{30}{128}\right)^2\right)^3 \times \left(\left(\frac{28}{128}\right)^2\right)^8 \times$$

$$\times \left(\left(\frac{26}{128}\right)^2\right)^{18} \times \left(\left(\frac{24}{128}\right)^2\right)^{39} = 2^{-257}$$

и, следовательно, 70 активных S-блоков позволяют осуществить переход шифра Мухомор-512 ($k_{\min} = 122$) к случайной подстановке за один цикл.

Напомним в заключение, что шифр Rijndael приходит к состоянию случайной подстановки по дифференциальным показателям на третьем цикле, а по линейным показателям лишь на четвёртом цикле.

Представленные результаты свидетельствуют о том, что шифры серии Мухомор не критичны к выбору S-блоков. Они обеспечивают предельные показатели стойкости и с S-блоками, выбранными случайным образом.

Более того, в качестве шифров с предельными криптографическими показателями могут выступать и шифры, использующие для построения своих цикловых преобразований функции усложения М-64, М-128 и М-256.

Таблица 2

Расчёт числа переходов разного типа в 61-й строках линейной таблицы случайной подстановки

Значение перехода	Число переходов в таблице ЛАТ	Число переходов в строке таблицы ЛАТ	Число переходов в 70-ти случайно взятых строках таблицы ЛАТ
±34	1,998	0,0078	0,546
± 32	4	0,0156	1,092
± 30	10	0,0392	2,744
± 28	28	0,1098	7,686
± 26	65	0,2588	18,116
± 24	146	0,572	40,04
± 22	298	1,164	81,48

ВЫВОДЫ

По нашим оценкам шифр Мухомор является одним из самых прогрессивных решений по построению блочных симметричных шифров. Он обладает предельными на сегодняшний день показателями случайности – становится случайной подстановкой уже с первого цикла, чего не позволяет осуществить ни один из современных шифров. Представляется, что разработчики, не владея данными этой работы, перестраховались, определив число циклов для серии шифров Мухомор большее 10-ти (11, 13, 18). На самом деле в этом шифре без снижения показателей стойкости может использоваться существенно меньшее число циклов (вплоть до четырех), а это значит, что шифр может реализовать показатели быстродействия существенно превышающие соответствующие показатели многих известных шифров, в том числе и шифра Rijndael. На обосновании справедливости последнего утверждения мы остановимся в отдельной работе.

Литература

[1] Горбенко І.Д. Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація / І.Д. Горбенко, М.Ф. Бондаренко, В.І. Долгов, Р.В. Олійников та інші // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. – Том. 6, №2. – С. 147–157.

[2] Gorbenko I.D. On Ciphers Coming to a Stationary State of Random Substitution / I.D. Gorbenko, K.E. Lisitskiy, D.S. Denisov // Copyright © 2013 Horizon Research Publishing.

[3] Горбенко И.Д. О динамике прихода шифров к случайной подстановке при использовании S-блоков с показателями нелинейности близкими к предельным / И.Д. Горбенко, К.Е. Лисицкий // Радиотехника: Всеукр. межвед. Науч.-техн. сб. – 2014. – Вып. № 176. – С. 27–39.

[4] Бондаренко М.Ф. Обґрунтування вимог та розробка основних рішень з побудування та властивості перспективного БСШ «Мухомор» / М.Ф. Бондаренко, І.Д. Горбенко, В.І. Долгов, Р, В. Олійников та ін. // Прикладная радиоэлектроника. – Харьков: ХНУРЭ. – 2007. – Том 6, № 2. – С. 174–185.

[5] Лисицкий К.Е. Динамические показатели прихода блочных шифров к состоянию случайной подстановки [Текст] / К.Е. Лисицкий // Издательский дом LAP LAMBERT Academic Publishing, 2014. – 60 с.

[6] Долгов Виктор Иванович. Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа: монография. / В.И. Долгов, И.В. Лисицкая. – Харьков. Издательство “Форт”, 2013. – 420 с.

[7] Горбенко И.Д. Свойства и возможности оптимизации криптографических преобразований в AES – RIJNDAEL / И.Д. Горбенко, Д.А. Чекалин // Радиотехника. Всеукр. межвед.: науч.-техн. сб. 2001. Вып. 119. – С. 36–42.

[8] Lisitskiy K.E. On Maxima Distribution of Full Differentials and Linear Hulls of Block Symmetric Ciphers [Text] / K.E. Lisitskiy // I.J. Computer Network and Information Security, 2014, 1, 11-18 Published Online November 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis. 2014.01.02.

Поступила в редколлегию 21.07.2014

Долгов Виктор Иванович, фото и сведения об авторе см. на стр. 216.

Лисицкая Ирина Викторовна, доктор технических наук, доцент кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники. Область научных интересов: криптография, методы криптоанализа.

Лисицкий Константин Евгеньевич, фото и сведения об авторе см. на стр. 212.

УДК 621. 3.06

Новий погляд на шифр Мухомор / В. І. Долгов, І. В. Лисицька, К.Є. Лисицький // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 221–225.

Виконується уточнення динамічних показників приходу шифру Мухомор до стану випадкової підстановки. Показано, що шифр Мухомор приходить до стану випадкової підстановки вже на першому циклі, чого не дозволяють всі сучасні шифри. Робиться висновок, що шифр Мухомор є на сьогоднішній день найпрогресивнішим рішенням з побудови блокових симетричних шифрів.

Ключові слова: динамічні показники шифру, випадкова підстановка, циклове перетворення.

Табл.: 2. Іл.: 1. Бібліогр.: 8 найм.

UDC

A new view on the Muhomor cipher / V.I. Dolgov, I.V. Lisitskaya, K.E. Lisitsky // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 221–225.

A revision of dynamic indicators of the Muhomor cipher coming to the state of random substitution is performed. It is shown that the Muhomor cipher comes to the state of random substitution already at the first cycle, which all modern ciphers cannot do. It is concluded that the Muhomor code is by far the most advanced solution to build a symmetric block ciphers.

Keywords: dynamic cipher indicators, random substitution, round transformation.

Tab.: 2.: Fig.: 1. Ref.: 8 items.