УДК 621. 391:519.2:519.7

ОЦЕНКИ МАКСИМАЛЬНЫХ ЗНАЧЕНИЙ ДИФФЕРЕНЦИАЛОВ И ЛИНЕЙНЫХ КОРПУСОВ МАРКОВСКИХ ШИФРОВ

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

Представляется краткий анализ существа известных подходов к оценке показателей доказуемой стойкости марковских блочных симметричных шифров к атакам дифференциального и линейного криптоанализа. Излагается сущность новой методологии оценки доказуемой стойкости БСШ к атакам дифференциального и линейного криптоанализа. Приводятся результаты оценки максимальных значений дифференциалов и линейных корпусов Марковских шифров. Выполняется обоснование процесса перехода шифров к стационарному состоянию. Формулируется новая редакция гипотезы статистической эквивалентности. Уточняются некоторые положения теории Марковских шифров, встречающиеся в публикациях.

Ключевые слова: Марковский шифр; дифференциальная вероятность; линейная вероятность; новая методология оценки доказуемой стойкости; стационарное состояние свойственное случайной подстановке.

ВВЕДЕНИЕ

В нашей предыдущей работе [1] был поднят вопрос об уточнении ряда принципиальных моментов, связанных с понятиями и определениями теории Марковских шифров. Было введено понятие Марковского шифра k-того порядка и сделан общий вывод о том, что все известные итеративные блочные шифры являются Марковскими шифрами (первого или второго порядка). В этой работе мы продолжаем обсуждение состояния ряда теоретических и практических вопросов в этом направлении, и здесь мы хотим привлечь внимание к подходам, имеющимся в публикациях, посвящённым оценкам максимальных значений дифференциалов и линейных корпусов Марковских шифров. Мы изложим сущность новой методологии формирования показателей доказуемой стойкости блочных симметричных шифров, развиваемой на кафедре БИТ ХНУРЭ, которая естественно применима и к Марковским шифрам, и покажем, что соответствующие показатели доказуемой стойкости для таких шифров могут быть получены расчётным путём.

1. ПОНЯТИЙНЫЙ АППАРАТ ЛИНЕЙНОГО И ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА

Уместно будет напомнить основной понятийный аппарат линейного и дифференциального криптоанализа, которым мы воспользуемся в дальнейшем. Следуя работе [2], приведём ряд определений.

Определение 1. (Дифференциальная и Линейная вероятности): *Дифференциальная вероятность DP^f и линейная вероятность LP^f соответственно для ключезависимой функции f с n-битным входом x и n-битным выходом y ($x, y \in GF(2^n)$) есть*

$$DP^f(\Delta x \to \Delta y) = \frac{\#\{x \in GF(2)^n \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y}{2^n};$$

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

где Δx и Δy являются входной и выходной разностями, а Γx и Γy – это входная и выходная маски; $x \cdot \Gamma x$ обозначает результат скалярного произведения x на Γx, $f(x) \cdot \Gamma y$ – результат скалярного произведения $f(x)$ на Γy/.

Определение 2. ($DP^f_{\max}$ и $LP^f_{\max}$): *Максимальное значение дифференциальной и линейной вероятностей для ключезависимой функции f определяются соответственно как*

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

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

Напомним также выражения для средних вероятностей *ADP*, *ALHP*, *MADP* і *MALHP* ключезависимой функции $f = f[k](x)$ с n-битным входом x и n-битным выходом, параметризованной ключом k, которые используются во многих публикациях по обоснованию показателей стойкости блочных шифров.

Определение 3. *Среднее значение дифференциальной вероятности (ADP) функции $f[k](x)$ есть*

$$ADP^f = \underset{k}{ave}\, DP^{f[k]}(\Delta x \to \Delta y).$$

Определение 4. *Среднее значение вероятности линейного корпуса (ALHP) функции $f = f[k](x)$ есть*

$$ALHP^f = \underset{k}{ave}\, LP^{f[k]}(\Gamma x \to \Gamma y).$$

Определение 5. *Максимум среднего значения дифференциальной вероятности (MADP) и максимум среднего значения вероятности линейного корпуса (MALHP) функции $f = f[k](x)$ есть*

$$MADP^f = \max_{\Delta x \neq 0, \Delta y} ADP^f(\Delta x \to \Delta y),$$

$$MALHP^f = \max_{\Gamma x,\, \Gamma y \neq 0} ALHP^f(\Gamma x \to \Gamma y).$$

Заметим теперь, что приведенные здесь определения *MADP* и *MALHP*, повсеместно используемые в публикациях, на наш взгляд не являются

адекватными задаче оценке потенциальных характеристик стойкости шифра к атакам дифференциального и линейного криптоанализа (они характеризуют лишь максимумы средних значений таких вероятностей, вычисленных для некоторого фиксированного перехода $\Delta x \to \Delta y$ или некоторого фиксированного сочетания масок $Гx \to Гy$).

Нами в [3] предложено определять не максимумы средних значений переходов и смещений, а средние (по множеству ключей) значения максимумов дифференциальных и линейных вероятностей – *AMDP* и *AMLHP* соответственно, которые определяются следующим образом:

Определение 6 (*AMDP*). *Среднее* (*по множеству из* 2^h *ключей*) *значение максимальных дифференциальных вероятностей ключезависимой функции* $f[k](x)$ *есть*

$$AMDP^f = \underset{k}{ave}\, DP_{\max}^{f[k]} = \frac{1}{2^h}\sum_{k=1}^{2^h} DP_{\max}^{f[k]} .$$

Определение 7 (*AMPLH*). *Среднее* (*по ключам*) *значение максимальных вероятностей линейных корпусов функции* $f[k](x)$ *есть*

$$AMLHP^f = \underset{k}{ave}\, LP_{\max}^{f}(Гx \to Гy) = \frac{1}{2^h}\sum_{k=1}^{2^h} LP_{\max}^{f[k]} .$$

В обоих случаях 2^h *– мощность используемого при вычислениях множества ключей зашифрования.*

Тут же можно отметить, что очевидны неравенства:

$$MADP^f < AMDP^f,$$
$$MALHP < AMLHP,$$

которые лишний раз свидетельствуют в пользу вновь введенных определений, не говоря уже о значительных вычислительных преимуществах предлагаемого подхода и полного согласования его результатов с соответствующими свойствами случайных подстановок.

Именно с использованием этих двух показателей выполнено обоснование новой идеологии оценки доказуемой стойкости БСШ в наших работах [4-7, и др.].

2. КРАТКИЙ АНАЛИЗ СУЩЕСТВА ИЗВЕСТНЫХ ПОДХОДОВ К ОЦЕНКЕ ПОКАЗАТЕЛЕЙ ДОКАЗУЕМОЙ СТОЙКОСТИ МАРКОВСКИХ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ К АТАКАМ ДИФФЕРЕНЦИАЛЬНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА

Достаточно детальный анализ широко эксплуатируемой сегодня концепции оценки показателей доказуемой стойкости блочных симметричных шифров представлен в нашей работе [4]. Мы здесь приведём уже сами выводы, следующие из этого анализа.

Первый вывод состоит в том, что в основе всех подходов к оценке показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа лежит процедура определения максимумов средних значений вероятностей (максимальных средних значений вероятностей) полного дифференциала (*MADP*) для всего шифра и смещения его линейного корпуса (*MALHP*).

Добавим здесь второй вывод, который состоит в том, что все развиваемые подходы ориентированы на формирование оценочных (граничных) значений соответствующих показателей.

Третий вывод состоит в том, что оценки соответствующих показателей отличаются в значительных пределах.

Четвёртый вывод состоит в том, что результирующие показатели стойкости шифров практически во всех работах связываются с соответствующими криптографическими показателями, входящих в шифры S блоковых конструкций.

В работе [4] делается обобщающее заключение, что существующие методики оценки показателей стойкости БСШ являются все еще далеко не совершенными.

Следует сказать, что недалеко от изложенного общего состояния и движения в отмеченном направлении находятся методы и подходы, используемые при формировании показателей стойкости Марковских шифров.

Мы здесь, однако, отметим две работы, в которых оценки стойкости Марковских шифров строятся на основе использования матриц переходных вероятностей одноцикловых преобразований.

В работе [9] авторы оперируют матрицами переходных вероятностей для цепей Маркова и рассматривают результат многоциклового преобразования с помощью возведения матрицы переходных вероятностей одноциклового преобразования в степень, равную числу циклов преобразования.

В работе [10] также считается справедливой сходимость последовательности матриц вероятностей дифференциальных аппроксимаций марковского блочного шифра к равновероятной матрице при увеличении количества циклов. И в ряде других работ матрица дифференциальных вероятностей шифра строится на возведении матрицы переходных вероятностей одноциклового преобразования в степень, равную числу циклов (раундов). Это, конечно, и в первом и во втором случаях не верно, как и не верно утверждение о сходимости последовательности матриц средних вероятностей шифра к равновероятной.

Возведение в степень справедливо лишь в том случае, когда над отсчётными значениями выборки, входящими в уравнение Марковского процесса, осуществляется линейное преобразование. Когда речь идёт о полных дифференциалах, то для практически всех известных итеративных шифров этого делать нельзя, так такие шифры цикловое преобразование строят с использованием нелинейных операций (*S*-блоков). Заметим, что шифры без *S*-блоков

тоже укладываются в эту общую схему (там тоже используются нелинейные операции).

Остановимся на этом принципиальном моменте более детально.

Начнём с Марковского процесса первого порядка, заданного уравнением для дифференциалов (см. работу [1]):

$$\Delta\mathbf{y}_r = F_r\{\mathbf{x}\} \oplus F_r\{\mathbf{x}^*\} = F_r^*\{\Delta\mathbf{x}\} = F_r^*\{\Delta\mathbf{y}_{r-1}\}, \quad (1)$$

В (1) F_r^* – функция циклового преобразования разностей.

Как следует из уравнения (1), при вычислении выходной разности $\Delta\mathbf{y}_r$ ключ последнего цикла $\mathbf{k}^{r+1}$, как и ключи предшествующих циклов вроде бы де уходят из уравнения (компенсируется). Однако это не так. Ключи текущего и предшествующих циклов шифрования (случайные компоненты) присутствуют в этом преобразовании через вполне определённые значения промежуточных разностей, участвующих в формировании разности шифртекстов на его выходе. И для выходной разности это, конечно, ключезависимый результат (в том смысле, что для каждого значения ключа будет формироваться своя разность).

Тем не менее, решение уравнения (1) для фиксированного набора цикловых подключей можно представить в виде $\mathbf{y}_r \oplus \mathbf{y}_r^* =$

$$= y_r \oplus y_r^* = F_r\{\mathbf{C}_{r-1}\} \oplus \mathbf{k}^{r+1} \oplus F_r\{\mathbf{C}_{r-1}^*\} + \mathbf{k}^{r+1} =$$
$$= F_r\{\mathbf{C}_{r-1}\} \oplus F_r\{\mathbf{C}_{r-1}^*\} = F_r^*\{\Delta\mathbf{C}_{r-1}\}$$

и далее

$$F_r^*\{\Delta\mathbf{y}_{r-1}\} = F_r\{\mathbf{y}_{r-1}\} \oplus F_r\{\mathbf{y}_{r-1}^*\} =$$
$$= F_r\{F_{r-1}\{\mathbf{y}_{r-2} \oplus \mathbf{k}^r\}\} \oplus F_r\{F_{r-2}\{\mathbf{y}_{r-1}^*\} \oplus \mathbf{k}^r\} =$$
$$= F_r^*\{F_{r-1}^*\{\mathbf{y}_{r-2} \oplus \mathbf{k}^r \oplus F_{r-1}\{\mathbf{y}_{r-2}^*\} \oplus \mathbf{k}^r\} =$$
$$= F_r^*\{F_{r-1}^*\{\Delta\mathbf{y}_{r-2}\}\} = \ldots = F_r^*\{F_{r-1}^*\{\cdots F_1^*\{\Delta\mathbf{y}_0\}\cdots\},$$

т.е.

$$\Delta\mathrm{y}_r = F_r^*\{F_{r-1}^*\{F_{r-2}^*\{\ldots\{F_1^*\{\Delta\mathrm{x}_0\}\}\ldots\}, \ \Delta\mathrm{x}_0 = \Delta\mathrm{y}_0. \quad (2)$$

Можно далее ввести в рассмотрение полное множество значений входных и выходных разностей и тогда произведение преобразований $F_r^* \cdot F_{r-1}^* \cdot F_{r-2}^* \cdot \ldots \cdot F_1^*$ рассматривать как матрицу переходных вероятностей, например в виде:

$$F_r^* \cdot F_{r-1}^* \cdot F_{r-2}^* \cdot \ldots \cdot F_1^* =$$

$$= \begin{vmatrix} f_{0,0} & f_{0,1} & \cdots & f_{0,2^{n-1}} \\ f_{1,0} & f_{1,1} & \cdots & f_{1,2^{n-1}} \\ \vdots & \vdots & \vdots & \vdots \\ f_{2^{n-1},0} & f_{2^{n-1},1} & \cdots & f_{2^{n-1},2^{n-1}} \end{vmatrix}.$$

В этой матрице каждый элемент $f_{i,j}$ определяет вероятность перехода i-той разности $\Delta\mathbf{x}_i$ на входе шифра в j-тую выходную разность $\Delta\mathbf{y}_j$ (в данном случае для r циклов зашифрования). Для марковского шифра, достигшего стационарного состояния, значения элементов матрицы подчиняются закону распределения вероятностей переходов случайной подстановки соответствующей степени (матрица имеет вполне определённое число нулей, число двоек, четвёрок и т.д.). Наращивание числа циклов в этом случае приводит к матрице с другим размещением элементов, но для неё всё равно сохраняется закон распределения переходов (она снова имеет прежнее число нулей, двоек, четвёрок и т.д., вплоть до единственного, как правило, максимального значения для определённого выхода).

Остаётся отметить, что для каждого числа циклов и каждого ключа зашифрования будет своя матрица переходных вероятностей (нормированная таблица дифференциальных разностей) и результирующая матрица переходных вероятностей для r циклового Марковского шифра будет определяться, как это следует из (2), на основе произведения подстановочных преобразований для одноцикловых переходов.

Большинство известных итеративных шифров используют однотипные цикловые преобразования. Поэтому результирующее подстановочное преобразование для таких шифров будет действительно представлять собой соответствующую степень одноциклового преобразования. Здесь надо помнить, что произведение подстановочных преобразований есть последовательное их выполнение одного за другим. Таким образом, мы пришли к последовательному выполнению r однотипных преобразований:

$$F_r^* = (F_1^*)^r, \quad (3)$$

но не к матричному возведению в степень.

Следовательно, попытки использования для вычисления оценок показателей стойкости Марковских шифров возведения в степень матриц переходных вероятностей для «нелинейной» цепи Маркова представляются ошибочными.

Что касается Марковских шифров второго порядка, то их сходимость к Марковским шифрам первого порядка можно объяснить тем, что для итеративных шифрующих преобразований (шифров) переход к стационарному режиму обозначает статистическую независимость соседних (смежных) значений блоков данных. Поэтому, например, для шифра ГОСТ компонента B_{i-1} в уравнении Марковского процесса второго порядка

$$A_i = f(A_{i-1} \left[+\right] K_j) \oplus B_{i-1}$$

с ростом числа циклов становится случайной по отношению к значениям A_i и A_{i-1}, а это и означает, что уравнение Марковского процесса второго порядка приобретает вид уравнения Марковского процесса первого порядка. Более удивительным,

однако, является тот факт, что шифр сохраняет свойства случайной подстановки и без цикловых подключей (без случайных компонент). Мы на этом моменте остановимся более детально. В табл. 1 представлены результаты экспериментов с шифрами Rijndael, Serpent и ГОСТ по оценке лавинных свойств этих шифров.

В левой части этой таблицы приводятся поцикловые лавинные показатели рассматриваемых шифров (среднее число изменившихся бит на выходе при изменении одиночного бита на входе) при выполнении шифрований с наборами ненулевых значений цикловых подключей, а в правой части таблицы приводятся лавинные показатели этих же шифров с нулевыми цикловыми подключами. Хорошо видно, что результаты как в случае использования ключей, так и в случае их отсутствия практически совпадают. Аналогичные результаты получаются при рассмотрении корреляционных характеристик, а также для дифференциальных и линейных показателей этих же шифров. Вот и получается, что и без случайных компонент шифры всё равно асимптотически ведут себя как случайные подстановки. Но если для Марковских шифров второго порядка есть возможность стать Марковским шифром первого порядка, то, как быть с Марковскими шифрами первого порядка? Получается, что отмеченный результат можно объяснить только тем, что сами цикловые преобразования рассмотренных шифров и без цикловых подключей обладают достаточно эффективным механизмом перемешивания блоков данных. По-видимому, свойство Марковости здесь переходит в сбалансированное статистическое усреднение. Мы возвратимся опять к этому вопросу немного позднее.

Далее будет уместным напомнить новую методологию оценки показателей доказуемой стойкости шифров (Марковских шифров) к атакам дифференциального и линейного криптоанализа, предложенную в нашей работе [4].

3. СУЩНОСТЬ НОВОЙ МЕТОДОЛОГИИ ОЦЕНКИ ДОКАЗУЕМОЙ СТОЙКОСТИ БСШ К АТАКАМ ДИФФЕРЕНЦИАЛЬНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА

В отмеченной работе она сформулирована следующим образом.

Все современные блочные шифры через определенное число циклов независимо от используемых в шифрах S-блоков (*конечно, здесь речь идет не о вырожденных их конструкциях*) *приобретают свойства случайных подстановок, т.е. по комбинаторным показателям* (*числу инверсий, возрастаний и циклов*), *а также по законам распределения переходов таблиц XOR разностей* (*полных дифференциалов*) *и законам распределения смещений таблиц линейных аппроксимаций* (*линейных корпусов*) *повторяют соответствующие показатели случайных подстановок. В результате значения максимумов полных дифференциалов и линейных корпусов могут быть определены расчетным путем из формул для законов распределения вероятностей переходов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок соответствующей степени.*

При этом, проверка показателей случайности больших шифров может быть выполнена на основе разработки и последующего анализа показателей случайности уменьшенных моделей, допускающих проведение вычислительных экспериментов в приемлемые (*реальные*) *сроки.*

Малые модели шифров, повторяющие своих прототипов, позволяют оценить не только средние значения максимумов таблиц дифференциальных вероятностей (*AMDP*), *и средних значений максимумов линейных вероятностей* (*AMLP*) *для ограниченного множества ключей, но и решить задачу определения* (*проверки*) *абсолютного значения максимума по полному множеству ключей.*

Для иллюстрации справедливости приведенных положений мы приведём здесь некоторые примеры анализа дифференциальных и

Таблица 1

Показатели лавинного эффекта для шифров AES, Serpent и ГОСТ при использовании случайных цикловых ключей и безключевые варианты

Число циклов	С ключом			Без ключа		
	AES	Serpent	ГОСТ	AES	Serpent	ГОСТ
1	16,2109	12,1302	2,3666	16,2133	12,137	2,09405
2	64,2589	57,356	5,40601	64,2624	57,3746	4,74361
3	64,0071	63,9972	10,2341	64	63,9977	8,06269
4	64,0062	63,9984	15,5382	64,0033	63,9955	12,4266
5	64,0073	63,9963	21,5132	63,9993	64,0019	17,9388
6	63,9965	64,0038	27,0884	64,0005	63,998	23,2881
7	64,0043	63,9903	30,2263	63,9983	64,0089	27,5203
8	63,9997	63,9951	31,4977	63,9963	64,0028	30,1418
9	64,0038	63,9901	31,8901	63,9979	63,9961	31,3863
10	64,0039	63,9921	31,9901	63,9991	64,0016	31,8744
11	63,9951	64,0013	31,9983	63,9967	64,0057	31,9727
12	63,9937	64,000	32,0002	63,9968	64,0069	31,9948

линейных свойств двух известных шифров AES и ГОСТ 28147-89 и ещё двух шифров Калина и Мухомор, представленных на украинский конкурс (здесь рассматриваются полные версии этих шифров). Длина ключа и блока для AES взята 256 бит, а для шифров Калина и Мухомор длина ключа и блока одинаковые и равны 128 битам.

В табл. 2 представлены поцикловые средние значения максимумов полных дифференциалов для этих шифров, полученные при их использовании в режиме зашифрования 16-битных блоков данных (в качестве результатов зашифрования из зашифрованного блока данных тоже вырезается 16-битный сегмент [5]).

Таблица 2

Поцикловые средние значения максимумов полных дифференциалов шифров вместе со среднеквадратическими отклонениями

Кол-во циклов	AES	ГОСТ 28147-89	Калина	Мухомор
1	65536	65536	65536	19,4
2	3652,26	65536	1382	19,2
3	**19,0666**	61952	**18,8**	19,6
4	19,0666	56008,6	18,8	19,2
5	18,8666	31358	19,2	19
6	19,1332	2046,7	18,8	19,2
7	19,2666	973,4	18,6	19,8
8	19,1332	52,2	18,8	19
9	19,0666	**19,1**	19	19,2
10	19,3333	19,5	18,8	19,6
11	19,4	18,7	19,4	19
13	18,8666	19,1	18,6	18,6
14	18,9332	19,4	19	19,2

В табл. 3 представлены поцикловые средние значения максимумов смещений линейных корпусов этих же шифров вместе со среднеквадратическими отклонениями.

Для всех трех шифров был выполнен подсчет максимумов дифференциалов и смещений линейных корпусов с использованием 10 различных случайно сгенерированных ключей.

В табл. 4 и 5 представлены ещё не опубликованные результаты экспериментов. Здесь рассматривались три шифра: Rijndael, Serpent, Threefish. Опять взяты полные версии данных шифров. Длина ключа и блока для Rijndael и Serpent одинакова и равна 128 битам, а в реализации шифра Threefish использовалась длина для блока и ключа равная 512 битам. Заметим, что в шифре Threefish не применяются S-блоки.

Для всех трех шифров и в этом случае был выполнен подсчет средних значений максимумов полных дифференциалов и смещений линейных корпусов с использованием 10 различных случайно сгенерированных ключей.

Представленные результаты хорошо иллюстрируют переход шифров к стационарному состоянию, повторяющему характеристики случайных подстановок соответствующей степени [11, 12] (наиболее «медленным» оказался шифр Threefish, а вот шифр Мухомор выходит на асимптотические показатели дифференциалов и смещений сразу после первого цикла).

Мы здесь уже не будем приводить результаты экспериментов, свидетельствующие о независимости асимптотических показателей шифров от свойств применяемых в них S-блоков. Отошлём читателей к нашим работам [6,7 и др.]. Остановимся теперь на одном из принципиальных моментов рассматриваемого подхода – приходу шифров к стационарному состоянию свойственному случайной подстановке.

Таблица 3

Поцикловые средние значения максимумов смещений линейных корпусов шифров

Кол-во циклов	AES	ГОСТ 28147-89	Калина	Мухомор
1	0	0	11008,392	**824,742**
2	9284.27	32768	**817,271**	818,621
3	**818.467**	17162	817,718	827,431
4	815	31181,7	814,19	824,193
5	818.5	16150,1	837,349	831,753
6	815.967	16669,5	810,733	814,155
7	832.1	2144,77	820,384	820,975
8	823.133	2380,93	837,917	823,024
9	829.9	**826,833**	809,273	810,196
10	827.4	828,1	821,755	821,316
11	815.6	823,767	827,462	822,385
12	819	821,433	820,291	816,753

Таблица 4

Поцикловые значения максимумов полных дифференциалов для 16-битных сегментов

Число циклов, *r*	MAX (Rijndael)	MAX (Serpent)	MAX (Threefish)
1	16384	18,93	65536
2	8904,25	19,24	65536
3	1911.47	18,64	65536
4	19,24	18,33	42440,04
5	20,31	18,75	30704,23
6	18,83	19,21	9534,57
7	19,21	18,98	37,75
8	19,4	18,37	19,27
9	18,33	19,24	18,78
10	19,17	19,63	18,44

Таблица 5

Математические ожидания максимальных смещений линейных корпусов полных моделей шифров

Число циклов, *r*	MAX (Rijndael)	MAX (Serpent)	MAX (Threefish)
1	0	810,4	32768
2	16313,36	825,0667	32680,93
3	7728,66	828,2667	31306,13
4	817,43	825,9333	23730,93
5	821,98	828,4667	19722,67
6	825,716	824,8667	19722,67
7	817,367	820,3333	7899,8
8	820,167	817,5333	844,0667
9	821,767	820,4	822,1333
10	820,167	816,6	815,8

Выше получен результат (2), в соответствии с которым для Марковского шифра первого порядка формирование матрицы переходных вероятностей всего шифра сводится к последовательному выполнению r однотипных (одноцикловых) преобразований (см. соотношение (3)). По результатам экспериментов можно сделать вывод о том, что *произведение одноцикловых преобразований после небольшого начального числа их повторений приобретает свойства случайной подстановки соответствующей степени независимо от показателей случайности исходного одноциклового преобразования*.

Мы не смогли найти теоретического обоснования этого свойства. Удалось лишь показать [4], что после достижения стационарного распределения при дальнейшем наращивании числа циклов это стационарное распределение сохраняется. Поэтому мы здесь представляем дополнительные обоснования правомерности приведенного утверждения. Наш интерес сосредоточился на процессах, происходящих при последовательном выполнении подстановочных преобразований.

В соответствии с этим далее приводятся результаты вычислительного эксперимента не с шифрами, а с подстановками 256-й степени (байтовыми подстановками). В табл. 6 представлены результаты вычислительного эксперимента по определению максимумов XOR таблиц последовательности подстановочных преобразований для двух байтовых подстановок.

Одна подстановка взята с показателем δ -равномерности равным 4-ём, а вторая с показателем δ -равномерности равным 8-и. Видно, что обе подстановки уже на втором цикле приходят к максимуму дифференциала равному 10-12, характерному для случайной подстановке степени 2^8 [11].

Интересно отметить, что результат не зависит от ключевых значений, если их ввести после каждого подстановочного преобразования.

Конечно, по законам комбинаторики этот процесс должен быть периодическим, но для интересующих нас значений мы, как правило, оказываемся очень далеко от циклового периода подстановки.

Далее мы представляем результат возведения подстановочного преобразования (10 2 0 6 15 1 12 4 14 11 7 13 9 5 3 8) в квадрат (произведения одинаковых полубайтовых подстановочных преобразований:

$$(10\ 2\ 0\ 6\ 15\ 1\ 12\ 4\ 14\ 11\ 7\ 13\ 9\ 5\ 3\ 8)\times$$
$$\times(10\ 2\ 0\ 6\ 15\ 1\ 12\ 4\ 14\ 11\ 7\ 13\ 9\ 5\ 3\ 8)=$$
$$=(7\ 0\ 10\ 12\ 8\ 2\ 9\ 15\ 3\ 13\ 4\ 5\ 11\ 1\ 6\ 14).$$

Ниже представляется произведение матриц переходов (матриц переходных вероятностей умноженных на *AMDP*) этого подстановочного преобразования (возведение матрицы в квадрат).

$$\begin{vmatrix}
16&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&2&2&0&4&0&2&2&2&0&2&0\\
0&0&0&2&2&2&2&0&0&2&4&0&0&2&0&0\\
0&2&2&2&0&0&2&0&0&0&\mathbf{0}&2&4&2&0&0\\
0&0&2&2&2&4&0&2&0&0&0&0&2&0&2&0\\
0&0&2&0&2&0&0&0&0&0&2&4&0&2&2&2\\
0&\mathbf{0}&0&2&0&0&4&2&2&0&0&0&0&2&2&2\\
0&2&2&0&2&0&2&0&2&2&0&0&0&0&4&0\\
0&0&0&0&4&0&2&2&0&2&0&2&2&0&0&2\\
0&4&0&0&2&0&0&2&2&0&2&\mathbf{0}&2&2&0&0\\
0&2&0&0&0&2&0&0&0&2&0&0&2&4&2&2\\
0&0&2&0&0&2&0&4&2&2&0&2&0&2&0&0\\
0&2&\mathbf{0}&4&0&0&0&2&0&2&2&2&0&0&2&0\\
0&2&0&2&2&2&0&0&2&0&0&2&0&0&0&4\\
0&0&2&2&0&0&0&0&2&4&2&0&2&0&0&2\\
0&2&4&0&0&2&2&2&0&0&2&0&\mathbf{0}&0&0&2
\end{vmatrix}\times$$

$$\times\begin{vmatrix}
16&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&2&2&0&4&0&2&2&2&0&2&0\\
0&0&0&2&2&2&2&0&0&2&4&0&0&2&0&0\\
0&2&2&2&0&0&2&0&0&0&\mathbf{0}&2&4&2&0&0\\
0&0&2&2&2&4&0&2&0&0&0&0&2&0&2&0\\
0&0&2&0&2&0&0&0&0&0&2&4&0&2&2&2\\
0&\mathbf{0}&0&2&0&0&4&2&2&0&0&0&0&2&2&2\\
0&2&2&0&2&0&2&0&2&2&0&0&0&0&4&0\\
0&0&0&0&4&0&2&2&0&2&0&2&2&0&0&2\\
0&4&0&0&2&0&0&2&2&0&2&\mathbf{0}&2&2&0&0\\
0&2&0&0&0&2&0&0&0&2&0&0&2&4&2&2\\
0&0&2&0&0&2&0&4&2&2&0&2&0&2&0&0\\
0&2&\mathbf{0}&4&0&0&0&2&0&2&2&2&0&0&2&0\\
0&2&0&2&2&2&0&0&2&0&0&2&0&0&0&4\\
0&0&2&2&0&0&0&0&2&4&2&0&2&0&0&2\\
0&2&4&0&0&2&2&2&0&0&2&0&\mathbf{0}&0&0&2
\end{vmatrix}\neq$$

$$\neq\begin{vmatrix}
16&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&2&0&0&\mathbf{0}&0&4&2&2&0&4&0&0&0&2&0\\
0&2&0&0&0&0&0&2&2&0&0&0&2&6&0&2\\
0&0&0&0&0&2&2&4&0&2&2&4&0&0&0&0\\
0&0&4&4&0&0&0&0&2&0&0&2&2&0&0&\mathbf{2}\\
0&0&2&2&0&6&2&0&2&0&2&0&0&0&0&0\\
0&0&2&2&2&2&0&0&0&0&0&0&0&0&4&4\\
0&0&0&0&2&2&0&\mathbf{0}&4&2&0&2&0&2&2&0\\
0&2&0&4&2&0&0&0&0&2&0&0&0&2&2&2\\
0&0&0&2&0&0&0&2&2&6&2&0&0&0&0&2\\
0&2&2&2&0&2&0&0&0&2&0&0&2&0&4&0\\
0&0&2&0&6&0&2&2&2&0&0&0&0&0&0&2\\
0&2&2&0&0&0&0&0&0&0&2&2&4&2&0&2\\
0&2&0&0&2&2&2&0&0&0&\mathbf{2}&4&2&0&0&0\\
0&4&2&0&0&0&0&2&0&0&2&0&2&2&2&0\\
0&0&0&0&2&0&4&2&0&2&0&2&2&2&0&0
\end{vmatrix}$$

Непосредственное выполнение расчётов показывает, что результат матричного произведения не совпадает с матрицей переходных вероятностей подстановочного преобразования, полученного его умножением самого на себя (она представлена в правой части неравенства).

Таблица 6

Распределение максимумов XOR таблиц
последовательности подстановочных преобразований байтовой подстановки

Число циклов (повторов)	1	2	3	4	5	6	7	8	9	10	11
Значение максимума XOR таблицы для AES S-блока	4	12	12	10	12	12	10	12	12	12	12
Значение максимума XOR таблицы для S-блока Мухомор	8	10	10	12	10	14	12	12	10	12	10

Таким образом, *произведение* (*последовательность*) *подстановочных преобразований нетривиального типа* (*а не только шифров*) *является с большой вероятностью случайной подстановкой, независимо от свойств подстановки, участвующей в формировании этого степенного преобразования.*

Мы посчитали, что это и приведенное выше утверждение является неким «законом природы» (законом хаотического преобразования), который выполняется независимо от нашего желания (может здесь надо более строго оговорить, какие подстановки удовлетворяют этому правилу, но это предмет отдельного исследования).

Аналогично к стационарному распределению свойственному случайной подстановке приходит и любой шифр. Стационарное распределение как раз соответствует тому, что шифр начинает повторять свойства случайной подстановки.

А вот тот факт, что произведение подстановок (и без случайной компоненты), как и последовательность шифрующих преобразований с нулевыми цикловыми подключами, становится случайной подстановкой, оказался всё же неожиданным. Объяснением этому факту может быть лишь то, что сами по себе подстановки (исключая тривиальные их конструкции), как правило, представляют собой набор случайных переходов (уже в самой подстановке заложен механизм случайного перемешивания).

Теперь можно привести дополнительные результаты, уточняющие ряд поднятых ранее вопросов.

О гипотезе статистической эквивалентности.

Как следует из приведенных выше и многочисленных других имеющихся результатов, стационарное состояние, к которому приходит шифр (Марковский шифр) практически не зависит от ключей зашифрования, что хорошо видно из таблиц 1-5. Это говорит о том, что гипотеза статистической эквивалентности, о которой упоминалось в предыдущей нашей работе [1], оказывается справедливой для всех Марковских шифров как первого, так и второго порядков (если их после приведенных особенностей можно называть Марковскими).

Гипотеза статистической эквивалентности в нашей интерпретации выглядит следующим образом:

Гипотеза статистической эквивалентности. *Для Марковских шифров значение максимума полных дифференциалов* (*также как и значение максимума смещений линейных корпусов*) *почти для всех ключей является одним и тем же, практически совпадающим с максимумом таблицы XOR переходов* (*максимумом смещения таблицы линейных аппроксимаций*) *случайной подстановки соответствующей степени.*

Более строгому обоснованию этого положения мы уделим внимание в отдельной работе.

Следующее наше уточнение связано с оценкой показателей стационарности для Марковских шифров.

Возвращаясь к теореме 3 работы [9], мы хотим обратить внимание на то, что по имеющимся многочисленным результатам экспериментов утверждение о том, что с увеличением числа циклов шифр приходит к равномерному стационарному распределению, встречающееся и в ряде других работ, является не верным. На самом деле каждый из известных итеративных шифров после нескольких начальных циклов приходит к стационарным распределениям, повторяющим законы распределения (дифференциалов и смещений таблиц линейных аппроксимаций) случайной подстановки соответствующей степени и дальнейшее наращивание числа циклов шифрующих преобразований не изменяет стационарного распределения [11,12]. В нашей работе [4] приводится теоретическое доказательство этого факта. Поэтому утверждение теоремы 3 во-первых, противоречит вроде бы де признанному многими факту о приходе Марковского шифра к стационарному состоянию, а во-вторых, – в соответствии с приведенными выше и другими имеющимися результатами стационарное состояние шифра соответствует характеристикам случайной подстановки, а для случайной подстановки законы распределения переходов XOR таблиц и смещений таблиц линейных аппроксимаций являются явно не равномерными.

ВЫВОДЫ

1. Как установлено, все итеративные шифры (а они все Марковские) имеют асимптотические значения максимальных значений дифференциалов и линейных корпусов, совпадающие со значениями максимумов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок соответствующей степени.

2. Все Марковские шифры подчиняются закону произведения подстановочных преобразований, в соответствии с которым произведение одноцикловых преобразований после небольшого начального числа их повторений приобретает свойства случайной подстановки соответствующей степени независимо от показателей случайности исходного одноциклового преобразования.

3. Для Марковских шифров асимптотическое значение максимума полных дифференциалов (также как и значение максимума смещений линейных корпусов) почти для всех ключей является одним и тем же, что позволяет при оценке показателей доказуемой стойкости шифров определять асимптотические значения максимумов дифференциальной и линейной вероятности для одного произвольно взятого ключа (или в безключевом варианте).

4. Стационарность распределения переходов таблицы полных дифференциалов также как стационарность смещений линейных корпусов обозначает, что с увеличением числа циклов шифрования эти распределения сохраняются (не меняются).

Литература

[1] *Лисицкая И.В.* Блочные симметричные шифры и Марковские процессы. / И.В. Лисицкая, В.И. Долгов // Прикладная радиоэлектроника, 2012. – Т. 11, № 2. – С. 12-18.

[2] *F. Sano, K. Ohkuma, H. Shimizu, S. Kawamura.* On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis/ IEICE Trans. Fundamentals, vol. E86-a, NO.1 January 2003, pp. 37-46.

[3] *Долгов В.И.* Новая методика оценки двухциклового дифференциала уменьшенной версии супер блока AES. / В.И. Долгов, И.В. Лисицкая, В. А. Феськов, К.Е. Лисицкий // Сборник трудов Второй Международной научно-технической конференции «Компьютерные науки и технологии», 8-10 октября 2011, Белгород, С. – 418-422.

[4] *Горбенко І.Д.* Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа. / І.Д. Горбенко, В.И. Долгов, И.В. Лисицкая, Р.В. Олейников // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 212-320.

[5] *Лисицкая И.В.* Большие шифры – случайные подстановки / И.В. Лисицкая, А.А. Настенко // Межведомственный научн. технический сборник «Радиотехника». 2011. вып. 166. – С. 50-55.6.

[6] *Кузнецов А.А.* Линейные свойства блочных симметричных шифров, представленных на украинский конкурс. / А.А. Кузнецов, И.В. Лисицкая, С.А. Исаев // Прикладная радиоэлектроника, 2011. – Т. 10, № 2. – С. 135-140.

[7] *Лисицкая И.В.* Об участии S-блоков в формировании максимальных значений дифференциальных вероятностей блочных симметричных шифров. / Лисицкая И.В., Казимиров А.В. // Proceedings International Conference SAIT 2011, Kyiv, Ukraine, May 23-28, 2011, c. 459.

[8] *Лисицкая И.В.* О новой методике оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа. Системы обработки информации. - Харьковский университет Противовоздушных Сил имени Ивана Кожедуба, – 2011. – Вып. 4(94). – С. 167-173.

[9] *X. Lai, J. Massey, and S. Murphy,* Markov ciphers and differentjal cryptanalysis, Advances in Cryptalogy – EUROCRYPT'93, LNCS 547, Springer-Verlag, pp. 17-38, 1991.

[10] *Joan Daemen, Vincent Rijmen* Probability distributions of Correlation and Differentials in Block Ciphers. / Joan Daemen, Vincent Rijmen // April 13, 2006, pp. 1–38.

[11] *Олейников Р.В.* Дифференциальные свойства подстановок / Р.В. Олейников, О.И. Олешко, К.Е. Лисицкий, А.Д. Тевяшев // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 326-333.

[12] *Долгов В.И.* Свойства таблиц линейных аппроксимаций случайных подстановок. / В.И. Долгов, И.В. Лисицкая, О.И. Олешко // Прикладная радиоэлектроника. – Харьков: ХНУРЭ. – 2010. – Т. 9 – № 3, С. 334-340.

Поступила в редколлегию 5.03.2012

Лисицкая Ирина Викторовна, фото и сведения об авторе см. на с. 143.

Долгов Виктор Иванович, фото и сведения об авторе см. на с. 143.

Настенко Андрей Александрович, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: криптографическая защита информации.

Лисицкий Константин Евгеньевич, студент 3-го курса кафедры БИТ ХНУРЭ. Область научных интересов: криптографическая защита информации.

УДК 621. 391:519.2:519.7

Оцінки максимальних значень диференціалів та лінійних корпусів Марковських шифрів / В.І. Долгов, І.В. Лисицька, А.А. Настенко, К.Є. Лисицький // Прикладна радіоелектроніка: наук.-техн. журнал. – 2012. – Том 11. № 2. – С. 144–151.

Представляється короткий аналіз сутності відомих підходів до оцінки показників доказової стійкості Марківських блокових симетричних шифрів до атак диференціального та лінійного криптоаналізу. Викладається сутність нової методології оцінки доказової стійкості БСШ до атак диференціального та лінійного криптоаналізу. Наводяться результати оцінки максимальних значень диференціалів та лінійних корпусів Марківських шифрів. Виконується обгрунтування процесу переходу шифрів до стаціонарного стану. Формулюється нова редакція гіпотези статистичної еквівалентності. Уточнюються деякі положення теорії Марківських шифрів, що зустрічаються в публікаціях.

Ключові слова: Марківський шифр, диференціальна ймовірність, лінійна ймовірність, нова методологія оцінки доказової стійкості, стаціонарний стан властивий випадковій підстановці.

Табл. 06. Бібліогр. 12 найм.

UDC 621. 391:519.2:519.7

Estimations of Maximal Values of Differentials and Linear Hulls of Markov Ciphers / V.I. Dolgov, I.V. Lysytska, A.A. Nastenko, K.E. Lysytskiy // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 144–151.

The paper provides a brief analysis of the essence of the known approaches to assessing indicators of provable security of Markov block symmetric ciphers (BSC) to attacks of differential and linear cryptanalysis as well as it describes the essence of the new assessment methodology of BSC demonstrable resistance to the attacks of differential and linear cryptanalysis. The results of evaluating the maximum values of the differentials and linear hulls of Markov ciphers are given. A grounding of the process of BSC transition to the stationary state is performed. A new version of the statistical equivalence hypothesis is formulated. Some points of the theory of Markov ciphers, found in the literature, are particularized.

Keywords: Markov cipher, differential probability, linear probability, new methodology for estimating provable security, steady state characteristic of random substitution.

Tab. 06. Ref. 12 items.