МЕТОДЫ И СРЕДСТВА АНАЛИЗА И СИНТЕЗА БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

УДК 681.3.06

НОВАЯ ИДЕОЛОГИЯ ОЦЕНКИ СТОЙКОСТИ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ К АТАКАМ ДИФФЕРЕНЦИАЛЬНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА

И.Д. ГОРБЕНКО, В.И. ДОЛГОВ, И.В. ЛИСИЦКАЯ, Р.В. ОЛЕЙНИКОВ

Предлагается подход к оценке безопасности блочных шифров, ориентированный, с одной стороны, на использование при определении ожидаемых показателей стойкости больших шифров результатов анализа показателей уменьшенных их версий, а с другой, на использование 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.

Ключевые слова: дифференциальный и линейный криптоанализ, показатели стойкости к атакам линейного и дифференциального криптоанализа, свойства случайных подстановок и шифрующих преобразований.

ВВЕДЕНИЕ

Последнее время появился ряд публикаций, в которых обсуждаются подходы к построению (получению) оценок доказуемой безопасности блочных симметричных шифров (БСШ) к атакам дифференциального и линейного криптоанализа [1-5 и др.].

Мы здесь кратко напомним результаты некоторых известных работ, относящихся к оценкам стойкости БСШ к атакам дифференциального и линейного криптоанализа.

В [1] изучается подстановочно-перестановочная схема (SPN), на которой строится AES. Вводится AES* – SPN шифр, идентичный AES за исключением того, что фиксированные S-блоки заменены случайными и независимыми перестановками. Доказывается, что эта конструкция сопротивляется линейному и дифференциальному криптоанализу начиная с 4-х внутренних циклов, несмотря на огромный совокупный эффект многопутевых характеристик, которые порождены симметрией AES. Показывается, что дифференциальная и линейная вероятности (*DP* и *LP* условия) обе стремятся к значению $1/(2^{128}-1)$ очень быстро с ростом числа циклов. Подчеркивается, что результат подтверждает предположение исследователей Keliher, Meijer и Tavares.

В [2] Keliher и др. представили новый метод определения верхней границы максимума средней вероятности линейного корпуса (*MALHP*) для SPN шифров – значения, которое позволяет, как считают они, обосновать утверждение о доказуемой безопасности к атакам линейного криптоанализа. Применение этого метода к Rijndael-ю (AES) с 7-ю и более циклами обеспечивает верхнюю границу $UB = 2^{-75}$, соответствующая нижняя граница сложности данных есть $\frac{32}{UB} = 2^{80}$ (для 96,7% отношения успеха).

В [3] улучшается эта верхняя граница для Rijndael-я на основе рассмотрения значений распределения линейных вероятностей для (уникального) S-блока Rijndael-я. Получена верхняя граница для *MALHP*. Для Rijndael-я с 9 циклами дается значение 2^{-92}, соответствующее нижней границе сложности данных 2^{97} (снова для 96,7% отношения успеха). (После проведения 43% вычислений, авторы полагают, что полученное значение уже стабилизировалось).

В [4] определены аналитические верхние оценки средних вероятностей дифференциальных и линейных характеристик блочных шифров, построенных по схеме шифра «Калина-128». В частности, в работе приводятся такие оценки для отмеченных показателей: $EDP \le 2^{-130}$, $ELP \le 2^{-130}$. Авторы относят эти оценки к показателям практической стойкости шифра.

В [5] расширяется теорема Хонга и др., которая дает верхние границы для максимумов средних вероятностей дифференциалов и линейных корпусов (*MADP* и *MALHP*), на SPN блоковых шифров с оптимальными или квазиоптимальными диффузионными слоями для случая вложенных SPN (NSPN) структур. Применение расширенной теоремы для двух NSPN шифров Hierocrypt-3 со 128-битными блоками и Hierocrypt-L1 с 64-битными блоками позволило авторам получить оценки для *MADP* и *MALHP* для 2-х циклового Hierocrypt-3 приводящие к границе 2^{-96} и для Hierocrypt-L1 с двумя циклами к границе 2^{-48}. Расширенная теорема была применена также для AES и позволила утановить, что *MADP* и *MALHP* для 4-х цикловой уменьшенной модели ограничены значением 2^{-96}. Этот результат, отмечают авторы, превосходит лучший предыдущий результат 2^{-92} для 10-ти циклов Keliher-а и др. Результат опять связывается с дифференциальными

и линейными свойствами входящих в шифр S-блоков и числом ветвлений.

Можно привести и много других работ, посвященных оценке показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа.

Первый вывод, который можно сделать из приведенных результатов, состоит в том, что оценки соответствующих показателей отличаются в значительных пределах. Второй вывод состоит в том, что результирующие показатели стойкости шифров практически во всех работах связываются с соответствующими криптографическими показателями, входящих в шифры S блоковых конструкций.

Следует заметить, что сам термин доказуемая безопасность уже давно введен в криптографии. Когда говорят о доказуемой Безопасности ("Provable" Security), отмечается в документе [6], то обычно имеют в виду одно из двух.

Во-первых, если можно показать, что взлом шифра является таким же трудным, как решение некоторой хорошо известной трудной проблемы (например, дискретного логарифмирования или факторизации), то шифр считается доказуемо безопасным. Здесь, конечно, есть рассогласование (ввод в заблуждение), так как трудная проблема, к которой сводятся рассуждения, обычно не доказуемо трудная. Это подход имеет отношение к фундаментальному открытому вопросу в компьютерной науке, являются ли трудные проблемы P или NP полными задачами? Фактически, доказуемая безопасность требует доказательства, что $P \neq NP$, и существования односторонних функций, которые в одну ″сторону″ являются трудными для вычисления *в среднем* (в вероятностном смысле), но в другую могут быть решены быстро при наличии некоторой экстра информации. Заметим, что меры сложности здесь *асимптотические* – уровень сложности оценивается через входной размер в битах на бесконечности. Отмечается, что стратегия отнесения задач оценки стойкости криптосистем к тяжелым проблемам очень полезна для практического анализа шифров, хотя эту модель изначально относили к криптосистемам с открытым ключом.

Во-вторых, шифр может показывать доказуемую безопасность против целого набора атак. Тем не менее, это, очевидно, не означает, что шифр безопасный против всех атак.

Начиная с работы K. Нюберг и Л. Кнудсена [7] для обозначения свойства блочного шифра иметь достаточно малую дифференциальную вероятность, тоже начали использовать понятие доказуемой безопасности (″Provable security″) к атакам дифференциального криптоанализа. В последующих публикациях [8 и др.] аналогичное понятие появилось для определения стойкости шифров и к атакам линейного криптоанализа.

На наш взгляд, однако, более адекватным для блочных шифров следует считать понятие практической безопасности (Practical Security) [6]. В этой модели блочный шифр считается вычислительно безопасным, если наилучшая из известных атак требует слишком много ресурсов из допустимого запаса. Это очень практичная модель, так как всегда можно протестировать шифр на устойчивость к различным известным атакам, изучая его слабости, а затем дать оценку устойчивости шифра к таким атакам с точки зрения необходимых ресурсов времени/пространства. Она позволяет получить большинство ответов, и большинство анализов, встречающихся в литературе, в том числе и на прошедших конкурсах AES и NESSIE было именно этого типа. Конечно, и в этом случае полученные результаты опять ничего не говорят об уровне безопасности по отношению ко все еще неизвестным атакам. Заключая этот небольшой анализ подходов к оценке безопасности шифров, можно отметить, что их авторы, по-видимому, под доказуемой безопасностью имели в виду то, что полученный ими результат можно считать надежно обоснованным. В этой редакции с ними можно согласиться.

В этой работе мы хотим высказать свою точку зрения по вопросу оценки безопасности блочных шифров, концептуально отличающуюся от известных, хотя в конечном итоге речь опять будет идти об определении максимальных значений полных дифференциалов и линейных корпусов (оболочек) БСШ.

Прежде всего, хотелось бы отметить, что все существующие подходы к оценке показателей стойкости БСШ опираются скорее на интуитивные соображения, подкрепленные результатами анализа под определенным углом зрения (субъективного) уменьшенных по числу циклов или упрощенных версий рассматриваемых БСШ. И это многим исследователям представляется вполне оправданным, так как полный анализ современного шифра при реальной длине битового размера входа является сегодня невыполнимой задачей. Собственно говоря, разработчики шифров и идут по пути увеличения размеров битового входа именно для того, чтобы сделать, по крайней мере, задачу полного перебора ключей или текстов не реализуемой в обозримом будущем. Поэтому многие подходы к оценке показателей стойкости больших шифров строятся скорее на основе накопленного опыта и некоторых соображений и оценок, позволяющих получить аргументы и данные для подтверждения предполагаемых высоких показателей стойкости предлагаемых решений. По этому пути пошли и разработчики шифра Rijendael. Они действительно предложили достаточно прозрачную для понимания и анализа конструкцию шифрующего преобразования, строящуюся на реализации популярной теперь стратегии широкого следа и допускающую достаточно убедительное прогнозирование ожидаемых показателей стойкости.

Конечно же, стратегия широкого следа не является открытием или новым словом в криптографии. Она по существу является реализацией классической стратегии перемешивания и перепутывания, обоснованной еще в работе К. Шеннона. Более того, общую идею практической реализации этой стратегии для SPN шифров уже давно (в 1973 году) продемонстрировал в своей работе [9] Х. Фейстель, своеобразно реализовавший ее затем и в шифре DES. Тем не менее, нужно отдать должное разработчикам Rijendael-я – их линейное преобразование оказалось существенно более эффективным (судя по данным экспериментов почти в два раза) по сравнению с простым (регулярным) перемешиванием (переключением) выходов и входов между слоями преобразований, как это сделано в решении Х. Фейстеля. Стремясь реализовать максимально возможные показатели преобразования по стойкости, они постарались использовать в своей конструкции и S-блоки с предельными дифференциальными и линейными показателями, даже допустив регулярность (алгебраичность) в построении нелинейных преобразований. В целом же простота и прозрачность их конструкции обеспечивается в основном за счет того, что они фактически повторили классическую схему SPN шифра, описанного Х. Фейстелем.

Интуиция их, правда, подвела при выборе конструкции S блоков. Они посчитали, что показатели S блоков оказывают решающее влияние на итоговые показатели стойкости шифра. На самом деле, как мы покажем, это не так и, соответственно, действительные показатели стойкости к атакам дифференциального и линейного криптоанализа будут несколько иными.

Излагаемые далее соображения и результаты строятся исходя из развитого нами нового подхода в теории и методах криптоанализа [10], ориентированного, 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.

Итак, для преодоления трудностей анализа полномасштабных моделей (алгоритмов) шифрования мы пошли по пути разработки и исследования уменьшенных моделей прототипов, для которых имеющихся вычислительных ресурсов оказывается уже вполне достаточно [10]. Наши проработки показывают, что большое число хорошо известных алгоритмов шифрования допускают масштабирование. Удается построить уменьшенные модели, которые сохраняют все свойства своих прототипов и позволяют решить многие задачи анализа и сравнения по показателям стойкости соответствующих больших версий.

Самый главный и неожиданный результат изучения уменьшенных моделей состоит в том, что общепринятая точка зрения, разрабатываемая во многих работах и состоящая в том, что линейные и дифференциальные свойства шифров непосредственно связаны со свойствами S-блоков, используемых при их построении, оказалась не верной или не совсем верной. На самом деле результирующие (т.е. получающиеся при использовании полного набора цикловых преобразований) показатели стойкости шифров определяются для большого числа вариантов выбора S блоков практически только размером битового входа в шифр.

Второй важный вывод, следующий из выполненных исследований, сводится к тому, что показатели стойкости больших (полных реализаций) шифров к атакам дифференциального и линейного криптоанализа (таких, как Rijndael и многих других известных шифров, а также шифров Лабиринт, Калина, Мухомор, ADE [11,12,13,14], представленных на украинский конкурс по выбору национального стандарта шифрования), могут быть получены расчетным путем.

В этой работе мы представляем некоторые из результатов проведенных исследований в развиваемом направлении и их интерпретацию в теоретическом и практическом понимании с наших позиций.

1. ПОНЯТИЙНЫЙ АППАРАТ ЛИНЕЙНОГО И ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА

Напомним кратко основной понятийный аппарат линейного и дифференциального криптоанализа. Следуя работе [14], введем ряд определений.

Определение 1 (Дифференциальная и Линейная вероятность)**:** *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*

$$DP^f(\Delta x \to \Delta y) = \frac{\#\{x \in GF(2)^n \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^n}, \quad (1)$$

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

где Δx *и* Δy *являются входным и выходным различием (разностью), а* Γx *и* Γy *входной и выходной масками;* $x\,\Gamma x$ *обозначает результат побитного произведения* x *и* Γx.

Определение 2 ($DP^f_{\max}$ и $DL^f_{\max}$)**:** *Максимальное значение дифференциальной и линейной вероятности для ключезависимой функции* f *определяется соответственно как*

$$DP^f_{\max} = \max_{\Delta x \neq 0,\ \Delta y} DP^f(\Delta x \to \Delta y), \quad (3)$$

$$DL^f_{\max} = \max_{x,\ y \neq 0} DL^f(\ y \to\ x). \quad (4)$$

В общем случае, ключезависимая функция f является сильной, если значения $DP^f_{\max}$ и $DL^f_{\max}$ функции f являются достаточно малыми [14].

Нас в дальнейшем и будут интересовать значения $DP^f_{\max}$ и $DL^f_{\max}$ для случаев, когда в качестве функции f выступают цикловые преобразования и последовательности цикловых преобразований итеративных шифров (ключезависимые функции), а также подстановочные преобразования (неключезависимые функции).

Пусть π – подстановочная таблица с n-битными входами и n-битными выходами. В [8] доказана лемма 1

Лемма 1. *Для любого преобразования* π: $Z_2^n \to Z_2^n$

$$\sum_{\Delta y \in Y} DP^{\pi}(\Delta x \to \Delta y) = 1, \quad (5)$$

$$\sum_{x \in X} LP^{\pi}(\ x \to\ y) = 1. \quad (6)$$

И, более того, *если* π *– подстановка, то*

$$\sum_{\Delta x \in X} DP^{\pi}(\Delta x \to \Delta y) = 1, \quad (7)$$

$$\sum_{y \in Y} LP^{\pi}(\ x \to\ y) = 1. \quad (8)$$

Эти результаты представляются достаточно очевидными, исходя из определений (1) и (2), примененных к подстановкам (неключезависимым преобразованиям). Они являются отражением известных фактов, заключающихся в том, что суммы ячеек таблицы XOR разностей и суммы квадратов ячеек таблиц линейных аппроксимаций подстановок по строкам и по столбцам равны 2^n и $\left(2^{n-1}\right)^2$ соответственно, где n – битовый размер входа и выхода подстановки порядка 2^n. Важным для дальнейшего является понятие случайной подстановки. Мы на нем остановимся отдельно.

2. СЛУЧАЙНЫЕ ПОДСТАНОВКИ

Напомним, что ранее в нашей работе [15] понятие случайной подстановки было определено следующим образом.

Определение 1. *Под случайной* (*квазислучайной*) *подстановкой понимается подстановка, которая удовлетворяет одновременно трем критериям случайности:*

1. *Число инверсий* η_n *в подстановке степени* n *приблизительно равно числу "антиинверсий", а практически, если*

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

2. *Число циклов* ξ_n *в подстановке степени* n *близко к* $\ln n$, *а практически, находится в границах*

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

3. *Число возрастаний* θ_n *в подстановке степени* n *приблизительно равно числу убываний, а практически*

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

В этих соотношениях a – параметр, выбираемый в значительной степени из субъективных соображений (по крайней мере, из условия, что множество допустимых подстановок не станет меньше некоторого практически целесообразного числа). В наших предложениях использовалось значение $a = 1$. Остается заметить, что из полного множества подстановок порядка 2^n в этом случае приведенные критерии отбора проходят 53% всех подстановок.

В последующих наших публикациях [16, 18], посвященных исследованию дифференциальных и линейных свойств случайных подстановок и подстановочных преобразований, развивающих результаты работ Luka O'Connor-a [17, 19], мы определили еще два условия, которым подчиняются случайные подстановки. Они основываются на двух утверждениях. Напомним здесь их, так как они являются важными для дальнейшего.

В обозначениях работы [16] пусть $\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right)$ будет вероятностью того, что значение ячейки дифференциальной таблицы случайно взятой подстановки π порядка 2^n для перехода входной разности ΔX в соответствующую выходную разность ΔY будет равно $2k$. Эта вероятность определяется теоремой.

Утверждение 1. *Для любых ненулевых фиксированных* ΔX, $\Delta Y \in Z_2^n$ *в предположении, что подстановка* π *выбрана равновероятно из множества* S_2^n *и* $0 \le k \le 2^{n-1}$,

$$\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right) = \left(\begin{matrix} 2^{n-1} \\ k \end{matrix}\right)^2 \cdot \frac{k! \cdot 2^k \cdot \Phi(2^{n-1} - k)}{2^n!}, \quad (9)$$

где функция $\Phi(d)$ определяется выражением

$$\Phi(d) = \sum_{i=0}^{d} (-1)^i \cdot \left(\begin{matrix} d \\ i \end{matrix}\right)^2 \cdot 2^i \cdot i! \cdot (2d - 2i)!. \quad (10)$$

Закон распределения вероятностей (9) получен для полного множества подстановок, однако замечательным его свойством является то, что он оказывается справедливым и для усеченного (причем, существенно) множества подстановок, формируемых симметричными шифрами. Такие преобразования, осуществляемые на различных ключах зашифрования, формируют множество подстановок случайного типа (это основное свойство, к которому стремятся разработчики

при построении шифра). Об этом свидетельствуют и многочисленные результаты экспериментов. И это еще не все! Получается, что для множества подстановок, определяемых шифрующими преобразованиями, выполняется свойство, напоминающее эргодическое свойство случайных процессов (среднее по множеству реализаций совпадает со средним по времени для одной достаточно длинной реализации [20]). Это свойство проявляется в том, что закон распределения (9), полученный на основе анализа всего множества $2^n!$ равновероятных подстановок, является справедливым и для множества ячеек таблицы XOR разностей каждой отдельно взятой случайной подстановки степени 2^n.

Подтверждением этого факта является то, что для закона вероятностей $\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k)$, рассматриваемого применительно к отдельной подстановке, с высокой точностью выполняется условие нормировки, характерное для полной группы событий

$$\sum_{k=0}^{k^*}\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k)=1. \qquad (11)$$

Здесь $\Lambda_\pi(\Delta X,\Delta Y)$ – значение XOR таблицы (её ячейки) для пары значений разностей входов и выходов $\Delta X,\Delta Y\in Z_2^m$, $\Delta X=X+X'$, $\Delta Y=\pi(X)+\pi(X')$ подстановки $\pi\in S_2^m$. Значение k^* представляет собой половину от максимального числа переходов XOR таблицы случайной подстановки (фактически соотношение (11) – это обобщение свойств (5)-(8)). Выполненные многочисленные проверки подтверждает и это положение.

Совершенно аналогичное по содержанию утверждение, справедливо для вероятности значений линейных аппроксимационных таблиц $LAT_\pi^*(\alpha,\beta)$ случайных подстановок [19, 21].

Утверждение 2. *Пусть* $\lambda^*(\alpha,\beta)$ *будет случайным значением распределения* $LAT_\pi^*(\alpha,\beta)=\left|LAT_\pi(\alpha,\beta)-2^{n-1}\right|$, *когда подстановка* π *выбрана равновероятно из множества* 2^n *и маски* α,β *не нулевые. Тогда* $\lambda^*(\alpha,\beta)$ *принимает только четные значения и*

$$\Pr(\lambda^*(\alpha,\beta)=2k)=\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\begin{pmatrix}2^{n-1}\\ 2^{n-2}+|k|\end{pmatrix} \qquad (12)$$

для $|k|\le 2^{n-2}$.

И для этого распределения справедлива нормировка

$$\sum_{k=0}^{k^*}\Pr(\lambda^*(\alpha,\beta)=2k^*)=1. \qquad (13)$$

Здесь k^* – половинное значение максимального для таблицы $LAT_\pi^*(\alpha,\beta)$ смещения.

Более того, можно убедиться, что для распределения (12) справедлива и нормировка (8), которая в этом случае записывается в виде

$$\frac{2^n-1}{\left(2^{n-1}\right)^2}\cdot\sum_{k=-2^{n-1}}^{2^{n-1}}\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\begin{pmatrix}2^{n-1}\\ 2^{n-2}+|k|\end{pmatrix}^2=1. \qquad (14)$$

На основе изложенных результатов представляется логичным в дополнение к уже известным подходам сформировать (сформулировать) новое (или уточненное) определение случайной подстановки, что и сделано в работе [23]. Мы здесь его напомним.

Определение 2. *Подстановка является случайной, если вместе с выполнением трех критериев случайности, предложенных в работе* [24], *для ячеек её XOR таблицы и таблицы линейных аппроксимаций выполняются законы распределения вероятностей* (9) (*критерий случайности* 4) *и* (12) (*критерий случайности* 5).

3. ШИФРУЮЩИЕ ПРЕОБРАЗОВАНИЯ КАК СЛУЧАЙНЫЕ ПОДСТАНОВКИ

Самый важный вывод работ [15] и [17] состоит в том, что приведенные выше критерии случайности подстановок выполняются и для шифрующих преобразований всех современных блочных симметричных шифров, рассматриваемых как подстановочные преобразования.

Само по себе отдельное шифрующее преобразование (отдельный цикл) не является случайной подстановкой, так как для него не выполняются законы распределения вероятностей (9) и (12). Оно не укладывается в рамки случайных подстановок и по инверсиям, и по возрастаниям, и по циклам (хотя бы потому, что имеются множества входов в подстановку, которые влияют не на все значения выходов). Однако при реализации механизмов перемешивания (линейных преобразований), используемых в каждом цикле, последовательность шифрующих преобразований приобретает свойства случайной подстановки (к чему как раз и стремятся все разработчики шифров). Этот, казалось бы, тривиальный вывод остался не замеченным разработчиками шифров и криптоаналитиками при формировании оценок показателей стойкости шифров к атакам дифференциального и линейного криптоанализа (они не могли правильно интерпретировать результаты, так как были связаны полномасштабными версиями шифров, не поддающимися вычислительным экспериментам). Как уже отмечалось выше, во всех известных работах показатели многоцикловых преобразований (стойкость к атакам дифференциального и линейного криптоанализа) непосредственно связывались и связываются с соответствующими показателями S-блоковых конструкций, используемых в качестве нелинейных преобразований каждой цикловой функции.

Наша позиция состоит в том, что итоговые (асимптотические) показатели стойкости (максимумы полных дифференциалов таблиц XOR разностей последовательностей шифрующих преобразований также как и максимумы линейных аппроксимационных таблиц этих же преобразова-

ний) зависят только от числа циклов шифрующего преобразования и размера его битового входа.

Зафиксируем этот вывод в виде утверждения.

Утверждение 3. *Для каждого блочного симметричного шифра* (*из числа известных итеративных БСШ*) *существует вполне определенное число циклов, после которого шифр приобретает свойства случайной подстановки. Дальнейшее наращивание числа циклов не влияет на итоговые дифференциальные и линейные свойства шифра. Это значение является одним и тем же для всех шифрующих преобразований с одинаковым битовым размером входа.*

Можно отметить, что это утверждение в первой части представляется в известном смысле достаточно очевидным в том смысле, что каждый реальный шифр строится так, чтобы набор его цикловых преобразований в той или иной мере обладал свойствами случайной подстановки. При нашем подходе это свойство определяется как промежуточный результат, переходящий в асимптотическое значение одинаковое для всех шифров (с одинаковым битовым размером входа), поддающийся расчету.

Нас в дальнейшем будет интересовать именно момент (число циклов), начиная с которого шифрующее преобразование становится случайной подстановкой. Именно в этом направлении мы и будем строить доказательство (обоснование) представленного утверждения.

Продемонстрируем справедливость этого утверждения на примере рассмотрения дифференциальных показателей шифра-подстановки. В качестве одного из таких показателей в нашем случае будет выступать максимальное значение полного дифференциала.

Мы начнем доказательство этого утверждения (скорее не доказательство, а объяснение его правомерности) с конца, т.е. предположим, что БСШ имеет некоторое определенное число циклов, после которых шифр становится случайной подстановкой, т.е. обладает законом распределения вероятностей переходов разностей (9).

Покажем, что дальнейшее наращивание числа циклов не влияет на итоговые дифференциальные свойства этого шифра.

Важно сразу отметить, что особенностью случайной подстановки, удовлетворяющей критерию 4, является то, что мы имеем дело не с фиксированным распределением переходов разностей $\Delta x \to \Delta y$ (закрепленным распределением значений входов (ячеек) таблицы XOR разностей), а со случайным. Таблица XOR разностей случайной подстановки определяется тем, что для нее является фиксированным число ячеек каждого типа, определяемых с помощью закона распределения $\Pr\left(\Lambda_f(\Delta x,\Delta y)=2k\right)$ в виде [15]

$$\Lambda_{m,2k} = (2^m-1)^2 \cdot \Pr(\Lambda_f(\Delta x,\Delta y) = \\ = \frac{(2^m-1)^2}{2^m!}\cdot\begin{pmatrix}2^{m-1}\\ k\end{pmatrix}^2 \cdot k!\cdot 2^k \cdot \Phi(2^{m-1}-k). \qquad (15)$$

В соответствии с этим соотношением таблица XOR разностей случайной подстановки имеет λ_0 ячеек, имеющих значение $\Lambda_{m,0}$, λ_1 ячеек, имеющих значение $\Lambda_{m,2}$, λ_2 ячеек, имеющих значение $\Lambda_{m,4}$, и т.д., – $\lambda_{k_f^*}$ ячеек, имеющих значение $\Lambda_{m,2k^*}$. Все эти значения вместе дают общее число ненулевых входов (ячеек) в подматрицу таблицы XOR разностей равное $2^{n-1}\times 2^{n-1}$, причем сами числа $\lambda_0, \lambda_1, \lambda_2, \ldots, \lambda_{k_f^*}$ определяются однозначно из (15).

Поэтому применительно к шифрующим многоцикловым преобразованиям – случайным подстановкам, – дифференциальные вероятности DP^f должны теперь интерпретироваться в обозначениях подстановочных преобразований для ключезависимой функции f не как фиксированные, а как случайные значения, принимаемые на множестве ключей зашифрования (на множестве подстановок)

$$DP^f(\Delta x,\Delta y) = DP^f(\Delta x \to \Delta y) = \\ = \Pr\left(\Lambda_f(\Delta x,\Delta y)=2k\right) \to \qquad (16) \\ \to\ DP^f\left(\Lambda_f(\Delta x,\Delta y)=2k\right),$$

причем эти вероятности следует считать одинаковыми для всех ячеек таблицы дифференциальных разностей (для всех вариантов фиксированных сочетаний входных и выходных разностей).

Возвратимся к нашей задаче. Итак, пусть r-цикловое шифрующее преобразование (последовательность r-цикловых преобразований) f_r с n-битным размером входа (и выхода) обладает свойством 4, т.е. закон распределения $DP^{f_r}(\Delta x,\Delta y)$ переходов входных разностей Δx в выходные разности Δy имеет вид (9) с нормировкой

$$\sum_{k=0}^{k^*} DP^{f_r}\left(\Lambda_f(\Delta x,\Delta y)=2k\right)=1.$$

Тогда, если на входы очередного циклового преобразования (подстановки) поступают некоторые сочетания пар выходов предшествующего преобразования случайного типа (предшествующей случайной подстановки) подчиняющиеся закону распределения XOR разностей таблицы полных дифференциалов (9), то цикловое преобразование может осуществить лишь переименование выходов и соответствующих им разностей, оставляя результирующий закон распределения разностей неизменным (для операции XOR подстановка вместе с последующим или предыдущим линейным цикловым преобразованием являются детерминированными преобразованиями и произведение случайной в оговоренном смысле подстановки на любую другую подстановку, является случайной подстановкой). Приведем математическое обоснование этого факта (который подтверждается многочисленными экспериментами с малыми шифрами).

Нас интересует закон распределения вероятностей $DP^{f_{r+1}}(\Delta x,\Delta z)$ для $r+1$ цикла преобразований (здесь удобнее будет перейти к компактной

форме записи, введенной ранее), где Δz является выходной разностью $r+1$-но циклового преобразования. У нас имеется цепочка $\Delta x \to \Delta y \to \Delta z$ разностей, совместный закон распределения вероятностей для которой обозначим:

$$DP^{f_{r+1}}(\Delta x, \Delta y, \Delta z) = DP^{f_{r+1}}(\Delta x \to \Delta y \to \Delta z).$$

В соответствии с формулой умножения вероятностей можем записать представление для этой вероятности в виде:

$$DP^{f_{r+1}}(\Delta x, \Delta y, \Delta z) =$$
$$= DP^{f_r}(\Delta x, \Delta y) DP^{f_1}(\Delta z / \Delta x, \Delta y).$$

Тогда дифференциальная вероятность $DP^{f_{r+1}}(\Delta x, \Delta z)$ для $r+1$-но циклового преобразования может быть определена из совместной вероятности $DP^{f_{r+1}}(\Delta x, \Delta y, \Delta z)$ путем ее усреднения по множеству промежуточных значений $\Delta y \in Z_2^n$, т.е.

$$DP^{f_{r+1}}(\Delta x, \Delta z) =$$
$$= \sum_{\Delta y \in Z_{2^n}} DP^{f_r}(\Delta x, \Delta y) DP^{f_1}(\Delta z / \Delta x, \Delta y).$$

Но в нашем случае закон распределения $DP^{f_r}(\Delta x, \Delta y) = \Pr\left(\Lambda_f(\Delta x, \Delta y) = 2k\right)$ является одним и тем же для каждой выходной разности r-циклового преобразования (для каждой ячейки таблицы дифференциальных разностей случайной подстановки), а поэтому

$$DP^{f_{r+1}}(\Delta x, \Delta z) =$$
$$= DP^{f_r}(\Delta x, \Delta y) \sum_{\Delta y \in Z_{2^n}} DP^{f_1}(\Delta z / \Delta x, \Delta y).$$

Очевидно далее, что при фиксированных значениях Δy выходные разности Δz не зависят от того, какие значения принимают входные разности Δx и, следовательно,

$$\sum_{\Delta y \in Z_{2^n}} DP^{f_1}(\Delta z / \Delta x, \Delta y) = \sum_{\Delta y \in Z_{2^n}} DP^{f_1}(\Delta z / \Delta y) =$$
$$= \sum_{\Delta y \in Z_{2^n}} DP^{f_1}(\Delta y \to \Delta z).$$

Но в соответствии с (5) для подстановочного одноциклового преобразования f_1

$$\sum_{\Delta y \in Y} DP^{f_1}(\Delta x, \Delta y) = \sum_{\Delta y \in Y} DP^{f_r}(\Delta x \to \Delta y) = 1,$$

и, в итоге, приходим к результату

$$DP^{f_{r+1}}(\Delta x, \Delta z) = DP^{f_r}(\Delta x, \Delta y) \Rightarrow$$
$$\Rightarrow DP^{f_{r+1}}(\Delta x \to \Delta z) = DP^{f_r}(\Delta x \to \Delta y),$$

где

$$DP^{f_r}(\Delta x \to \Delta y) = \Pr\left(\Lambda_f(\Delta x, \Delta y) = 2k\right).$$

Последнее и обозначает, что дополнительные цикловые преобразования уже не изменяют закона распределения разностей на выходе шифра.

Остается теперь прокомментировать первую часть утверждения. Для этого заметим, что эффективность перемешивания входного текста при зашифровании в криптографии оценивается такими параметрами статистической безопасности, как лавинный эффект, коэффициент сжатия, ряд корреляционных показателей [21].

Если рассматривать тонкую структуру циклового преобразования, то в самом начале процедуры зашифрования (в первом цикле) при применяемых при построении большинства шифров решений, как правило, не удается реализовать связь каждого выходного бита циклового преобразования с каждым входным битом. Например, биты входа влияют на вход только одного S-блока многоблочного нелинейного преобразования, а используемое последующее линейное преобразование не обладает полнотой в том смысле, что оно передает воздействие входа не на все выходы текущего преобразования. Для характеристики этого свойства разработчики шифра Rijndael ввели специальную характеристику – коэффициент ветвления, а сам механизм распространения активных битов в последовательных слоях (циклах) преобразований назвали стратегией широкого следа [22]. Но эту же стратегию пытались реализовать все разработчики известных шифров, хотя она была часто не такой эффективной, как, скажем, у Rijndael-я (умножение выходов нескольких S-блоков на матрицу МДР кода). С другой стороны, известны и более эффективные конструкции линейного слоя (например, в шифре Лабиринт, или в шифре управляемой подстановки [25]). Естественно, что если есть механизм расширения числа активных (задействованных) в ходе преобразования битов блока данных, то рано или поздно наступит момент, когда любой бит входа будет одинаково эффективно действовать на любой бит выхода. Этот момент как раз и будет обозначать, что шифрующее преобразование стало случайной подстановкой (результирующий закон распределения переходов разностей пар входов в соответствующие им разности пар выходов принимает вид (9)).

Совершенно аналогичные рассуждения могут быть приведены по отношению к линейным показателям многоцикловых итеративных процедур шифрующих преобразований.

4. РАСЧЕТНЫЕ СООТНОШЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ ПОКАЗАТЕЛЕЙ СТОЙКОСТИ К АТАКАМ ДИФФЕРЕНЦИАЛЬНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА

Расчетные соотношения для определения максимальных значений полных дифференциалов и максимальных значений линейных корпусов могут быть получены применением законов (9) и (14), справедливых для случайных подстановок, к шифрам, рассматриваемым как случайные подстановки, что и сделано в наших работах [16] и [18].

Как показано в работе [16], среднее значение максимума таблицы XOR разностей случайной подстановки порядка 2^n находится путем определения максимального значения $k = k_{\max}$, при котором выполняется соотношение

$$\frac{(2^n-1)^2}{2^n!}\cdot\binom{2^{n-1}}{k}^2\cdot k!\cdot 2^k\cdot\Phi(2^{n-1}-k)\approx 1. \quad (19)$$

Если это соотношение применить к шифру с n-битовым размером входа, то для интересующего нас максимального значения дифференциальной вероятности (максимальной вероятности полного дифференциала) $DP^f_{\max}$ можем записать выражение

$$DP^f_{\max}=\frac{k_{\max}}{2^n}. \quad (20)$$

В работе [16] также приведено расчетное соотношение, являющееся хорошей аппроксимацией соотношений (19) и (21)

$$DP^f_{\max}=\frac{n+4}{2^n}. \quad (21)$$

В работе [18] показано, что среднее значение максимума таблицы линейных аппроксимаций для случайной подстановки определяется аналогично предыдущему случаю путем нахождения значения k^*, являющегося целым решением (округлением в сторону ближайшего целого) уравнения

$$\frac{(2^n-1)^2\cdot\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+|k^*|}=1. \quad (22)$$

Соответственно для шифра с n-битовым размером входа максимальное значение линейной вероятности (максимальной вероятности линейного корпуса) $DL^f_{\max}$ представляется в виде

$$DP^f_{\max}=\left(\frac{k_{\max}}{2^{n-1}}\right)^2. \quad (23)$$

Приведем здесь также соотношение, полученное на основе обработки результатов вычислительных экспериментов, являющееся удобной заменой выполнению расчетов по соотношению (22)

$$DL^f_{\max}=\left(\frac{\left(\frac{3}{2}\right)^n}{2^{n-1}}\right)^2. \quad (24)$$

ЗАКЛЮЧЕНИЕ

На основе приведенных результатов и обоснований можно утверждать, что:

1. Современные блочные симметричные шифры (при полном наборе шифрующих многоцикловых преобразований) обладают свойствами случайных подстановок и для них справедливы законы распределения вероятностей для полных дифференциалов и линейных корпусов свойственные таблицам дифференциальных разностей и линейных аппроксимаций подстановок соответствующей степени (порядка) (9) и (12).

2. Максимальные значения полных дифференциалов и линейных корпусов для современных БСШ, определяющие по современным меркам показатели стойкости шифров к атакам дифференциального и линейного криптоанализа, могут быть получены расчетным путем. Они не зависят (при достаточном числе цикловых преобразований ни от свойств используемых в шифрах подстановочных конструкций, ни от методов введения в цикловые функции цикловых подключей, ни от способа построения расширяющего линейного преобразования цикловой функции, а являются функцией только размера битового входа в шифр (порядка подстановки).

3. Для оценки стойкости блочных симметричных шифров (с битовым размером входа равным n) к атакам дифференциального и линейного криптоанализа можно пользоваться простыми соотношениями (23) и (24).

Литература.

[1] Thomas Baignoires and Serge Vaudenay Proving the Security of AES Substitution-Permutation Network. http://lasecwww.epfl.ch. 2004. p. 16.

[2] Liam Keliher. Toward Provable Security Against Differential and Linear Cryptanalysis for Camellia and Related Ciphers, International Journal of Network Security, Vol.5, No.2, pp.167–175, Sept. 2007.

[3] *L. Keliher, H. Meier, and S. Tavares.* New method for upper bounding the maximum average linear hull prodadility for SPNs, Advances in Cryptology – EUROCRYPT 2001, LNCS 2045, Springer-Verlag, pp. 420-436, 2001.

[4] *L. Keliher, H. Meijer, and S. Tavares,* Improving the upper bound on the maximum average linear hull probability for Rijndael, Eighth Annual International Workshop on Selected Areas in Cryptography (SAC 2001), LNCS 2259, pp. 112-128, Springer-Verlag, 2001.

[5] *Алексийчук А.Н., Ковальчук Л.В., Скрыпник Е.В., Шевцов А.С.* Оценки практической стойкости блочного шифра "Калина" относительно методов разностного, линейного криптоанализа и относительно алгебраических атак, основанных на гомоморфизмах // Прикладная радиоэлектроника. – 2008. – Т.7. – №3. – С. 203-209.

[6] Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004— Version 0.15 (beta), Springer-Verlag.

[7] *K. Nyberg and L. Knudsen,* Provable security against differential cryptanalysis, Journal of Cruptology, vol.8, no.1,1995.

[8] *M. Matsui.* On a Structure of Block Ciphers with Provable Security against Differential and Lintar Cryptanalysis. IEICE TRANS. FUNDAMENTALS, Vol. E82–A, NO. 1 JANUARY 1999, p. 117-122.

[9] *H. Feistel,* Cryptography and computer privacy. Scientific American, 228(5): 15-23,1973.

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

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

[12] *Горбенко І.Д., Бондаренко М.Ф., Долгов В.И., Олійников Р.В., Руженцев В.І., Міхайленко М.С., Колесников П.О.* Перспективний блоковий симетричний шифр

"Мухомор" – основні положення та специфікація // Прикладная радиоэлектроника. – 2007. – Т. 6. – № 2. – С. 147-157.

[13] *Горбенко І. Д., Долгов В.І., Олійников Р.В., Руженцев В.І., Михайленко М.С., Горбенко Ю.І., Тоцкій О.С., Казьміна С.В.* Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікація // Прикладная радиоэлектроника. – 2007. – Т.6. – № 2. – С. 195-208.

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

[14] *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.

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

[16] *Олейников Р.В., Олешко О.И., Лисицкий К.Е.* Дифференциальные свойства случайных подстановок // Прикладная радиоэлектроника: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 326-333.

[17] *L.J. O'Connor.* On the Distribution of Characteristics in Bijective Mappings. Advances in Cryptology. EUROCRIPT 93, Lecture Notes in Computer Science, vol. 795, T. Hellesethed., Springer-Verlag, pages 360–370, 1994.

[18] *Долгов В.И., Лисицкая И.В., Олешко О.И.* Свойства таблиц линейных аппроксимаций случайных подстановок // Прикладная радиоэлектроника: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 334-340.

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

[20] *Вентцель Е.С.* Теория вероятностей. – М.: Наука, 1964. – 564 с.

[21] *Luke O'Connor.* On Linear Approximation Tables and Ciphers secure against Linear Cryptanalysis. Email: oconnor@dsts. Edu. au, 1995. (семь страниц).

[22] *Бронштейн И.Н., Семендяев К.А.* Справочник по математике для инженеров и учащихся вузов. Издво – М:. "Наука" 1980. – 976 с.

[23] *Долгов В.И., Лисицкая И.В., Лисицкий К.Е.* Случайные подстановки в криптографии. Доклад, представленный на конференцию. Кировоград, 2010.

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

[25] *Долгов В.И., Лисицкая И.В., Казимиров А.В.* Вариации на тему шифра Rijndael. // Прикладная радиоэлектроника: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 321-325.

Поступила в редколлегию 21.06.2010.

Горбенко Иван Дмитриевич, доктор технических наук, профессор, заведующий кафедрой БИТ ХНУРЭ, главный конструктор ЗАО «Институт информационных технологий». Область научных интересов: криптографические системы и протоколы, проектирование и разработка систем, комплексов и средств криптографической защиты информации.

Долгов Виктор Иванович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: математические методы защиты информации.

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

Олейников Роман Васильевич, кандидат технических наук, докторант кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.

УДК 681.3.06

Нова ідеологія оцінки стійкості блокових симетричних шифрів до атак диференційного і лінійного криптоаналізу / І.Д. Горбенко, В.І. Долгов, І.В. Лисицька, Р.В. Олійников // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 312-320.

Пропонується підхід до оцінки безпеки блокових шифрів, що орієнтується, з одного боку, на використання при визначенні очікуваних показників стійкості блокових шифрів результатів аналізу показників їх зменшених версій, а з іншого, на використання уточненої в останній час на основі дослідження властивостей та показників випадкових підстановок і зменшених моделей шифрів, які розглядаються як підстановочні перетворення, концепції (нової ідеології) визначення показників стійкості блокових шифрів до атак диференційного та лінійного криптоаналізу .

Ключові слова: диференційний і лінійний криптоаналіз, показники стійкості до атак лінійного і диференційного криптоаналіза, властивості випадкових підстановок і перетворень, що шифрують.

Бібліогр.: 25 найм.

UDC 681.3.06

A new ideology of evaluating block symmetric ciphers strength to differential and linear cryptanalysis attacks / I.D. Gorbenko, V.I. Dolgov, I.V. Lisitskaya, R.V. Oleinikov // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 312-320.

An approach to evaluating the security of block ciphers is suggested which, on the one hand, is oriented on the use of the results of analyzing the reduced versions of big ciphers in determining the anticipated strength indices of the said big ciphers and, on the other hand, on the concept (new ideology) of determining the indices of block symmetric ciphers strength to attacks of differential and linear cryptanalysis, which has been lately defined more exactly on the basis of studying the properties and indices of random substitutions and reduced models of ciphers considered as substitution transformations.

Key words: differential and linear cryptanalysis, strength indexes to differential and linear cryptanalysis attacks, properties of random substitutions and encryption transformations.

Ref.: 25 items.