УДК 681.3.06

И.В. ЛИСИЦКАЯ

МЕТОДОЛОГИЯ ОЦЕНКИ СТОЙКОСТИ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Излагается новый подход к оценке показателей доказуемой стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, который основывается на результатах изучения свойств шифров как случайных подстановок. Для преодоления вычислительных трудностей, свойственных анализу показателей стойкости больших шифров, развивается методика, которая строится на результатах изучения свойств уменьшенных версий больших прототипов. В соответствии с этой методикой максимумы полных дифференциалов и линейных корпусов шифров могут быть получены расчетным путем из формул, выведенных для случайных подстановок. В отличие от известных результатов, связывающих показатели стойкости шифров с дифференциальными и линейными свойствами входящих в шифры нелинейных преобразований, делается вывод, что максимальные значения полных дифференциалов и линейных корпусов современных шифров не зависят (при достаточном числе цикловых преобразований) ни от свойств используемых в шифрах подстановочных конструкций, ни от методов введения в цикловые функции подключей, ни от способа построения расширяющего линейного преобразования, а являются функцией только размера битового входа в шифр (степени подстановки).

Введение

В последнее время появился ряд публикаций, в которых обсуждаются подходы к получению оценок доказуемой безопасности блочных симметричных шифров (БСШ) к атакам дифференциального и линейного криптоанализа [1-8 и др.].

Мы здесь не будем детально рассматривать сущность каждого из этих предложений, а приведем сразу итоговые выводы, следующие из анализа этих работ [9].

Первый вывод состоит в том, что в основе всех известных подходов к оценке показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа лежит процедура определения максимумов средних значений дифференциальных вероятностей (MADP) и максимумов средних значений вероятностей линейных корпусов (MALHP).

Второй вывод заключается в том, что результирующие показатели стойкости шифров практически во всех работах связываются с соответствующими показателями, входящими в шифры S-блоковых конструкций.

Третий вывод состоит в том, что предлагаемые в отмеченных работах оценки доказуемой стойкости отличаются в значительных пределах.

Формулируется общий вывод о том, что существующая методика оценки показателей стойкости БСШ является все еще не совершенной. Более того, в работе будет показано, что известные подходы и их результаты не могут претендовать на объективность.

В данной статье мы хотим ещё раз высказать свою точку зрения по вопросу оценки безопасности БСШ, концептуально отличающуюся от известных, хотя в конечном итоге речь опять будет идти об определении максимальных значений полных дифференциалов и линейных корпусов (оболочек) БСШ. Основой здесь станут материалы нашей работы [9], дополненные уточнениями и разъяснениями.

1. Краткая сущность известных подходов к оценке стойкости и идеи, на которых строится новый подход

Прежде всего отметим, 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 такой подход многим исследователям представляется вполне оправданным, так как полный анализ дифференциальных и линейных свойств современного шифра при реальной

длине битового размера входа является сегодня невыполнимой задачей. Собственно говоря, разработчики шифров и идут по пути увеличения размеров битового входа шифров именно для того, чтобы сделать задачу полного перебора ключей или текстов заведомо не реализуемой в обозримом будущем. Поэтому многие оценки показателей стойкости больших шифров строятся больше на основе накопленного опыта и некоторых соображений и оценок, позволяющих получить аргументы и данные для подтверждения предполагаемых высоких показателей стойкости предлагаемых решений. По этому же 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.

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.

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, обоснованные ими показатели стойкости к атакам дифференциального и линейного криптоанализа несколько иные.

Излагаемые далее соображения и результаты строятся исходя из развиваемого нами нового подхода в теории и методах криптоанализа, ориентированного, с одной стороны, на использование при определении ожидаемых результатов стойкости больших шифров результатов анализа уменьшенных их версий, а с другой – на развитую на основе изучения свойств и показателей случайных подстановок и уменьшенных моделей шифров, рассматриваемых как подстановочные преобразования, концепцию (новую методологию) определения показателей стойкости БСШ к атакам дифференциального и линейного криптонализа.

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. Наши проработки показывают, что большое число хорошо известных алгоритмов шифрования допускают масштабирование. Удается во многих случаях построить уменьшенные модели, которые сохраняют (с учетом масштабирования) все свойства своих прототипов и позволяют решить многие задачи анализа и сравнения по показателям стойкости больших версий шифров [10-13 и др.].

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 практически только размером битового входа в шифр.

Другой важный вывод, следующий из выполненных исследований, приводит к тому, что показатели стойкости больших (полных реализаций) шифров к атакам дифференциального и линейного криптоанализа (таких шифров, как Rijndael и многих других известных шифров, а также шифров Лабиринт, Калина, Мухомор, ADE [14-16], представленных на украинский конкурс по выбору национального стандарта шифрования) могут быть получены расчетным путем.

Этот вывод сделан на основе установленного в ходе исследований факта, что практически все известные шифры (большие и малые их версии) с увеличением числа циклов шифрования приходят к установившимся (стационарным) состояниям, свойственным случайным подстановкам соответствующей степени, для которых сегодня уже определены аналитические выражения для законов распределения переходов XOR таблиц и смещений таблиц линейных аппроксимаций. В результате появилась возможность найти максимумы интересующих нас распределений из формул путём расчётов (для шифров с операциями

введения цикловых подключей, отличными от XOR, необходимо рассматривать соответствующие таблицы для ключенезависимых переходов).

В работе обобщаются результаты по обоснованию предлагаемой методологии.

2. Понятийный аппарат линейного и дифференциального криптоанализа

Напомним кратко основной понятийный аппарат линейного и дифференциального криптоанализа. Следуя работе [17], 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 ($\mathrm{x}, \mathrm{y} \in \mathrm{GF}(2^{\mathrm{n}})$) *есть*

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

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

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

Определение 2 ($\mathrm{DP}^{\mathrm{f}}_{\max}$ и $\mathrm{LP}^{\mathrm{f}}_{\max}$). *Максимальное значение дифференциальной и линейной вероятности для ключезависимой функции f определяется соответственно как*

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

$$\mathrm{LP}^{\mathrm{f}}_{\max} = \max_{\Gamma \mathrm{x}, \Gamma \mathrm{y} \neq 0} \mathrm{LP}^{\mathrm{f}}(\Gamma \mathrm{y} \to \Gamma \mathrm{x}).$$

Напомним также выражения для средних вероятностей ADP, ALHP, MADP и MALHP ключезависимой функции $f = f[k](x)$ с n-битным входом x и n-битным выходом y, $(\mathrm{x}, \mathrm{y} \in \mathrm{GF}(2^{\mathrm{n}}))$, параметризованной ключом k, используемых во многих публикациях по обоснованию показателей стойкости блочных шифров.

Определение 3. *Среднее значение дифференциальной вероятности* (ADP) *функции* f[k](x) *есть* $\mathrm{ADP}^{\mathrm{f}} = \operatorname{ave}_{\mathrm{k}} \mathrm{DP}^{\mathrm{f[k]}}(\Delta \mathrm{x} \to \Delta \mathrm{y})$.

Определение 4. *Среднее значение вероятности линейного корпуса* (ALHP*) функции* f[k](x) *есть* $\mathrm{ALHP}^{\mathrm{f}} = \operatorname{ave}_{\mathrm{k}} \mathrm{LP}^{\mathrm{f[k]}}(\Gamma \mathrm{x} \to \Gamma \mathrm{y})$.

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

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

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

В наших разработках [18 и др.] развивается новая точка зрения к формированию оценок стойкости БСШ к атакам дифференциального и линейного криптоанализа, которая формализуется как два новых метода (подхода).

Предлагается для оценки стойкости БСШ к атакам дифференциального и линейного криптоанализа пользоваться не MADP (максимумом средней дифференциальной вероятности) для некоторого фиксированного перехода входной разности Δx в выходную разность Δy, а средним (по множеству ключей) значением максимумов дифференциальных

вероятностей (AMDP) ключезависимой функции f[k](x), а для линейного криптоанализа - соответственно пользоваться не MALHP, а AMLHP.

Определение 6 (AMDP)**.** *Среднее* (*по множеству из* 2^h *ключей*) *значение максимальной дифференциальной вероятности ключезависимой функции* f[k](x) *есть*

$$\mathrm{AMDP}^f = \operatorname*{ave}_k \mathrm{DP}_{\max}^{f[k]} = \frac{1}{2^h}\sum_{k=1}^{2^h} \mathrm{DP}_{\max}^{f[k]}.$$

Определение 7 (AMPLH)**.** *Среднее* (*по множеству из* 2^h *ключей*) *значение максимальной вероятности линейных корпусов функции* f[k](x) *есть*

$$\mathrm{AMLHP}^f = \operatorname*{ave}_k \mathrm{LP}_{\max}^{f}(\Gamma x \to \Gamma y) = \frac{1}{2^h}\sum_{k=1}^{2^h} \mathrm{LP}_{\max}^{f[k]}.$$

В обоих случаях 2^h - мощность множества ключей зашифрования, использованных при вычислениях.

Можно также отметить, что очевидны неравенства:

$$\mathrm{MADP}^f < \mathrm{AMDP}^f,\ \mathrm{MALHP}^f < \mathrm{AMLHP}^f.$$

Помимо большей адекватности формируемых оценок их значения совпадают с соответствующими дифференциальными и линейными показателями случайных подстановок и характеризуют максимально достижимые значения дифференциальных и линейных вероятностей. В последнем случае обеспечиваются и значительные вычислительные преимущества (нет необходимости запоминать полностью все таблицы, а достаточно только определить и запомнить их максимальные значения).

Важным для дальнейшего является понятие случайной подстановки. Мы на нем остановимся отдельно.

3. Математическая модель случайных подстановок

Напомним, что ранее в нашей работе [19] понятие случайной подстановки было определено следующим образом.

Определение 8. *Под случайной понимается подстановка, которая удовлетворяет одновременно трем критериям случайности*:

Число инверсий h_n *в подстановке степени* n *приблизительно равно числу "антиинверсий", а практически*

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

Число циклов x_n *в подстановке степени* n *близко к* ln*n, а практически, находится в границах*

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

Число возрастаний q_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 оправданного числа – использовались значения $a \le 1$).

В других наших публикациях [20,21], посвященных исследованию дифференциальных и линейных свойств случайных подстановок и подстановочных преобразований, развивающих результаты работ Luka O'Connor [22-24], мы определили еще два утверждения,

которые справедливы для случайных подстановок. Напомним здесь их, так как они являются важными для дальнейшего.

В обозначениях работ [20,22] пусть $\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k$ будет вероятностью того, что значение ячейки дифференциальной таблицы случайно взятой подстановки p 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 p выбрана равновероятно из множества* S_2^n *и* $0 \le k \le 2^{n-1}$,

$$\Pr(\Lambda(\Delta X,\Delta Y)=2k)=\binom{2^{n-1}}{k}^2 \cdot \frac{k!\cdot 2^k \cdot \Phi(2^{n-1}-k)}{2^n!}, \qquad (3)$$

где функция $\Phi(d)$ *определяется выражением*

$$\Phi(d)=\sum_{i=0}^{d}(-1)^i \cdot \binom{d}{i}^2 \cdot 2^i \cdot i!(2d-2i)!.$$

Закон распределения вероятностей (5) 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. Об этом свидетельствуют многочисленные результаты экспериментов. И это еще не все! Оказывается, что закон распределения (5), 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:

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

Здесь $\Lambda_\pi(\Delta X,\Delta Y)$ – значение XOR таблицы для пары значений разностей входов и выходов ΔX, $\Delta Y \in Z_2^n$: $\Delta X = X + X'$, $\Delta Y \in \pi(X)+\pi(X')$ подстановки $\pi \in S_2^n$. Значение k* представляет собой половину от максимального числа переходов XOR таблицы случайной подстановки.

Совершенно аналогичное по содержанию утверждение справедливо для вероятности смещений линейных аппроксимационных таблиц $LAT_\pi^*(\alpha,\beta)$ случайных подстановок [21,23].

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 p выбрана равновероятно из множества* 2^n *и маски* α,β *не нулевые. Тогда* $\lambda^*(\alpha,\beta)$ *принимает только четные значения и*

$$\Pr(\lambda^*(\alpha,\beta)=2k)=\frac{(2^{n-1}!)}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+|k|}^2 \qquad (4)$$

для $|k| \le 2^{n-2}$.

Связь новых обозначений с представленными выше устанавливается равенством $LAT_\pi^*(\alpha,\beta)=LP^f(\Gamma y \to \Gamma x)$.

И для этого распределения справедлива нормировка

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

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

На основе полученных результатов представляется логичным в дополнение к уже известным подходам сформировать (сформулировать) новое (или уточненное) определение случайной подстановки [25].

Определение 9. *Подстановка является случайной, если вместе с выполнением критериев случайности* 1-3 *для ячеек её XOR таблицы и таблицы линейных аппроксимаций выполняются законы распределения вероятностей* (3) (*критерий случайности* 4) *и* (4) (*критерий случайности* 5).

С использованием предложенных критериев случайности был выполнен достаточно широкий объём исследований по реализации конкретных значений критериев отбора случайных подстановок [25-27 и др.], подтвердивших практическую возможность реализации подстановочных преобразований с показателями, которые повторяют весьма близко распределения, следующие из теоретических результатов (имеющих комбинаторные, дифференциальные и линейные характеристики, полученные из теоретических расчётов).

Таким образом, приведенные определения и утверждения можно считать теоретической и практической базой для формирования понятия математической модели случайной подстановки.

4. Обоснование методологии оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа на основе моделей случайных подстановок

В основе развиваемого подхода лежит рассмотрение шифрующих преобразований как случайных подстановок.

Самый важный вывод работ [21, 23 и др.] 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 (3) и (4). 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 таблицы XOR разностей последовательности шифрующих преобразований, также как и максимумы линейных аппроксимационных таблиц этих же преобразований, зависят только от числа циклов шифрующего преобразования и размера его битового входа.

Этот вывод зафиксирован 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.*

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.

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

Начнем доказательство приведенного 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 (3).

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 наборов 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 являются фиксированными числа ячеек каждого типа, определяемых с помощью закона распределения $\Pr(\Lambda_f(\Delta x, \Delta y) = 2k$ в виде [21]

$$\Lambda_{m,2k} = (2^m - 1)^2 \cdot \Pr(\Lambda_f(\Delta x, \Delta y)) = \frac{(2^m - 1)^2}{2^m!} \begin{pmatrix} 2^{m-1} \\ k \end{pmatrix}^2 \cdot k! 2^k \cdot \Phi(2^{m-1} - k) \ . \qquad (5)$$

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 (5).

Поэтому применительно к шифрующим многоцикловым преобразованиям-случайным подстановкам дифференциальные вероятности DP^f должны теперь интерпретироваться в обозначениях подстановочных преобразований для ключезависимой функции *f* как

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

причем эти вероятности следует считать одинаковыми для всех ячеек таблицы дифференциальных разностей (для всех вариантов 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 (3) с нормировкой

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

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 (3), то цикловое преобразование может осуществить лишь переименование выходов и соответствующих им разностей, оставляя результирующий закон распределения разностей неизменным (для операции XOR подстановка вместе с линейным цикловым преобразованием является детерминированным преобразованием и произведение случайной в оговоренном смысле подстановки на любую другую подстановку является случайной). 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, где Δz является выходной разностью r + 1-го 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

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

И тогда дифференциальная вероятность $DP^{f_{r+1}}(\Delta x, \Delta z)$ для r + 1-го 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), 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

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

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.

Остановимся теперь на одном из принципиальных моментов рассматриваемого подхода – приходу шифров к стационарному состоянию, свойственному случайной подстановке. Здесь мы опять будем вести речь о дифференциальных характеристиках.

Заметим для начала, что для R-циклового шифра SPN структуры формирование результирующего закона распределения вероятностей переходов таблицы полных дифференциалов сводится к последовательному выполнению R однотипных (одноцикловых) преобразований (R итераций). Для иллюстрации процесса прихода шифров к стационарным состояниям в табл. 1 представлены результаты экспериментов с малыми их версиями. Значение

максимума таблиц разностей, равное 19-20, как раз соответствует показателю случайной подстановки. Представленные результаты свидетельствуют, что произведение одноцикловых преобразований после небольшого начального числа их повторений приобретает свойства случайной подстановки, соответствующей степени независимо от показателей случайности исходного одноциклового преобразования.

Таблица 1

Средние значения максимумов таблиц XOR разностей ($AMDPr2^{16}$) малых версий шифров вместе со среднеквадратическими отклонениями

Шифр / г	Шифр Хейса		Мини-AES	Мини-ADE	Мини-Лабиринт	Мини-Мухомор		Мини-Калина	
Число циклов	S-блок δ = 8	S-блок δ = 4	S-блок δ = 4	S-блок δ = 4	S-блок δ = 4	S-блок δ = 8	S-блок δ = 4	S-блок δ = 8	S-блок δ = 4
1	32768	16384	16384	16384	-	65536	65536	6082,56	3732,48
2	12288	4096	3036,16	3353,6	-	14187,5	5770,24	826,88	382,4
3	2326,81	439	274,24	307,2	37,5	2496,32	1802,24	24,8	19,36
4	216,803	56,964	19,326	20,54	19,04	542,72	125,53	19,04	19,14
5	65,38	26,18	19,02	19,08	19,24	46,28	29,7	19,14	19,2
6	24,108	19,108	18,812	19,24	19,04	19,48	18,88	19,14	19,36
7	19,021	19,086	18,87	19,00	19,14	19,47	18,87	19,27	18,73
8	19,16	19,1	19,27	18,93	19,24	19,33	19,27	19,02	19,00

В работе [9] мы не смогли привести теоретического обоснования утверждения 3 (была доказана только приведенная выше часть о том, что если шифр пришёл к стационарному состоянию, то дальнейшее наращивание числа циклов этого состояния не меняет). Поэтому здесь представляется дополнительное обоснование самого перехода шифра к стационарному состоянию.

Мы заинтересовались процессами, происходящими при последовательном выполнении подстановочных преобразований вообще, а не только шифрующих преобразований.

Были рассмотрены подстановки 256-й степени (байтовые подстановки). В табл. 2 представлены результаты вычислительного эксперимента по определению максимумов XOR таблиц последовательности (произведения) подстановочных преобразований для двух различных байтовых подстановок. Одна подстановка взята с показателем d-равномерности, равным 4, а вторая с показателем d-равномерности, равным 8. Видно, что обе подстановки уже на втором IциклеI приходят к максимуму дифференциала, равному 10-12, характерному для случайной подстановки степени 2^8 [20]. Интересно отметить, что результат не зависит от ключевых значений, если их ввести после каждого подстановочного преобразования.

Таблица 2

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	12

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

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

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

Подобным же образом к стационарному распределению, свойственному случайной подстановке, приходит и любой шифр. Переход к стационарному распределению как раз соответствует тому моменту, с которого 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) и именно этим определяется важнейшая роль подстановочных преобразований в шифрах.

Аналогичные аргументы могут быть приведены по отношению к линейным показателям многоцикловых итеративных процедур шифрования.

В результате мы приходим к тому, что утверждение 3 оказывается справедливым практически для всех современных блочных симметричных шифров. Но раз так, то для оценки показателей доказуемой стойкости этих шифров можно воспользоваться расчётными соотношениями, справедливыми для математических моделей случайных подстановок. Приведём их далее.

5. Расчетные соотношения для определения показателей стойкости шифров к атакам дифференциального и линейного криптонализа

Расчетные соотношения для определения максимальных значений полных дифференциалов и максимальных значений линейных корпусов могут быть получены применением законов (3) и (4), справедливых для случайных подстановок, к шифрам, рассматриваемым как случайные подстановки, что и сделано в работах [20] и [21].

Как показано в [20], среднее значение максимума таблицы дифференциальных разностей случайной подстановки порядка 2^n находится путем определения максимального значения $k = k_{max}$, при котором выполняется соотношение

$$\frac{(2^n-1)^2}{2^n!}\cdot\binom{2^{n-1}}{k}^2\cdot k!2^k\cdot\Phi(2^{n-1}-k)\approx 1. \qquad (6)$$

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

$$DP^f_{max}=\frac{k_{max}}{2^n}. \qquad (7)$$

В работе [20] также приведено расчетное соотношение, являющееся хорошей аппроксимацией соотношений (6) и (7):

$$DL^f_{max}=\frac{n+4}{2^n}.$$

В [21] показано, что среднее значение максимума таблицы линейных аппроксимаций для случайной подстановки определяется аналогично предыдущему случаю путем нахождения значения k^*, являющегося целым решением уравнения

$$\frac{(2^n-1)^2\cdot\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+|k^*|}^2=1. \qquad (8)$$

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

$$DL^{f}_{max} = \left(\frac{k_{max}}{2^{n-1}} \right)^2 .$$

Приведем здесь также соотношение, полученное на основе обработки результатов вычислительных экспериментов, являющееся удобной заменой выполнению расчетов по соотношению (8):

$$DL^{f}_{max} = \left(\frac{\left(\frac{3}{2} \right)^2}{2^{n-1}} \right)^2$$

Выводы

На основе накопленных результатов и обоснований можно утверждать следующее.

1. Современные блочные симметричные шифры при полном наборе шифрующих многоцикловых преобразований обладают свойствами случайных подстановок, т.е. для них справедливы законы распределения вероятностей для комбинаторных показателей (инверсий, возрастаний и циклов), а также законы распределения вероятностей полных дифференциалов и линейных корпусов, свойственные случайным подстановкам соответствующей степени.

2. Максимальные значения полных дифференциалов и линейных корпусов блочных симметричных шифров, определяющие по современным меркам показатели их доказуемой стойкости 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.

3. Впервые предложена и обоснована методология оценки стойкости блочных симметричных шифров к атакам линейного и дифференциального криптоанализа, которая предусматривает использование для формирования выводов относительно уровня доказуемой безопасности шифров показателей их уменьшенных моделей, что позволило существенно ускорить процесс выполнения экспертизы и сравнения решений по построению алгоритмов блочного симметричного шифрования.

4. Впервые установлен принцип определения максимумов дифференциальной и линейной вероятностей современных БСШ на основе использования показателей случайных подстановок соответствующей степени, не связанный с показателями нелинейных преобразований (S-блоков) шифров, что позволило значительно упростить процесс нахождения показателей доказуемой безопасности шифров к атакам линейного и дифференциального криптоанализа.

Список литературы: **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. P.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. 2001. P. 420-436. **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.* Оценки практической стойкости блочного шифра ІКалинаІ относительно методов разностного, линейного криптоанализа и относительно алгебраических атак, основанных на гомоморфизмах / А.Н. Алексийчук, Л.В. Ковальчук, Е.В. Скрыпник, А.С. Шевцов // 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. 1995.Vol.8. No.1. **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.** *Горбенко І.Д.* Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / Горбенко І.Д., Долгов В.И., Лисицкая И.В., Олейников Р.В. // Прикладная радиоэлектроника. 2010. Т. 9, № 3. С. 312-320. **10.** *Лисицкая И.В.* Криптографические свойства уменьшенной версии шифра IМухоморI. / И.В. Лисицкая, О.И. Олешко, С.Н. Руденко, Е.В. Дроботько, А.В. Григорьев // Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць. Київ, 2010. Вип. 2(18). С. 33-42. **11.** *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.**12.** *Долгов В.И.* Криптографические свойства уменьшенной версии шифра "Калина" / В.И. Долгов, Р.В. Олейников, А.Ю. Большаков, А.В. Григорьев, Е.В. Дробатько // Прикладная радиоэлектроника. 2010. Т.9, № 3. С. 349-354.**13.** *Головашич С.А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника. Харьков: ХТУРЭ. 2007. Том. 6, №2, С. 230-240. **14.** *Горбенко І.Д.* Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація / І.Д. Горбенко, М.Ф. Бондаренко, В.І. Долгов, Р.В. Олійников, В.І. Руженцев, М.С. Михайленко , Ю.І. Горбенко, О.І. Олешко, С.В. Казьміна // Прикладная радиоэлектроника. Харьков: ХТУРЭ. 2007. Том. 6, №2. С. 147-157. **15.** *Горбенко І. Д.* Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікації / І.Д. Горбенко, В.І. Долгов, Р.В. Олейніков, В.І. Руженцев, М.С. Михайленко, Ю.І. Горбенко, О.С. Тоцкій, С.В. Казьміна // Прикладная радиоэлектроника. 2007. Т.6, № 2. С. 195-208. **16.** *Кузнецов А.А.* Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) / А.А. Кузнецов, Р.В. Сергиенко, А.А. Наумко // Прикладная радиоэлектроника. 2007. Том 6, №2. С. 241-249. **17.** *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. Janiary 2003.Vol. E86-A. No.1. P. 37-46. **18.** *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 IКомпьютерные науки и технологииI, 8-10 октября, Белгород. 2011. С. 418-422.**19.** *Горбенко И.Д.* Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 28147-89 / Горбенко И.Д., Лисицкая И.В. // Радиотехника. 1997. Вып 103. С. 121-130. **20.** *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. **21.** *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. **22.** *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. Helleseth ed., Springer-Verlag, pages 360-370, 1994. **23.** *Luke O'Connor*. Properties of Linear Approximation Tables. Email: oconnor@dsts. Edu. au, 1995. **24.** *Luke O'Connor*. On Linear Approximation Tables and Ciphers secure against Linear Cryptanalysis. Email: oconnor@dsts. Edu. au, 1995. **25.** *Долгов В.И.* Случайные подстановки в криптографии / В.И. Долгов, И.В. Лисицкая, К.Е. Лисицкий // Радіоелектронні та комп'ютерні системи. 2010. № 5 (46). С. 79-85. **26.** *Лисицкая И.В.* Экспериментальная проверка работоспособности новых критериев отбора случайных подстановок / И.В. Лисицкая, К.Е. Лисицкий, А.В. Широков, Е.Д. Мельничук // Радіоелектронні та комп'ютерні системи. 2010. № 6 (47). С. 87-93. **27.** *Лисицкая И.В.* Оценка числа случайных подстановок с заданным распределением парных разностей XOR таблиц и смещений таблиц линейных аппроксимаций / И.В. Лисицкая, А.В. Широков, Е.Д. Мельничук, К.Е. Лисицкий // Прикладная радиоэлектроника. Харьков: ХНУРЭ. 2010. Т. 9, № 3. С. 341-345.

Поступила в редколлегию 10.09.2011

Лисицкая Ирина Викторовна, канд. техн. наук, доцент кафедры БИТ ХНУРЭ. Научные интересы: защита информации, методы криптоанализа блочных шифров. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 340-84-60.