6. Еколого-технологічний газоаналітичний комплекс [Текст] : патент України / Бородавка В. П., Дашковський О. А., Воробйов С. С., Приміський В. П. та інші. — № 64586. — 2004. — Бюл. 2.
7. Безрук, З. Д. Еколого-технологічний моніторінг переробки відходів [Текст] : сборник материалов конференции Пятой научно-технической конференции «Современные информационные и електронные технологии» / З. Д. Безрук, В. П. Приміський. — Одесса, 2004. — 100 с.
8. Визнюк, А. А. Создание систем технолого-экологического мониторинга утилизации промышленных отходов [Текст] : материалы Международной конф. Кацивели, АРК / А. А. Визнюк, З. Д. Безрук, В. П. Приміський // Материалы и покрытия в экстремальных условиях: исследования, применение, экологические чистые технологии производства и утилизации изделий. — Крым, 2004. — С. 563—564.
9. Инструментальный контроль выбросов в атмосферу киевского мусоросжигательного завода «Энергия» [Текст] : материалы II науч.-практ. конф. с междунар. участием / Н. М. Мовчан, З. Д. Безрук, А. А. Дашковский, В. Ф. Примиский и др. // Сотрудничество для решения проблемы отходов. — Харьков, 2005. — 250 с.
10. Безрук, З. Д. Газоаналітичні системи промислового моніторингу [Текст] : матеріали з шостої міжнародної науч.-практ. конф. / З. Д. Безрук, Н. М. Мовчан, О. А. Дашковський // Сучасні інформаційні і електронні технології. — Одесса, 2005. — С. 391.

МОДЕЛИ ДИАГНОСТИКИ И ПОВЫШЕНИЯ НАДЕЖНОСТИ ГАЗОАНАЛИТИЧЕСКИХ СИСТЕМ

Рассмотрена методология диагностирования многоканальных газоаналитических систем и определена эффективность их работы. Проанализированы причины потерь измерительной информации. Предложена методология определения времени восстановления работы газоаналитической системы. Приведены зависимости действия тестового сигнала на выходной сигнал газоанализатора. Проведено сравнение тестового и функционального диагностирования, определены средние временные характеристики работы и восстановления систем.

Ключевые слова: методология диагностирования, многоканальные газоаналитические системы, измерительная информация, микропроцессорные системы (МПС).

Безрук Зоя Домініковна, *асистент, кафедра аналітичного екологічного приладобудування, Національний технічний університет України «Київський політехнічний інститут», Україна,* ***e-mail: kpi_naeps@ukr.net****.*

Порєв Володимир Андрійович, *доктор технічних наук, професор, завідувач кафедри аналітичного екологічного приладобудування, Національний технічний університет України «Київський політехнічний інститут», Україна,* ***e-mail: kpi_naeps@ukr.net****.*

Приміський Владислав Пилипович, *кандидат технічних наук, доцент, старший науковий співробітник, кафедра аналітичного екологічного приладобудування, Національний технічний університет України «Київський політехнічний інститут», Україна,* ***e-mail: kpi_naeps@ukr.net****.*

Безрук Зоя Доминиковна, *ассистент, кафедра аналитического и экологического приборостроения, Национальный технический университет Украины «Киевский политехнический институт», Украина.*

Порев Владимир Андреевич, *доктор технических наук, профессор, заведующий кафедрой аналитического экологического приборостроения, Национальный технический университет Украины «Киевский политехнический институт», Украина.*

Примиский Владислав Филиппович, *кандидат технических наук, доцент, старший научный сотрудник, кафедра аналитического экологического приборостроения, Национальный технический университет Украины «Киевский политехнический институт», Украина.*

Bezruk Zoe, *National Technical University of Ukraine «Kyiv Polytechnic Institute», Ukraine,* ***e-mail: kpi_naeps@ukr.net****.*

Poryev Vladimir, *National Technical University of Ukraine «Kyiv Polytechnic Institute», Ukraine.*

Primisky Vladislav, *National Technical University of Ukraine «Kyiv Polytechnic Institute», Ukraine,* ***e-mail: kpi_naeps@ukr.net***

УДК 621. 391: 519. 2: 519.7

Лисицкий К. Е.

МАКСИМАЛЬНЫЕ ЗНАЧЕНИЯ ПОЛНЫХ ДИФФЕРЕНЦИАЛОВ И ЛИНЕЙНЫХ КОРПУСОВ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Приводятся расчетные соотношения для определения максимальных значений переходов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок, на основе которых в соответствии с новой методологией оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа расчетным путем определяются показатели доказуемой безопасности ряда современных шифров.

Ключевые слова: *случайная подстановка, блочные симметричные шифры, показатели доказуемой стойкости.*

1. Введение

Как известно, в качестве показателей доказуемой стойкости блочных симметричных шифров к атакам линейного и дифференциального криптоанализа рассматриваются максимальные значения линейных и дифференциальных вероятностей, определяемые соответствующими максимальными значениями переходов XOR таблиц (полных дифференциалов) и смещений таблиц линейных аппроксимаций (линейных оболочек), получающихся на полноцикловой длине этих шифров.

В известных работах, посвященных этой тематике, в качестве таких показателей используются MADP (максимум средней дифференциальной вероятности) и MALP (MALHP) (максимум средней линейной вероятности, или максимум средней линейной вероятности линейного корпуса), причем, как правило, эти показатели непосредственно связываются с соответствующими дифференциальными и линейными свойствами подстановок, входящих в шифры. Все известные результаты, полученные в этом направлении, ориентированы на получение оценочных значений дифференциальных и линейных вероятностей, которые, несмотря на порой стройные математические теории, лежащие в основе обоснования получаемых оценочных значений, отличаются в значительных пределах друг от друга и, как установлено в последнее время [1—16], не могут претендовать на точность (являются весьма грубыми).

В этой работе речь будет идти о новой методологии оценки показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа [1, 3], основой которой являются положение, в соответствии с которым показатели стойкости блочных симметричных шифров от свойств S-блоков, входящих в цикловые шифрующие преобразования, не зависят, а определяются свойствами случайных подстановок соответствующей степени, к которым все современные шифры приходят асимптотически (на полноцикловой длине).

В этой методологии вместо показателей стойкости в виде MADP и MALP, используемых в большинстве известных публикаций, предлагаются новые показатели стойкости в виде AMDP (среднего значения максимумов дифференциальных вероятностей) и AMLP (среднего значения максимумов линейных вероятностей), которые как показано в работе [2] более адекватно характеризуют дифференциальные и линейные свойства шифров.

В соответствии с новой методологией получается, что могут быть получены не оценочные значения показателей стойкости, а точные значения этих показателей расчетным путем из формул для определения максимумов таблиц XOR разностей и смещений таблиц линейных аппроксимаций случайных подстановок соответствующей степени. В этой работе мы и хотим представить эту методологию в действии.

В первой части работы излагаются результаты анализа ряда известных подходов к определению показателей доказуемой стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, и делается вывод об их не совершенстве.

Во второй части работы приводятся необходимые расчетные соотношения из теории случайных подстановок, а в третьей части работы эти расчетные соотношения применяются для определения показателей доказуемой безопасности ряда современных шифров.

2. Краткий анализ известных подходов к определению показателей доказуемой стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа

Следуя работе [4], кратко напомним результаты некоторых известных работ, относящихся к оценкам стойкости БСШ к атакам дифференциального и линейного криптоанализа. Далее будут сделаны ссылки на шесть таких работ.

В работе [5] изучается подстановочно-перестановочая 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 работах [6, 7] авторы 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 шифру Rijndael (AES) с 7-ю и более циклами обеспечивает верхнюю границу $UB = 2^{-75}$, соответствующая нижняя граница сложности данных есть $32/UB = 2^{80}$ (для 96,7 % отношения успеха).

В работе [8] 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 работе [9] получены аналитические верхние оценки вероятностей дифференциальных и линейных характеристик блочных шифров, построенных по схеме шифра «Калина-128». Значения оценок, следующие из расчетов, выполненных в работе, составили: MADP $\le 2^{-230}$, MALHP $\le 2^{-212}$.

В работе [10] расширяется теорема Хонга и др., которая дает верхние границы для максимумов средних вероятностей дифференциалов и линейных корпусов (MADP и MALHP), на SPN блоковые шифры 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 установить, 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.

В [4] отмечается, что можно привести и много других работ, посвященных оценке показателей доказуемой стойкости БСШ к атакам дифференциального

и линейного криптоанализа, которые в большинстве своем строятся на идеях привязки показателей стойкости шифров к свойствам используемых в них S-блоков. Для нас важными будут выводы, которые были сделаны из анализа результатов затронутых публикаций.

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

Второй вывод состоит в том, что результирующие показатели доказуемой стойкости (доказуемой безопасности) шифров практически во всех работах связываются с соответствующими криптографическими показателями, входящих в шифры S-блоковых конструкций.

Третий вывод сводится к тому, что практически во всех работах показатели стойкости шифров к атакам дифференциального и линейного криптоанализа оцениваются с помощью показателей MADP — максимальная средняя дифференциальная вероятность и MALP (MALHP) — максимальная средняя линейная вероятность (максимальная средняя вероятность линейного корпуса), которые характеризуют не потенциальные, а средние значения соответствующих показателей.

Мы здесь добавим еще один вывод, состоящий в том, что во многих работах (в том числе и в [5]) утверждается, что асимптотически шифры приходят к равномерным законам распределения полных дифференциалов и смещений линейных корпусов.

Анализ приведенных и не приведенных здесь работ позволяет заключить [4], что все существующие подходы к оценке показателей стойкости БСШ опираются скорее на интуитивные (не лишенные здравого смысла) 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 Rijndael. 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. 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, в которой применили более эффективную конструкцию линейного преобразования (умножения байтовых векторов на проверочную матрицу МДР кода), допускающего простое математическое описание. Они посчитали, что показатели S-блоков оказывают решающее влияние на итоговые показатели стойкости шифра и предложили достаточно убедительную концепцию обеспечения доказуемой безопасности с помощью таких S-блоков.

Исследования, проведенные учеными кафедры БИТ ХНУРЭ [3, 4], показали, что это точка зрения не правильная или не совсем правильная. На самом деле показатели стойкости шифров к атакам дифференциального и линейного криптоанализа от свойств, входящих в шифры S-блоков не зависят (от свойств S-блоков зависит, но не во всех случаях динамика прихода шифра к состоянию случайной подстановки). Основное положение новой методологии состоит в том, что все итеративные шифры после небольшого начального числа циклов шифрования приобретают свойства случайных подстановок. Это положение уже проверено на большом числе примеров уменьшенных и полномасштабных моделей современных шифров [4].

Сегодня уже имеются и результаты по определению дифференциальных и линейных свойств случайных подстановок. Поэтому в соответствии с развиваемой концепцией показатели стойкости блочных симметричных шифров могут быть определены из формул, полученных для случайных подстановок. Целью статьи и является изложение сущности и реализация этого подхода для определения показателей доказуемой стойкости ряда современных шифров.

3. Расчетные соотношения для определения максимальных значений дифференциальных и линейных вероятностей случайных подстановок

Мы здесь напомним выражения для вычисления теоретических законов распределения вероятностей переходов XOR таблиц и смещений таблиц линейных аппроксимаций для случайных подстановок из наших работ [11, 12], одна из которых выполнена с участием автора этой статьи.

Отметим, что решение близкой по подстановке задачи нам удалось найти в работах американского ученого Luke O'Connor [13, 14], однако манера преставления материалов этим автором, особенно в части доказательств и интерпретации конечных результатов, нас не удовлетворила и сделала целесообразным изложение собственной позиции по этому вопросу [11, 12]. Далее мы представляем содержание доказанных в [11—14] утверждений и их интерпретацию.

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

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

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

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

ISSN 2226-3780

Для перехода от вероятности к числу ячеек XOR таблицы используется формула:

$$\Lambda_\pi(\Delta X,\Delta Y)=2k=\frac{\left(2^n-1\right)^2}{2^n!}\cdot\left(\begin{matrix}2^{n-1}\\k\end{matrix}\right)^2\cdot k!\cdot 2^k\cdot\Phi(2^{n-1}-k). \quad (3)$$

Совершенно аналогичное по содержанию утверждение справедливо для вероятности значений линейных аппроксимационных таблиц $LAT^*_\pi(\alpha,\beta)$ случайных подстановок.

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

$$\Pr\left(\lambda^*(\alpha,\beta)=2k\right)=\frac{\left(2^{n-1}!\right)^2}{2^n!}\cdot\left(\begin{matrix}2^{n-1}\\2^{n-2}+\left|k\right|\end{matrix}\right)^2, \quad (4)$$

для $\left|k\right|\le 2^{n-2}$.

И в этом случае на основе последней формулы можно вычислить число ячеек таблицы LAT^*_π, имеющих заполнением значение $2k$, как простое умножение формулы на общее число ячеек таблицы подстановки с исключением первой строки и первого столбца:

$$E[\lambda(\pi,2k)]=\frac{(2^n-1)^2\left(2^{n-1}!\right)^2}{2^n!}\cdot\left(\begin{matrix}2^{n-1}\\2^{n-2}+\left|k\right|\end{matrix}\right)^2.$$

Значение максимума таблицы дифференциальных разностей случайной подстановки степени 2^n находится путем определения максимального значения $k=k^*_D$, при котором выполняется соотношение:

$$\frac{(2^n-1)}{2^n!}\cdot\left(\begin{matrix}2^{n-1}\\k^*_D\end{matrix}\right)^2\cdot k^*_D!\cdot 2^{k^*_D}\cdot\Phi(2^{n-1}-k^*_D)\approx 1. \quad (5)$$

Уместно здесь будет привести результаты расчетов из нашей работы [11], выполненные в соответствии с соотношением (4) для подстановок степени 2^n, дополненных значениями n = 14,16,32 из работы [4]. Они представлены в табл. 1.

В работе [12] показано, что значение максимума таблицы линейных аппроксимаций для случайной подстановки определяется аналогично предыдущему случаю путем нахождения значения k^*_L являющегося целым решением (округлением в сторону ближайшего целого) уравнения:

$$\frac{(2^n-1)^2\cdot\left(2^{n-1}!\right)^2}{2^n!}\cdot\left(\begin{matrix}2^{n-1}\\2^{n-2}+\left|k^*_L\right|\end{matrix}\right)^2\approx 1. \quad (6)$$

Для линейной аппроксимационной таблицы предлагается оценочное соотношение, полученное на основе обработки результатов вычислительных экспериментов в [12], являющееся удобной заменой выполнению расчетов по соотношению (4):

$$LP^f_{\max}\le\left(\frac{\left(\frac{3}{2}\right)^n}{2^{n-1}}\right)^2. \quad (7)$$

Приведем и для этого случая результаты расчетов, выполненных по формуле (4) для значений $n\le 16$ (табл. 2).

Таблица 1

Сравнение расчетных и экспериментальных результатов для случайных подстановок различных степеней

n	$\Lambda_\pi(\Delta X,\Delta Y)=2k$	$2k$	Эксперимент
7	2,641 0,221	10 12	10,3 $\le(n+4)$
8	10,26 0,8748	10 12	11,4 $\le(n+4)$
9	3,474 0,248	12 14	12,5 $\le(n+4)$
10	13,8495 0,99	12 14	13,4 $\le(n+4)$
11	3,952 0,247	14 16	14,5 $\le(n+4)$
12	15,787 0,987	14 16	15,3 $\le(n+4)$
14	15,76 0,87	16 18	17,6 $\le(n+4)$
16	14,01 0,7	18 20	19,5 $\le(n+4)$
32	8,155 0,239	32 34	— $\le(n+4)$

Таблица 2

Сравнение теоретических и экспериментальных результатов

n	$2k^*$	$E\left[\lambda(\pi,2k)\right]$	Эксперимент
4	4 6 8	3,89 1,118 0,017	5,498 $\left(\frac{3}{2}\right)^8=5,06$
6	12 14 16	9,013 1,7 0,239	14,48 $\left(\frac{3}{2}\right)^6=11,39$
8	32 34	2,12 0,7457	34,68 $\left(\frac{3}{2}\right)^8=25,62$
10	74 76	1,16 0,64	78,8 $\left(\frac{3}{2}\right)^8=57,66$
12	162 164	1,129 0,82	116,24 $\left(\frac{3}{2}\right)^8=129,74$
14	350 352	1,069 0,900	314 $\left(\frac{3}{2}\right)^{14}=291$
16	748 750	1,027 0,93	720 $\left(\frac{3}{2}\right)^{17}=657$

В в правой колонке табл. 2 представляются результаты расчетов по упрощенной формуле, предложенной нами на основе простого подбора ($k_{\max}=2k^*_D=n+4$). Результаты реально свидетельствуют, что экспериментальные данные и данные расчетов практически повторяют друг друга (оказываются достаточно близкими).

Приведенные выше соотношения, к сожалению, однако, не позволяют выполнить вычисления для значений $n>16$ (получаемые числа выходят за сетку вычислительной машины). Поэтому были предприняты шаги по поиску подходящих аппроксимаций.

4. Аппроксимации расчетных соотношений для значений n > 16

В работе [15] была установлена справедливость аппроксимации выражений (1) и (2) с помощью Пуассоновского закона распределения вероятностей в виде:

$$\Pr\left(\Lambda_{\pi}(\Delta X,\Delta Y)\right)=e^{-1/2}\cdot\frac{1}{2^k k!}, \qquad (8)$$

из которого для распределения числа переходов отдельно взятой строки таблицы XOR разностей случайной подстановки степени 2^n можно получить расчетное соотношение:

$$\Lambda_{n,2k}=(2^n-1)^2\cdot\frac{e^{-1/2}}{2^k k!}. \qquad (9)$$

Результаты расчетов по соотношению (9) для $E\left[\lambda(\pi,2k)\right]$ 128-битного шифра иллюстрирует табл. 3.

Таблица 3

Расчетные значения количества переходов подстановки степени 2^{128}

Значение перехода $2k$	Число переходов
96	20
98	0,2
100	0,002

Из табл. 3 следует, что ожидаемое максимальное значение перехода дифференциальной таблицы для 128-битного шифра равно 96.

Для значений линейной аппроксимационной таблицы при больших значениях n в [12] предложено воспользоваться теоремой 9 из работы [16].

Теорема. *Для случайной n-битовой подстановки, с* $n \geq 5$ *дисбаланс* $\mathrm{Im}b(v, u)$ *аппроксимации является случайным значением с распределением, которое может быть аппроксимировано в виде:*

$$\Pr(\mathrm{Im}\,b(v,u)=z)\approx 2Z\left(\frac{z}{2^{(n-2)/2}}\right), \qquad (10)$$

для z четного и ноль для z нечетного.

В наших обозначениях дисбаланс $\mathrm{Im}b(v, u) = z$ при $z = 2k$ как раз соответствует $DL^f = E\left[\lambda(\pi,2k)\right]$.

В табл. 4 приводятся для сравнения результаты оценки максимального значения смещения линейной аппроксимационной таблицы случайной подстановки, полученные при использовании аппроксимирующих выражений (10), аппроксимации, использованной в выражении (7) и точного расчета по формуле (6).

В итоге, если вспомнить выражение для интересующего нас значения максимальной дифференциальной вероятности (максимальной вероятности полного дифференциала) $DP^f_{\max}$, то для $k_{\max}=2k^*_D$ можем записать:

$$DP^f_{\max}=\frac{2k^*_D}{2^n}.$$

Таблица 4

Сравнение результатов, полученных различными путями

n	Значение x для нормального закона	Значение x для нашей аппроксимации	Расчетное значение x
8	16	12,81	16—17
16	334 ($2^{8,38}$)	328,42	374
20	1466	1662,62	1670
24	6342	8417	7302
28	27142	42611,346	31504
32	115080 (2^{17})	215719	135649
128	62316975567822669939 ≈ ≈ 2^{67} → » 2^{-122}	17324119207854702237560 ≈ ≈ 2^{75} → ≈ 2^{-104}	—

В работе [12] приведено расчетное соотношение, являющееся хорошей аппроксимацией решения уравнения (5):

$$DP^f_{\max}=\frac{n+4}{2^n}. \qquad (11)$$

Приведем теперь результаты оценки максимума дифференциальной вероятности для 128-битного шифра.

Из формулы (11) получаем:

$$DP^f_{\max}\leq\frac{128+4}{2^{128}}=2^{-121}.$$

Расчет по точному соотношению для $n = 128$ приводит к максимальному значению перехода равному 96-и.

$$DP^f_{\max}\leq\frac{96}{2^{128}}=2^{-121,4}.$$

Видно, что использование более точного значения не меняет результата.

Напомним также, что в работе [12] было показано, что для шифра с n-битовым размером входа максимальное значение линейной вероятности (максимальной вероятности линейного корпуса) $LP^f_{\max}$ представляется в виде ($k_{\max}=2k^*_L$):

$$LP^f_{\max}=\left(\frac{2k^*_L}{2^{n-1}}\right)^2.$$

Для линейной аппроксимационной таблицы соотношение (4) для расчета $k_{\max}=2k^*_L$ при больших значениях $n > 20$ оказывается трудным для вычислений. Приведем здесь также оценочное соотношение, предложенное на основе обработки результатов вычислительных экспериментов в [12], являющееся удобной заменой выполнению расчетов по соотношению (4):

$$LP^f_{\max}\leq\left(\frac{\left(\frac{3}{2}\right)^n}{2^{n-1}}\right)^2.$$

Использование представленных аппроксимирующих соотношений для 128-ми битного шифра позволяет получить граничные значения (слева и справа) такого вида:

$$2^{-122}\leq LP^f_{\max}\leq 2^{-104}.$$

ISSN 2226-3780

Заметим, однако, что аппроксимация нормальным законом для значений $n \geq 24$ получается существенно точнее нашей аппроксимации (судя по приведенным данным, отношение расчетного и аппроксимирующего выражений для аппроксимации в виде нормального закона принимает значения: при $n = 20 \rightarrow \frac{1670}{1466} = 1{,}139$ при $n = 24 \rightarrow \frac{7302}{6384} = 1{,}144$, при $n = 32 \rightarrow \frac{135649}{115080} = 1{,}178$). Если считать, что близкое к этому соотношение (отношение меньше двойки) сохранится и для больших значений n, то можно прийти к ожидаемому значению вероятности более близкому к левой из двух приведенных границ, т. е. в качестве достаточно точной оценки линейной вероятности для интересующего нас битового размера входа в шифр n = 128 следует рассматривать значение $LP^f_{\max} = 2^{-122}$.

5. Выводы

В итоге получены расчетные соотношения для определения максимальных значений полных дифференциалов и линейных корпусов блочных симметричных шифров. С помощью этих соотношений найдены значения вероятностей максимумов дифференциалов и смещений линейных корпусов для шифра Rijndael (и других 128-битных шифров, в частности шифров, представленных на Украинский конкурс), которые можно рассматривать как показатели доказуемой безопасности этих шифров.

Как следует из полученных результатов показатели стойкости шифров к атакам дифференциального и линейного криптоанализа получаются близкими друг к другу, а практически равными одному и тому же значению $DP^f_{\max} = LP^f_{\max} = 2^{-121}$.

Литература

1. Лисицкая, И. В. Методология оценки стойкости блочных симметричных шифров [Текст] / И. В. Лисицкая // Автоматизированные системы управления и приборы автоматики. — 2011. — № 163. — С. 123—133.
2. Лисицкая, И. В. Сравнение по эффективности суперблоков некоторых современных шифров [Текст] / И. В. Лисицкая // Радіоелектроніка. Інформатика. Управління. — Запоріжжя, 2012. — № 1(26). — С. 37—43.
3. Горбенко, И. Д. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа [Текст] / И. Д. Горбенко, В. И. Долгов, И. В. Лисицкая, Р. В. Олейников // Прикладная радиоэлектроника. — 2010. — Т. 9, № 3. — С. 212—320.
4. Лисицкая, И. В. Методология оценки стойкости блочных симметричных криптопреобразований на основе уменьшенных моделей [Текст] : дисс. ... докт. тех. наук: 05.13.05 / И. В. Лисицкая. — 2012. — 293 с.
5. Baignoires, T. Proving the Security of AES Substitution-Permutation Network [Electronic resource] / Thomas Baignoires, Serge Vaudenay. — 2004. — 16 p. — Available at: \www/URL: http://lasecwww.epfl.ch
6. Keliher, L. Toward Provable Security Against Differential and Linear Cryptanalysis for Camellia and Related Ciphers [Text] / Liam Keliher // International Journal of Network Security. — Sept. 2007. — Vol. 5, No. 2. — P. 167—175.
7. Keliher, L. New method for upper bounding the maximum average linear hull probability for SPNs [Text] / L. Keliher, H. Meier, S. Tavares // Advances in Cryptology. EUROCRYPT 2001, LNCS 2045. — Springer-Verlag, 2001. — P. 420—436.
8. Keliher, L. Improving the upper bound on the maximum average linear hull probability for Rijndael [Text] / L. Keliher, H. Meijer, S. Tavares; S. Vaudenay, A. M. Youssef (Eds.) // Advances in Cryptology, Selected Areas in Cryptography'01, LNCS 2259. — Springer-Verlag, 2001. — P. 112—128.
9. Алексийчук, А. Н. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и относительно алгебраических атак, основанных на гомоморфизмах [Текст] / А. Н. Алексийчук, Л. В. Ковальчук, Е. В. Скрыпник, А. С. Шевцов // Прикладная радиоэлектроника. — 2008. — Т. 7, № 3. — С. 203—209.
10. Sano, F. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis [Text] / F. Sano, K. Ohkuma, H. Shimisu, S. Kawamura // IEICE Trans. Fundamentals. — January 2003. — Vol. E86-A, No. 1. — P. 37—46.
11. Олейников, Р. В. Дифференциальные свойства подстановок [Текст] / 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 [Текст] / В. И. Долгов, И. В. Лисицкая, О. И. Олешко // Прикладная радиоэлектроника. — Харьков: ХНУРЭ, 2010. — Т. 9, № 3. — С. 334—340.
13. O'Connor, L. J. On the Distribution of Characteristics in Bijective Mappings [Text] / Luke O'Connor; T. Helleseth (ed.) // Advances in Cryptology. EUROCRIPT 93, Lecture Notes in Computer Science. — Springer-Verlag, 1994. — Vol. 795. — P. 360—370.
14. O'Connor, L. Properties of Linear Approximation Tables [Text] / Luke O'Connor // Fast Software Encryption Lecture Notes in Computer Science. — 1995. — Vol. 1008. — P. 131—136.
15. Лисицкая, И. В. Свойства законов распределения XOR таблиц и таблиц линейных аппроксимаций случайных подстановок [Текст] / И. В. Лисицкая // Вісник Харківського національного університету імені В. Н. Каразіна. — 2011. — № 960, Вип. 16. — С. 196—206.
16. Daemen, J. Probability distributions of Correlation and Differentials in Block Ciphers [Electronic resource] / Joan Daemen, Vincent Rijmen. — April 13, 2006. — P. 1—38. — Available at: \www/URL: http://eprint.iacr.org/2005/212.pdf

МАКСИМАЛЬНІ ЗНАЧЕННЯ ПОВНИХ ДИФЕРЕНЦІАЛІВ І ЛІНІЙНИХ КОРПУСІВ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

Наводяться розрахункові співвідношення для визначення максимальних значень переходів XOR таблиць і зміщень таблиць лінійних апроксимацій випадкових підстановок, на основі яких у відповідності з новою методологією оцінки стійкості блокових симетричних шифрів до атак диференціального та лінійного криптоаналізу розрахунковим шляхом визначаються показники доказової безпеки ряду сучасних шифрів.

Ключові слова: випадкова підстановка, блокові симетричні шифри, показники доказової стійкості.

Лисицкий Константин Евгеньевич, *кафедра безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, Украина,* ***e-mail: konstantin.lisickiy@mail.ru****.*

Лисицький Костянтин Євгенійович, *кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Україна.*

Lysytskiy Konstantin, *Kharkiv National University of Radio Electronics, Ukraine,* ***e-mail: konstantin.lisickiy@mail.ru***