УДК 621. 391:519.2:519.7

И.В. Лисицкая

Харьковский национальный университет радиоэлектроники, Харьков

О НОВОЙ МЕТОДИКЕ ОЦЕНКИ СТОЙКОСТИ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ К АТАКАМ ДИФФЕРЕНЦИАЛЬНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА

Приводится анализ существующих подходов к оценке показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа. Отмечаются недостатки и ограничения существующих методик. Излагается сущность новой идеологии (системы взглядов) к оценке стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, опирающейся на возможности предложенного ускоренного метода криптоанализа БСШ, основой которого является разработка и исследование свойств уменьшенных моделей прототипов, а также использующей установленный в процессе исследований факт, (положение) что современные шифры асимптотически (при полном наборе цикловых преобразований) повторяют свойства случайных подстановок соответствующей степени.

Ключевые слова: *блочные симметричные шифры, доказуемая безопасность, дифференциальный криптоанализ, линейный криптоанализ, малые модели шифров, законы распределения переходов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок, случайные шифры.*

Введение

Последнее десятилетие стало особым для Украинской криптографии. Передовые в технологиях защиты страны пошли на принятие новых стандартов блочного симметричного шифрования. Необходимость принятия нового (национального) стандарта шифрования стала очевидной и для Украины. Повторяя шаги, предпринятые США и Европейскими странами, Украина тоже прошла через свой внутренний конкурс по выдвижению кандидатов на национальный стандарт БСШ, на который было представлено пять предложений.

Опыт показывает, что выполнение экспертизы современного блочного шифра и уровень ответственности при принятии соответствующего решения является непростой задачей, требующей привлечения значительных временных и интеллектуальных ресурсов. За короткое время проведения конкурса потребовалось в ограниченные временные сроки найти не только убедительные теоретические обоснования принимаемым решениям, получить которые в криптографии, как правило, очень непросто, но и прийти к реальным практическим результатам, позволяющим, в конце концов, накопить фактические данные для сравнительного анализа претендентов. Уже сама обстановка и условия проведения конкурса определили необходимость не только освоения последних достижений теоретической криптографии, но и поиска и разработки новых подходов и приемов в методах криптоанализа, позволяющих существенно сократить временные затраты на проведение экспертизы и оценку основных криптографических показателей представленных решений.

В процессе анализа существующих подходов и методик, оценки их возможностей и объективности (точности) представляемых ими данных накопился значительный критический материал. Кроме того, возникли новые идеи и предложения, позволившие в значительной степени изменить всю систему взглядов к оценке показателей стойкости БСШ, и, прежде всего, к формированию оценок стойкости БСШ к атакам дифференциального и линейного криптоанализа.

В этой работе в первом и втором разделах мы выполняем анализ состояния и возможностей современного научно-методического аппарата, применяемого в криптографии для оценки показателей стойкости блочных симметричных шифров (БСШ) к атакам дифференциального и линейного криптоанализа, и затем в третьем разделе излагаем наши идеи по реализации ускоренных методов криптоанализа блочных симметричных шифров и сущность новой идеологии (системы взглядов) по оценке стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, родившейся в процессе совершенствования научно-методического аппарата теории стойкости.

1. Формирование и содержание научно-методического аппарата оценки доказуемой безопасности БСШ

Мы здесь кратко напомним результаты некоторых известных работ, посвященных формированию оценок доказуемой безопасности блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, характеризующих подходы и методы, используемые и развиваемые в настоящее время.

Начнем с того, что довольно быстро стало ясно [1], что понятие ″ характеристика″, использованное

первооткрывателями дифференциального криптоанализа Эли Бихамом и Ади Шамиром, не полностью характеризует показатель стойкости шифра к атакам дифференциального криптоанализа. Более полным и точным отражением существа вопроса является понятие ″дифференциала″ (полного дифференциала) шифра.

Четырьмя годами позже, Nyberg и Knudsen [2] первыми показали пример блокового шифра, чья максимальная дифференциальная вероятность оказалась достаточно малой; они назвали такое свойство ″доказуемой безопасностью″ против дифференциального криптоанализа.

С легкой руки K. Nyberg [3] в криптографической литературе появилось понятие δ-равномерности. Напомним здесь его, так как оно является весьма популярным:

Определение. Пусть G_1 и G_2 конечные Абелевые группы. Отображение $F: G_1 \to G_2$ называется дифференциально δ-равномерным, если для всех $\alpha \in G_1$, $\alpha \neq 0$ и $\beta \in G_2$

$$|\{z \in G_1 | F(z + \alpha) - F(z) = \beta\}| \leq \delta.$$

В соответствии с этим определением высокие характеристики стойкости преобразования F к атакам дифференциального криптоанализа связаны с малыми значениями δ-равномерности. Очевидно, что требование малых значений δ-равномерности эквивалентно требованию малых значений максимумов дифференциальной таблицы отображения.

В это же время K. Nyberg замечает, что подобная ситуация складывается и в линейном криптоанализе. В своей публикации [4] она показывает, что коллекция (полный набор) линейных характеристик, которую она назвала ″линейным корпусом″ (″linear hull″) должна быть принята к рассмотрению для точной оценки устойчивости шифра против атак линейного криптоанализа. С тех пор все подходы к оценке стойкости шифров к дифференциальному и линейному криптоанализу строятся с пользованием максимальных значений полных дифференциалов и линейных корпусов. Следует отметить, что уже с этих первых работ прослеживается стремление авторов связать показатели стойкости шифров с дифференциальными и линейными свойствами входящих в шифры нелинейных преобразований, получивших название после работ Эли Бихама и Ади Шамира S-блоков.

Отметим здесь и работу Мицури Мацуи [5], в которой предлагается новая методология для исследования блоковых (Фейстель-подобных) шифров с доказуемой безопасностью к атакам дифференциального и линейного криптоанализа. Не касаясь существа предложения Мацуи, отметим, что и в этой работе автор связывает формируемые оценки показателей доказуемой стойкости шифров с дифференциальными свойствами S-блоков, входящих в рассматриваемые преобразования.

Отмеченные работы инициировали целый поток публикаций по обоснованию подходов к оценке показателей доказуемой безопасности к атакам линейного и дифференциального криптоанализа и для шифров с SPN структурой. Приведем примеры некоторых их них.

В [6], как утверждают авторы, доказывается, что SPN (подстановочно-перестановочная схема) структура с максимальным, как они говорят, диффузионным слоем обеспечивает доказуемую безопасность против дифференциального и линейного криптоанализа в том смысле, что вероятность каждого дифференциала (соответственно линейного корпуса) ограничена значением p^n (соответственно q^n), где p (соответственно q) является максимальной дифференциальной (соответственно линейной) вероятностью n S-блоков, используемых в подстановочном слое.

В [7] 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 по их расчётам верхнюю границу MALHP SPN шифров $UB = 2^{-75}$ и соответствующую нижнюю границу сложности данных $\frac{32}{UB} = 2^{80}$ (для 96,7% отношения успеха). Полученные результаты связываются с линейными свойствами входящих в шифр S-блоков.

В [8] на основе рассмотрения значений распределения линейных вероятностей для (уникального) S-блока Rijndael-я эта верхняя граница улучшается. Получена новая верхняя граница для MALHP. Для Rijndael-я с 9 циклами приводится 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 [9] 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. По-

казывается, 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 других исследователей Keliher-a, Meijer-a, и Tavares-a.

В [10] определены аналитические верхние оценки средних вероятностей дифференциальных и линейных характеристик блочных шифров, построенных по схеме шифра ″Калина-128″, представленного на украинский конкурс по отбору кандидата на национальный стандарт блочного симметричного шифрования. В частности, в работе приводятся такие оценки для отмеченных показателей: $\mathrm{EDP} \le 2^{-130}$, $\mathrm{ELP} \le 2^{-130}$. Авторы относят эти оценки к показателям практической стойкости шифра.

В [11] расширяется теорема Хонга и др., которая дает верхние границы для максимумов средних вероятностей дифференциалов и линейных корпусов (MADP и MALHP) 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 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-a и др. Результат опять связывается с дифференциальными и линейными свойствами входящих в шифр S-блоков и числом ветвлений.

Можно привести и ряд других работ, посвященных оценке показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа, в которых S-блоки выступают как одна из главных составляющих обеспечения стойкости.

2. Результаты анализа известных работ

Первый вывод, который можно сделать из приведенных результатов, состоит в том, что в основе всех подходов к оценке показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа лежат процедуры определения максимальных вероятностей полного дифференциала всего шифра и смещения его линейного корпуса (линейной оболочки).

Второй вывод состоит в том, что оценки соответствующих показателей отличаются в значительных пределах. Авторы приводят в своих работах цифры, которые нельзя проверить экспериментом, так что предлагаемые оценки, изменяющиеся в больших пределах, можно считать в значительной степени субъективными.

Третий вывод состоит в том, что результирующие показатели стойкости шифров практически во всех (в большом числе работ) работах связываются с соответствующими криптографическими показателями, входящих в шифры S блоковых конструкций.

В целом можно заключить, что существующая методика оценки показателей стойкости БСШ является все еще далеко не совершенной. До сих пор всё ещё не удалось получить оценки доказуемой стойкости, обладающие высокой степенью доверия.

Следует заметить, что сам термин доказуемая безопасность введен в криптографии уже давно. Когда говорят о доказуемой Безопасности ("Provable Security"), отмечается в документе [12], 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 $P \ne NP$, 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 К. Нюберг и Л. Кнудсена [2], 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 [4, 5 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) [12]. 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 к 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 выскажем 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.

Возвращаясь пока к обсуждению содержания приведенных здесь работ, хотелось бы отметить, что все развиваемые в них 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 [13] 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. Между прочим, 16-битный шифр Хейса [14], построенный по идеям Х. Фейстеля, при 10 циклах преобразований демонстрирует те же показатели стойкости, что и уменьшенная модель шифра Rijendael. Отметим здесь, что на асимптотические значения показателей стойкости (максимальные значения полных дифференциалов и линейных корпусов) шифр Rijendael выходит за четыре цикла, а шифр Хейса – за шесть-семь.

Стремясь реализовать максимально возможные показатели преобразования по стойкости, разработчики Rijndael-я 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 прозрачную структуру SPN шифра Х. Фейстеля.

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 установили в процессе экспериментов, это не так и, соответственно, действительные показатели стойкости шифров к атакам дифференциального и линейного криптоанализа будут не такими, на которые они рассчитывают.

Все отмеченное выше позволяет заключить, что актуальной является задача разработки новой (усовершенствованной) методики (новой идеологии) оценки показателей стойкости БСШ, обладающей большей адекватностью и точностью. И решение этой непростой задачи удалось найти, опираясь на

идеи и возможности предложенного нами ускоренного метода криптоанализа БСШ, строящегося на основе разработки и исследования свойств уменьшенных моделей прототипов [15].

Применение этого метода позволило детально изучить дифференциальные и линейные свойства уменьшенных моделей многих современных шифров и установить ряд новых принципиальных фактов (положений), относящихся к их дифференциальным и линейным показателям, которые позволили подойти к решению задачи оценки максимальных значений полных дифференциалов и линейных корпусов шифров с совершенно новых позиций. Всё это выразилось в формировании новой методики оценки показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, к изложению сущности которой мы переходим в следующем разделе.

3. Сущность новой методики оценки стойкости блочных симметричных шифров 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 [15], для которых имеющихся вычислительных ресурсов оказывается уже вполне достаточно даже для реализации атак переборного типа. Наши проработки [16, 17, 18, 19, 20, 21, 22] показывают, что большое число хорошо известных алгоритмов шифрования допускают масштабирование (полное масштабирование допускает только шифр Idea, в остальных случаях при ″масштабировании″ приходится отдельные преобразования заменять укрупнёнными). Тем не менее, удается построить уменьшенные модели, которые сохраняют (с учетом ″масштабирования″) все свойства своих прототипов и позволяют решить многие задачи анализа и сравнения показателей стойкости больших версий шифров.

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. На самом деле, результирующие (т.е. получающиеся при использовании полного набора цикловых преобразований) показатели стойкости шифров определяются практически только размером битового входа в шифр.

Второй важный вывод, следующий из выполненных исследований, сводится к тому, что современные шифры, такие как Rijndael и многие другие известные шифры, а также шифры Лабиринт, Калина, Мухомор, ADE [23, 24, 25, 26], представленные на украинский конкурс по выбору национального стандарта шифрования, ассимтотически (при полном числе цикловых преобразований) ведут себя как представители семейства случайных шифров, т.е. повторяют дифференциальные и линейные свойства случайных подстановок соответствующей степени, причем с весьма высокой точностью. Если говорить более точно, то законы распределения переходов XOR таблиц (таблиц полных дифференциалов) и смещений таблиц линейных аппроксимаций (линейных корпусов) уменьшенных моделей изученных шифров повторяют соответствующие законы распределения вероятностей случайных подстановок.

Последний факт приводит к третьему важному выводу, заключающемуся в том, что значения максимумов полных дифференциалов и линейных корпусов таких шифров могут быть получены расчетным путем. Для этого можно воспользоваться соответствующими соотношениями, полученными для случайных подстановок.

У нас появились, однако, скептики, которые встали на позицию, что то, что свойственно малым моделям шифров, может оказаться не справедливым для их больших прототипов. Хотя это и противоречит на наш взгляд очевидной идее улучшения характеристик случайности подстановок с увеличением их степени, мы, тем не менее, выполнили комплекс исследований по изучению показателей случайности больших шифров.

Конечно, здесь возможности существенно ограничены размерностью решаемых задач, но и того, что позволяет вычислительный эксперимент, оказалось достаточным, чтобы удостовериться в справедливости нашего вывода. Большие шифры, такие как Rijndael, FOX, ГОСТ при использовании их в режиме зашифрования усеченных (до длины 16 и 32 битов) блоков данных продемонстрировали дифференциальные свойства, повторяющие свойства их уменьшенных версий. Полученные результаты полностью согласуются с соответствующими значениями законов распределения вероятностей случайных подстановок необходимого порядка. Сейчас выполняются исследования линейных показателей больших шифров. Здесь конечно возможности ещё более ограниченные. Однако и в этом случае можно надеяться на подтверждение ожидаемых значений смещений для выборочных значений пар масок входов-выходов линейной аппроксимационной таблицы, имеющих для случайной подстановки специфические значения.

В итоге, сложилась вполне конкретная система взглядов, которую можно рассматривать как новую методологию оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа.

Выводы

1. Существующие подходы к оценке показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа строятся на основе оценки максимумов средних значений дифференциальных и линейных вероятностей (MADP и MALHP), определяемых из таблиц полных дифференциалов и таблиц смещений линейных корпусов.

2. Имеющиеся граничные значения и оценки, полученные для ряда современных шифров, отличаются в значительных пределах, что свидетельствует о несовершенстве существующих подходов.

3. Результирующие показатели стойкости шифров во многих работах связываются с соответствующими криптографическими показателями входящих в шифры S блоковых конструкций.

4. Задача создания и разработки новой (усовершенствованной) методики (новой идеологии) оценки показателей стойкости БСШ, обладающей большей адекватностью и точностью, может быть решена, опираясь на идеи и возможности предложенного ускоренного метода криптоанализа БСШ, строящегося на основе разработки и исследования свойств уменьшенных моделей прототипов.

5. Применение предлагаемого метода позволило установить, что линейные и дифференциальные свойства шифров от свойств S-блоков, используемых при их построении, не зависят. S-блоки влияют лишь на динамику (число циклов) перехода к установившемуся (ассимптотическому) значению. Результирующие (т.е. получающиеся при использовании полного набора цикловых преобразований) показатели стойкости шифров определяются практически только размером битового входа в шифр.

6. С применением развиваемого подхода установлено, что современные шифры, такие как Rijndael и многие другие известные шифры, а также шифры Лабиринт, Калина, Мухомор, ADE, представленные на украинский конкурс по выбору национального стандарта шифрования, ассимтотически (при полном числе цикловых преобразований) ведут себя как представители семейства случайных шифров, т.е. повторяют дифференциальные и линейные свойства случайных подстановок соответствующей степени.

7. Значения максимумов полных дифференциалов и линейных корпусов таких шифров могут быть получены расчетным путем, пользуясь соответствующими соотношениями, полученными для случайных подстановок.

Общим результатом работы, проведенной в отмеченном направлении, следует считать предложенную и апробированную новую идеологию оценки показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа, обладающую большей адекватностью и точностью, и новую методику ускоренного криптоанализа современных шифров, позволяющую выполнить оценки показателей доказуемой стойкости в реальные временные сроки.

Список литературы

1. Lai X. Marcov cipher and differential cryptanalysis, / X. Lai, J.L. Massey, S. Murply // Advances in Cryptology – Eurocrypt'91, Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991.

2. Nyberg K. Provable security against differential cryptanalysis / K. Nyberg, L. Knudsen // Journal of Cryptology. – 1995. – Vol.8, no.1.

3. Nyberg K. Differentially uniform mapping for cryptography / K. Nyberg. – Copyright (c) 1998, Springer-Verlag.

4. Nyberg K. Linear approximation of block ciphers / K. Nyberg // Advances in Cryptology – Eurocrypt'94, Lecture Notes in Computer Science, vol. 950, Springer-Verlag, 1994.

5. Matsui M. On a Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis. IEICE Trans / M. Matsui // FundaMENTALS, vol. E82-A, No. 1 January 1999, P. 117-122.

6. Hong S. Provable Security against Differential and Linear cryptanalysis for SPN Structure / S. Hong, S. Lee, J. Lim, J. Sung, D. Cheon, I. Cho; B. Schneier (Ed.). – FSE 2000, LNCS 1978. – 2001. – P. 273-283.

7. Keliher L. New method for upper bounding the maximum average linear hull probability for SPNs / 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 / L. Keliher, H. Meier, S. Tavares // Eighth Annual International Workshop on Selected Areas in Cryptography (SAC 2001), LNCS 2259, Springer-Verlag, 2001. – P. 112-128.

9. Baignoires Thomas. Proving the Security of AES Substitution-Permutation Network / Thomas Baignoires, Serge Vaudenay [Электронный ресурс]. − 2004. – P. 16. – Режим доступа к ресурсу: http://lasecwww.epfl.ch.

10. Алексийчук А.Н. Оценки практической стойкости блочного шифра "Калина" 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.

11. Sano F. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis / F. Sano, K. Ohkuma, H. Shimizu, S. Kawamura // IEICE Trans. Fundamentals, vol. E86-a, No.1 January 2003. – P. 37-46.

12. 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.

13. Feistel H. Cryptography and computer privacy / H. Feistel // Scientific American, 228(5): 1973. – P. 15-23.

14. Heys H.M. A Tutorial on Linear and Differential Cryptanalysis / H.M. Heys // CRYPTOLOGIA. – 2002. – V. 26, N 3. – P. 189-221.

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

16. Лисицкая И.В. Криптографические свойства уменьшенной версии шифра "Мухомор" / И.В. Лисицкая, О.И. Олешко, С.Н. Руденко, Е.В. Дроботько, А.В. Григорьев // Прикладная радиоэлектроника. – 2010. – Т .9, № 1. – С. 53-59.

17. Долгов В.И. Исследование циклических и дифференциальных свойств уменьшенной модели шифра Лабиринт / В.И. Долгов, И.В. Лисицкая, А.В. Григорьев, А.В. Широков // Прикладная радиоэлектроника. – 2009. – Т.8, №3. – С. 283-289.

18. Долгов В.И. Атака на полный дифференциал уменьшенной версии шифра Rijndael / В.И. Долгов, И.В. Лисицкая, В.Э. Хряпин // Прикладная радиоэлектроника. – 2010. – Т.9, №3. – С. 355-360.

19. Лисицкая И.В. Вариации на тему шифра Rijndael / В.И. Долгов, И.В. Лисицкая, А.В. Казимиров // Прикладная радиоэлектроника. – 2010. – Т.9, №3. – С. 321-325.

20. Лисицкая И.В. Анализ усовершенствований шифра Rijndael / И.В. Лисицкая, А.В. Казимиров, Е.Д. Мельничук, А.В. Широков // XIII Международная научно-практическая конференция Безопасность информации в информационно-телекоммуникационных системах, 18-21 мая 2010 г.. – К., С. 46.

21. Долгов В.И. Исследование показателей стойкости БСШ, представленных на Украинский конкурс / В.И. Долгов, И.В. Лисицкая, Р.В. Олейников, В.И. Руженцев // XII Международная научно-практическая конференция "Безопасность информации в информационно-телекоммуникационных системах, 18-21 мая 2009 г. – К., С. 43.

22. Долгов В.И. Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES / В.И. Долгов, А.А. Кузнецов, Р.В. Сергиенко, О.И. Олешко // Прикладная радиоэлектроника. – 2009. – Т.8, № 3. – С. 252-257.

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

24. 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. Кузьміна // Прикладная радиоэлектроника. – 2007. – Том. 6, № 2. – С. 147-157.

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

26. 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.

Поступила в редколлегию 7.04.2011

Рецензент: д-р техн. наук, проф. А.В. Потий, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ПРО НОВУ МЕТОДИКУ ОЦІНКИ СТІЙКОСТІ БЛОЧНИХ СИМЕТРИЧНИХ ШИФРІВ ДО АТАК ДИФЕРЕНЦІЙНОГО ТА ЛІНІЙНОГО КРИПТОАНАЛІЗУ

І.В. Лисицька

Приводиться аналіз існуючих підходів до оцінки показників стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу. Відзначаються недоліки і обмеження існуючих методик. Викладається сутність нової ідеології (системи поглядів) до оцінки стійкості блокових симетричних шифрів до атак диференціального і лінійного криптоаналізу, що спирається на можливості запропонованого прискореного методу криптоаналізу БСШ, основою якого є розробка і дослідження властивостей зменшених моделей прототипів, а також що використовує встановлений в процесі досліджень факт, (положення) що сучасні шифри асимптотично (при повному наборі циклових перетворень) повторюють властивості випадкових підстановок відповідного степеня.

Ключові слова: *блокові симетричні шифри, доказова безпека, диференційний криптоаналіз, лінійний криптоаналіз, зменшені моделі шифрів, закони розподілу переходів XOR таблиць і зсувів таблиць лінійних апроксимацій.*

ABOUT THE NEW METHOD OF FIRMNESS ESTIMATION OF SYMMETRIC BLOCK CIPHERS TO DIFFERENTIAL ATTACK AND LINEAR CRYPTANALYSIS

I.V. Lysytska

There is the analysis of existing approaches to evaluation of stability indices symmetric block cipher to differential attack and linear cryptanalysis in this work. The given work insisted upon the shortcomings and limitations of existing methods. The given work is set forth the essence of the new ideology (belief system) to assess stability of symmetric block cipher to differential attack and linear cryptanalysis, which rests on the possibility of a rapid method of cryptanalysis BSSH which basis is to develop and study the properties of reduced models of prototypes, and using established in fact the research, that modern ciphers asymptotically (with full set of cyclic transformations) repeating properties of random substitutions corresponding degree.

Keywords: *symmetric block ciphers, provable security, differential cryptanalysis, linear cryptanalysis, reduced model ciphers, laws conversions XOR distribution tables and table bias linear approximations.*