УДК 681.3.06: 519.248.681

О МЕТОДАХ ОЦЕНКИ СТОЙКОСТИ К АТАКЕ УСЕЧЕННЫХ ДИФФЕРЕНЦИАЛОВ

РУЖЕНЦЕВ В.И.

Рассматриваются существующие методы выполнения оценки стойкости байт-ориентированных шифров к атаке усеченных дифференциалов. Обосновывается подход, позволяющий оценить стойкость фейстель-подобных шифров с rijndael-подобным цикловым преобразованием и большим размером блока (более 128 битов) к атаке усеченных дифференциалов.

1. Состояние проблемы

Одна из разновидностей дифференциальных атак на блочные симметричные шифры (БСШ) была предложена в середине 90-х годов Л. Кнудсеном [1]. В своей работе он показал, что для организации атаки иногда эффективнее предсказывать не полную разность, а лишь некоторую ее часть. Такая методика получила название криптоанализ усеченных дифференциалов. Считается, что для байт-ориентированных шифров естественным является изучение усеченных дифференциалов особого вида, для которых усечение заключается не в исключении из рассмотрения отдельных битов входной или выходной разности, а в рассмотрении активности S-блоков. Поскольку используемые в современных шифрах S-блоки (S-подстановки) чаще всего задают закон отображения байт-в-байт, то дифференциалы, рассматривающие активность S-блоков, часто называют байтовыми дифференциалами. В литературе существует описание атак усеченных (байтовых) дифференциалов на ослабленные варианты байт-ориентированных шифров SAFER, E2 [2,3]. В дальнейшем под усеченными понимаются байтовые дифференциалы.

Для оценки стойкости (n+1)-циклового БСШ к атаке усеченных дифференциалов выполняют поиск байтовых дифференциалов или байтовых дифференциальных характеристик, покрывающих n циклов и обладающих достаточно высокой вероятностью. Известные методы выполнения такого поиска [4, 5] разработаны для 128-битных шифров, но, как показано далее, не позволяют оценить стойкость фейстель-подобных шифров с размером блока 256 и более битов. В то же время тенденции развития симметричной криптографии связаны с увеличением размера блока БСШ и уже в ближайшее время могут появиться байт-ориентированные фейстель-подобные БСШ с размером блока 256 и более битов. В этих условиях актуальной является задача обоснования подхода, который позволил бы тестировать стойкость таких шифров. Решение этой задачи для определенного класса шифров и является **целью** данного исследованя.

2. Методы и алгоритмы оценки стойкости шифров

Прежде чем перейти к рассмотрению известных методов оценки стойкости шифров, остановимся на некоторых особенностях усеченных дифференциалов. В таких дифференциалах разность представляется в виде последовательности битов, каждый из которых отражает активность одного S-блока (1 – ненулевая разность – S-блок активный; 0 – S-блок неактивный). Последовательность битов, описывающих активность всех байтов блока (полублока), будем называть вектором активизации.

Рассмотрение работ [2,3,5] позволило выделить требования, которым должен отвечать байтовый дифференциал для того, чтобы он был эффективным, т.е. на его основе могла бы быть организована атака, обладающая меньшей сложностью, чем атака полного перебора. В соответствии с первым требованием для выполнения атаки на n-цикловый шифр байтовый дифференциал должен покрывать, по крайней мере, n-1 цикл. Второе требование заключается в том, что вероятность эффективного усеченного дифференциала $p_{усд}$ должна быть больше вероятности получения на выходе того же вектора активизации при произвольном (случайном) векторе активизации на входе ($p_{усд} > p_{сл}$). Случайный входной вектор активизации предполагает равновероятность всех значений выходной разности, и тогда $p_{сл} = (2^{-8})^{na}$, где na – число неактивных байтов в выходной разности. Следует заметить, что для усеченного дифференциала, отвечающего рассмотренным требованиям, будет выполняться и традиционное для обычных дифференциалов ограничение: $p_{усд} > 2^{-L}$, где L – длина блока в битах.

Теперь перейдем к рассмотрению существующих подходов к выполнению оценки стойкости байт-ориентированных БСШ к атаке усеченных дифференциалов.

В работе [4] предложен метод нахождения вероятностей байтовых дифференциалов, однако, как показывают наши исследования [6], он требует больших вычислительных затрат (время его работы растет экспоненциально с ростом числа циклов) и поэтому позволяет оценить вероятность дифференциалов, покрывающих небольшое число циклов 128-битных шифров. Процедура поиска эффективных усеченных дифференциалов на основе такого метода требует еще большей вычислительной сложности, а значит, он будет работать для еще меньшего числа циклов 128-битных БСШ. Увеличение размера блока БСШ приводит к резкому увеличению времени, необходимого для выполнения такого поиска.

В [5] предложен метод поиска эффективных байтовых характеристик для фейстель-подобного шифра со 128-битным блоком. Напомним основные этапы алгоритма, реализующего этот метод.

2.1. Алгоритм поиска эффективных байтовых характеристик для R-циклового фейстель-подобного шифра со 128-битным блоком [5]

На предвычислительном этапе формируется таблица, отражающая вероятности переходов различных векторов активизации на входе 64-битной (8-байтной) шифрующей функции в различные комбинации активных байтов на ее выходе. Размер такой таблицы $2^8 \times 2^8$ ячеек памяти (2^8 возможных вариантов векторов активизации S-блоков на входе и столько же на выходе). Затем в каждой строке, соответствующей определенному входному вектору активизации, выходные векторы активизации сортируются по убыванию вероятности перехода в них.

1. Для каждого входного вектора активизации (2^{16} вариантов) вызывается процедура r_roundf.

2. r_roundf: Из таблицы, полученной на предвычислительном этапе, в порядке убывания вероятности выбираются возможные значения выходного вектора активизации. Если результирующая вероятность с учетом вероятности текущего перехода меньше, чем 2^{-128}, то выбирается следующее значение (текущее отбрасывается). Если же вероятность больше, чем 2^{-128}, то вызывается процедура r_xor.

3. r_xor: При сложении по XOR двух 8-байтовых полублоков соответствующие им биты активизации складываются по правилам, представленным в табл. 1.

Таблица 1

Знач. 1-го бита	Знач. 2-го бита	Результат	Вероятность
0	0	0	1
0	1	1	1
1	0	1	1
1	1	0	2^{-8}
		1	$1-2^{-8}\approx 1$

Для каждого из возможных результатов операции XOR (число возможных результатов равно 2^a, где a – число случаев, когда складываются активные байты) проверяются два условия:

а) результирующая вероятность $p_{rez} < 2^{-128}$;

б) результирующая вероятность $p_{rez} < 2^{-8c}$, где c – число неактивных байтов в выходной разности.

Если хотя бы одно из условий выполняется – выбирается следующее значение результата операции XOR (текущее значение отбрасывается).

Если номер текущего цикла равен числу циклов R, то найденная характеристика записывается в файл, если нет – вызывается процедура r_roundf.

Данный метод, как и предыдущий, основан на переборе всех возможных выходных векторов активизации в каждом цикле, но поскольку производится поиск байтовой характеристики, а не байтового дифференциала, результирующая вероятность может контролироваться в ходе построения дифференциальной характеристики. Если после какого-либо цикла эта вероятность будет ниже порогового значения, то такой вариант сразу отбрасывается. Таким образом, если среди всех *r*-цикловых байтовых дифференциальных характеристик нет эффективных, то поиск характеристик, покрывающих большее число циклов, не приведет к увеличению вычислительной сложности этого алгоритма.

Этот метод, как и метод из [4], чувствителен к увеличению размера блока. Если при поиске *r*-цикловых эффективных байтовых характеристик для 128-битного фейстель-подобного шифра в предельном случае (когда в каждом цикле возможны переходы во все выходные векторы активизации) приходится рассматривать 2^{8r} вариантов байтовых характеристик, то уже для 256-битного шифра аналогичный поиск потребует рассмотрения 2^{16r} вариантов.

В целях сравнения методов из [4] и [5] их применили для оценки стойкости одинаковых шифров. Рассматривались фейстель-подобные шифры с “rijndael-подобным” цикловым преобразованием и небольшим размером блока (не более 128 битов). Под “rijndael-подобным” цикловым преобразованием понимается последовательное выполнение следующих операций: сложение с подключом, нелинейные байтовые подстановки, линейные преобразования двух видов. Первый вид линейных преобразований аналогичен процедуре MixColumn шифра Rijndael и заключается в умножении каждого *n*-байтного вектора, называемого колонкой, на специальную матрицу размером $n \times n$ байтов. Аналогом преобразований второго вида является процедура ShiftRow, суть которой заключается в равномерном распределении байтов каждой колонки по всем колонкам. Для каждой эффективной байтовой характеристики, найденной по методу [5], была вычислена вероятность соответствующего байтового дифференциала с помощью метода из [4]. Некоторые из полученных результатов представлены в табл. 2.

Таблица 2

Размер блока, байты	Число колонок в полублоке, *nc*	Число байтов в колонке, *n*	Макс. число циклов	Макс. вер. байтовой дифф. хар.	Число байтовых хар. в байт. дифф.	Вер. байтового дифф.
8	1	4	2	1	1	1
16	2	4	4	2^{-16}	1	2^{-16}
16	1	8	2	1	1	1

Как следует из полученных результатов, во всех случаях эффективная байтовая характеристика оказывалась единственной в соответствующем дифференциале. Это свидетельствует об идентичности оценок, получаемых с использованием методов из работ [4, 5].

Для того чтобы стало возможным тестирование стойкости фейстель-подобных БСШ с большим размером блока, появилась идея дополнить метод из [5] тем, что на каждой итерации рассматривать не все возможные выходные векторы активизации, а лишь некоторые из них – “наиболее перспективные”.

Остановимся на обосновании предлагаемого подхода более подробно. Рассмотрим фейстель-подобные шифры с rijndael-подобным строением цикловой функции. Линейные преобразования в таких шифрах построены на основе МДР-кодов (коды с

максимально-допустимым расстоянием). Главное преимущество МДР-преобразований заключается в том, что они гарантируют максимальный лавинный эффект для покрываемых преобразованием S-блоков (сумма активных S-блоков в контексте дифференциального или линейного криптоанализа до и после такого линейного преобразования будет максимально возможной, т.е. $n+1$, где n – число S-блоков, покрываемых МДР-преобразованием).

Остановимся на некоторых особенностях реализации алгоритма из [5] для шифров, использующих МДР-преобразования. В упомянутом алгоритме применяется таблица, которая содержит вероятности переходов различных векторов активизации на входе линейного преобразования в различные векторы активизации на его выходе. Если в шифрующей функции используются такие линейные преобразования как умножение n-байтных векторов на МДР-матрицу размером n×n, то для таблицы потребуется (n+1)×(n+1) ячеек памяти. Это следует из свойства линейных преобразований на основе МДР-кодов (коды с максимально-допустимым расстоянием), которое заключается в том, что вероятность перехода входной активизации байтов в выходную при умножении на МДР-матрицу зависит от числа активных байтов на входе и выходе и не зависит от расположения активных байтов во входном и выходном векторах активизации. Так, для шифра Rijndael размер таблицы составит 5×5 ячеек памяти. В шифре Rijndael, как известно, в ходе преобразований рассеивания производится умножение каждой 4-байтовой колонки на МДР-матрицу размером 4×4 байта, поэтому на входе, как и на выходе, может быть 0, 1, 2, 3 или 4 активных байта, т.е. 5 возможных вариантов на входе и 5 – на выходе. Рассмотрим процесс создания такой таблицы для МДР-преобразования, покрывающего n S-блоков. Для её построения будем использовать свойство МДР-преобразований, которое было выявлено эмпирическим путем при анализе МДР-преобразований небольшой размерности. Суть этого свойства заключается в том, что при вариации по всем возможным разностям на входе МДР-преобразования число случаев ns, когда произойдет переход некоторого входного вектора активизации с ina активными байтами в некоторый выходной вектор активизации с *ota* активными байтами, будет одинаково для вариантов с равными значениями суммы ina+ot*a*. Поскольку сумма ina+ota при умножении на МДР-матрицу размером n×n может принимать n значений (от n+1 до 2n), то будет всего n различных значений для параметра ns. Эти значения могут быть последовательно вычислены по следующей формуле:

$$ns_i = 255^i - \sum_{j=1}^{i-1} ns_j \cdot C_m^j;\ i = ina + ota - n = \overline{1,n},$$

где 255 – число вариантов разности для активного байта; C_y^x – число сочетаний из x по y; n – размерность МДР-матрицы. Используя массив ns, можно вычислить вероятность любого перехода. Для этого необходимо определить число активных байтов ina во входном векторе активизации и число активных байтов ota в выходном векторе активизации. Вероятность перехода вычисляется по формуле

$$P_{mds} = \frac{ns_{ina+ota-n}}{255^{ina}}.$$

В табл. 3 приведены вероятности переходов векторов активизации с различным числом активных S-блоков на входе и выходе МДР-преобразования, покрывающего 8 S-блоков (n = 8).

Таблица 3

Вых. / Вх.	0	1	2	3	4	5	6	7	8
0	2^0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	2^0
2	0	0	0	0	0	0	0	$2^{-7.99}$	$2^{-0.04}$
3	0	0	0	0	0	0	$2^{-15.9}$	$2^{-8.04}$	$2^{-0.04}$
4	0	0	0	0	0	$2^{-23.9}$	$2^{-16.0}$	$2^{-8.04}$	$2^{-0.04}$
5	0	0	0	0	$2^{-31.9}$	$2^{-24.0}$	$2^{-16.0}$	$2^{-8.04}$	$2^{-0.04}$
6	0	0	0	$2^{-39.9}$	$2^{-32.0}$	$2^{-24.0}$	$2^{-16.0}$	$2^{-8.04}$	$2^{-0.04}$
7	0	0	$2^{-47.9}$	$2^{-40.0}$	$2^{-32.0}$	$2^{-24.0}$	$2^{-16.0}$	$2^{-8.04}$	$2^{-0.04}$
8	0	$2^{-55.9}$	$2^{-48.0}$	$2^{-40.0}$	$2^{-32.0}$	$2^{-24.0}$	$2^{-16.0}$	$2^{-8.04}$	$2^{-0.04}$

С помощью такой таблицы может быть вычислена вероятность перехода входного вектора активизации в выходной для одного цикла шифра, в котором применяются МДР-преобразования.

Рассмотрим теперь два последовательных цикла фейстель-подобного шифра, использующего в шифрующей функции "rijndael-подобные" преобразования. Очевидно, что для первого цикла чем больше активных S-блоков в выходной разности, тем выше вероятность перехода. Во втором цикле чем больше активных S-блоков в каждой активной колонке (которая содержит хотя бы один активный S-блок), тем, в соответствии с табл. 3, больше возможных вариантов выходного вектора активизации, а вероятности переходов при этом остаются неизменными. Тогда на выходе первого цикла среди всех векторов активизации с одинаковой комбинацией активных колонок наиболее перспективным является тот, который содержит максимальное число активных S-блоков в каждой из активных колонок. Следуя такому отбору перспективных выходных векторов активизации, число рассматриваемых вариантов на каждом цикле может быть значительно уменьшено. Число рассматриваемых на каждом цикле выходных векторов активизации будет равно числу возможных комбинаций активных колонок и может быть вычислено по формуле

$$V = \sum_{i=1}^{nc-1} C_{nc}^i, \qquad (1)$$

где C_{nc}^i – число сочетаний из i по nc; nc – число колонок в полублоке. Значение V зависит от числа колонок и обычно не превосходит нескольких десятков, следовательно, становится возможным тестирование шифров с большим размером блока. Приведем итоговый алгоритм, реализующий предлагаемый подход.

2.2. Алгоритм поиска эффективных байтовых характеристик для R-цикловых фестель-подобных шифров с "rijndael-подобной" шифрующей функцией и размером блока L битов

На предвычислительном этапе формируется таблица с расчетными значениями вероятностей переходов различных комбинаций активных байтов на входе МДР-

преобразования в различные комбинации на его выходе.

1. Для того чтобы на первом цикле не происходило уменьшение вероятности байтовой характеристики, в качестве претендентов на входные векторы активизации рассматриваются векторы с нулевым правым полублоком (все байты неактивны). Для каждого такого входного вектора активизации вызывается процедура r_roundf.

2. r_roundf: Если текущий цикл последний, то в качестве выходного вектора активизации рассматривается вариант с максимальным числом активных байтов. Такой переход имеет наибольшую вероятность.

Если текущий цикл не последний, то перебираются все возможные комбинации активных колонок для выходного вектора активизации (число таких комбинаций V определяется по формуле (1)).

Для каждой комбинации активных колонок формируется выходной вектор активизации с максимальным количеством активных S-блоков в активных колонках и вычисляется вероятность получения такого вектора.

Если результирующая вероятность меньше, чем 2^{-L}, то переходим к рассмотрению следующего варианта комбинации активных колонок. В противном случае вызывается функция r_xor.

3. r_xor: С помощью правил сложения из табл. 1 вычисляется вероятность получения после операции XOR нужной комбинации активных колонок с максимальным числом активных байтов в каждой активной колонке. С учетом этой вероятности формируется значение результирующей вероятности и проверяются два условия:

а) результирующая вероятность $p_{rez} < 2^{-L}$;

б) результирующая вероятность $p_{rez} < 2^{-8c}$, где c – число неактивных байтов в текущей выходной разности.

Если хотя бы одно из условий выполняется – выбирается следующее значение результата операции XOR (текущее значение отбрасывается).

Если номер текущего цикла равен числу циклов, то найденная характеристика записывается в файл, если нет – вызывается функция r_roundf.

3. Сравнение результатов и выводы

В целях проверки справедливости предлагаемого подхода и сравнения его с известным аналогом поиск эффективных байтовых характеристик для шифров с размером блока, не превышающим 128 битов, был проведен с использованием известного [5] и предлагаемого методов. Применение метода из [5] позволило найти гораздо больше эффективных характеристик. В то же время лучшие по вероятностным показателям, а значит, и наиболее эффективные байтовые характеристики были найдены в обоих случаях, при этом предлагаемый метод требует значительно меньших вычислительных затрат. Все это свидетельствует о работоспособности предлагаемого подхода для фейстель-подобных шифров с "rijndael-подобной" шифрующей функцией.

С помощью предлагаемого метода были протестированы варианты шифра с большим размером блока. Полученные результаты сведены в табл. 4.

Таблица 4

Размер блока, байты (биты)	Число байтов в колонке, n	Число колонок, nc	Макс. число циклов	Вер. усеч. дифф. хар., $p_{усд}$	$p_{усд}/p_{сл}$
32 (256)	4	4	6	$2^{-88.14}$	232
32 (256)	8	2	4	$2^{-32.11}$	1,5e+7
64 (512)	8	4	6	$2^{-176.42}$	191,3
128 (1024)	8	8	6	$2^{-184.82}$	145,1

Основной результат работы состоит в том, что, на наш взгляд, нам удалось обосновать возможность снижения вычислительной сложности известного метода поиска эффективных байтовых дифференциальных характеристик для фейстель-подобных БСШ. Эта возможность состоит в том, что на каждой итерации рассматриваются не все возможные выходные векторы активизации, как это делалось в известном методе, а лишь некоторые из них – "наиболее перспективные".

Развиваемый подход позволяет выполнить оценку стойкости байт-ориентированных фейстель-подобных БСШ с большим размером блока (вплоть до 1024 битов) и "rijndael-подобной" шифрующей функцией к атаке усеченных дифференциалов.

Литература: 1. *Knudsen L.R.* Truncated and Higher Order Differentials. In B. Preneel, editor, Fast Software Encryption — Second International Workshop, Volume 1008 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, New York, 1995. P. 196–211. **2.** *Knudsen L.R., Berson T.A.* Truncated differentials of SAFER, In Fast Software Encryption - Third International Workshop, FSE'96, Vol. 1039 of Lecture Notes in Computer Science, Berlin, Heidelberg, New York, Springer-Verlag, 1996. **3.** *Matsui M., Tokita T.* Cryptanalysis of reduced version of the block cipher E2, in pre-proceedings of Fast Software Encryption'99. 1999. P. 70-79. **4.** *Sugita M., Kobara K.* Relationships among differential, truncated differential, impossible differential cryptanalyses against word-oriented block cipher like Rijndael, E2 // National Institute of Standards and Technology, http://www.nist.gov/aes. **5.** *Moriai S.*, *Sugita M.*, *Aoki K.* Security of E2 against Truncated Differential Cryptanalysis. In H. Heys and C. Adams, editors, Selected Areas in Cryptography — 6th Annual International Workshop, SAC'99, Vol. 1758 of Lecture Notes in Computer Science, Berlin, Heidelberg, New York, Springer-Verlag, 2000. P. 106–117. **6.** *Долгов В.И., Руженцев В.И.* О методе выполнения оценки стойкости шифра Rijndael к дифференциальным атакам // Радиоэлектроника и информатика. 2002. №1. С. 136-138.

Поступила в редколлегию 20.03.2003

Рецензент: д-р техн. наук, проф. Горбенко И.Д.

Руженцев Виктор Игоревич, аспирант кафедры БИТ ХНУРЭ. Научные интересы: криптография, защита информации. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-94-25.