УДК 004.056.55

В.И. РУЖЕНЦЕВ, канд. техн. наук

ОБ УСЛОВИЯХ ОТСУТСТВИЯ ЭФФЕКТИВНЫХ УСЕЧЕННЫХ БАЙТОВЫХ ДИФФЕРЕНЦИАЛОВ ДЛЯ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Со времени публикации работы [1] общепризнанной является точка зрения о необходимости рассмотрения дифференциалов и их вероятностей для анализа стойкости блочного симметричного шифра (БСШ) к дифференциальным атакам. Только доказав отсутствие дифференциалов, обладающих достаточно высокой вероятностью, можно гарантировать защищенность алгоритма шифрования от дифференциального криптоанализа. В то же время, на практике для новых алгоритмов шифрования обычно оценивают верхнюю границу вероятности дифференциальных характеристик (выполняют проверку практического критерия стойкости по классификации, предложенной в [2]). Такой способ является более простым для реализации, однако в меньшей степени позволяет гарантировать безопасность шифра в случае позитивных результатов проверки.

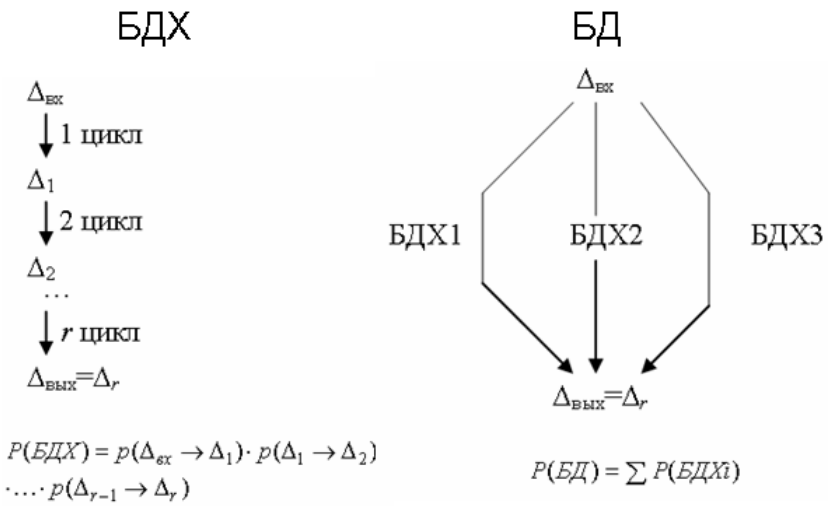
Один из вариантов атаки – атака байтовых дифференциалов – была предложена в работах [3, 4]. В этой атаке также можно выделить байтовые дифференциальные характеристики и байтовые дифференциалы. Для этой разновидности атаки ситуация аналогична: рассмотрение байтовых дифференциальных характеристик (БДХ) – значительно проще реализовать, но рассмотрение байтовых дифференциалов (БД) – дает больше гарантий стойкости. В работах [5, 6] были проанализированы БДХ и БД для rijndael-подобных шифров и во всех случаях отсутствие эффективных БДХ позволяло сделать вывод об отсутствии и эффективных БД. Целью настоящей работы является выявление и описание тех свойств шифрующих преобразований, которые позволяют сделать вывод и об отсутствии эффективных БД для БСШ.

Для достижения поставленной цели в первом разделе рассмотрены основные сведения об атаке усеченных байтовых дифференциалов, во втором разделе рассмотрены основные этапы предложенного в [5] подхода к доказательству отсутствия эффективных БД, в третьем разделе проанализирован и уточнен этот подход и выделены достаточные условия для отсутствия эффективных БД для блочного шифра.

1. Атака усеченных байтовых дифференциалов. Основные термины и определения

В ходе атаки усеченных байтовых дифференциалов [3, 4] через преобразования шифра пытаются провести *векторы активизации*. Каждый бит вектора активизации отражает активность одного байта в обычной разности. Таким образом, вектор активизации содержит столько битов, сколько байтов в блоке, а значение бита определяется активностью байта: «1» – байт активный, «0» – байт пассивный.

Совокупность значений входного и выходного векторов активизации для одного цикла преобразований называется *одноцикловой байтовой дифференциальной характеристикой* (БДХ). По аналогии с обычным дифференциальным криптоанализом «сшивку» нескольких одноцикловых БДХ (условие «сшивки»: входной вектор активизации каждой последующей одноцикловой БДХ равен выходному вектору активизации предыдущей) будем называть *многоцикловой БДХ*. Вероятность такой характеристики вычисляется как произведение вероятностей всех входящих в нее одноцикловых характеристик. БДХ, покрывающие одинаковое число циклов и имеющие одинаковые значения входных векторов активизации и одинаковые значения выходных векторов активизации, принадлежат одному и тому же *байтовому дифференциалу* (БД). Вероятность БД есть сумма вероятностей всех входящих в него БДХ. Рисунок поясняет термины БДХ, БД и то, как вычисляются их вероятности.



Следует отметить, что при таком подходе к анализу прохождения байтовой разности основная неопределенность в изменении значения векторов активизации будет приходиться на линейные преобразования рассеивания. Например, для Rijndael-подобных преобразований с вероятностью 1 известно как меняется активность байтов при выполнении операций ByteSub, AddKey и ShiftRow, а неопределенность возникает только при выполнении MixColumn. В работе [7] представлен подход к определению вероятностей перехода векторов активизации через это преобразование. Эти вероятности представлены в табл. 1 и 2 для разных вариантов преобразования MixColumn.

Таблица 1

Log_2 вероятности перехода вектора активизации через 4-байтный MixColumn

Выход / Вход	0	1	2	3	4
0	0	-	-	-	-
1	-	-	-	-	0
2	-	-	-	-7,99	-0,023
3	-	-	-15,99	-8,017	-0,0226
4	-	-23,983	-16,0115	-8,0171	-0,0226

Таблица 2

Log_2 вероятности перехода вектора активизации через 8-байтный MixColumn

Вых. / Вх.	0	1	2	3	4	5	6	7	8
0	0	-	-	-	-	-	-	-	-
1	-	-	-	-	-	-	-	-	0
2	-	-	-	-	-	-	-	-7,99	-0,046
3	-	-	-	-	-	-	-15,9	-8,04	-0,045
4	-	-	-	-	-	-23,9	-16,0	-8,04	-0,045
5	-	-	-	-	-31,9	-24,0	-16,0	-8,04	-0,045
6	-	-	-	-39,9	-32,0	-24,0	-16,0	-8,04	-0,045
7	-	-	-47,9	-40,0	-32,0	-24,0	-16,0	-8,04	-0,045
8	-	-55,9	-48,0	-40,0	-32,0	-24,0	-16,0	-8,04	-0,045

Преобразование MixColumn, выполняющее обработку каждой отдельной колонки блока данных, на наш взгляд, может быть названо преобразованием со случайными усеченными байтовыми дифференциалами.

Определение 1. Байт-ориентированное преобразование, покрывающее m байтов $Y = g(X)$ ($X = (X_1, X_2,..., X_m) \in GF(2^8)^m$, $Y = (Y_1, Y_2,..., Y_m) \in GF(2^8)^m$) с числом ветвей активизации B, называется преобразованием со случайными усеченными байтовыми дифференциалами, если усредненная для всех возможных значений $\Delta X \in GF(2^8)^m$ вероятность перехода входного вектора активизации $\alpha = \chi(\Delta X)$ в выходной вектор активизации $\beta = \chi(\Delta Y)$ может быть вычислена так:

$$P(\alpha \to \beta) \approx (2^{-8})^{m-h(\beta)}, \text{ если } 2m \ge (h(\alpha) + h(\beta)) \ge B;$$

$$P(\alpha \to \beta) = 0, \text{ если } (h(\alpha) + h(\beta)) < B;$$

$$P(\alpha \to \beta) = 1, \text{ если } h(\alpha) = h(\beta) = 0,$$

где $h(f)$ – вес Хемминга аргумента f; χ – функция-характеристика, ставит 1 на месте активных S-блоков в аргументе и 0 – в противном случае; $\Delta X = (\Delta X_1, \Delta X_2,..., \Delta X_m)$ и $\Delta Y = (\Delta Y_1, \Delta Y_2,..., \Delta Y_m)$ есть, соответственно, входная и выходная разности.

Напомним также, что БДХ или БД считаются *эффективными*, когда их вероятность $p_{БДХ}$ или $P_{БД}$ значительно больше вероятности получения на выходе того же вектора активизации при произвольном (случайном) векторе активизации на входе (случайный входной вектор активизации предполагает равновероятность всех значений выходной разности):

$$P_{БД} >> p_{сл};\ p_{БДХ} >> p_{сл}, \qquad (1)$$

где $p_{сл} \approx (2^{-8})^u$, u – число неактивных байтов в выходной разности или число нулевых битов в выходном векторе активизации. Следует заметить, что для эффективных БД или БДХ непременно будет выполняться и традиционное для обычных дифференциалов ограничение: $P_{БД} > 2^{-n}$ или $p_{БДХ} > 2^{-n}$), где n – длина блока в битах.

Если удается найти эффективный дифференциал, то обычно на последнем цикле, где известны выходное значение разности (на основе известных значений криптограмм) и входной вектор активизации (в соответствии с используемым байтовым дифференциалом). Эта информация позволяет получить информацию о подключе последнего цикла. Таким образом, для выполнения атаки необходимо, чтобы БД или БДХ покрывали почти все циклы шифра.

2. Используемый подход к доказательству отсутствия эффективных байтовых дифференциалов

В этой части работы напомним основные этапы предложенного в [4] подхода к доказательству отсутствия эффективных байтовых дифференциалов.

В начале для Rijndael-подобных шифров была доказана лемма об активных колонках в эффективных байтовых дифференциальных характеристиках.

Лемма 1 [5]. Эффективная байтовая дифференциальная характеристика для Rijndael-подобного шифра не может содержать ни одного цикла со всеми активными колонками на входе преобразования MixColumns.

Сделан вывод о возможности использования этой леммы в целях доказательства отсутствия эффективных БДХ для шифров с 1 или 2 колонками в блоке.

Далее была доказана теорема об отсутствии эффективных БДХ для 128-битного Rijndael (с 4 колонками в блоке).

Теорема 1 [5]. Для шифра Rijndael с размером блока 128 битов нет эффективных БДХ для 3 или более циклов с полным набором преобразований.

Следующим этапом в [5] стало рассмотрение БДХ, которые входят в состав БД. Начиная с этого этапа анализ в [5] выполнялся для 128-битного варианта шифра Rijndael. Первое свойство БД сформулировано в виде утверждения 1.

Утверждение 1 [5]. Для каждого не невыполнимого *r*-циклового ($r \geq 3$) БД всегда есть одна и только одна БДХ с вероятностью примерно $p_{\text{сл}} * 2^{-0,0904*r}$.

Такие БДХ в [5] были названы основными БДХ. Остальные БДХ были названы дополнительными. Второе свойство относится к дополнительным БДХ.

Утверждение 2 [5]. Для каждого БД с 3 или более циклами любая дополнительная БДХ с *k* дополнительными пассивными байтами имеет вероятность примерно в 2^{8k} раз ниже, чем основная БДХ этого БД.

Однако, как показало более детальное исследование, результаты которого будут представлены в разд. 3, есть ряд дополнительных нетипичных БДХ, которые не попадают под это утверждение. Как раз за их счет может быть получен эффективный БД при отсутствии эффективных БДХ.

Далее в работе [5] доказана теорема.

Теорема 2 [5]. Для вариантов шифра Rijndael с размером блока 128 битов нет эффективных БД для 3 и более циклов.

Таким образом, можно выделить следующие основные этапы предложенного в [5] подхода к доказательству отсутствия эффектиных БД:

1. Определение количества циклов, когда для шифра отсутствуют эффективные БДХ.
2. Определение вероятностей основной и дополнительных БДХ.
3. Оценка количества дополнительных БДХ.
4. Оценка вероятностей БД.

3. Условия отсутствия эффективных r-цикловых БД

В этом разделе на основе анализа подхода к доказательству отсутствия эффективных БД, представленного в работе [5], выделим и обобщим основные условия, при выполнении которых можно утверждать об отсутствии эффективных БД для любого блочного шифра.

Первое условие является достаточно очевидным.

Условие 1. Отсутствие эффективных r-цикловых БДХ.

Для поиска эффективных БДХ могут быть использованы известные методы [7,8].

Для выделения остальных условий следует проанализировать итоговую формулу для вероятности R-циклового БД, полученную в работе [5] для rijndael-подобных шифров.

$$P_{БД} = \sum_{k=0}^{\infty} (C_R^k \cdot b^k \cdot 2^{-8k} \cdot 2^{-0,0904 \cdot R} \cdot p_{сл}), \qquad (2)$$

где b – размер блока в байтах, k – количество пассивных байтов в дополнительных БДХ, R – количество циклов, $p_{сл} \approx (2^{-8})^u$, u – число неактивных байтов в выходной разности или число нулевых битов в выходном векторе активизации.

Теперь рассмотрим природу основных элементов формулы (2).

1) $C_R^k \cdot b^k$ – количество вариантов размещения k дополнительных пассивных битов (которые соответствуют пассивным байтам в разности) в b-битных векторах активизации. Данное значение отражает ситуацию, когда пассивные байты будут размещены по одному в различных циклах. В таком случае количество размещений максимальное и остальными вариантами можно пренебречь. Это значение зависит от размера блока b и количества циклов R и всегда будет оставаться таким же независимо от вида используемых преобразований.

2) $2^{-0,0904 \cdot R} \cdot p_{сл}$ – вероятность основной БДХ для R-циклового 128-битного шифра Rijndael. Большинство циклов основной БДХ – это переходы разностей со всеми активными байтами на входе и выходе, поэтому значение $2^{-0,0904}$, как указано в [5], формируется так: вероятность перехода разности с одновременно всеми активными байтами в такую же раз-

ность на выходе для одной колонки (значение в правом нижнем углу в табл. 1) возводится в степень количества колонок в блоке: $2^{-0,02264} = 2^{-0,0904}$. Из табл. 1 и 2 видно также, что значение в правом нижнем углу почти полностью повторяется и в других ячейках последней колонки начиная со строки, которая соответствует двум активным байтам во входной разности. Значение в этой строке в последней колонке формируется как $1 - C_m^{m-1} \cdot \frac{1}{255} = 1 - \frac{m}{255}$, где m – количество байтов в колонке блока. Тогда можно записать общую формулу для значения $2^{-0,0904}$:

$$2^{-0,0904} \approx \left(1 - C_m^{m-1} \cdot \frac{1}{255}\right)^{\frac{b}{m}} = \left(1 - \frac{m}{255}\right)^{\frac{b}{m}}. \quad (3)$$

Из формулы (3) видно, что увеличение m приводит, с одной стороны, к незначительному уменьшению значения в скобках, с другой стороны, – к уменьшению показателя степени. В итоге, изменение общего значения не существенное, что и подтверждается вычислительными экспериментами, результаты которых представлены в табл. 3.

Таблица 3

Вероятности перехода векторов активизации
со всеми активными байтами на входе и выходе преобразования MixColumn

b	m	b/m	Вероятность перехода
16	16	1	0.93725490196078
	8	2	0.93823913879277
	4	4	0.93871587874477
	2	8	0.93895056138023
32	32	1	0.87450980392157
	16	2	0.87844675124952
	8	4	0.88029268156260
	4	8	0.88118750100757
	2	16	0.88162815671624

Таким образом, можно сказать, что рассматриваемое значение в большей степени зависит от размера блока, чем от структуры цикловых преобразований, но только при условии, что в каждом цикле присутствуют одно или несколько преобразований со случайными байтовыми дифференциалами, которые в совокупности покрывают весь блок. Таким образом, можно сформировать второе условие.

Условие 2. В каждом цикле шифра должно присутствовать преобразование со случайными байтовыми дифференциалами, которое покрывает весь блок, или несколько таких преобразований, которые покрывают весь блок в совокупности.

3) 2^{-8k} – во столько раз в соответствии с [5] должна снижается вероятность любой БДХ при добавлении k дополнительных пассивных байтов в каких-либо циклах к основной БДХ.

Если цикловое преобразование содержит операцию, которая покрывает весь блок и является преобразованием со случайными усеченными байтовыми дифференциалами (см. определение 1), то это гарантирует снижение вероятности БДХ на 2^{-8} для каждого дополнительного пассивного байта. Однако часто встречается и ситуация, когда блок данных покрывается несколькими преобразованиями со случайными усеченными байтовыми дифференциалами, например, преобразование MixColumn в шифре Rijndael с размером блока 128 битов состоит из четырех таких отдельных преобразований для четырех колонок. В этом случае возможны многоцикловые эффективные БДХ, которые получаются за счет подачи нулевой разности на одну или несколько частей такого преобразования.

Под условие снижения вероятности дополнительных БДХ не попадают *r*-цикловые БДХ, первые *r*-1 циклов которых покрывают эффективные (*r*-1)-цикловые БДХ. Вероятность таких БДХ выше, чем вероятность основной БДХ умноженная на 2^{-8k}, но, обязательно, ниже вероятности основной БДХ. Будем называть их *нетипичными* дополнительными БДХ. Разница в вероятностях основной и нетипичной БДХ, принадлежащих одному БД, равняется, как правило, вероятности эффективной (*r*-1)-цикловой БДХ, которая лежит в основе нетипичной БДХ. Следовательно, для определения добавочной вероятности для БД от нетипичных БДХ необходимо определить количество и вероятности эффективных (*r*-1)-цикловых БДХ. Количество и вероятности найденных с помощью метода из [8] эффективных БДХ для 2-циклового шифра Rijndael с размером блока 128 битов представлены в табл. 4.

Таблица 4

Эффективные (r-1)-цикловые БДХ
для Rijndael с размером блока 128 битов

Вероятность БДХ	Максимальное количество БДХ для фиксированного входного вектора активизации	Общая добавочная вероятность от нетипичных r-цикловых БДХ, где $P_{ОснБДХ}$ – вероятность основной БДХ
2^{-8}	4	$P_{ОснБДХ}*4*2^{-8} = P_{ОснБДХ}*2^{-6}$
2^{-16}	6	$P_{ОснБДХ}*6*2^{-16} = P_{ОснБДХ}*2^{-13,4}$
2^{-24}	60	$P_{ОснБДХ}*60*2^{-24} = P_{ОснБДХ}*2^{-18}$

Из табл. 1 видно, что с уменьшением вероятности количество БДХ увеличивается, но общая добавочная вероятность сокращается. В итоге, наибольшая добавочная вероятность от нетипичных БДХ, в основе которых лежат эффективные (r-1)-цикловые БДХ с максимальной вероятностью. Максимальная вероятность для таких БДХ будет составлять 2^{-8}. Для шифра Rijndael с размером блока 128 битов количество таких 2-цикловых БДХ равно 4 и определяется количеством возможных комбинаций байтовой разности с одной пассивной колонкой и максимальным количеством активных байтов в остальных активных колонках на входе в операцию MixColumn во втором цикле. Скорее всего, добавочную вероятность $P_{ОснБДХ}*4*2^{-6}$ нельзя считать решающим перевесом для того, чтобы БД можно было считать эффективным, то есть удовлетворяющим выражению (1).

Дальнейшее увеличение количества циклов будет снижать общую добавочную вероятность для каждого (*r*+1)-циклового БД по сравнению с *r*-цикловым БД в $2^{-0,0904}$ раз. Происхождение этого значения было рассмотрено ранее в этой работе.

Таким образом, можно сформулировать третье условие отсутствия эффективных *r*-цикловых БД.

Условие 3. Количество эффективных (*r*-1)-цикловых БДХ с максимальной вероятностью (обычно равняется 2^{-8}) для фиксированного входного вектора активизации должно не превосходить 256, тогда будет выполняться неравенство

$$\max (P_{БД}) < 2p_{сл},$$

что свидетельствует об отсутствии эффективных БД.

Выводы

Первым из основных результатов работы стал усовершенствованный в области учета количества и вероятностей нетипичных дополнительных БДХ метод доказательства отсутствия эффективных БД для Rijndael-подобных шифров, который был предложен в работе [5].

Второй результат связан с выявлением основных условий (условия (1) – (3), когда отсутствие эффективных БДХ свидетельствует и об отсутствии эффективных БД и, следовательно, о стойкости блочного шифра к атаке усеченных байтовых дифференциалов.

Список литературы: 1. *X. Lai.* Markov ciphers and differential cryptanalysis. / X. Lai, J.L. Massey, S. Murphy // Advanced in Cryptology, Proceeding Eurocrypt'91, LNCS 547 / D.W. Davies, Ed., Springer-Verlag, 1991, pp. 17-38. 2. «*Supporting* Document on E2», Nippon Telegraph and Telephone Corporation, June 14, 1998. 3. *M. Matsui*. Cryptanalysis of reduced version of the block cipher E2 / M. Matsui, T. Tokita // In pre-proceedings of Fast Software Encryption'99, pp. 70-79, 1999. 4. *L. R. Knudsen.* Truncated differentials of SAFER / L. R. Knudsen, T. A. Berson // In Fast Software Encryption – Third International Workshop, FSE'96, Volume 1039 of Lecture Notes in Computer Science, Berlin, Heidelberg, New York, Springer-Verlag, 1996. 5. *Руженцев, В. И.* Доказуемая стойкость Rijndael-подобных шифров к атаке усеченных дифференциалов. / В. И. Руженцев // Радіоелектронні і комп'ютерні системи. – 2012. – №5. – С. 51-55. 6. *Руженцев, В. И.* О стойкости к атаке усеченных дифференциалов rijndael-подобных шифров с большими размерами блоков / В. И. Руженцев // Електронний науково-технічний журнал: Вісник НУК ім. адмірала Макарова. – 2013. – №1. – С. 44-51. 7. *Руженцев, В. И.* О методах оценки стойкости к атаке усеченных дифференциалов / В. И. Руженцев // Радиоэлектроника и информатика. – 2003. – №4. – С. 130-133. 8. *S. Moriai*. Security of E2 against Truncated Differential Cryptanalysis / S. Moriai, M. Sugita, K. Aoki // In H. Heys and C. Adams, editors, Selected Areas in Cryptography – 6th Annual International Workshop, SAC'99, Volume 1758 of Lecture Notes in Computer Science, pp. 106–117, Berlin, Heidelberg, New York, Springer-Verlag, 2000.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 09.01.2014