УДК 621. 391:519.2:519.7

О МЕТОДЕ ДОКАЗАТЕЛЬСТВА СТОЙКОСТИ БЛОЧНЫХ ШИФРОВ К АТАКЕ НЕВЫПОЛНИМЫХ ДИФФЕРЕНЦИАЛОВ

В.И. РУЖЕНЦЕВ

Анализируются существующие методы поиска невыполнимых дифференциалов. Предлагается метод, который позволяет обосновать отсутствие невыполнимых дифференциалов. Сложность метода, в отличие от известных, в меньшей степени зависит от размера блока. Метод применяется к Rijndael-подобным SPN шифрам и фейстель-подобным шифрам.

Ключевые слова: блочный шифр, атака невыполнимых дифференциалов, невыполнимый дифференциал, Rijndael-подобные преобразования.

ВВЕДЕНИЕ

Атака невыполнимых дифференциалов (НД) является одним из наиболее эффективных нападений на современные блочные симметричные шифры (БСШ). Этот криптоаналитический метод успешно позволяет атаковать как SPN-шифры [1–3], так и шифры, построенные с использованием цепи фейстеля [4–7] и других структур. Для шифра Rijndael с уменьшенным количеством циклов данную атаку можно считать одной из самых успешных. Подтверждением сказанного является большое количество работ, появившихся за последнее десятилетие и направленных, главным образом, на поиск невыполнимых дифференциалов [1–11]. Целью настоящей работы является рассмотрение существующих подходов к оценке стойкости БСШ к атаке невыполнимых дифференциалов, а также предложение еще одного подхода, который, как будет показано в работе, в ряде случаев является полезным. Например, как будет продемонстрировано, предлагаемый подход позволяет обосновать стойкость группы Rijndael-подобных шифров с 4-мя и более циклами к атаке НД, а также стойкость шифров, использующих цепь фейстеля.

1. ОБЩАЯ ХАРАКТЕРИСТИКА АТАКИ. ИСПОЛЬЗУЕМЫЕ ОБОЗНАЧЕНИЯ

Атака НД впервые была предложена Э. Бихамом в [4,5] для шифров SkipJack, IDEA, Khufu. Позже оказалось, что атака НД применима и для других шифров, в том числе и для шифра AES с 5 циклами [1].

Атака НД на блочные симметричные шифры, как большинство криптоаналитических нападений, относится к классу атак на цикловую функцию, и для ее реализации необходимо иметь некоторое количество пар — открытый текст–криптограмма, полученных на одном и том же секретном ключе.

Данная криптоаналитическая методика называется атакой невыполнимых дифференциалов, поскольку в атаке используются дифференциалы специального вида – те, которые не могут выполняться, т. е. имеющие нулевую вероятность. Атака невыполнимых дифференциалов на r-цикловой шифр обычно становится возможной, когда имеется (r-1)-цикловой невыполнимый дифференциал.

При наличии (r-1)-циклового НД с входной разностью $\Delta_{НДвх}$ и выходной разностью $\Delta_{НДвых}$ атака на r-цикловой шифр состоит из следующих шагов. Выполняется поиск пары с выходной разностью $\Delta_{НДвых}$. Если такая пара найдена, то, в соответствии с НД, после первого цикла не могла быть разность $\Delta_{НДвх}$. И все ключи первого цикла, которые будут приводить к этой разности после одноциклового шифрования, являются неверными. Путем отсева всех неверных ключей определяется правильный подключ первого цикла.

Один из вариантов атаки – атака байтовых или усеченных невыполнимых дифференциалов – была предложена в работах [1, 2, 6]. В ходе атаки через преобразования шифра пытаются провести вектора 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.

В остальной части работы будем, главным образом, обсуждать байтовые НД.

2 АНАЛИЗ ИЗВЕСТНЫХ МЕТОДОВ ПОИСКА НД

2.1 Известные НД для структур, которые используются в БСШ

Для многих структур, которые часто используются при построении БСШ, известны НД. В полной мере это относится к цепи фейстеля. В работе [5] упоминается о том, что если в фейстель-подобном шифре используется биективная шифрующая функция, то всегда существует 5-цикловой НД, который имеет вид (a, 0) $\rightarrow$ (a, 0) для любой ненулевой разности a.

Из работ [1] известно о наличии 4-цикловых НД для Rijndael-подобных БСШ с сокращенным последним циклом. Входная разность в таком НД содержит один активный байт, а выходная – пассивные байты (с нулевой разностью) на позициях, которые соответствуют минимум одной

пассивной колонке (все байты колонки содержат нулевую разность) до преобразования ShiftRow.

Известен также ряд работ, посвященных исследованию НД для различных обобщенных цепей фейстеля [8, 11].

В работе [10] представлены критерии наличия НД для Rijndael-подобных БСШ с различным числом циклов.

В целом, если в шифре используется одна из структур, для которой известно о наличии НД, то НД с аналогичной входной и выходной разностями может существовать и для этого шифра. Однако для таких шифров может существовать и НД для значительно большего количества циклов, следовательно, требуется более подробное исследование. Так, например, для фейстельподобного шифра Camellia, который использует цепь фейстеля, а значит – существует 5-цикловый НД, в процессе анализа были найдены 8-цикловые НД [7].

2.2 Расхождение посередине (miss-in-the-middle)

В работе [5] упоминается о достаточно универсальном подходе к построению НД для БСШ. Подход заключается в поиске двух достоверных дифференциалов (вероятность каждого равна 1), первый из которых определяет движение разности в первой половине шифра в прямом направлении, а второй – во второй половине шифрующих преобразований в обратном направлении. Если конечные разности таких достоверных дифференциалов не равны, то расхождение дифференциалов дает НД.

Используя данный подход построены многие из известных НД, в том числе и все представленные в предыдущем подразделе. Данный подход не редко используется для доказательства стойкости БСШ к атаке НД, хотя о строгом доказательстве невозможности построения НД другими способами не известно.

2.3 Поиск НД полным перебором

Интересный подход к поиску НД был предложен в [5]. Для шифра создавалась уменьшенная модель (уменьшенный размер блока и ключа) и путем перебора всех возможных входных разностей и ключей выполнялся поиск НД. Затем результаты поиска анализировались и выполнялась попытка построения НД для полноразмерного шифра.

Основной недостаток метода заключается в том, что свойства уменьшенной модели и полноразмерного шифра могут существенно отличаться и доказать обратное очень сложно. Поэтому и структура НД для шифров тоже может иметь существенные отличия, а отсутствие или присутствие НД для уменьшенной модели не гарантируют того же для полноразмерного шифра.

2.4 U и UID методы поиска НД

Попытка автоматизировать процесс поиска НД сделана в работах [8, 9]. Методы действуют в соответствии с принципом miss-in-the-middle. Путем полного перебора разностей выполняется поиск достоверных усеченных (байтовых) дифференциалов для обоих половин шифрующих преобразований, а затем проверяется совместимость этих дифференциалов. В случае несовместимости найден НД.

Недостаток методов – значительное увеличение сложности с ростом размера блока и числа циклов в шифре. Для шифров, которые сегодня используются при построении хеш-функций (размер блока 512 или 1024 бита) эти методы не будут работать.

3. ПРЕДЛАГАЕМЫЙ ПОДХОД

В отличие от большинства известных подходов, которые направлены на поиск НД, наш подход направлен на обоснование отсутствия НД. В основе лежит следующая теорема.

Теорема 1. Если для БСШ существует некоторая разность Δ, которая может быть получена из любой ненулевой входной разности за r_1 циклов преобразований и которая может быть получена из любой ненулевой выходной разности за r_2 циклов, выполняемых в направлении дешифрования, то для такого БСШ не существует НД с r_1+r_2 и более циклами.

Доказательство. Справедливость теоремы достаточно очевидна, т. к. если любая входная разность и любая выходная разность могут прийти к промежуточному значению разности Δ, то возможен переход любой входной разности в любую выходную разность, а это значит, что не существует НД. Теорема доказана.

Таким образом, для доказательства отсутствия НД необходимо определить количество циклов r_1 и r_2, за которые любая входная разность и любая выходная могут прийти к некоторому значению разности Δ.

Когда речь идет о байтовой разности, то Δ обычно содержит сразу все активные байты (вектор активизации состоит из всех «1»).

С помощью теоремы 1 можно, например, объяснить отсутствие НД для многих Rijndaelподобных шифров, в том числе для шифра Rijndael со 128 битным блоком. Коротко напомним основные особенности строения таких шифров, а затем продемонстрируем обоснование отсутствия НД.

4. АНАЛИЗ RIJNDAEL-ПОДОБНЫХ ШИФРОВ

В настоящей работе рассматриваются Rijndael-подобные шифры, т. е. алгоритмы шифрования, которые содержат в каждом цикле (даже в последнем) четыре вида преобразований аналоги преобразований шифра Rijndael: ByteSub (BS), ShiftRow(SR), MixColumns (MC) и AddKey. В зависимости от размера блока может меняться количество и размер колонок, из которых состоит блок (рис. 1).

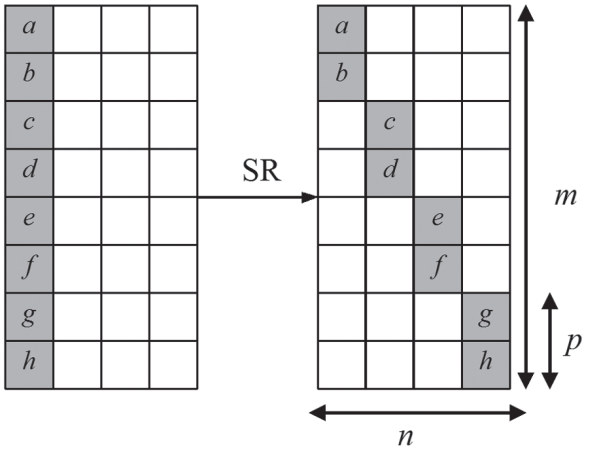

Рис. 1

Когда количество колонок n больше количества строк m, то операция ShiftRow выполняет циклический сдвиг каждой строки на различное количество байтов. В результате операции каждая колонка будет содержать не более одного байта из каждой колонки до преобразования. Для всех вариантов шифра Rijndael [12] выполняется условие $n \geq m$.

Когда $m \geq n$, то количество байтов, которые из одной исходной колонки будут поступать в одну колонку на выходе преобразования ShiftRow, будем обозначать p (см. рис. 1).

В этих случаях всегда выполняется $m = np$.

Такая схема преобразований используется в шифре «Калина» [13].

Прежде чем перейти к рассмотрению стойкости Rijndael к атаке рассмотрим особенности преобразования MixColumns, т. к. именно это преобразование вносит неопределенность в прохождение векторов активизации через циклы шифра. В работе [14] проведен анализ этого преобразования и определены правила определения вероятностей переходов векторов активизации через MixColumns. В табл. 1 и 2 для преобразования MixColumns, которое покрывает 4 и 8 байтов, соответственно, представлены двоичные логарифмы от вероятностей перехода векторов активизации через MixColumns для различного числа активных битов на входе (меняется по столбцам) и выходе (по строкам).

В табл. 1 и 2 переходы, обладающие вероятностью 0, отмечены прочерками.

Справедливо следующее утверждение.

Утверждение 1. Для Rijndael-подобных шифров с блоком, в котором строк не меньше, чем колонок ($m > n$), не существует байтовых НД для 4 и более циклов с полным набором преобразований.

Доказательство. Для доказательства утверждения необходимо показать, что разность с одновременно всеми активными байтами может быть получена при любой начальной разности как после двухциклового зашифрования, так и после двухциклового расшифрования. В этом случае выполняется теорема 1.

Таблица 1

Двоичный логарифм от вероятности перехода вектора активизации через 4-байтный MixColumns

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

Двоичный логарифм от вероятности перехода вектора активизации через 8-байтный MixColumns

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

Двухцикловое зашифрование содержит последовательность преобразований: MC, SR, MC; а двухцикловое расшифрование – последовательность тех же обратных преобразований: MC^{-1}, SR^{-1}, MC^{-1}.

Рассмотрим двухцикловое зашифрование. Любая ненулевая усеченная (байтовая) разность имеет по крайней мере одну активную колонку на входе первого преобразования MC. В соответствии с табл. 1 и 2, для любой ненулевой входной разности всегда может быть получена на выходе MC разность со всеми активными байтами. Преобразование SR распространит активные байты этой колонки на все без исключения остальные колонки (поскольку $m > n$). Завершающее преобразование MC всегда может преобразовать такую разность на входе в разность со всеми активными байтами. Аналогичные рассуждения справедливы и для двухциклового расшифрования. Утверждение доказано.

Полученный результат полностью согласуется с известными результатами для шифра Rijndael со 128-битным блоком, т. к. наилучшие НД, которые были найдены или использованы в известных работах, покрывают 3 полных и один (последний) неполный циклы [3].

Для Rijndael-подобных шифров с блоком, в котором строк меньше, чем колонок ($m < n$), для того, чтобы гарантировать отсутствие НД, потребуется, по крайней мере, два дополнительных цикла преобразований (по одному с каждой стороны). То есть, для таких шифров можно говорить об отсутствии НД не менее, чем для 6 полных циклов.

5. АНАЛИЗ ШИФРОВ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ЦЕПИ ФЕЙСТЕЛЯ

Схема фейстеля – одна из наиболее распространенных схем современных БСШ. В качестве шифра, стойкость которого будем исследовать, взят алгоритм, который рассматривался в работе [17]. В каждом цикле выполняется SL-преобразование, схема которого представлена на рис. 2.

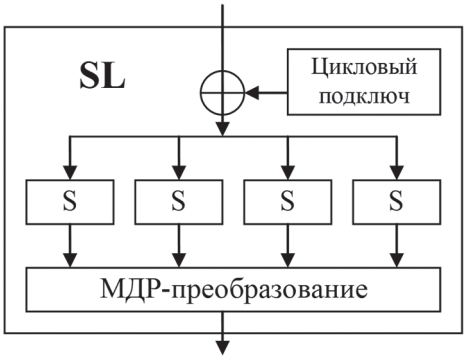

Рис. 2

Важным моментом является то, что МДР-преобразование (аналог MixColumn в Rijndael-подобных шифрах) охватывает весь обрабатываемый полублок. Поэтому за один цикл такое SL-преобразование может любую ненулевую разность на входе трансформировать в разность со всеми активными байтами в полублоке на выходе (см. табл. 1 и 2). Общая схема трех циклов преобразований представлена на рис. 3.

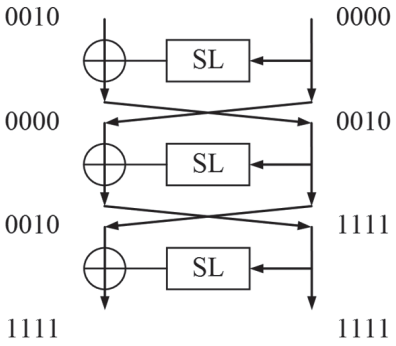

Рис. 3

Используя теорему 1, покажем справедливость следующего утверждения.

Утверждение 2. Для рассматриваемого шифра (схема фейстеля и в цикловом преобразовании МДР-преобразование покрывает весь полублок) не существует НД, покрывающих 6 и более циклов.

Доказательство. Для доказательства утверждения необходимо показать, что за 3 цикла любая начальная разность может быть преобразована в разность с одновременно всеми активными байтами.

Первый цикл может содержать тривиальный переход нулевой разности через первое SL-преобразование (см. рис. 3). Тогда, независимо от вида начальной разности в левом полублоке, на вход SL-преобразования второго цикла поступит ненулевая разность (содержит, по крайней мере, один активный байт). В соответствии с вероятностями переходов из табл. 1, выход такого SL-преобразования всегда может содержать сразу все активные байты для всего полублока независимо от входного значения (для всех ненулевых входных разностей последняя колонка табл. 1 содержит значения вероятности значительно большие, чем 0).

Далее, это значение разности поступит на вход SL-преобразования третьего цикла. Следовательно, на выходе опять может быть получена разность с одновременно всеми активными байтами (см. рис. 3). Таким образом, после 3 циклов всегда есть возможность получения выходной разности с одновременно всеми активными байтами в блоке для любой входной разности.

Так как расшифрование выполняется по такой же схеме, то 3 цикла расшифрования также позволяют для любой начальной разности получить разность с одновременно всеми активными байтами в блоке. Тогда в терминах теоремы 1 для данного шифра $r_1 = r_2 = 3$. Утверждение доказано.

ВЫВОДЫ

В работе рассмотрены существующие методы поиска НД. Проанализированы их слабые и сильные стороны. Предложен метод, который позволяет обосновать отсутствие НД. Сложность метода в меньшей степени зависит от размера блока, в отличие от известных, поэтому он может быть использован для БСШ с большими размерами блока. Продемонстрировано применение метода для Rijndael-подобных шифров и для шифров, которые используют схему фейстеля.

Литература

[1] Biham, E., Keller, N.: Cryptanalysis of Reduced Variants of Rijndael, 3rd AES Conference, New York, USA (2000), http://csrc.nist.gov/encryption/aes/round2/conf3/aes3papers.html.

[2] Cheon, J.H., Kim, M., Kim, K., Lee, J.-Y., Kang, S.: Improved Impossible Differential Cryptanalysis of Rijndael and Crypton. In: Kim, K.-c. (ed.) ICISC 2001. LNCS, vol. 2288, pp. 39–49. Springer, Heidelberg (2002).

[3] Jiqiang Lu, Orr Dunkelman, Nathan Keller and Jongsung Kim. New Impossible Differential Attacks on AES. IACR Cryptology ePrint Archive 2008: 540 (2008).

[4] Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials, Technion, CS Dept, Tech Report CS0947 (1998).

[5] Biham, E., Biryukov, A., Shamir, A.: Miss-in-the-Middle Attacks on IDEA, Khufu and Khafre. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 124–138. Springer, Heidelberg (1999).

[6] Lu, J., Kim, J., Keller, N., Dunkelman, O.: Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1, Archive available at: http://jiqiang.googlepages.com.

[7] Wenling Wu, Wentao Zhang and Dengguo Feng. Impossible differential cryptanalysis of reduced-round ARIA and Camellia. Journal of Computer Science and Technology, 22(3):449-456, 2007. Springer.

[8] J. Kim, S. Hong, J. Sung, S. Lee and J. Lim: Impossible differential cryptanalysis for block cipher structures, INDOCRYPT 2003, LNCS 2904, pp. 82-96, 2003.

[9] Yiyuan Luo, Zhongming Wu, Xuejia Lai and Guang Gong. A Unified Method for Finding Impossible Differentials of Block Cipher Structures. IACR Cryptology ePrint Archive 2009: 627 (2009).

[10] Ruilin Li, Bing Sun and Chao Li. Impossible Differential Cryptanalysis of SPN Ciphers. IACR Cryptology ePrint Archive 2010: 307 (2010).

[11] H. Yap, Impossible Differential Characteristics of Extended Feistel Networks with Provable Security against Differential Cryptanalysis. SecTech 2008, CCIS 29, pp. 103-121, 2009.

[12] J. Daemen, V. Rijmen. AES Proposal Rijndael, AES Round 1 Technical Evaluation CD1: Documentation, National Institute of Standards and Technology, Aug 1998. See http://www.nist.gov/aes.

[13] Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікація / І. Д. Горбенко, В. І. Долгов, Р. В. Олійников, В. І. Руженцев та ін. // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Харьков. Том 6, №2, 2007. – С. 195-208.

[14] Руженцев В.И. О методах оценки стойкости к атаке усеченных дифференциалов / В. И. Руженцев // Радиоэлектроника и информатика. 2003. – №4. – С. 130-133.

[15] FOX Specifications Version 1.2 appeared on http://crypto.junod.info.

[16] Перспективний блоковий симетричний шифр «Мухомор» - основні положення та специфікація / І. Д. Горбенко, В. І. Долгов, Р. В. Олійников, В. І. Руженцев та ін. // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Харьков. Том 6, №2, 2007. – С. 168-185.

[17] Руженцев В.И. О стойкости блочных шифров с rijndael-подобными преобразованиями к интегральным атакам. // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Харьков. Том 11, №2, 2012. – С. 160–164.

Поступила в редколлегию 12.03.2013

Руженцев Виктор Игоревич, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Научные интересы: криптография, криптоанализ блочных симметричных шифров.

УДК 621. 391:519.2:519.7

Про метод доведення стійкості блокових шифрів до атаки нездійснених диференціалів / В.І. Руженцев // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 215–219.

Аналізуються відомі методи пошуку нездійснених диференціалів. Пропонується метод, який дозволяє обгрунтувати відсутність нездійснених диференціалів. Складність цього методу, на відміну від відомих, меншою мірою залежить від розміру блоку. Метод застосовується для Rijndael-подібних SPN шифрів та фейстель-подібних шифрів.

Ключові слова: блоковий шифр, атака нездійснених диференціалів, нездійснений диференціал, Rijndael-подібні перетворення.

Табл.: 2. Іл.: 3. Бібліогр.: 12 найм.

UDC 621. 391:519.2:519.7

On the method of proving the resistance of block ciphers to impossible differential attack / V.I. Ruzhentsev // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 215–219.

The known methods of proving the security of block ciphers against impossible differentials attacks are considered. A new method is proposed which allows to validate the absence of impossible differentials. The complexity of the method, unlike the known ones, to a less extent depends on the block size. This method is applied to Rijndael-like SPN ciphers and to ciphers which use the Fiestel scheme.

Keywords: block cipher, impossible differential attack, impossible differential, Rijndael-like transformations.

Tab.: 2. Fig.: 3. Ref.: 12 items.