УДК 004.056.55
DOI: 10.15587/1729-4061.2017.108413

Разработка подхода к доказательству стойкости блочных шифров к атаке невыполнимых дифференциалов

В. И. Руженцев, Ю. Н. Онищенко

Пропонується метод, який дозволяє обгрунтувати відсутність нездійснених диференціалів. Складність цього методу, на відміну від відомих, в меншій мірі залежить від розміру блоку. Метод застосовується до Rijndael-подібних SPN шифрів та фейстель-подібних шифрів. Обговорюються результати обчислювальних експериментів з пошуку нездійснених диференціалів для зменшених моделей блокових шифрів. Підтверджується справедливість висновків, отриманих за допомогою запропонованого методу обґрунтування відсутності нездійснених диференціалів

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

1. Введение

В современном информационном мире использование защищенных протоколов передачи данных и криптографических алгоритмов позволяет защититься от многих угроз информационной безопасности. Одно из основных требований к симметричным криптографическим алгоритмам – это стойкость к известным аналитическим атакам.

Атака невыполнимых дифференциалов (НД) является одним из наиболее эффективных нападений на современные блочные симметричные шифры (БСШ). Этот криптоаналитический метод успешно позволяет атаковать любые виды блочных шифров, в том числе и такие наиболее распространенные, как SPN-подобные [1–3] и фейстель-подобные шифры [4–7]. Для шифра Rijndael или AES (FIPS-197) с уменьшенным количеством циклов данную атаку можно считать одной из самых успешных. Rijndael-подобными SPN шифрами являются шифр «Калина» (ДСТУ 7624:2014) со всеми размерами блоков, 512 битные блочные шифры, которые используются в хеш-функциях Whirlpool, Groestl и «Купина» (ДСТУ 7564:2014).

Подтверждением актуальности исследования вопросов стойкости блочных шифров к атаке невыполнимых дифференциалов является большое количество работ, появившихся за последнее десятилетие и направленных, главным образом, на поиск невыполнимых дифференциалов [1–11]. При этом область использования многих из известных методов ограничена размером блока шифра 256 битов, что говорит об актуальности поиска путей доказательства стойкости к рассматриваемой атаке для шифров с большими размерами блоков.

2. Анализ литературных данных и постановка проблемы

Атака НД впервые была предложена 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. Для реализации атаки атакующий должен 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 выполниться, т. е. имеющие нулевую вероятность. Атака невыполнимых дифференциалов на *r*-цикловый шифр обычно становится возможной, когда имеется (*r*-1)-цикловый невыполнимый дифференциал.

На рис. 1 представлена схема выполнения атаки НД.

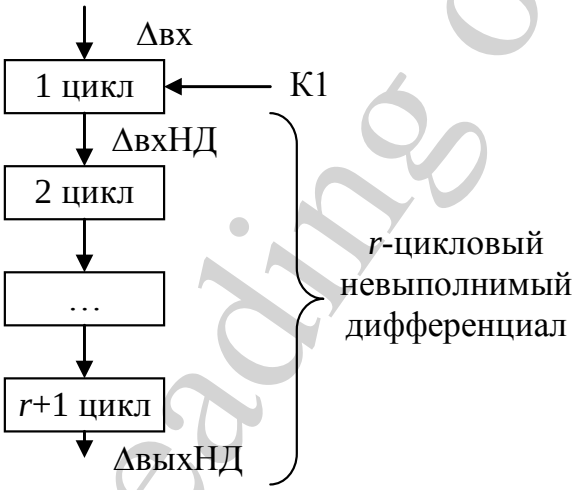

Рис. 1. Схема атаки НД

При наличии *r*-циклового НД с входной разностью $\Delta_{\text{вхНД}}$ и выходной разностью $\Delta_{\text{выхНД}}$ атака на (*r*+1)-цикловый шифр состоит из следующих шагов. Выполняется поиск пары с некоторой входной разностью $\Delta_{\text{вх}}$ и выходной разностью $\Delta_{\text{выхНД}}$. При этом переход $\Delta_{\text{вх}}$ в $\Delta_{\text{вхНД}}$ на первом цикле должен быть возможен лишь для некоторых значений ключа первого цикла К1. Если такая пара найдена, то, в соответствии с НД, после первого цикла не могла быть разность $\Delta_{\text{вхНД}}$. 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 К1.

Один из вариантов атаки – атака байтовых или усеченных невыполнимых дифференциалов (БНД) – была предложена в работах [1–3]. 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.

Преимуществом БНД перед просто НД является то, что в ходе атаки каждая найденная правильная пара позволяет отсеять не один или несколько неправильных ключей первого цикла, а сразу несколько сотен или тысяч неправильных ключей первого цикла.

Для многих структур, которые часто используются при построении БСШ, известно о наличие 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-цикловый НД, который имеет вид $(a, 0) \rightarrow (a, 0)$ для любой ненулевой разности a.

Из работы [1] известно о наличии 4-цикловых БНД для Rijndael-подобных БСШ с сокращенным последним циклом. Входная разность в таком БНД содержит один активный байт, а выходная – 4 пассивных байта (с нулевой разностью). Эти 4 байта расположены на позициях, которые соответствуют 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 фейстель-подобного шифра Camellia, который использует цепь фейстеля, а значит – существует 5-цикловый НД, в процессе анализа были найдены 8-цикловые НД [7].

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. Данный подход нередко используется для доказательства стойкости БСШ к атаке НД, хотя о строгом доказательстве невозможности построения НД другими способами не известно.

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.

Попытка автоматизировать процесс поиска НД сделана в работах [8, 9]. Методы действуют в соответствии с принципом расхождение-по-середине (miss-in-the-middle). Путем полного перебора разностей выполняется поиск достоверных (обладающих вероятностью 1) усеченных (байтовых) дифференциалов для обоих половин шифрующего преобразования, а затем проверяется совместимость этих дифференциалов. В случае несовместимости – найден НД.

Недостаток рассмотренных в разделе методов – значительное увеличение сложности с ростом размера блока и числа циклов в шифре. В результате, для шифров, которые сегодня используются при построении хеш-функций (размер блока 512 или 1024 бита), эти методы не будут работать, так как обладают нереализуемой на практике сложностью.

3. Цель и задачи исследования

Целью настоящей работы является разработка подхода, который позволил бы обосновывать отсутствие НД или БНД для шифров и с большими размерами блока (более 256 битов).

Для достижения поставленной цели необходимо решить следующие задачи:

– сформулировать общее правило, когда отсутствуют НД и БНД для БСШ;

– применить это правило для наиболее распространенных видов БСШ;

– разработать уменьшенные модели (с размером блока и ключа до 16 битов) рассматриваемых видов БСШ;

– для разработанных уменьшенных моделей проверить справедливость полученных теоретических выводов об отсутствии НД и БНД на практике.

4. Предлагаемый подход к обоснованию отсутствия невыполнимых дифференциалов для блочных симметричных шифров

В отличие от большинства известных подходов [2–12], которые были рассмотрены ранее и которые направлены на поиск НД или БНД, разрабатываемый подход будет направлен на обоснование отсутствия НД.

Основная идея предлагаемого подхода заключается в том, чтобы обосновать существование некоторой разности на промежуточном этапе шифрования, которая может быть получена для любой входной разности при выполнении зашифрования и для любой выходной разности при выполнении расшифрования. Рис. 2 поясняет эту идею.

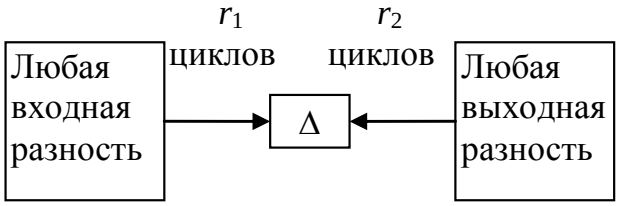

Рис. 2. Предлагаемый подход к обоснованию отсутствия НД

В основе предлагаемого подхода 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, так как 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 векторах активизации или о байтовой разности на входе, выходе и на промежуточных этапах, то Δ обычно содержит сразу все активные байты (вектор активизации состоит из всех «1»). Такие НД будем называть байтовыми НД (БНД). Теорему 1 можно переформулировать следующим образом для БНД.

Теорема 2. Если для БСШ существует некоторая байтовая разность Δ, которая может быть получена для любого входного вектора активизации за r_1 циклов преобразований и которая может быть получена для любого выходного вектора активизации за r_2 циклов, выполняемых в направлении дешифрования, то для такого БСШ не существует БНД с r_1+r_2 и более циклами.

С помощью теоремы 2 можно, например, объяснить отсутствие БНД для многих Rijndael-подобных шифров, в том числе для шифра Rijndael со 128 битным блоком. Коротко напомним основные особенности строения таких шифров, а затем продемонстрируем обоснование отсутствия БНД.

При этом, область использования теоремы 2 не ограничивается только этим видом шифров. Далее будут рассмотрены также фейстель-подобные шифры и шифры, построенные с использованием схемы Лея-Мэсси (Lai-Massey).

Для каждой из рассматриваемых разновидностей шифров была построена уменьшенная модель, на которой с помощью вычислительных экспериментов выполнялась проверка справедливости полученных теоретических результатов.

В табл. 1, 2 приведены алгоритмы, которые были использованы для вычислительных экспериментов по поиску НД и БНД для уменьшенных 16 битовых моделей шифров.

Таблица 1
Алгоритм поиска НД

	Входные данные: Шифрующее преобразование E. Пустая строка таблицы разности соответствующего размера.
1	Перебор всех вариантов входной разности d
1. 1	Обнуление строки таблицы разности
1. 2	Перебор вариантов ключа k
1. 2. 1	Перебор всех вариантов входного значения x
1. 2. 1. 1	Инкрементируем ячейку с индексом $E_k(x)+E_k(x+d)$
1. 3	Проверяем строку таблицы разности на наличие «0». Каждый такой «0» соответствует НД
	Выходные данные: Найденные НД.

Таблица 2
Алгоритм поиска байтовых НД (БНД)

	Входные данные: Шифрующее преобразование E. Пустая строка таблицы разности соответствующего размера.
1	Перебор всех вариантов входного вектора активизации
1. 1	Обнуление строки таблицы разности для вектора активизации
1. 2	Перебор всех вариантов входной разности d, отвечающих выбранному входному вектору активизации
1. 2. 1	Перебор вариантов ключа k
1. 2. 1. 1	Перебор всех вариантов входного значения x
1. 2. 1. 1. 1	Инкрементируем ячейку с индексом $E_k(x)+E_k(x+d)$
1. 3	Перебор элементов полученной таблицы разности
1. 3. 1	Наличие элемента с ненулевым значением свидетельствует об отсутствии БНД с данным выходным вектором активизации
1. 3. 2	Если отсеяны все возможные выходные вектора активизации, то БНД не найдены и переходим к следующему значению входного вектора активизации
1. 4	Если остались неотсеянные выходные вектора активизации, то каждый соответствует найденному БНД
	Выходные данные: Найденные БНД.

В алгоритмах, представленных в табл. 1, 2, действия, выполняемые внутри цикла, указываются с дополнительным номером (например, действие с номером 1.2.1 будет выполняться в цикле, который организуется действием с номером 1.2); $E_k()$ – обозначает операцию зашифрования указанного в скобках аргумента с использованием ключа k.

4. 1. Используемые уменьшенные модели

В рамках проводимых исследований будут рассматриваться криптографические свойства фейстель-подобных, SPN блочных шифров и шифров, построенных с использованием схемы Lai-Massey, с уменьшенным размером блока и ключа (8 или 16 битов). Целесообразность рассмотрения именно уменьшенных моделей шифров объясняется тем, что полноценный поиск НД можно провести только для шифров с небольшим размером блока. В качестве операций перемешивания и рассеивания были взяты преобразования, предложенные в [13] для уменьшенной версии шифра Rijndael. На рис. 3, 4 схематически представлены преобразования, которые выполняются в рассматриваемых моделях SPN и фейстель-подобных шифров.

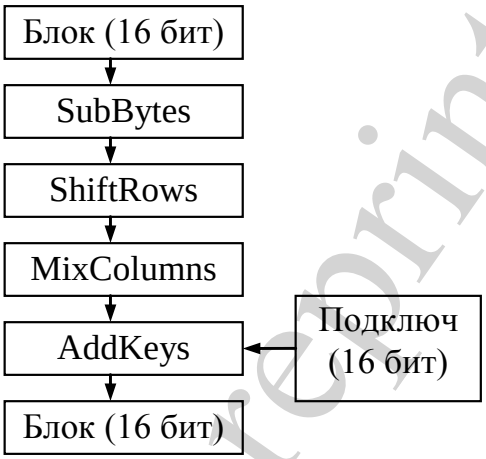

Рис. 3. Схема одного цикла SPN-шифра

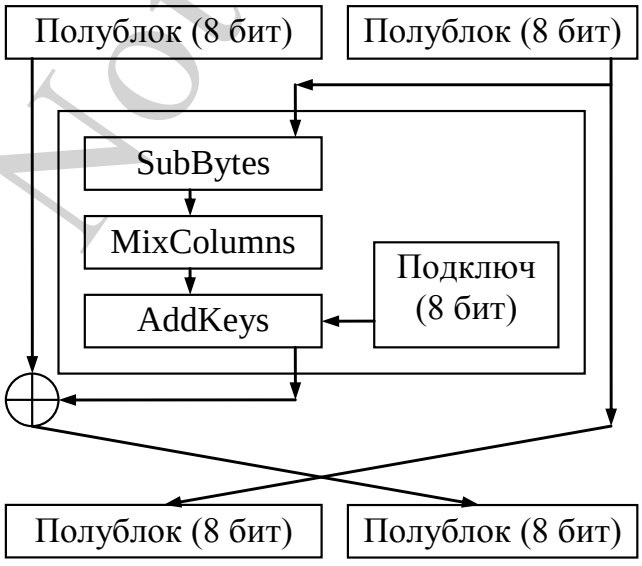

Рис. 4. Схема одного цикла фейстель-подобного шифра

К основным особенностям предложенных уменьшенных моделей шифров следует отнести:

– размер блока 16 бит, размер ключа 8 или 16 бит;

– структура блока для SPN: 2 колонки по 2 4-битовых элемента;

– структура полублока для фейстель-подобного: 2 4-битовых элемента;

– умножение элементов каждой колонки на фиксированную МДР-матрицу размером 2 на 2 над $GF(2^4)$ (MixColumns);

– подстановка 4 в 4 бита (SubBytes);

– число ветвей активизации линейного преобразования MixColumns B=3.

5. Анализ Rijndael-подобных шифров

Рассматриваются Rijndael-подобные шифры, то есть алгоритмы шифрования, которые содержат в каждом цикле (даже в последнем) четыре вида преобразований – аналоги преобразований шифра Rijndael: ByteSub (BS), ShiftRows(SR), MixColumns (MC) и AddKey. В зависимости от размера блока может меняться количество и размер колонок, из которых состоит блок (рис. 5).

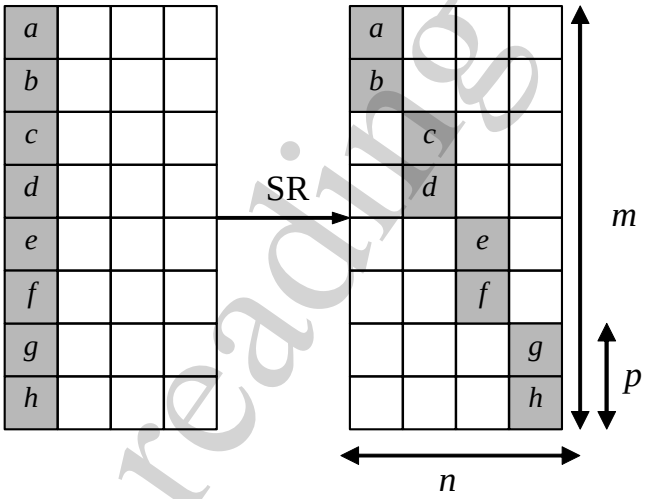

Рис. 5. Схема преобразования ShiftRows(SR)

Когда количество колонок n больше количества строк m, то операция ShiftRows выполняет циклический сдвиг каждой строки на различное количество байтов (рис. 5). 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 ShiftRows, будем обозначать p (рис. 5).

В этих случаях всегда будет выполняться $m=np$.

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

Прежде чем перейти к рассмотрению стойкости Rijndael к атаке, рассмотрим особенности преобразования MixColumns, так как именно это преобразо-

вание 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. 3, 4 для преобразований MixColumns, которые покрывают 4 и 8 байтов, соответственно, представлены двоичные логарифмы от вероятностей перехода векторов активизации (количество активных битов на входе и выходе преобразования меняется по столбцам и по строкам таблиц, соответственно).

Таблица 3

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 4

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

В табл. 3, 4 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.

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, 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. В известных атаках на этот шифр используется НД, покрывающий 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.

С помощью представленных в табл. 1, 2 алгоритмов был проведен поиск НД и БНД для уменьшенной 16-битной версии алгоритма AES. Результаты представлены в табл. 5 и 6.

Таблица 5

Результаты поиска НД для уменьшенной версии AES

Количество циклов	Количество найденных НД	Комментарии
4	510	Для каждой входной разности с 1 активным S-блоком
5	0	–

Таблица 6

Результаты поиска БНД для уменьшенной версии AES

Количество циклов	Количество найденных БНД	Комментарии
4 неполных (без MC в последнем цикле)	24	По 6 для каждого входного вектора активизации с 1 активным S-блоком
4	0	–

5. 1. Обсуждение результатов для Rijndael-подобных шифров

Результаты вычислительных экспериментов из табл. 6 подтверждают справедливость доказанного ранее утверждения 1.

Результаты, представленные в табл. 5, показывают, что при отсутствии БНД могут присутствовать обычные НД. Для 4 полных циклов уменьшенного AES не найдено БНД, но найдены НД. Найденные НД можно назвать полубайтовыми, так как входную разность можно описать вектором активизации с одним активным битом, а для выходной разности важны сами значения в каждом из активных байтов. В выходной разности должно быть два активных полубайта, которые до последнего ShiftRows находятся в одной колонке. Значение разности в этих полубайтах должно быть таким, чтобы при выполнении последней операции MC в обратном направлении была получена ненулевая разность только в одном полубайте. Подобные полубайтовые НД для 4 полных циклов существуют и для полноразмерных Rijndael-подобных шифров, но сведений о них в доступной литературе найдено не было. Возможно, использование этих полубайтовых НД может сделать известные атаки более эффективными. Однако данный вопрос требует более тщательного исследования.

Под условия утверждения 1 попадают многие Rijndael-подобные SPN шифры. Это позволяет доказать отсутствие байтовых НД для 4 и более циклов шифра «Калина» (ДСТУ 7624:2014) со всеми размерами блоков, для 512 битных блочных шифров, которые используются в хеш-функциях Whirlpool, Groestl и «Купина» (ДСТУ 7564:2014).

6. Анализ шифров, построенных с использованием цепи фейстеля

Схема фейстеля – одна из наиболее распространенных схем современных БСШ. В качестве шифра для исследований взят алгоритм, который по структуре близок к шифрам Торнадо [15] и Лабиринт [16]. В каждом цикле выполняется SL-преобразование, схема которого представлена на рис. 6.

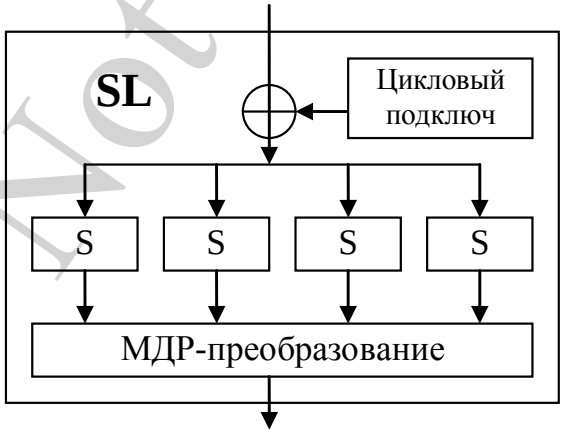

Рис. 6. SL-преобразование

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 (табл. 3, 4). Общая схема трех циклов преобразований и один вариант прохождения вектора активизации представлены на рис. 7.

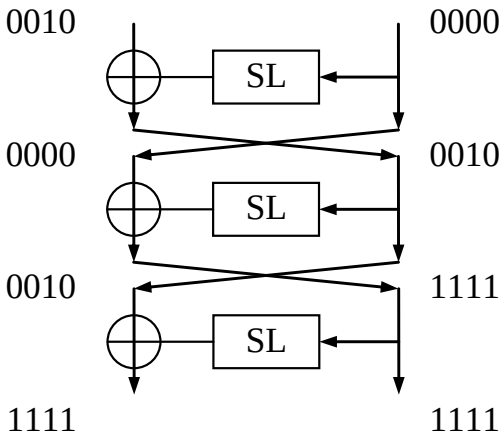

Рис. 7. Схема трех циклов преобразований и вариант прохождения вектора активизации

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 БНД, 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 (рис. 7). 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. 3, выход такого SL-преобразования всегда может содержать сразу все активные байты.

Далее, это значение разности поступит на вход SL-преобразования третьего цикла. Следовательно, на выходе опять может быть получена разность с одновременно всеми активными байтами (рис. 7). 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 2 для данного шифра $r_1=r_2=3$. Утверждение доказано.

Как и в предыдущей части работы, для проверки полученных теоретических выводов с помощью представленных в табл. 1, 2 алгоритмов был проведен поиск НД и БНД для уменьшенной 16-битной версии алгоритма. Результаты представлены в табл. 7 и 8.

Таблица 7

Результаты поиска НД для уменьшенной версии фейстель-подобного шифра

Количество циклов	Количество найденных НД	Комментарии
7 (S-блок max_dif=10)	12	Например, 0x0100-0x0001
7 (S-блок max_dif=4)	8	Например, 0x0100-0x0001
8	0	–

Таблица 8

Результаты поиска БНД для уменьшенной версии фейстель-подобного шифра

Количество циклов	Количество найденных БНД	Комментарии
5	4	По два для входных векторов активизации 1000 и 0100
6	0	–

6. 1. Обсуждение результатов для фейстель-подобных шифров

Эксперименты по поиску обычных НД были проведены для уменьшенных моделей шифров с различными параметрами подстановок. В качестве изменяемого параметра подстановок использовалось максимальное значение в таблице разности. Это значение указано в первой колонке табл. 7 для случаев, когда были найдены НД. В первом случае (первая строка табл. 7) максимальное значение в таблице разности для подстановки 4 в 4 бита составляет 10 (S-блок max_dif=10), а во втором (вторая строка табл. 7) – 4 (S-блок max_dif=4).

Представленные результаты показывают, что дифференциальные свойства нелинейных подстановок не оказывают решающего влияния на стойкость БСШ к атаке НД. При этом вполне ожидаемо, что при большем максимальном значении в таблице разности найдено больше НД, так как большее максимальное значение свидетельствует о большем количестве нулей (запрещенных переходов) в таблице разности подстановки.

Как и при рассмотрении SPN-шифров, отсутствие БНД не означает отсутствие НД для рассматриваемого шифра. В отличие от SPN шифров, где разница в числе циклов, необходимых для отсутствия БНД, от числа циклов, необходимых для отсутствия НД, составляет 1 цикл (табл. 5, 6), в данном случае эта разница составляет 2 цикла. При этом результаты из табл. 8 подтверждают справедливость утверждения 2.

Под условия утверждения 2 попадают фейстель-подобные шифры с цикловой функцией, в которой используется МДР-преобразование, покрывающее весь полублок. Следовательно, с помощью этого утверждения можно доказать отсутствие байтовых НД для 6 и более циклов шифров Торнадо и Лабиринт с размером блока 128 битов.

7. Выводы

1. Сформулированы и доказаны теоремы, которые определяют критерии отсутствия невыполнимых дифференциалов (НД) (Теорема 1) и отсутствия байтовых невыполнимых дифференциалов (БНД) (Теорема 2) для блочных симметричных шифров (БСШ). Для отдельных разновидностей БСШ проверка этих критериев может быть выполнена независимо от размера блока, что позволяет анализировать и БСШ с большими размерами блока.

2. Проанализировано два распространенных вида блочных симметричных шифров: Rijndael-подобные SPN шифры и фейстель-подобные шифры. Для группы Rijndael-подобных шифров доказано утверждение 1, в котором обосновно отсутствие БНД для 4 и более циклов. Для группы фейстель-подобных шифров доказано утверждение 2, в котором обосновно отсутствие БНД для 6 и более циклов. Утверждение 1 позволило доказать отсутствие байтовых НД для 4 и более циклов шифра «Калина» (ДСТУ 7624:2014) со всеми размерами блоков, для 512 битных блочных шифров, которые используются в хеш-функциях Whirlpool, Groestl и «Купина» (ДСТУ 7564:2014). С помощью утверждения 2 доказано отсутствие байтовых НД для 6 и более циклов шифров Торнадо и Лабиринт с размером блока 128 битов.

3. В рамках экспериментальных исследований были реализованы уменьшенные 16-битные шифрующие преобразования для SPN и фейстель-подобных шифров. Вычислительные эксперименты по поиску байтовых невыполнимых дифференциалов для уменьшенных моделей шифров подтвердили справедливость полученных теоретических выводов. Показано, что при отсутствии БНД могут присутствовать обычные НД. Для уменьшенных шифров, построенных по схеме SPN и по схеме фейстеля, обычные НД покрывают, соответственно, на 1 и на 2 цикла больше, чем БНД. В связи с этим, одним из перспективных направлений будущих исследований представляется изучение возможностей использования найденных обычных НД, которые покрывают большее количество циклов, чем БНД, в атаках на БСШ.

Литература

1. Biham, E. Cryptanalysis of Reduced Variant of Rijndael [Text] / E. Biham, N. Keller // The Third Advanced Encryption Standard Candidate Conference. – New York, 2000.

2. Cheon, J. H. Improved Impossible Differential Cryptanalysis of Rijndael and Crypton [Text] / J. H. Cheon, M. Kim, K. Kim, L. Jung-Yeun, S. Kang // Lecture Notes in Computer Science. – 2002. – P. 39–49. doi: 10.1007/3-540-45861-1_4

3. Lu, J. New Impossible Differential Attacks on AES [Text] / J. Lu, O. Dunkelman, N. Keller, J. Kim // Lecture Notes in Computer Science. – 2008. – P. 279–293. doi: 10.1007/978-3-540-89754-5_22

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

5. Biham, E. Miss in the Middle Attacks on IDEA and Khufu [Text] / E. Biham, A. Biryukov, A. Shamir // Lecture Notes in Computer Science. – 1999. – P. 124–138. doi: 10.1007/3-540-48519-8_10

6. Lu, J. Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1 [Text] / J. Lu, J. Kim, N. Keller, O. Dunkelman // Lecture Notes in Computer Science. – 2008. – P. 370–386. doi: 10.1007/978-3-540-79263-5_24

7. Wu, W.-L. Impossible Differential Cryptanalysis of Reduced-Round ARIA and Camellia [Text] / W.-L. Wu, W.-T. Zhang, D.-G. Feng // Journal of Computer Science and Technology. – 2007. – Vol. 22, Issue 3. – P. 449–456. doi: 10.1007/s11390-007-9056-0

8. Kim, J. Impossible Differential Cryptanalysis for Block Cipher Structures [Text] / J. Kim, S. Hong, J. Sung, S. Lee, J. Lim, S. Sung // Lecture Notes in Computer Science. – 2003. – P. 82–96. doi: 10.1007/978-3-540-24582-7_6

9. Luo, Y. A Unified Method for Finding Impossible Differentials of Block Cipher Structures [Text] / Y. Luo, Z. Wu, X. Lai, G. Gong // IACR Cryptology ePrint Archive. – 2009.

10. Li, R. Impossible Differential Cryptanalysis of SPN Ciphers [Text] / R. Li, B. Sun, C. Li // IACR Cryptology ePrint Archive. – 2010.

11. Yap, H. Impossible Differential Characteristics of Extended Feistel Networks with Provable Security against Differential Cryptanalysis [Text] / H. Yap // Communications in Computer and Information Science. – 2009. – P. 103–121. doi: 10.1007/978-3-642-10240-0_9

12. Daemen, J. AES proposal: Rijndael [Text] / J. Daemen, V. Rijmen // First Advanced Encryption Standard (AES) Conference. – Ventura, CA, 1998.

13. Горбенко, І. Д. Перспективний блоковий симетричний шифр «Калина» – основні положення та специфікація [Текст] / І. Д. Горбенко, В. І. Долгов, Р. В. Олійников, В. І. Руженцев та ін. // Прикладная радиоэлектроника. – 2007. – Т. 6, № 2. – С. 195–208.

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

15. Горбенко, И. Д. Алгоритм блочного симметричного шифрования «Торнадо». Спецификация преобразования [Текст] / И. Д. Горбенко, С. А. Головашич // Радиотехника. – 2003. – № 134. – С. 60–80.

16. Головашич, С. А. Спецификация алгоритма блочного симметричного шифрования «Лабиринт» [Текст] / С. А. Головашич // Прикладная радиоэлектроника. – 2007. – Т. 6, № 2. – С. 230–240.