УДК 004.056.55

ПРОВЕРКА МЕТОДА ДОКАЗАТЕЛЬСТВА СТОЙКОСТИ БЛОЧНЫХ ШИФРОВ К АТАКЕ НЕВЫПОЛНИМЫХ ДИФФЕРЕНЦИАЛОВ

В.И. РУЖЕНЦЕВ

Обсуждаются результаты вычислительных экспериментов по поиску невыполнимых дифференциалов для уменьшенных моделей блочных симметричных шифров. Подтверждается справедливость выводов, полученных с помощью предложенного в работе [1] метода обоснования отсутствия невыполнимых дифференциалов. Демонстрируются новые найденные для отдельных видов шифров невыполнимые дифференциалы, которые покрывают большее число циклов, чем известные.

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

ВВЕДЕНИЕ

В работе [1] был предложен метод, который позволяет обосновать отсутствие невыполнимых дифференциалов (НД) для блочных симметричных шифров (БСШ). Сложность метода, в отличие от известных, в меньшей степени зависит от размера блока. Метод был применен к Rijndael-подобным SPN шифрам и фейстель-подобным шифрам. В этой работе представлены результаты вычислительных экспериментов по поиску НД для уменьшенных моделей БСШ. Полученные результаты, с одной стороны, подтверждают справедливость предложенного в [1] метода, с другой стороны, на наш взгляд, демонстрируют новые потенциальные возможности в организации атак невыполнимых дифференциалов.

1. АТАКА НЕВЫПОЛНИМЫХ ДИФФЕРЕНЦИАЛОВ. ВИДЫ НЕВЫПОЛНИМЫХ ДИФФЕРЕНЦИАЛОВ

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 [2 – 4], так и шифры, построенные с использованием цепи фейстеля и других структур [5 – 9]. Подтверждением сказанного является большое количество работ, появившихся за последнее десятилетие и направленных, главным образом, на поиск невыполнимых дифференциалов [2 – 12]. Для шифра Rijndael с уменьшенным количеством циклов данную атаку можно считать одной из самых успешных.

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 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.

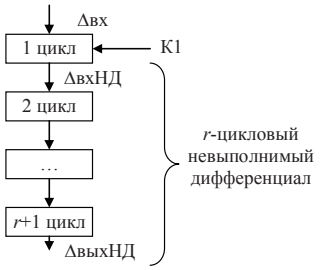

Рис. 1. Схема атаки НД

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 [2 – 4]. 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 каждая найденная правильная пара позволяет отсеять не один или несколько неправильных ключей первого цикла, а сразу несколько сотен или тысяч неправильных ключей первого цикла.

2. ПРЕДЛАГАЕМЫЙ МЕТОД

В отличие от большинства известных подходов [2 – 12], которые были рассмотрены в [1] и которые направлены на поиск НД, наш подход 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 или выходной разности. Рис. 2 поясняет эту идею.

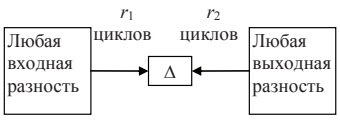

Рис. 2. Предлагаемый подход к обоснованию отсутствия НД

В [1] сформулирована и доказана следующая теорема, которую можно считать критерием отсутствия НД.

Теорема 1 ([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.

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 1 в [1] объясняется отсутствие БНД для многих Rijndael-подобных шифров, в том числе для шифра Rijndael со 128-битным блоком. 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 таблицах 1 и 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
2	Обнуление строки таблицы разности
3	Перебор вариантов ключа k
4	Перебор всех вариантов входного значения x
5	Инкрементируем ячейку с индексом $E_k(x)+E_k(x+d)$
6	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
2	Обнуление строки таблицы разности активизации
3	Перебор всех вариантов входной разности *d*, отвечающих выбранному входному вектору активизации
4	Перебор вариантов ключа *k*
5	Перебор всех вариантов входного значения *x*
6	Инкрементируем ячейку с индексом $E_k(x)+E_k(x+d)$
7	Перебор элементов полученной таблицы разности
8	Наличие элемента с ненулевым значением свидетельствует об отсутствии БНД с данным выходным вектором активизации
9	Если отсеяны все возможные выходные вектора активизации, то БНД не найдены и переходим к следующему значению входного вектора активизации
10	Если остались неотсеянные выходные вектора активизации, то каждый из них соответствует найденному БНД
	Выходные данные: Найденные БНД.

3. 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 и 4 схематически представлены преобразования, которые выполняются в рассматриваемых моделях SPN и фейстель-подобных шифров.

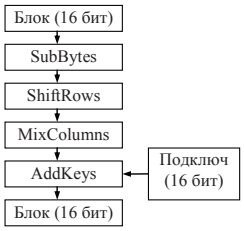

Рис. 3. Схема одного цикла SPN-шифра

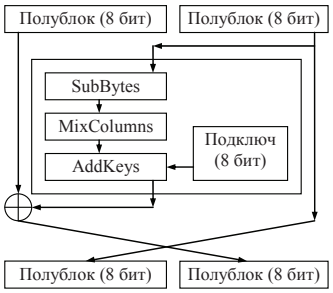

Рис. 4. Схема одного цикла фейстель-подобного шифра

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 24-битовых элемента;

структура полублока для фейстель-подобного: 24-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 $B = 3$.

4. АНАЛИЗ RIJNDAEL-ПОДОБНЫХ ШИФРОВ

В работе [1] выполнен анализ условий, при которых теоремы 1 и 2 могут быть применены к Rijndael-подобным SPN шифрам. Доказано следующее утверждение.

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

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 [2 – 4, 8 – 10].

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 о доказательстве отсутствия НД не менее, чем для 6 полных циклов.

С помощью представленных в таблицах 1 и 2 алгоритмов был проведен поиск НД и БНД для уменьшенной 16-битной версии алгоритма AES. Результаты представлены в таблицах 3 и 4.

Таблица 3

Результаты поиска НД для уменьшенной версии AES

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

Таблица 4

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 вх. вектора активизации с 1 активным S-блоком
4	0	

Результаты вычислительных экспериментов из табл. 4 подтверждают справедливость доказанного утверждения 1.

Результаты, представленные в табл. 3, 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, т.к., 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 ShiftRow 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 четырех полных циклов существуют и для полноразмерных Rijndael-подобных шифров, но сведений о них в доступной литературе найдено не было. Возможно, использование этих полубайтовые НД может сделать известные атаки более эффективными. Однако данный вопрос требует более тщательного исследования.

Под условия утверждения 1 попадают все Rijndael-подобные SPN шифры, что позволяет впервые 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).

5. 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 [14] и Лабиринт [15]. В каждом цикле выполняется SL-преобразование, схема которого представлена на рис. 5.

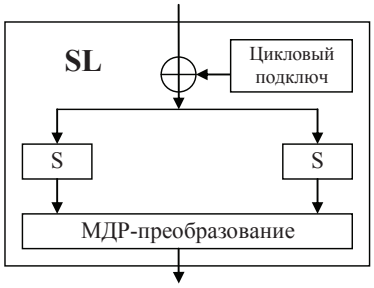

Рис. 5. SL-преобразование

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. Общая схема трех циклов преобразований представлена на рис. 6.

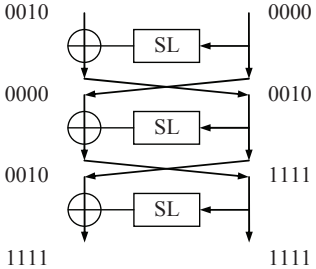

Рис. 6. Схема трансформации байтовой разности для трех циклов

В [1] показана 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.

Как и в предыдущей части для проверки полученных теоретических выводов с помощью представленных в таблицах 1 и 2 алгоритмов был проведен поиск НД и БНД для уменьшенной 16-битной версии алгоритма. Результаты представлены в таблицах 5 и 6.

Таблица 5

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 6

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	

Эксперименты по поиску обычных НД были проведены для подстановок с различным максимальным значением в таблице разности. Это значение указано в первой колонке табл. 5 для случаев, когда были найдены НД. В первом случае (первая строка табл. 5) максимальная вероятность прохождения ненулевой разности для подстановки 4 в 4 бита составляет 10/16 (S-блок max_dif = 10), а во втором (вторая строка табл. 5) - 4/16 (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, т. к., большее максимальное значение свидетельствует о большем количестве нулей (запрещенных переходов) в таблице разности.

Как и в предыдущем подразделе, отсутствие БНД не означает отсутствие НД для рассматриваемого шифра. В отличие от SPN шифров, где разница в числе циклов, необходимых для отсутствия БНД, от чис-

ла циклов, необходимых для отсутствия НД, составляет 1 цикл (см. табл. 3 и 4), в данном случае эта разница составляет 2 цикла. При этом результаты из табл. 6 подтверждают справедливость утверждения 2.

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

6. АНАЛИЗ ШИФРОВ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ СХЕМЫ ЛЕЯ-МЭССИ (LAI-MASSEY)

К наиболее известным шифрам, которые используют схему Lai-Massey, относятся шифры семейства Fox [16], шифр Мухомор [17]. Схема не является очень распространенной, поэтому и недостаточно изучена. В частности, один из пробелов – стойкость к атаке невыполнимых дифференциалов. В доступной литературе мы не встретили обоснование стойкости шифров с использованием схемы Lai-Massey к атаке невыполнимых дифференциалов. В этом подразделе продемонстрировано, как с использованием теоремы 2 может быть обоснована стойкость шифра, который использует схему Lai-Massey.

В качестве шифра, стойкость которого будем исследовать, взят алгоритм, в каждом цикле которого выполняется такое же SL-преобразование как и в предыдущем подразделе (см. рис. 5).

Схема двух циклов схемы Lai-Massey представлена на рис. 7.

Используя теорему 2 и лемму 3.4 из [16], покажем справедливость следующего утверждения.

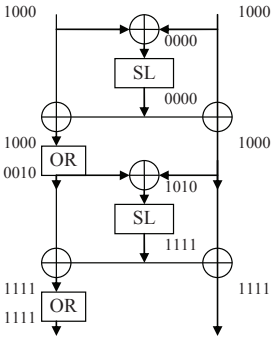

Рис. 7.Схема трансформации байтовой разности для двух циклов

Утверждение 3. Для рассматриваемого шифра (схема Lai-Massey и в цикловом преобразовании МДР-преобразование покрывает весь полублок) не существует БНД, покрывающих 4 и более цикла.

Доказательство. В соответствии с леммой 3.4 [16], в одном из двух подряд идущих циклов всегда будет ненулевая разность на входе SL-преобразования. Тогда МДР-преобразование может распространить эту разность на все байты полублока. После такого цикла всегда может быть получена разность со всеми активными байтами.

Дешифрование выполняется по такой же схеме, как и шифрование (отличие только в OR преобразовании), поэтому два цикла дешифрования также гарантируют возможность получения из любой ненулевой разности разность со всеми активными байтами. Тогда в соответствии с теоремой 2, для такого шифра не существует БНД, покрывающих 4 и более цикла. Утверждение доказано.

Для проверки полученных теоретических выводов с помощью представленных в таблицах 1 и 2 алгоритмов был проведен поиск НД и БНД для уменьшенной 16-битной версии алгоритма. Результаты представлены в таблицах 7 и 8.

Для уменьшенной модели шифра, который использует схему Lai-Massey и Rijndael-подобное цикловое преобразование, вычислительные эксперименты подтвердили отсутствие 4-цикловых БНД (см. табл. 8). В то же время, обычные НД не были найдены лишь для 7 циклов.

Как и при анализе фейстель-подобных шифров, в табл. 7 для максимального количества циклов, когда еще существуют НД, представлены результаты проверки шифров с подстановками, обладающими различной максимальной вероятностью прохождения ненулевой разности. В первом случае максимальная вероятность прохождения ненулевой разности для подстановки 4 в 4 бита составляет 10/16 (S-блок max_dif = 10), а во втором – 4/16 (S-блок max_dif = 4). Представленные результаты демонстрируют отсутствие решающего влияния дифференциальных свойств нелинейных подстановок на стойкость БСШ данного вида к атаке НД.

Таблица 7

Результаты поиска НД для уменьшенной версии шифра, который использует схему Lai-Massey

Количество циклов	Количество найденных НД	Комментарии
6(S-блок max_dif = 10)	Около 50	Для каждой входной разности типа $0y0y_{16}$, где y – произвольное 16-ричное значение
6 (S-блок max_dif = 4)	Около 20	Для каждой входной разности типа $0y0y_{16}$, где y – произвольное 16-ричное значение
7	0	

Таблица 8

Результаты поиска БНД для уменьшенной версии шифра, который использует схему Lai-Massey

Количество циклов	Количество найденных НД	Комментарии
3	1	Вх. вект. активиз. 1000, вых. вект. активиз.0010
4	0	

ЗАКЛЮЧЕНИЕ

Продемонстрировано применение предложенного в [1] метода для шифров, построенных по схеме SPN, по схеме фейстеля и по схеме Lai-Massey. Во всех случаях 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, по схеме фейстеля и по схеме Lai-Massey обычные НД покрывают на 1, 2 и 3 цикла больше, чем БНД.

Представленные результаты показали, что дифференциальные свойства нелинейных подстановок не оказывают решающего влияния на стойкость БСШ к атаке НД и максимальное количество циклов, покрываемых НД, не меняется при различных параметрах подстановок. 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.

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] Руженцев В.И. О методе доказательства стойкости блочных шифров к атаке невыполнимых дифференциалов [Текст] / Руженцев В.И. // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Харьков. Том 12, №2, 2013. – С. 215 - 219.

[2] Biham E. Cryptanalysis of Reduced Variant of Rijndael [Electronic resource] / E. Biham, N. Keller // The Third Advanced Encryption Standard Candidate Conference, New York, USA, April 13–14, 2000. – Mode of access : www. URL: http://csrc.nist.gov/archive/aes/index.html.

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

[4] New Impossible Differential Attacks on AES [Electronic resource] / J. Lu, O. Dunkelman, N. Keller, J. Kim // IACR Cryptology ePrint Archive 2008: 540 (2008).

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

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

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

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

[9] A Unified Method for Finding Impossible Differentials of Block Cipher Structures [Electronic resource] / Y. Luo, Z. Wu, X. Lai, G. Gong // IACR Cryptology ePrint Archive 2009: 627 (2009).

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

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

[12] Biham E. Miss in the Middle Attacks on Idea and Khufu [Text] / E. Biham, A. Biryukov, A. Shamir // Fast Software Encryption : proceedings of the 6th International Workshop, FSE'99, Rome, Italy, March 24–26, 1999. – Berlin ; Heidelberg : Springer, 1999. – P. 124–138. – (Lecture Notes in Computer Science ; vol. 1636).

[13] Kleiman E. The XL and XSL attacks on Baby Rijndael [Electronic resource] / E. Kleiman // Thesis, 2005. Mode of access : http://orion.math.iastate.edu/dept/thesisarchive/MS/EKleimanMSSS05.pdf.

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

[15] Головашич, С. А. Спецификация алгоритма блочного симметричного шифрования «Лабиринт» [Текст] / С. А. Головашич // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Харьков. Том 6, №2, 2007. – С. 230 – 240.

[16] Junod P. FOX: a new family of block ciphers [Text] / P. Junod, S. Vaudenay // Selected Areas in Cryptography. – Berlin ; Heidelberg : Springer, 2005. – P. 114–129.

[17] Перспективний блоковий симетричний шифр «Мухомор»: основні положення та специфікація [Текст] / Р. В. Олійников, І. Д. Горбенко, М. Ф. Бондаренко, В. І. Руженцев // Прикладная радиоэлектроника. – 2007. – Т. 6, № 2. – С. 147–157.

Руженцев Виктор Игоревич, доктор технических наук, доцент, профессор кафедры БИТ ХНУРЭ. Научные интересы: симметричная криптография, криптоанализ.

УДК 004.056.55

Перевірка методу доведення стійкості блокових шифрів до атаки нездійснених диференціалів / В.І. Руженцев // Прикладна радіоелектроніка: наук.-техн. журнал. – 2016. Том 15, № 3. – С. 184 – 190.

Обговорюються результати обчислювальних експериментів з пошуку нездійснених диференціалів для зменшених моделей блокових шифрів. Підтверджується справедливість висновків, отриманих за допомогою запропонованого в роботі [1] методу. Демонструються нові знайдені нездійснені диференціали, які покривають більшу кількість циклів, ніж відомі.

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

Табл.: 08. Іл.: .07. Бібліогр.: 17 назв.

UDC 004.056.55

Analysis of the method of proving the resistance of block ciphers to impossible differential attack / V.I. Ruzhentsev // Applied Radio Electronics: Sci. Journ. 2016. – Vol. 15, № 3. – P. 184 – 190.

The results of computing experiments on impossible differentials searching for reduced models of block symmetrical ciphers are discussed . The validity of the conclusions obtained with the help of the method of substantiating the lack of impossible differentials, that is suggested in the work [1], is confirmed. New impossible differentials which cover more rounds than the known ones are presented for some types of ciphers.

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

Tab.: 08. Fig.: 07. Ref.: 17 items.