УДК 004.056.55
Р 83

О СТОЙКОСТИ К АТАКЕ УСЕЧЕННЫХ ДИФФЕРЕНЦИАЛОВ RIJNDAEL-ПОДОБНЫХ ШИФРОВ С БОЛЬШИМИ РАЗМЕРАМИ БЛОКОВ

В. И. Руженцев, канд. техн. наук, доц.

Харьковский национальный университет радиоэлектроники, г. Харьков

Аннотация. Проанализирована стойкость Rijndael-подобных блочных шифров к атаке усеченных дифференциалов. Доказано отсутствие усеченных байтовых дифференциалов, которые могут быть положены в основу атаки.
Ключевые слова: блочный симметричный шифр, атака усеченных дифференциалов, байтовая дифференциальная характеристика, байтовый дифференциал.

Анотація. Проаналізовано стійкість Rijndael-подібних блокових шифрів до атаки усічених диференціалів. Доведено відсутність усічених байтових диференціалів, які можуть бути покладені в основу атаки.
Ключові слова: блоковий симетричний шифр, атака усічених диференціалів, байтова диференціальна характеристика, байтовий диференціал.

Abstract. The attack strength of truncated differentials of Rijndael-like block ciphers has been considered. The absence of truncated byte differentials which may be the basis for the attack has been proved.
Keywords: block symmetric cipher, truncated differentials attack, byte differential characteristic, byte differential.

ПОСТАНОВКА ПРОБЛЕМЫ

История симметричной криптографии в эру компьютерных технологий связана с увеличением размеров блока и ключа для блочных шифров. Объясняется это тем, что эти параметры определяют стойкость шифра к атакам «грубой силы», а постоянно возрастающие возможности вычислительной техники расширяют возможности потенциальных злоумышленников для реализации этих атак. На сегодняшний день нередко встречается использование блочных шифров с размером 1024 бита, например в составе хеш-функций. При этом многие новые шифры и хеш-функции используют элементы наиболее распространенного сегодня блочного симметричного шифра (БСШ) Rijndael [8]. Анализ криптографической стойкости Rijndael-подобных шифров со значительно увеличенным блоком является актуальной задачей.

АНАЛИЗ ПОСЛЕДНИХ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ

В работах [4, 6] предложено доказательство отсутствия эффективных байтовых дифференциалов для Rijndael-подобных шифров. В отличие от известных до этого подходов из работ [11, 12], процесс доказательства не связан с какими-либо вычислительными процессами, сложность которых резко возрастает с увеличением размера блока и количества циклов. Однако в [4, 6] продемонстрировано применение этого подхода лишь для шифра Rijndael со 128-битным блоком.

ЦЕЛЬЮ РАБОТЫ является, с одной стороны, демонстрация возможности применения подхода из [4, 6] к шифрам с большим размером блока (в настоящей работе рассматриваются шифры с размером блока до 1024 битов), с другой стороны изучение криптостойкости таких шифров.

ИЗЛОЖЕНИЕ ОСНОВНОГО МАТЕРИАЛА

Атака усеченных дифференциалов. Методика реализации атаки усеченных дифференциалов была предложена Л. Кнудсеном [9]. Отличие от обычной дифференциальной атаки заключается в том, что через циклы проводится не полная разность, а некоторая ее часть. В работе [9] показано, что такая методика эффективна в случаях, когда в шифре используется недостаточно хорошее рассеивание и прохождение разности через несколько циклов может рассматриваться независимо от значения разности в некоторой части блока.

Один из вариантов атаки – атака байтовых дифференциалов – была предложена в работах [7, 10]. В ходе атаки 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. При этом 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 – сумма вероятностей всех входящих в него БДХ.

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):

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

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 r-цикловый дифференциал, то может быть организована атака на $(r + 1)$-цикловый шифр. Для последнего цикла будут известны выходное значение разности (на основе известных значений криптограмм) и входной вектор активизации (в соответствии с используемым байтовым дифференциалом). Эти данные позволяют получить информацию о подключе последнего цикла. Таким образом, для выполнения атаки необходимо, чтобы БД или БДХ покрывали почти все циклы шифра.

Рассматриваемые Rijndael-подобные шифры с большими размерами блоков. В настоящей работе рассмотрена стойкость Rijndael-подобных шифров, то есть алгоритмов шифрования, которые построены по принципу Substitution-Permutation Network (SPN) и 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 изменяться количество и размер колонок.

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 [8] 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 (рис. 1).

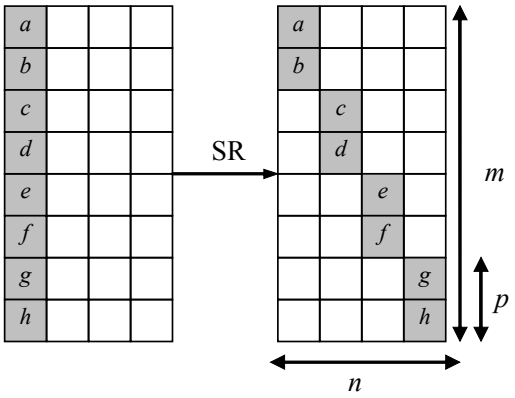

Рис. 1

В этих случаях всегда будет выполняться условие

$$m = np. \quad (2)$$

Такая схема преобразования используется в шифре «Калина» [3].

Прежде чем перейти к рассмотрению стойкости Rijndael к атаке, выделим особенности преобразования MC, так как именно это преобразование вносит неопределенность в прохождение векторов активизации через циклы шифра. В работе [5] проведен анализ этого преобразования и определены вероятности переходов векторов активизации через MC. В табл. 1 и 2 для преобразования MC, которое покрывает 4 и 8 байтов соответственно, представлены двоичные логарифмы от вероятностей перехода векторов активизации через MC для различного числа активных битов на входе (меняется по столбцам) и выходе (по строкам).

Таблица 1. **Log_2 вероятности перехода вектора активизации через 4-байтный MC**

Вход	Выход				
	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 MC**

Вход	Выход								
	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

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. Эффективная байтовая дифференциальная характеристика для Rijndael-подобного шифра не может содержать ни одного цикла со всеми активными колонками на входе преобразования MC [4].

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

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

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

В этой работе удалось доказать подобную теорему, но не для отдельного шифра, а для отдельного класса шифров.

Следующим этапом в [4] стало рассмотрение БДХ, которые входят в состав БД. Начиная с этого этапа, анализ выполнялся для 128-битного варианта шифра Rijndael. Первое свойство БД сформулировано в виде утверждения 1.

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

Такие БДХ в [4] были названы основными БДХ. Остальные БДХ были названы дополнительными. Второе свойство относится к дополнительным БДХ.

Утверждение 2. Для каждого БД с тремя или более циклами любая дополнительная БДХ с k дополнительными пассивными байтами имеет вероятность примерно в 2^{8k} раза ниже, чем основная БДХ этого БД [4].

Теорема 2. Для вариантов шифра Rijndael с размером блока 128 битов нет эффективных БД для трех и более циклов.

Таким образом, можно выделить следующие основные этапы предложенного в [4] подхода к доказательству отсутствия эффективных 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.

В настоящей работе предпринята попытка распространить этот подход на Rijndael-подобные шифры с большим размером блока.

Исследование шифров с большими блоками. На первом этапе предложенной в [4] методики необходимо определить минимальное число циклов, при котором для шифров отсутствуют эффективные БДХ.

Докажем теорему, которая является аналогом теоремы 1 из [6], но для более широкого класса шифров.

Теорема 3. Для Rijndael-подобного шифра с равномерным распределением байтов каждой колонки по всем колонкам в ходе процедуры SR не существует эффективных байтовых дифференциальных характеристик для трех и более циклов.

Доказательство. Рассмотрим 3-цикловую БДХ для такого шифра. Пусть на входе MC-преобразования 1-го, 2-го и 3-го циклов будет соответственно a, b и c активных колонок ($a > 0$, $b > 0$ и $c > 0$). В первом цикле после операции MC в каждой активной колонке должно быть не более bp активных байтов (в противном случае во втором цикле будет больше, чем b, активных колонок на входе MC). Тогда, учитывая, что каждый пассивный байт на выходе преобразования MC уменьшает вероятность БДХ примерно в 2^8 раза, верхняя граница вероятности БДХ после первого цикла составит $2^{-(m-bp)\cdot 8a}$.

Исходя из аналогичных соображений после двух циклов вероятность БДХ составит не более чем $2^{-(m-bp)\cdot 8a} \cdot 2^{-(m-cp)\cdot 8b}$.

При этом, если считать, что в третьем цикле после преобразования MC в каждой из c активных колонок будут активны все байты, то, используя выражение (1) для вычисления нижней границы вероятности эффективной БДХ, будет получено

$$p_{сл} = 2^{-(n-c)\cdot 8m}.$$

Для того чтобы теорема была справедлива, должно выполняться неравенство

$$-(m-bp)\cdot 8a-(m-cp)\cdot 8b \leq -(n-c)\cdot 8m. \qquad (3)$$

Следует отметить, что каждый дополнительный пассивный байт на выходе операции MC третьего цикла будет добавлять множитель 2^{-8} в обе части этого неравенства.

Неравенство (3) равносильно неравенству

$$-(m-bp)\cdot 8a-(m-cp)\cdot 8b \leq -(n-c)\cdot 8m. \qquad (4)$$

В соответствии с леммой о числе активных колонок [4] можно записать $a + c \geq n + 1$. Поскольку $n \geq b$, то $(m - bp) \geq 0$, а следовательно, $-(m - bp)\cdot 8a \leq 0$. Поэтому в выражение (4) можно подставить вместо a минимальное значение, т. е. сделать замену $a = n + 1 - c$. Раскрыв после этого в (4) скобки, выполнив элементарные преобразования и учитывая уравнение (2), неравенство (4) сводится к неравенству

$$b \leq n,$$

которое всегда является справедливым. Теорема доказана.

Для проверки подлинности теоретических выводов были проведены вычислительные эксперименты по поиску эффективных БДХ с использованием метода Мораи [11] для шифров с размером блока до 128 битов и модифицированного метода из [5] для больших размеров блока. Результаты представлены в табл. 3, цветом выделены варианты шифров, попадающие под условие приведенной теоремы.

Таблица 3. **Минимальное количество циклов, при котором не существует эффективных БДХ**

Размер колонки	Количество колонок в блоке	Число циклов
4 байта	4	3
	6	4
	8	6
8 байтов	2	3
	4	3
	8	3
	16	7

Представленные результаты подтверждают справедливость доказанной теоремы, а также демонстрируют недостаток вариантов шифров, для которых число колонок больше числа строк ($n > m$). Эффективные БДХ в этих случаях могут покрывать значительно большее количество циклов.

Еще одно наблюдение, связанное с анализом результатов вычислительных экспериментов, заключается в том, что все рассмотренные варианты шифров БДХ, которые обладают максимальной вероятностью, обычно содержат минимальное количество активных колонок. При этом в соответствии с леммой 1 нет ни одного цикла, где одновременно все колонки активны на входе преобразования MC. Так, для случаев, когда в рамках операции SR выполняется циклический сдвиг каждой из строк на различное количество байтов, эффективные БДХ, покрывающие максимальное количество циклов, в основном состоят из циклов с количеством активных колонок $\frac{m}{2}+1$. Например, для всех вариантов Rijndael это значение равняется 3, то есть эффективные БДХ, представленные в табл. 3 для 4-байтных колонок, будут содержать по три активных колонки в каждом из циклов. При этом каждая активная колонка обычно содержит $\frac{m}{2}+1$ активных байтов на входе и выходе. Пример одного такого цикла для шифра со 128-битным блоком представлен на рис. 2.

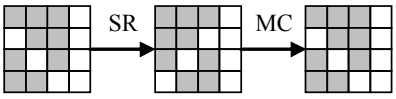

Рис. 2

На втором этапе подхода из [4] следует оценить вероятности основной и дополнительных БДХ. В работе [4] для выполнения этих оценок доказаны утверждения 1 и 2. Утверждение 2 с определенными коррективами справедливо для всех Rijndael-подобных SPN-шифров. В утверждении 1 численный множитель в показателе степени граничного значения зависит от размера колонки и соответствующих вероятностей переходов из табл. 1 или 2 и от количества колонок в блоке. Таким образом, вероятность основной БДХ

$$P_{\text{осн}} = p_{\text{сл}} \cdot (p_{\text{MC}})^{nr},$$

где r – число циклов; n – число колонок в блоке; p_{MC} – вероятность перехода вектора активизации для одной колонки со всеми активными байтами на входе и выходе (значение вероятности в нижнем правом углу табл. 1 или 2).

Соответствующие граничные значения вероятностей основной и дополнительных БДХ представлены в табл. 4.

Таблица 4. **Вероятности основной и дополнительных БДХ**

Размер колонки	Количество колонок в блоке	Вероятность основной БДХ	Вероятность дополнительной БДХ с k дополнительными пассивными байтами
4 байта	4	$p_{\text{сл}} \cdot 2^{-0,0904r}$	$p_{\text{сл}} \cdot 2^{-0,0904r} \cdot 2^{-8k}$
	6	$p_{\text{сл}} \cdot 2^{-0,1356r}$	$p_{\text{сл}} \cdot 2^{-0,1356r} \cdot 2^{-8k}$
	8	$p_{\text{сл}} \cdot 2^{-0,1808r}$	$p_{\text{сл}} \cdot 2^{-0,1808r} \cdot 2^{-8k}$
8 байтов	2	$p_{\text{сл}} \cdot 2^{-0,08r}$	$p_{\text{сл}} \cdot 2^{-0,08r} \cdot 2^{-8k}$
	4	$p_{\text{сл}} \cdot 2^{-0,16r}$	$p_{\text{сл}} \cdot 2^{-0,16r} \cdot 2^{-8k}$
	8	$p_{\text{сл}} \cdot 2^{-0,32r}$	$p_{\text{сл}} \cdot 2^{-0,32r} \cdot 2^{-8k}$
	16	$p_{\text{сл}} \cdot 2^{-0,64r}$	$p_{\text{сл}} \cdot 2^{-0,64r} \cdot 2^{-8k}$

Третий этап связан с оценкой количества возможных дополнительных БДХ. В [4] показано, что наибольшее количество дополнительных БДХ набирается в случаях, когда дополнительные пассивные байты будут располагаться в отдельных циклах. Остальными вариантами расположения дополнительных пассивных байтов можно пренебречь, так как их количество будет значительно меньше. Обозначив количество байтов в блоке b, количество дополнительных БДХ с распределением дополнительных k пассивных байтов по одному в цикле может быть оценено как

$$C_r^k \cdot b^k = \frac{r!}{k! \cdot (r-k)!} \cdot b^k \approx \frac{(r^k \cdot b^k)}{k!}. \qquad (5)$$

В табл. 5 представлено количество различных r-цикловых БДХ с k дополнительными пассивными байтами, которые принадлежат одному и тому же БД, то есть имеют фиксированные входную и выходную активизации байтов.

На четвертом этапе следует оценить суммарную вероятность от всех БДХ, входящих в состав одного БД. Для этого нужно просуммировать произведения количества БДХ из табл. 5 на их вероятность из табл. 4. Результаты представлены в табл. 6.

Таблица 5. **Количество различных r-цикловых БДХ с k дополнительными пассивными байтами**

Размер колонки	Количество колонок в блоке	Количество БДХ
4 байта	4	$(r^k \cdot 16^k)/k!$
	6	$(r^k \cdot 24^k)/k!$
	8	$(r^k \cdot 32^k)/k!$
8 байтов	2	$(r^k \cdot 16^k)/k!$
	4	$(r^k \cdot 32^k)/k!$
	8	$(r^k \cdot 64^k)/k!$
	16	$(r^k \cdot 128^k)/k!$

Таблица 6. **Вероятность БД с числом циклов R, при котором отсутствуют эффективные БДХ**

Размер колонки	Количество колонок в блоке	Вероятность БД
4 байта	4	$\left(e^{\frac{1}{16}} \cdot 2^{-0,0904}\right)^R \cdot p_{сл} \approx 1^R \cdot p_{сл}$
	6	$\left(e^{\frac{3}{32}} \cdot 2^{-0,1356}\right)^R \cdot p_{сл} \approx 1^R \cdot p_{сл}$
	8	$\left(e^{\frac{1}{8}} \cdot 2^{-0,1808}\right)^R \cdot p_{сл} \approx 1^R \cdot p_{сл}$
8 байтов	2	$\left(e^{\frac{1}{16}} \cdot 2^{-0,09}\right)^R \cdot p_{сл} \approx 1^R \cdot p_{сл}$
	4	$\left(e^{\frac{1}{8}} \cdot 2^{-0,18}\right)^R \cdot p_{сл} \approx 1^R \cdot p_{сл}$
	8	$\left(e^{\frac{1}{4}} \cdot 2^{-0,36}\right)^R \cdot p_{сл} \approx 1^R \cdot p_{сл}$
	16	$\left(e^{\frac{1}{2}} \cdot 2^{-0,72}\right)^R \cdot p_{сл} \approx 1^R \cdot p_{сл}$

Из представленных в табл. 6 результатов видно, что во всех случаях получено значение вероятности БД, равное $p_{сл}$, а значит БД с большим числом циклов, чем может покрыть эффективная БДХ, не являются эффективными (не удовлетворяют условию (1)).

Исследование шифров, использующих цепь Фейстеля и Rijndael-подобные преобразования. В этом подразделе сделана попытка применить предложенный в [4, 6] подход к шифрам, в основе которых лежит цепь Фейстеля, а цикловое преобразование использует Rijndael-подобные преобразования. К известным шифрам этого вида можно отнести «Торнадо» [2] и «Лабиринт» [1].

Выполняя вычислительные эксперименты по поиску эффективных БДХ с помощью методов из [5, 11], был сделан вывод, что при использовании цепи Фейстеля и Rijndael-подобных преобразований важным становится порядок выполнения линейных преобразований в цикле. Порядок преобразований BS, SR, MC, AddKey, используемый в Rijndael, не является оптимальным. На рис. 3 представлена 4-цикловая итеративная БДХ, которая может быть многократно повторена и обладает вероятностью $\approx 2^{-56}$. Для сравнения: при порядке преобразований BS, MC, SR, AddKey лучшая 4-цикловая итеративная БДХ будет иметь вероятность $\approx 2^{-96}$ (рис. 4). В обоих случаях возможна 3-цикловая итеративная БДХ (рис. 5), в которой каждый третий цикл использует переход нулевой разности с вероятностью 1. Но вероятность такой БДХ $\approx 2^{-128}$, что значительно ниже, чем у упомянутых ранее.

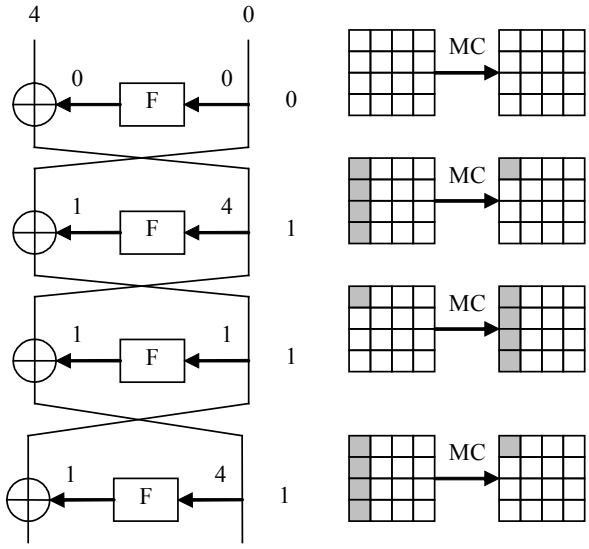

Рис. 3

На рис. 3–5 справа представлены переходы векторов активизации, которые происходят при выполнении операции MC в соответствующих циклах. Цифрами обозначено количество активных колонок на входе и выходе циклового преобразования, а справа – количество активных колонок на входе преобразования MC.

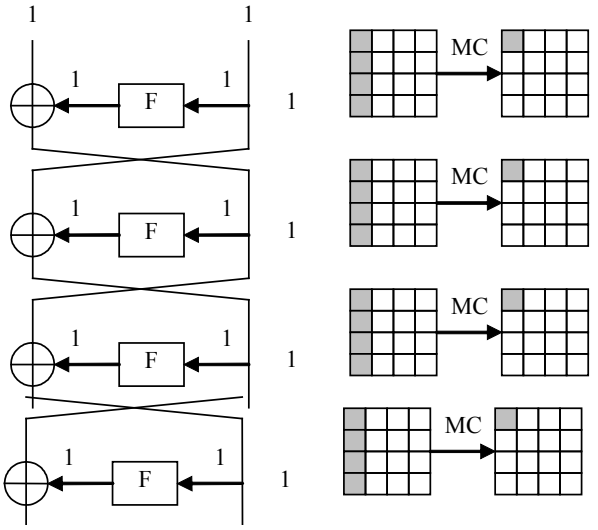

Рис. 4

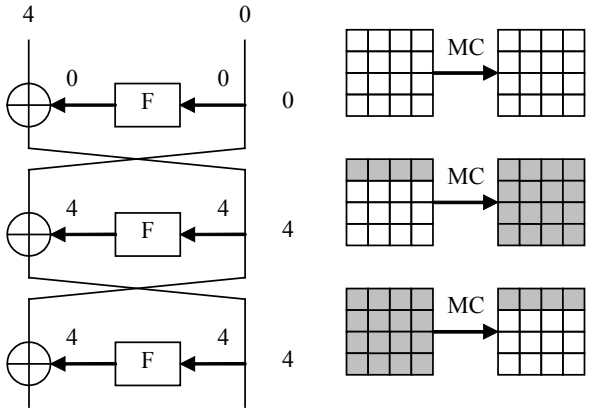

Рис. 5

Далее рассмотрим варианты Фейстель-подобных шифров с порядком преобразований в цикле BS, MC, SR, AddKey, как обладающие более высоким уровнем защищенности от рассматриваемого вида атак.

В табл. 7 представлены результаты выполнения первого этапа исследования таких шифров.

Таблица 7. **Минимальное количество циклов, при котором не существует эффективных БДХ**

Размер колонки	Количество колонок в полублоке	Число циклов
4 байта	2	5
	4	8
8 байтов	1	3
	2	6
	4	9
	8	16

Анализ результатов позволяет сделать вывод о значительно меньшей защищенности Rijndael-подобных шифров с применением цепи Фейстеля по сравнению с использованием схемы SPN (см. табл. 3). Исключением является вариант цепи Фейстеля с единственной колонкой в блоке.

На втором этапе следует оценить вероятности основной и дополнительных БДХ.

Как и в случае с SPN-схемой, основная БДХ будет содержать переходы, обладающие максимальной вероятностью и максимальным количеством активных байтов на выходе всех операций MC и всех XOR-сложений полублоков во всех циклах, кроме нескольких последних. В нескольких последних циклах количество и позиции активных байтов на выходе преобразований будут диктоваться значением выходного вектора активизации.

Вероятность такой r-цикловой БДХ может быть оценена следующим образом:

$$P_{\text{осн}} = \left(\left(p_{\text{MC}}\right)^n \cdot \left(\frac{254}{255}\right)^{mn} \right)^r \cdot p_{\text{сл}},$$

где m, n – соответственно число строк и колонок в полублоке; p_{MC} – вероятность перехода вектора активизации для одной колонки со всеми активными байтами на входе и выходе (значение вероятности в нижнем правом углу табл. 1 или 2). В последнем выражении первый множитель в скобках учитывает снижение вероятности БДХ при прохождении преобразований MC, а второй – при прохождении XOR-суммы полублоков.

Тогда вероятность каждой дополнительной БДХ с k дополнительными пассивными байтами будет

$$P_{\text{доп}} = P_{\text{осн}} \cdot 2^{-8k}.$$

В табл. 8 представлены вероятности основной и дополнительных БДХ для шифров с использованием цепи Фейстеля и количеством циклов, при котором отсутствуют эффективные БДХ (аналог табл. 4 для SPN-шифров).

Таблица 8. **Вероятности БДХ для шифров с использованием цепи Фейстеля**

Размер колонки	Количество колонок в полублоке	Вероятность основной БДХ
4 байта	2	$p_{\text{сл}} \cdot 2^{-0{,}0902r}$
	4	$p_{\text{сл}} \cdot 2^{-0{,}1811r}$
8 байтов	1	$p_{\text{сл}} \cdot 2^{-0{,}09r}$
	2	$p_{\text{сл}} \cdot 2^{-0{,}1807r}$
	4	$p_{\text{сл}} \cdot 2^{-0{,}3614r}$
	8	$p_{\text{сл}} \cdot 2^{-0{,}7228r}$

На третьем этапе необходимо оценить количество возможных дополнительных БДХ. Как и для SPN-шифров, наибольшее количество дополнительных БДХ набирается в случаях, когда дополнительные пассивные байты будут располагаться в отдельных циклах. Остальными вариантами расположения дополнительных пассивных байтов можно пренебречь, так как их количество будет значительно меньше.

Обозначив количество байтов в блоке b, количество дополнительных БДХ с распределением дополнительных k пассивных байтов по одному в цикле может быть оценено как

$$C_r^k \cdot \left(\frac{b}{2}+\frac{b}{2}\right)^k = C_r^k \cdot b^k \approx \frac{(r^k \cdot b^k)}{k!}.$$

Полученное значение идентично тому, что было найдено в выражении (5) для SPN-шифров, а данные из табл. 5 практически повторяют данные из табл. 4 для одинаковых размеров блока. Таким образом, как и для схемы SPN (см. табл. 6), во всех случаях шифров, построенных с использованием цепи Фейстеля, граничная вероятность БД будет составлять $\approx p_{сл}$, то есть БД не будут эффективными.

ВЫВОДЫ

Главным результатом работы стал вывод об отсутствии эффективных байтовых дифференциалов для всех рассмотренных шифров, использующих схему SPN или Фейстеля и Rijndael-подобную структуру цикловых преобразований, когда число циклов больше граничного значения, при котором уже не существуют эффективные байтовые дифференциальные характеристики.

Вторым важным результатом является вывод о возможности применения подхода из [4, 6] для достаточно широкого класса шифров с Rijndael-подобной структурой цикловых преобразований.

В работе также отмечены преимущества с точки зрения криптостойкости SPN-шифров, в блоке которых количество колонок не превышает количества строк. Доказана теорема о том, что такие шифры с тремя и более циклами не содержат эффективных байтовых дифференциальных характеристик.

Показано, что криптостойкость SPN-шифров выше, чем у Фейстель-подобных шифров при равном размере блока и количестве циклов. Исключением является ситуация, когда полублок Фейстель-подобного шифра содержит всего одну колонку.

Выявлена зависимость криптостойкости от очередности преобразований в цикловой функции для шифров, использующих схему Фейстеля.

Перспективным направлением исследований представляется анализ возможности использования усеченных байтовых характеристик и усеченных байтовых дифференциалов в атаках на алгоритмы хеширования, где обычно и применяются шифры с большими размерами блоков.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

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

[2] **Долгов, В. И.** Криптостойкость шифра «Торнадо» [Текст] / В. И. Долгов, С. А. Головашич, В. И. Руженцев // Радиотехника. – 2003. – № 134. – С. 81–88.

[3] 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. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – 2007. – № 2, т. 6. – С. 195–208.

[4] **Руженцев, В. И.** Доказуемая стойкость Rijndael-подобных шифров к атаке усеченных дифференциалов [Текст] / В. И. Руженцев // Радіоелектронні і комп'ютерні системи : науково-технічний журнал. – 2012. – № 5. – С. 51–55.

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

[6] **Руженцев, В. И.** Про доказательство отсутствия эффективных байтовых дифференциальных характеристик для Rijndael-подобных шифров [Текст] / В. И. Руженцев // Радиотехника. – 2012. – № 170. – С. 130–133.

[7] Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms [Text] / K. Aoki, T. Ichikawa, M. Kanda [et al.] // Selected Areas in Cryptography – 7th Annu. Intern. Workshop, SAC2000, Lecture Notes in Computer Science. – Berlin : Springer-Verlag, 2001. – P. 39–56.

[8] **Daemen, J.** AES Proposal Rijndael [Электронный ресурс] / J. Daemen, V. Rijmen // AES Round 1 Technical Evaluation CD1: Documentation, Nat. Inst. of Standards and Technology, Aug. 1998. – Режим доступа: http://www.nist.gov/aes.

[9] **Knudsen, L. R.** Truncated and Higher Order Differentials [Text] / L. R. Knudsen // Fast Software Encryption – Second Intern. Workshop, Vol. 1008 of Lecture Notes in Computer Science. – Berlin ; Heidelberg ; New York : Springer-Verlag, 1995. – P. 196–211.

[10] **Knudsen, L. R.** Truncated differentials of SAFER [Text] / L. R. Knudsen, T. A. Berson // In Fast Software Encryption – Third Intern. Workshop, FSE'96, Vol. 1039 of Lecture Notes in Computer Science. – Berlin ; Heidelberg ; New York : Springer-Verlag, 1996.

[11] **Moriai, S.** Security of E2 against Truncated Differential Cryptanalysis [Text] / S. Moriai, M. Sugita, K. Aoki // Selected Areas in Cryptography — 6th Annu. Intern. Workshop, SAC'99, Vol. 1758 of Lecture Notes in Computer Science. – Berlin ; Heidelberg ; New York : Springer-Verlag, 2000. – P. 106–117.

[12] **Sugita, M.** Relationships among differential, truncated differential, impossible differential cryptanalyses against word-oriented block cipher like Rijndael, E2 [Электронный ресурс] / M. Sugita, K. Kobara // Nat. Inst. of Standards and Technology. – Режим доступа: http://www.nist.gov/aes.

© В. І. Руженцев

Надійшла до редколегії 12.02.13
Статтю рекомендує до друку
канд. фіз.-мат. наук, доц. *Д. М. Самойленко*
Статтю розміщено у Віснику НУК № 1, 2013