УДК 004.056.55

ВЕРОЯТНОСТИ ДВУХЦИКЛОВЫХ ДИФФЕРЕНЦИАЛОВ RIJNDAEL-ПОДОБНОГО ШИФРА С ПРОИЗВОЛЬНЫМИ ПОДСТАНОВКАМИ

В.И. РУЖЕНЦЕВ

Работа посвящена анализу двухцикловых дифференциалов Rijndael-подобного шифра. Предложенный в одной из предыдущих работ подход к оценке вероятностей дифференциалов применяется для шифров с неалгебраически построенными подстановками. Демонстрируются отличия в получаемых результатах. Справедливость полученных в работе теоретических результатов проверяется вычислительными экспериментами.

Ключевые слова: AES, дифференциал, дифференциальная характеристика, разность, таблица разности.

ВВЕДЕНИЕ

В работе [1] был предложен метод оценки максимальной вероятности двухцикловых дифференциалов для Rijndael-подобных шифров. Этот метод, в отличие от аналогичного ранее предложенного метода из [2], не зависит от вида используемых нелинейных подстановок и может быть использован для любых подстановок. Однако в работе [1] было продемонстрировано применение этого метода только для шифров с алгебраически построенными подстановками, которые обладают предельными дифференциальными и линейными показателями. Целью данной работы является демонстрация возможности применения метода из [1] для шифров с произвольными подстановками, каким, например, можно считать шифр «Калина» [3], который стал победителем на украинском конкурсе блочных алгоритмов [4].

1. СУПЕР-S-БЛОКИ AES

Как и в работах [1, 2] будем рассматривать супер-S-блок, который состоит из последовательности операций ByteSub, MixColumns, AddKey и ByteSub и работает с одной колонкой блока данных. Супер-S-блок AES работает с 32-битным блоком, а в настоящей работе мы будем рассматривать 16-битный вариант супер-S-блока, который содержит четыре 4-битных S-блока. Для такого варианта супер-S-блока имеется возможность более подробно изучить свойства в ходе вычислительных экспериментов.

В качестве 4-битовых S-блоков взята произвольно построенная подстановка, представленная в табл. 1.

Таблица 1

Используемая подстановка

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
5	9	B	2	3	6	F	8	7	C	0	E	1	D	4	A

Эта подстановка не является алгебраически построенной и не обладает предельными дифференциальными показателями, что видно из представленной таблицы разностей (см. табл. 2).

Для дальнейших расчетов важным является количество различных значений в этой таблице для случаев, когда входная и выходная разности не равны 0 (см. табл. 3).

Таблица 2

Таблица разностей

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	2	0	2	0	2	0	2	4	0	4	0
2	0	0	2	0	0	2	0	4	0	0	0	2	2	0	4	0
3	0	0	2	0	0	0	0	2	0	6	0	4	2	0	0	0
4	0	2	0	0	6	0	4	0	0	0	2	0	0	0	0	2
5	0	0	0	4	0	0	0	0	0	0	8	0	0	4	0	0
6	0	4	0	4	2	0	2	0	2	0	2	0	0	0	0	0
7	0	2	0	0	0	0	2	0	2	0	0	0	0	8	0	2
8	0	0	6	0	0	2	0	0	0	0	0	6	2	0	0	0
9	0	0	2	0	0	4	0	2	0	2	0	0	2	0	4	0
A	0	0	0	0	0	4	0	4	0	0	0	0	4	0	4	0
B	0	0	4	0	0	2	0	2	0	6	0	2	0	0	0	0
C	0	0	0	0	6	0	2	0	2	0	2	0	0	0	0	4
D	0	6	0	0	0	0	2	0	6	0	0	0	0	0	0	2
E	0	2	0	4	2	0	0	0	4	0	2	0	0	0	0	2
F	0	0	0	4	0	0	4	0	0	0	0	0	0	4	0	4

Таблица 3

Статистическая информация для таблицы разности

Значение	Количество значений в таблице разностей
“8”	2
“6”	8
“4”	22
“2”	36
“0”	157

Таким образом, при условии, что входная и выходная разности не равны 0, доля ненулевых значений в таблице разности составляет 68/225=0,3.

В преобразовании MixColumns (MC) используется матрица вида

$$\begin{vmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{vmatrix}.$$

2. АНАЛИЗ СУПЕР-S-БЛОКА «СИЛОВЫМ» СПОСОБОМ

Используя полный перебор возможных значений входной пары был определен двухцикловый дифференциал, обладающий максимальной вероятностью 3/128. Входная разность этого дифференциала 5550, выходная – 00D1. Принадлежит этому дифференциалу только одна

дифференциальная характеристика, которая представлена на рис. 1.

5	5	5	0	
B		S		8 8 8
A	A	A	0	
M		C		
0	0	7	D	
B		S		8 6
0	0	D	1	

Рис. 1

На рис. 1 справа напротив преобразований BS (ByteSubstitution) представлены значения из таблицы разности, на которые попадают указанные переходы разности для отдельных S-блоков, которые содержат на входе ненулевую разность.

Следует заметить, что использовать упомянутый выше полный перебор возможных значений входной пары возможно лишь для супер-S-блока размером до 32 битов. Для супер-S-блоков большего размера, которые, например, используются в шифре «Калина», в шифрующих преобразованиях функций хеширования Whirlpool, Groestl, значение максимальной вероятности можно получить только на основании анализа особенностей шифрующих преобразований. Продемонстрируем как это может быть сделано для рассматриваемого шифра. Для этого будем придерживаться основных этапов предложенного в [1] подхода:

1. Определение минимального количества активных S-блоков.
2. Определение вида ДХ, обладающей максимальной вероятностью.
3. Определение количества и вероятностей дополнительных ДХ.
4. Определение максимальной вероятности двухциклового дифференциала.

В соответствии с числом ветвей активизации (branch number) МДР-преобразования при ненулевой входной разности всегда будет минимум пять активных S-блоков. Возможны различные варианты для количества активных S-блоков на входе и выходе: 1 и 4, 2 и 3, 3 и 2, 4 и 1. Рассмотрим эти варианты.

3. КОЛИЧЕСТВО АКТИВНЫХ S-БЛОКОВ: 1 НА ВХОДЕ, 4 НА ВЫХОДЕ

В табл. 4 представлены 16 вариантов разности на входе в MC и соответствующие значения разности на выходе MC.

Выходные значения для преобразования MC являются входными для второго уровня S-блоков. Как видно из табл. 4, трое из четырех тетрад всегда содержат различную разность. Так как в таблице разности (табл. 2) присутствует только два перехода с вероятностью 8/16, то вероятность того, что для всех четырех активных S-блоков 2-го уровня может быть выполнен переход разности с максимальной вероятностью (8/16) равна 0:

$$P_{1\to 4}(4\_\text{перехода\_разности}\_\text{с\_вероятностью}\_\frac{8}{16}) = 0.$$

Таблица 4

Вход MC	Выход MC
1000	2113
2000	4226
3000	6335
4000	844c
5000	a55f
6000	c66a
7000	e779
8000	388b
9000	1998
A000	7AAD
B000	5BBE
C000	BCC7
D000	9DD4
E000	FEE1
F000	DFF2

Оценим вероятность того, что для всех пяти активных S-блоков может быть выполнен переход разности с вероятностью не менее, чем 6/16. Для этого, сначала, рассмотрим таблицу разности (табл. 3). Из 15 строк и столбцов с ненулевой входной и выходной разностью значения 6 и более присутствуют в 8 строках и 8 столбцах. Поэтому, если считать, что три различных значения разности на втором уровне S-блоков появляются случайно, то вероятность того, что для всех четырех активных S-блоков 2-го уровня может быть выполнен переход разности с вероятностью 6/16 и более равна:

$$P_{1\to 4}(4\_\text{перехода\_разности}\_\text{с\_вероятностью} \ge \frac{6}{16}) = \left(\frac{8}{15}\right)^3.$$

Учитывая наличие 8 вариантов разности для активного S-блока первого уровня, когда может быть выполнен переход разности с вероятностью 6/16 и более, ожидаемое количество случаев, когда все 5 переходов разности выполнятся с вероятностью 6/16 и более, составит:

$$OK_{1\to 4}(5\_\text{переходов\_разности}\_\text{с\_вероятностью} \ge \frac{6}{16}) = 8\cdot\left(\frac{8}{15}\right)^3 \approx 1.$$

Этот прогноз подтвердили вычислительные эксперименты. Найдена дифференциальная характеристика (ДХ), в которой все 5 переходов разности выполняются с вероятностью 6/16 (см. рис. 2).

Оценим вероятность существования дополнительных ДХ, принадлежащих такому дифференциалу. Дополнительные ДХ должны содержать одинаковые с основной ДХ входную и выходную разности, но другие промежуточные значения разностей.

4	0	0	0	
B		S		6
4	0	0	0	
M		C		
8	4	4	C	
B		S		6666
2	4	4	4	

Рис. 2

Учитывая, что доля ненулевых значений в таблице разности (см. табл. 3) 68/225 = 0,3, а в каждой строке таблицы разности со значением 6 и более в среднем присутствует 3 других ненулевых значения, то ожидаемое количество дополнительных ДХ составит:

$$\text{ОК}_{1\to 4}(\text{дополнительных\_ДХ}) = 3\cdot 0{,}3^3 = 0{,}081,$$

следовательно, очень маловероятно наличие дополнительных ДХ, что также подтвердили вычислительные эксперименты.

В значительно меньшем количестве дополнительных ДХ состоит главное отличие шифрующего преобразования с произвольными подстановками от преобразования с алгебраически построенными подстановками с предельными дифференциальными и линейными показателями.

4. КОЛИЧЕСТВО АКТИВНЫХ S-БЛОКОВ: 2 НА ВХОДЕ, 3 НА ВЫХОДЕ

В случае, когда на входе в МС 2 активных тетрады, то только при определенном соотношении разности в этих тетрадах на выходе МС может быть получена нулевая разность в одной из четырех тетрад. Например, для получения нулевой разности в третьей тетраде на выходе МС две первые тетрады на входе в МС должны содержать одинаковое значение разности (см. примеры на рис. 3).

7	7	0	0	
	B	S		88
D	D	0	0	
	M	C		
D	4	0	9	
	B	S		664
1	4	0	5	

5	5	0	0	
	B	S		88
A	A	0	0	
	M	C		
A	D	0	7	
	B	S		468
5	1	0	D	

Рис. 3

В любом случае, из 5 активных S-блоков в трех всегда будет различная разность, а следовательно, в соответствии с табл. 3, все пять переходов разности с вероятностью 8/16 произойти не могут.

Вернемся к рассматриваемому варианту прохождения разности, когда две первые тетрады на входе в МС содержат одинаковое значение разности и нулевая разность в третьей тетраде на выходе МС. Вероятность того, что 3 перехода разности на втором уровне S-блоков могут быть выполнены с вероятностью 6/16 и более:

$$P_{2\to 3}(3\text{\_перехода\_разности\_с\_вероятностью} \ge \frac{6}{16}) = \left(\frac{8}{15}\right)^3 = 0{,}15.$$

Учитывая наличие 8 вариантов разности для двух активных S-блоков первого уровня, содержащих одинаковую разность, когда может быть выполнен переход разности с вероятностью 6/16 и более, ожидаемое количество случаев, когда все 5 переходов разности выполнятся с вероятностью 6/16 и более, составит:

$$OK_{2\to 3}(5\text{\_переходов\_разности\_с\_вероятностью} \ge \frac{6}{16}) = 8\cdot\left(\frac{8}{15}\right)^3 \approx 1.$$

При этом последняя оценка справедлива для каждого отдельного варианта расположения тетрады с нулевой разностью на выходе преобразования МС. Так как есть 4 варианта такого расположения, то можно ожидать такое же количество различных ДХ при фиксированной позиции входных активных S-блоков.

На рис. 4, *а* представлена ДХ с вероятностью всех переходов 6/16 и более и третей нулевой тетрадой на выходе МС, а на рис. 4, *б* представлена ДХ с вероятностью всех переходов 6/16 и более и второй нулевой тетрадой на выходе МС.

4	4	0	0	
	B	S		66
4	4	0	0	
	M	C		
4	C	0	8	
	B	S		666
4	4	0	2	

а

3	7	0	0	
	B	S		68
9	D	0	0	
	M	C		
5	0	4	5	
	B	S		868
A	0	4	A	

б

Рис. 4

Для каждой такой ДХ ожидаемое количество дополнительных ДХ рассчитывается также как и в предыдущем разделе и составляет:

$$\text{ОК}_{2\to 3}(\text{дополнительных\_ДХ}) = 3\cdot 0{,}3^3 = 0{,}081.$$

5. КОЛИЧЕСТВО АКТИВНЫХ S-БЛОКОВ: 3 НА ВХОДЕ, 2 НА ВЫХОДЕ

В случае, когда на входе в МС 3 активных тетрады, то только при определенном соотношении разности в этих тетрадах на выходе МС может быть получена нулевая разность в двух из четырех тетрад. Например, для получения нулевой разности в первой и во второй тетрадах на выходе МС три первые тетрады на входе в МС должны содержать одинаковое значение разности (см. пример на рис. 5).

7	7	7	0	
B		S		888
D	D	D	0	
M		C		
0	0	9	4	
B		S		46
0	0	5	4	

Рис. 5

При этом для дальнейших оценок важно, что значения в активных тетрадах на выходе МС будут всегда разные. Оценим вероятность того, что из этих двух различных значений разности будут возможны преходы с вероятностью 8/16.

$$P_{3\to 2}(2\text{\_перехода\_разности\_с\_вероятностью\_}\frac{8}{16}) = \frac{2}{15}\cdot\frac{1}{15} \approx 0{,}009.$$

Тогда ожидаемое количество случаев, когда все 5 переходов разности произойдут с вероятностью 8/16:

$$OK_{3\to 2}(5\text{\_переходов\_разности\_с\_вероятностью\_}\frac{8}{16}) = 2\cdot\frac{2}{15}\cdot\frac{1}{15} \approx 0{,}018.$$

Вычислительные эксперименты подтвердили отсутствие таких случаев.

Вероятность того, что для двух активных тетрад на выходе МС будут существовать переходы с вероятностью 6/16 и больше, будет значительно выше:

$$P_{3\to 2}(2\_\text{перехода\_разности\_с\_вероятностью} \ge \frac{6}{16}) = \frac{8}{15}\cdot\frac{7}{15} \approx 0{,}25.$$

Ожидаемое количество случаев, когда все 5 переходов разности произойдут с вероятностью 6/16 и более составит

$$OK_{3\to 2}(5\_\text{переходов\_разности\_с\_вероятностью} \ge \frac{6}{16}) = 8\cdot\frac{8}{15}\cdot\frac{7}{15} \approx 2 \quad .$$

Эти случаи представлены на рис. 6.

5	5	5	0	
	B	S		888
a	A	A	0	
	M	C		
0	0	7	D	
	B	S		86
0	0	d	1	

4	4	4	0	
	B	S		666
4	4	4	0	
	M	C		
0	0	8	C	
	B	S		66
0	0	2	4	

Рис. 6

Ожидаемое количество дополнительных ДХ:

$$\text{ОК}_{3\to 2}(\text{дополнительных\_ДХ}) = 3\cdot 0{,}3^2 = 0{,}27.$$

Вариант с четырьмя активными S-блоками на входе и 1 на выходе идентичен варианту с переходом 1 в 4 и поэтому рассматривать отдельно не будем.

ВЫВОДЫ

1. Определена максимальная вероятность для двухцикловых дифференциалов для рассматриваемого 16-битного супер-S-блока, в котором используется произвольная подстановка. Эта вероятность $1536/2^{16}$, что значительно больше, чем та же вероятность для случая с алгебраически построенными подстановками – $72/2^{16}$. Этот результат вполне ожидаем, т. к. произвольная подстановка обладает в два раза более высокой максимальной вероятностью прохождения ненулевой разности.

2. Определен вид обладающего максимальной вероятностью дифференциала, который отличается от аналогичного дифференциала, найденного в [1].

3. Одно из главных отличий шифрующего преобразования с произвольными подстановками от преобразования с алгебраически построенными подстановками с предельными дифференциальными и линейными показателями состоит в том, что для всех рассмотренных дифференциалов было найдено значительно меньшее количество дополнительных ДХ (все рассмотренные дифференциалы состояли из одной ДХ).

4. Еще одной обнаруженной особенностью стало отсутствие среди рассмотренных дифференциалов таких, вероятность которых изменялась бы для разных ключей.

5. По прежнему актуальным остается вопрос получения точных значений вероятностей дифференциалов с большим размером блока и большим количеством циклов.

Литература

[1] Руженцев В.И. Оценка вероятностей двухцикловых дифференциалов шифра AES / В.И. Руженцев // Прикладная радиоэлектроника. – 2011. – № 2. – Т. 10. – С. 116–121.

[2] J.Daemen, V. Rijmen. Two-Round AES Differentials. IACR Eprint archive, 2006. available from http://eprint.iacr.org/2006/039.

[3] 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.

[4] Офіційний ресурс департамента спеціальних телекомунікаційних систем та захисту інформації: «Положення про проведення відкритого конкурсу криптографічних алгоритмів», 2006. Доступно по адресу http://www.dstszi.gov.ua/dstszi/control/ru/publish/article/.

Поступила в редколлегию 22.08.2014

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

УДК 004.056.55

Ймовірності двоциклових диференціалів Rijndael-подібних шифрів з довільними підстановками / В.І. Руженцев // Прикладна радіоелектроніка: наук.-техн. журнал. – 2014. – Том 13. – № 3. – С. 235–238.

Робота присвячена аналізу двоциклових диференціалів Rijndael-подібних шифрів. Запропонований в попередній роботі підхід щодо оцінки ймовірностей диференціалів застосовується для шифрів з неалгебраїчно побудованими підстановками. Демонструються відмінності в отриманих результатах. Слушність отриманих теоретичних висновків перевіряється обчислювальними експериментами.

Ключові слова: AES, диференціал, диференційна характеристика, різниця, таблиця різниці.

Табл.: 4. Іл.: 6. Бібліогр.: 4 найм.

UDC 004.056.55

The probabilities of two-round differentials for Rijndael-like ciphers with random substitutions / V.I. Ruzhentsev // Applied Radio Electronics: Sci. Journ. – 2014. – Vol. 13. – № 3. – P. 235–238.

The paper is devoted to analyzing two-round differentials of Rijndael-like ciphers. The approach to estimating differential probabilities, which was suggested in one of the previous works, is used for ciphers with nonalgebraically formed substitutions. The main differences in the results obtained are demonstrated. The theoretical results are then compared with results of computing experiments.

Keywords: AES, differential, differential characteristic, difference, difference table.

Tab.: 4. Fig.: 6. Ref.: 4 items.