УДК 621. 391:519.2:519.7

ОЦЕНКА ВЕРОЯТНОСТЕЙ ДВУХЦИКЛОВЫХ ДИФФЕРЕНЦИАЛОВ ШИФРА AES

В.И. РУЖЕНЦЕВ

Работа посвящена анализу двухцикловых дифференциалов шифра AES. Предлагаемый в работе подход к оценке вероятностей дифференциалов является, на наш взгляд, более простым и понятным по сравнению с известным методом, который представлен в работе [1]. Справедливость полученных в работе теоретических результатов проверяется вычислительными экспериментами.

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

ВВЕДЕНИЕ

На сегодня общепризнанной является точка зрения о необходимости рассмотрения дифференциалов и их вероятностей для анализа стойкости блочного симметричного шифра (БСШ) к дифференциальным атакам. Подтверждением этого факта могут служить работы [2-4], в которых изучаются вероятности дифференциалов для наиболее популярного современного шифра – алгоритма AES. При этом следует заметить, что большинство полученных оценок является достаточно грубым приближением, подробно изучены лишь 2-цикловые дифференциалы AES в работе [1].

Предлагаемая в работе [1] теория обладает, на наш взгляд, несколькими недостатками. Во-первых, статья перенасыщена новыми терминами, такими как планарный дифференциал (planar differential), плато-след (plateau trail), пучок (bundles). Во-вторых, непонятно как то, что дифференциалы AES обладают свойством планарности влияет на процесс оценки вероятностей 2-цикловых дифференциалов и как действовать, если дифференциалы другого шифра не обладают этим свойством.

Целью настоящей работы является изложение нашего подхода к оценке вероятностей двухцикловых дифференциалов. В основном, полученные результаты совпадают с результатами работы [1], однако путь их получения нам кажется более простым и понятным, в нашем варианте оценка вероятностей двухцикловых дифференциалов происходит на основе анализа свойств таблиц разностей S-блоков шифра.

1. СУПЕР-S-БЛОКИ AES

Как и в [1] 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 4 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 взяты подстановки из шифра baby-rijndael [5]. Таблица подстановки представлена в табл. 1.

Таблица 1

Подстановка 4 в 4 бита

0	1	2	3	4	5	6	7	8	9	a	b	c	D	e	F
a	4	3	b	8	e	2	c	5	7	6	f	0	1	9	D

Подобно подстановке оригинального шифра AES, она состоит из инверсии в поле $GF(2^4)$ с образующим полиномом 0x13 (табл. 2) и последующего линейного преобразования (табл. 3).

Таблица 2

Инверсия в поле $GF(2^4)$

0	1	2	3	4	5	6	7	8	9	A	b	c	d	e	F
0	1	9	e	d	b	7	6	f	2	C	5	a	4	3	8

Таблица 3

Линейная часть подстановки

0	1	2	3	4	5	6	7	8	9	A	B	c	D	e	F
a	4	7	9	1	f	c	2	d	3	0	e	6	8	b	5

При рассмотрении прохождения разности через S-блок можно отдельно выделить отображение разности, выполняемое линейной частью подстановки – табл. 4.

Таблица 4

Отображение разности линейной частью подстановки

0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	e	d	3	b	5	6	8	7	9	a	4	c	2	1	F

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. ДИФФЕРЕНЦИАЛЫ С 1 АКТИВНЫМ S-БЛОКОМ НА ВХОДЕ И 4 – НА ВЫХОДЕ

Рассмотрим супер-S-блок уменьшенного AES, на вход которого подается 2^{16} пар открытых текстов {P,P'}, где P пробегает все значения от

0 до 2^{16}-1, а P'=P xor $d_{вх}$, где в $d_{вх}$ первая тетрада принимает одно значение из набора {1, ..., 15}, а остальные три тетрады равны 0, например, пусть в шестнадцатеричном представлении $d_{вх}$ = 1000. В соответствии с таблицей разности (см. табл. 5), на выходе 1-го S-блока первого уровня может появиться всего 7 значений, при чем одно значение (для $d_{вх}$ = 1000 – это E000) 2^{14} раз, а остальные 6 значений (двойки в строке табл. 5, соответствующей входной разности 1) по 2^{13} раз. На выходе трех остальных S-блоков первого уровня всегда нулевые разности.

Таблица 5

Таблица разности S-блока уменьшенного AES

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

В силу линейности преобразования MC, значение разности на выходе MC полностью определяется значением разности на входе. Поэтому на входе S-блоков второго уровня появится 2^{14} раз одно значение разности (для $d_{вх}$ = 1000 – это FEE1), а еще 6 значений разности – по 2^{13} раз.

Рассмотрим случаи, когда на входе S-блоков второго уровня 2^{14} раз появляется одинаковое значение разности (для $d_{вх}$ = 1000 – это FEE1). В соответствии с таблицей разности (см. табл. 5) в каждой строке есть «4», а значит для любого значения разности на входе S-блока всегда есть наиболее часто встречающееся выходное значение. Следовательно, имеется одно значение выходной разности $d_{вых}$, которое будет встречаться чаще других (для разности на входе во второй уровень S-блоков FEE1 – это $d_{вых}$ = 733E). Ожидаемое количество таких случаев:

$$2^{14}\left(\frac{4}{16}\right)^4 = 2^6,$$

то есть, из 2^{16} входных пар с одинаковой разностью $2^6 = 64$ пары дадут одно и то же выходное значение $d_{вых}$ = 733E. Для этих пар все промежуточные значения разности также будут совпадать, другими словами, они пройдут по одному и тому же «дифференциальному следу» (differential trail) или принадлежат одной и той же дифференциальной характеристике.

Однако получение указанного значения выходной разности возможно и при следовании другими «дифференциальными следами». Для оценки количества таких пар следует рассмотреть оставшиеся 6 2^{13}-элементных структур.

Каждой структуре соответствует одно значение разности на выходе активного S-блока. В табл. 6 в первой колонке возможные при $d_{вх}$ = 1000 значения разности на входе преобразования MixColumns (MC) отмечены «+». Во второй колонке представлены соответствующие значения разности на выходе преобразования MC.

Таблица 6

Вход MC	Выход MC	Возможн. перех. в 733e
1000 +	2113	0000
2000 +	4226	2222+
3000	6335	0000
4000 +	844c	0000
5000	a55f	0000
6000 +	c66a	0000
7000	e779	2222
8000 +	388b	2222+
9000 +	1998	0000
A000	7Aad	2222
B000	5BbE	2222
C000	BCc7	2222
D000	9Dd4	0000
E000 +	fEe1	4444+
F000	dFf2	0000

Каждое из представленных во второй колонке табл. 6 значений состоит из четырех элементов, каждый из которых является произведением над GF(2^4) значения разности в активном S-блоке на входе в MC на 1, 2 или 3 (в соответствии с используемой в MC матрицей). Например, значение в первой строке 2113 – это произведение числа 1 на указанные множители: 2 = 1*2, 1 = 1*1, 1 = 1*1, 3 = 1*3. Значение во второй строке – это произведение числа 2 на те же множители и т.д. Поскольку переход в выходное значение разности для основного пути происходит из разности FEE1 через «4» в таблице разности для каждого из S-блоков, то значение разности 733E связано со значением FEE1. 733E состоит из инверсий в GF(2^4) для каждой тетрады входных значений разности с последующим применением линейной части подстановки, которая представлена в табл. 4. Обозначив преобразование разности представленное в табл. 4 как L, можно записать

$$7 = L(F^{-1}) = L(8) \text{ или}$$

$$7 = L((2*E)^{-1}) = L(2^{-1}*E^{-1}) = L(9*3) = L(8);$$

$$3 = L(E^{-1}) = L(3);$$

$$E = L(1^{-1}) = L(1) \text{ или}$$

$$E = L((3*E)^{-1}) = L(3^{-1}*E^{-1}) = L(E*3) = L(1).$$

Таким образом, когда мы обсуждаем возможность попадания различных вариантов разности на выходе MC (вторая колонка табл. 2) в выходное значение разности 733E, то должны анализировать вероятности переходов разности 2*X в $L((2*E)^{-1}) = 7$ для первого S-блока второго уровня, разности X в $L((E)^{-1}) = 3$ для второго и третьего S-блоков второго уровня и разности 3*X в $L((3*E)^{-1}) = E$ для четвертого S-блока второго уровня, где X – разность на выходе активного S-блока первого уровня. Но, в соответствии со следствием 3 (corollary 3) из [1], все эти три перехода имеют одинаковую вероятность и поэтому каждое из представленных во второй колонке табл. 2 значений может одновременно для всех четырех S-блоков второго уровня либо иметь потенциальную возможность перехода в выходную разность $d_{вых}$ = 733E (в таблице разности на соответствующих позициях «2») либо не иметь (в таблице разности на соответствующих позициях «0»).

В соответствии с тем, что каждая колонка таблицы разности (как и строка) кроме «0» содержит одну «4», шесть «2», то кроме варианта для основного пути (разность на выходе MC FEE1) есть еще 6 вариантов разности на выходе MC, которые имеют потенциальную возможность получить требуемую выходную разность. Эти варианты отмечены в третьей колонке табл. 6 значением «2222», где каждая из четырех цифр – значение из таблицы разности для перехода на соответствующем S-блоке в $d_{вых}$ = 733E. Но учитывая, что входное значение разности $d_{вх}$ = 1000 позволяет получить лишь 6 дополнительных вариантов разности после преобразования MC, то нужная выходная разность $d_{вых}$ = 733E может быть получена только двумя дополнительными путями (эти варианты вместе с вариантом основного пути отмечены «+» в третьей колонке табл. 6). Для других вариантов входной разности количество дополнительных путей может отличаться. Вероятность того, что окажется k дополнительных путей эквивалентна вероятности того, что в числе наугад выбранных 6 шаров из корзины с 14 шарами, 6 из которых - белые, а 8 - черные, окажется k белых шаров. Эта вероятность может быть вычислена так

$$P(k \text{ дополнительных путей}) = \frac{C_6^k \cdot C_{14-6}^{6-k}}{C_{14}^6} = \frac{C_6^k \cdot C_8^{6-k}}{C_{14}^6}.$$

Для данного вида дифференциала возможно 15 вариантов входной разности, поэтому для получения ожидаемого количества дифференциалов с k дополнительными путями необходимо вероятность умножить на 15. Результаты расчетов представлены в табл. 7.

В итоге, результаты показывают, что на практике должны встречаться варианты с числом дополнительных путей от 1 до 4, а максимальное количество дополнительных путей – 4. В этом случае, ожидается, что другими путями к той же выходной разности придет еще $4 \cdot 2^{13}\left(\frac{2}{16}\right)^4 = 8$ пар.

Таблица 7

k	P (k дополнительных путей)	Ожидаемое количество дифференциалов с k дополнительными путями
0	0,0093	0,14
1	0,112	1,67
2	0,35	5,24
3	0,373	5,59
4	0,14	2,1
5	0,016	0,24
6	0,0003	0,005

Тогда ожидаемое общее количество пар, которые при фиксированном $d_{вх}$ дадут наиболее вероятное $d_{вых}$, составит 64 + 8=72 пары, а вероятность соответствующего дифференциала $72/2^{16}$.

В подтверждение правильности наших рассуждений приводим результаты вычислительных экспериментов (см. табл. 8), из которых видно, что для дифференциала с 1 активным S-блоком на входе и 4 – на выходе максимальное количество пар 72.

Таблица 8

Входная разность, $d_{вх}$	Выходная разность, $d_{вых}$	Кол-во пар по основному пути	Кол-во пар по дополн. путям	Общее кол-во пар
1000	733E	64	4	68
2000	EDDF	64	8	72
3000	9EE1	64	4	68
4000	2778	64	6	70
5000	F22A	64	4	68
6000	1FF5	64	2	66
7000	A88C	64	8	72
8000	B779	64	8	72
9000	DBB2	64	6	70
A000	5AA6	64	8	72
B000	C447	64	4	68
C000	6CCB	64	8	72
D000	4553	64	4	68
E000	8114	64	8	72
F000	366D	64	2	66

Применим те же рассуждения для 32-битного супер-S-блока полномасштабного AES. На вход подадим 2^{32} пар открытых текстов {P,P'}, где P пробегает все значения от 0 до 2^{32}-1, а P'=P xor $d_{вх}$, где в $d_{вх}$ первый байт принимает одно значение из набора {1, ..., 255}, а остальные три байта равны 0, например, пусть в шестнадцатеричном представлении $d_{вх}$ = 01 00 00 00. В соответствии с таблицей разности S-блока AES, на выходе 1-го S-блока первого уровня может появиться всего 127 значений, при чем одно значение (для $d_{вх}$ = 01 00 00 00 – это F1000000) 2^{26} раз, а остальные 126 значений (двойки в строке таблицы разности, со-

ответствующей входной разности 1) по 2^{25} раз. На выходе трех остальных S-блоков первого уровня всегда нулевые разности.

Дальнейшие рассуждения для 32-битного супер-S-блока аналогичны уменьшенному варианту. В итоге, ожидаемое количество пар, которые пройдут по основному пути, составит

$$2^{26}\left(\frac{4}{256}\right)^4 = 2^2 = 4.$$

Вероятность наличия k дополнительных путей может быть определена по формуле

$$P(k \text{ дополнительных путей}) = \frac{C_{126}^{k} \cdot C_{254-126}^{126-k}}{C_{254}^{126}} = \frac{C_{126}^{k} \cdot C_{128}^{126-k}}{C_{254}^{126}}.$$

Умножая полученные значения на 255, получим ожидаемое количество дифференциалов с k дополнительными путями. Максимальное количество дополнительных путей, при котором ожидаемое количество дифференциалов выше 1 – 72. Это значит, что ожидаемое количество пар, которые будут принадлежать тому же дифференциалу, но пройдут по дополнительным путям, составит

$$72 \cdot 2^{25}\left(\frac{2}{256}\right)^4 = 9 \text{ пар.}$$

Ожидаемое максимальное количество пар, принадлежащих дифференциалу, 4 + 9 = 13, а вероятность дифференциала $13/2^{32}$.

3. ДИФФЕРЕНЦИАЛЫ С 2 И БОЛЕЕ АКТИВНЫМИ S-БЛОКАМИ НА ВХОДЕ И МИНИМАЛЬНЫМ ОБЩИМ КОЛИЧЕСТВОМ АКТИВНЫХ S-БЛОКОВ

Рассмотрим ситуацию, когда входная разность содержит два активных S-блока, а выходная разность – три. Два активных входных S-блока могут содержать одинаковые и отличающиеся значения разности. При этом и в одном и во втором случае, если на всех пяти S-блоках происходят переходы разности через «4» в таблице разности, то количество пар для основного пути будет одинаковым и составит $2^{16} \cdot \left(\frac{4}{16}\right)^5 = 64$ пары. Отличия будут в количестве дополнительных путей.

Рассмотрим эти два варианта на примере двух дифференциалов (B700-0D1D) и (BB00-470C), сравнение которых представлено в табл. 9. По основному пути каждый из дифференциалов проходит через «4» в таблице разности. Значения разности для основного пути выделены в табл. 9 жирным шрифтом.

Основное отличие между двумя дифференциалами заключается в количестве возможных вариантов разности на выходе 1 уровня S-блоков, которые после MC будут содержать 0 на нужной позиции (см. 3 строку табл. 9). Для дифференциала с одинаковыми значениями разности для двух активных S-блоков на входе всегда гарантировано будет 6 таких вариантов разности (см. 3 строку табл. 9), – эти варианты содержат одинаковые значения разности на выходах обоих активных S-блоков. Для дифференциала с различными значениями разности на входе активных S-блоков количество дополнительных вариантов разности на выходе 1 уровня S-блоков, которые после MC будут содержать 0 на нужной позиции, ограничено сверху значением 6, но на практике всегда будет меньше (например, в рассматриваемом примере их 2).

Таблица 9

Входная разность	Дифференциал B700-0D1D				Дифференциал BB00-470C			
	B	7	0	0	B	B	0	0
Вых. разности для каждого S-блока	2, 3, 4, 5, 7, C, E	3, 6, 7, 8, D, E, F	0	0	2, 3, 4, 5, 7, C, E	2, 3, 4, 5, 7, C, E	0	0
Возможные разности на вых. 1 уровня S-блоков, кот. после MC будут содержать 0 на нужной позиции	(5600), (2D00), (C800)				(5500), (2200), (3300), (4400), (7700), (CC00), (EE00)			
Разность после MC	(0939)+, (0BFB)-, (0F4F)+				(5F0A)+, (2604)-, (3506)+, (4C08)-, (790E)-, (C70B)+, (E10F)-			
Вых. разность	0D1D				470C			

Точно также как и для дифференциалов с одним активным S-блоком на входе, для обоих рассматриваемых дифференциалов все значения разности, полученные на выходе MC, могут одновременно для всех S-блоков второго уровня либо иметь, либо не иметь потенциальную возможность перехода в выходное значение разности. Количество вариантов, которые имеют потенциальную возможность перехода в выходную разность, для первого дифференциала зависит от числа возможных вариантов разности после первого уровня S-блоков (3 строка табл. 9), а для второго дифференциала определяется также как и для случая с 1 активным S-блоком на входе и составит от 1 до 4 для уменьшенной модели супер-S-блока и от 53 до 72 для 32-битного супер-S-блока.

В итоге, максимальное значение вероятности для дифференциалов с 2 и более активными S-блоками на входе составит $72/2^{16}$ для 16-битного супер-S-блока и $13/2^{32}$ для 32-битного супер-S-блока и может быть достигнуто в случае, когда разность в активных S-блоках на входе одинаковая, а общее количество активных S-блоков минимальное, то есть – 5.

Следует заметить, что указанные значения вероятностей дифференциалов являются максимальными при усреднении по всем ключам. Если

взять один ключ, то, например, для 16-битного супер-S-блока всегда присутствует максимальное значение $128/2^{16}$, а иногда и $132/2^{16}$, однако для таких дифференциалов, как показывают вычислительные эксперименты, будет гораздо меньшее значение на других ключах и при усреднении по всем ключам вероятность не будет превосходить указанного выше максимума.

4. ДИФФЕРЕНЦИАЛЫ С ОБЩИМ КОЛИЧЕСТВОМ АКТИВНЫХ S-БЛОКОВ 6 И БОЛЕЕ

Рассмотрим к чему будет приводить увеличение количества активных S-блоков. Проанализируем дифференциал с шестью активными S-блоками (2 на входе, 4 на выходе). Для примера возьмем дифференциал BA00-B3D1, который представлен в табл. 10.

Таблица 10

Входная разность	Дифференциал BA00-B3D1			
	B	A	0	0
Варианты вых. разностей для каждого S-блока	2,3,4,5, 7,C,E	1,2,3,6, B,C,D	0	0
Разность на входе в MC	5C00			
Разность после MC	DE93			
Выходная разность	B3D1			

Основной путь дифференциала содержит переходы через «4» в таблице разности. Значения разности для основного пути представлены в табл. 10 и выделены жирным шрифтом.

Сразу можно оценить количество пар, которые пройдут основным путем:

$$2^{16} \cdot \left(\frac{4}{16}\right)^6 = 2^4 = 16 \text{ пар.}$$

Теперь оценим количество дополнительных путей и ожидаемое количество пар, которые пройдут этими путями.

Всего, после 1-го уровня S-блоков, возможно 48 дополнительных к основному вариантов разности. Из них 12 разностей повторятся по 2^{11} раз (в одном из активных S-блоков переход разности с вероятностью 4/16, во втором – с вероятностью 2/16), а 36 разностей повторятся по 2^{10} раз (в обоих активных S-блоках переходы разности с вероятностью 2/16). Для каждого варианта разности на выходе 1-го S-блока существует 4 значения разности на выходе 2-го S-блока, при которых после преобразования MC будет получена нулевая разность в одной из тетрад и в этом случае нужное значение выходной разности $d_{\text{вых}}$ никак не сможет быть достигнуто. Поскольку среди возможных вариантов выхода каждого из активных S-блоков всегда присутствует примерно половина всех возможных значений (7 из 15), то в среднем можно ожидать, что в числе вариантов разностей 2-го S-блока всегда будет присутствовать 2 из 4 значений разности, приводящих к нулевой разности в одной из тетрад после MC. Учитывая возможность получения неподходящих разностей после MC, из 48 дополнительных вариантов разности нам подойдут 8 из 12 вариантов разности первого типа и 24 из 36 вариантов разности второго типа.

Для каждого из оставшихся вариантов разности вероятность того, что существует потенциальная возможность получения нужной выходной разности (в таблице разности на нужных позициях не «0») составит $\left(\frac{7}{15}\right)^4 \approx 2^{-4}$.

При наличии потенциальной возможности получения нужной выходной разности переходы разности для всех 4 S-блоков обычно будут иметь вероятность 2/16. Поэтому, в результате приблизительных оценок, ожидаемое число пар для дополнительных путей составит

$$8 \cdot 2^{11} \cdot 2^{-4} \cdot \left(\frac{2}{16}\right)^4 + 24 \cdot 2^{10} \cdot 2^{-4} \cdot \left(\frac{2}{16}\right)^4 =$$

$$= 2^{-2} + 3 \cdot 2^{-3} = 0{,}625.$$

Таким образом, итоговая вероятность дифференциала $(16+0{,}625)/2^{16}$.

В результате вычислительных экспериментов при усреднении по всем ключам ожидаемое значение вероятности для дифференциала составило $16{,}75/2^{16}$. Незначительное отклонение от теоретической оценки объясняется округлениями и допущениями, которые присутствовали в представленных рассуждениях, а также возможностью попадания на переходы разности с вероятностями 4/16 для S-блоков второго уровня.

Общий вывод для дифференциалов данного вида заключается в том, что увеличение количества активных S-блоков приводит к снижению как количества пар, которые проходят по основному пути, так и к снижению количества пар, проходящих по дополнительным путям, а в результате и к снижению вероятности дифференциала.

Аналогичная ситуация для 32-битного супер-S-блока. Применяя такие же рассуждения, получим ожидаемое число пар для основного пути $2^{32} \cdot \left(\frac{4}{256}\right)^6 = 2^{-4}$; для дополнительных путей

$$2 \cdot 124 \cdot 2^{19} \cdot 2^{-4} \cdot \left(\frac{2}{256}\right)^4 +$$

$$+126 \cdot 124 \cdot 2^{18} \cdot 2^{-4} \cdot \left(\frac{2}{256}\right)^4 \approx 2^{-5} + 1.$$

Общее ожидаемое количество пар – 1, и это значительно меньше, чем для дифференциалов с 5 активными S-блоками.

ВЫВОДЫ

Среди двухцикловых дифференциалов AES максимальной вероятностью обладают те, которые содержат минимальное количество активных S-блоков (то есть 5) и у которых основной след

(путь) содержит переходы разности через «4» в таблице разностей. Максимальная вероятность дифференциала для 16-битного супер-S-блока $72/2^{16}$, для 32-битного супер-S-блока $13/2^{32}$.

Основной результат работы – предложенный подход к оценке вероятностей двухцикловых дифференциалов шифра AES, который в отличие от известного является более простым, понятным и, как нам кажется, может быть применен для большего класса шифров.

Дальнейших, более тщательных исследований требуют дифференциалы, вероятности которых меняются в зависимости от ключа.

Актуальным остается вопрос оценки вероятностей дифференциалов с большим количеством циклов.

Литература

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

[2] *Hong, S., Lee, S., Lim, J., Sung, J., and Cheon, D.* 'Provable security against differential and linear cryptanalysis for the SPN structure'.Proc. Fast Software Encryption (FSE 2000), LNCS, 1978, 2001, edited by Schneier, B., (Springer), pp. 273–283.

[3] *Keliher, L., Meijer, H., and Tavares, S.*: 'Improving the upper bound on the maximum average linear hull probability for Rijndael'. Proc. Workshop on Selected Areas in Cryptography (SAC 2001), LNCS, 2259, 2001, edited by Vaudenay, S., and Youssef, A., (Springer), pp. 112–128.

[4] *F.Sano, K. Ohkuma, H. Shimizu, S.Kawamura*. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis. IEICE Trans. Fundamentals, vol. E86-A, No. 1 January 2003. pp. 37-46.

[5] E. Kleiman. The XL and XSL attacks on Baby Rijndael. Thesis, 2005, available from http://orion.math.iastate.edu/dept/thesisarchive/MS/EKleimanMSSS05.pdf.

Поступила в редколлегию 5.04.2011

Руженцев Виктор Игоревич, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, криптоанализ блочных симметричных шифров.

УДК 621. 391:519.2:519.7

Оцінка ймовірностей двохциклових диференціалів шифру AES. / В.І. Руженцев // Прикладна радіоелектроніка: наук.-техн. журнал. – 2011. Том 10. № 2. – С. 116–121.

Робота присвячена аналізу двохциклових диференціалів шифру AES. Запропонований в роботі підхід до оцінки ймовірностей диференціалів є, на наш погляд, більш простим та зрозумілим у порівнянні з відомим методом.

Ключові слова: AES, диференціал, диференційна характеристика, різність, таблиця різності.

Табл. 10. Бібліогр.: 5 найм.

UDC 621. 391:519.2:519.7

Two-round AES differentials probability estimation / V.I. Ruzhentsev // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 116–121.

This paper is devoted to the analysis of AES two-cycle differentials. The proposed method of probability estimation is more simple and understandable then the known method which is presented in [1]. The theoretical results are then compared with the results of computing experiments.

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

Tab. 10. Ref.: 5 items.