УДК 621. 391:519.2:519.7

Лисицкая И. В.

Канд. техн. наук, доцент Харьковского национального университета радиоэлектроники

СРАВНЕНИЕ ПО ЭФФЕКТИВНОСТИ СУПЕРБЛОКОВ НЕКОТОРЫХ СОВРЕМЕННЫХ ШИФРОВ

Излагается новая методика оценки показателей доказуемой безопасности блочных симметричных шифров. С применением этой методики выполняется анализ дифференциальных свойств суперблоков трех шифров: AES-а, уменьшенной версии шифра Мухомор и шифра MISTY1. Излагается оригинальная методика оценки максимального значения дифференциала уменьшенной модели двухциклового AES суперблока, и уточняется действительное значение этого максимума. Демонстрируется, что стойкость больших шифров и, в частности шифра Rijndael (AES-а) не зависит от дифференциальных показателей *S*-блоков, используемых в шифрах. Представляется как одно из перспективных решений по построению суперблоков преобразование FI шифра MISTY1, которое примечательно тем, что реализует (за один цикл) дифференциальные свойства случайной подстановки соответствующей степени.

Ключевые слова: доказуемая безопасность, дифференциал, суперблок, случайная подстановка.

ВВЕДЕНИЕ

В этой работе под суперблоком мы будем понимать функционально законченный узел шифра, включающий в себя композицию нескольких преобразований цикловой функции. В частности, в работах [1, 2] AES суперблоком названо отображение 4-х байтового массива $a = [a_0, a_1, a_2, a_3]$ в 4-х байтовый массив $e = [e_0, e_1, e_2, e_3]$, принимающее 4-байтовый ключ k $[k_0, k_1, k_2, k_3]$. Оно состоит из последовательности четырех преобразований:

SubBytes $b_i = S[a_i]$, с S являющимся AES S-блоком;

MixColumns $c = \mathrm{M}_c b$, с M_c являющейся 4 Ч 4 матрицей;

AddRoundKey $d = c \oplus k$, с k являющимся цикловым ключом;

SubBytes $e_i = S[d_i]$.

Авторами отмечается, что дифференциальные вероятности над этой структурой эквивалентны двум AES циклам и доказывается с использованием достаточно громоздких и сложных для понимания теоретических построений с привязкой к дифференциальным характеристикам S-блока AES, что точным значением максимальной ожидаемой дифференциальной вероятности ($MEDP$[1]) для AES супер блока является значение $12{,}34\times2^{-32}$ (есть и варианты значения $MEDP_{32} \approx 13{,}25\times2^{-32}$ [3]).

В итоге формируется граница для дифференциалов над AES, уменьшеному до четырех циклов, следующая из применения границы Хонга и др. [3]:

$$MEDP_{32} \le \left(\max_{x\neq 0, y} DP(x, y) \right)^4$$

к мега блоку, что приводит к результату:

$$MEDP_{128} \le (MEDP_{32})^4 \approx 1{,}881\times 2^{-114}.$$

Имеются работы, где подобным же образом (с привязкой к свойствам S-блоков) выполняется оценка линейных показателей SPN шифров [4]. Этот подход к определению доказуемой стойкости блочных симметричных шифров (БСШ) уже давно вызывает у нас сомнение, так как полученные результаты привязываются к дифференциальным и линейным свойствам S-блоков, используемых в шифрах, что, как показывают наши эксперименты, методически оказывается не верным. Не вызывает удовлетворения и сама методика определения показателей доказуемой стойкости БСШ в виде максимумов средних значений дифференциальных и линейных вероятностей ($MADP$ и соответственно $MALP$).

Мы далее обоснуем свою позицию к определению показателей доказуемой стойкости БСШ, и, в частности, дифференциальных показателей AES суперблока, приведем сравнение для него значений $MADP$ и оценок, полученных с использованием предлагаемого подхода, и заодно обсудим дифференциальные свойства суперблоков еще двух конструкций, где под суперблоками, как уже отмечено выше, будут пониматься функционально обособленные элементы цикловых преобразований других шифров.

1. ПОНЯТИЙНЫЙ АППАРАТ ДИФФЕРЕНЦИАЛЬНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА

Напомним сначала, следуя работе [4], понятийный аппарат линейного и дифференциального криптоанализа.

[1] *В ряде работ наряду с аббревиатурой MEDP (максимум ожидаемой дифференциальной вероятности) используется обозначение MADP (максимум среднего значения дифференциальной вероятности)*

Определение 1. (Дифференциальная и Линейная вероятность): *Дифференциальная вероятность DP^f и линейная вероятность LP^f соответственно для ключезависимой функции f с n-битным входом x и n-битным выходом y* ($x, y \in GF(2^n)$) *есть*:

$$DP^f(\Delta x \to \Delta y) = \frac{\#\{x \in GF(2)^n \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y}{2^n};$$

$$LP^f(\Gamma x \to \Gamma y) = \left(\frac{\#\{x \in GF(2)^n \mid x \cdot \Gamma x) = f(x) \cdot \Gamma y}{2^{n-1}} - 1 \right)^2,$$

где Δx и Δy является входной и выходной разностями, а Γx и Γy является входной и выходной масками; $x \cdot \Gamma x$ обозначает результат скалярного произведения x и Γx.

Определение 2. ($DP^f_{\max}$ и $LP^f_{\max}$): *Максимальным значением дифференциальной и линейной вероятности для ключезависимой функции f называется соответственно*:

$$DP^f_{\max} = \max_{\Delta x \neq 0, \Delta y} DP^f(\Delta x \to \Delta y),$$

$$LP^f_{\max} = \max_{\Gamma x,\ \Gamma x \neq 0,} LP^{f[k]}(\Gamma x \to \Gamma y).$$

Напомним теперь выражения для средних вероятностей *ADP*, *ALHP*, *MADP* и *MALHP* ключезависимой функции $f = f[k](x)$ с *n*-битным входом *x* и *n*-битным выходом $y \in \mathrm{GF}(2^n)$, которая параметризована ключом *k*, используемые во многих публикациях по обоснованию показателей стойкости блочных шифров.

Определение 3. Средним значением дифференциальной вероятности (*ADP*) функции $f[k](x)$ является:

$$ADP^f = \underset{k}{ave}\, DP^{f[k]}(\Delta x \to \Delta y).$$

Определение 4. Средним значением вероятности линейной оболочки (*ALHP*) функции $f = f[k](x)$ является:

$$ALHP^f = \underset{k}{ave}\, LP^{f[k]}(\Gamma x \to \Gamma y).$$

Определение 5. Максимумом среднего значения дифференциальной вероятности (*MADP*) и максимумом среднего значения вероятности линейной оболочки (*MALHP*) функции $f[k](x)$ есть:

$$MADP^f = \max_{\Delta x \neq 0, \Delta y} ADP^f(\Delta x \to \Delta y),$$

$$MALHP^f = \max_{\Gamma x,\ \Gamma y \neq 0} ALHP^f(\Gamma x \to \Gamma y).$$

Из приведенных определений видно, что приведенные показатели определяются максимумом среднего значения дифференциальной вероятности для некоторого фиксированного перехода входной разности Δx в выходную разность Δy, и максимумом среднего значения смещения для маски входа Γx и маски выхода Γy. Эти показатели представляют собой далеко не максимально возможные значения дифференциальных и линейных вероятностей, которые по идее и должны рассматриваться как показатели доказуемой безопасности.

Новая точка зрения к формированию оценок стойкости БСШ к атакам дифференциального и линейного криптоанализа, которая формализуется как два новых метода, состоит в следующем.

Предлагается для оценки стойкости БСШ к атакам дифференциального и линейного криптоанализа пользоваться не *MADP* и *MALHP*, а средними (по множеству ключей) значениями максимумов дифференциальных и линейных вероятностей ключезависимой функции $f[k](x)$, а именно *AMDP* и *AMLHP*.

Определение 6. (*AMDP*). *Среднее* (*по множеству из* 2^h *ключей*) *значение максимальных дифференциальных вероятностей ключезависимой функции* $f[k](x)$ *есть*:

$$AMDP^f = \underset{k}{ave}\, DP^{f[k]}_{\max} = \frac{1}{2^h} \sum_{k=1}^{2^h} DP^{f[k]}_{\max}.$$

Определение 7. (*AMPLH*). *Среднее* (*по ключам*) *значение максимальных вероятностей линейных оболочек функции* $f[k](x)$ *есть*:

$$AMLHP^f = \underset{k}{ave}\, LP^f_{\max}(\Gamma x \to \Gamma y) = \frac{1}{2^h} \sum_{k=1}^{2^h} LP^{f[k]}_{\max}.$$

В обоих случаях 2^h – мощность множества ключей зашифрования, использованных при вычислениях.

Здесь можно отметить сразу, что очевидны неравенства: $MADP^f < AMDP^f$, $MALHP < AMLHP$.

Помимо большей адекватности формируемых оценок (значение оценок для шифров совпадают с соответствующими дифференциальными и линейными показателями случайных подстановок и характеризуют максимально достижимые значения дифференциальных и линейных вероятностей), в последнем случае обеспечиваются и значительные вычислительные преимущества (нет необходимости запоминать полностью все таблицы, а достаточно только определять и помнить их максимальные значения).

2. ОБ УЧАСТИИ S-БЛОКОВ В ФОРМИРОВАНИИ МАКСИМАЛЬНЫХ ЗНАЧЕНИЙ ДИФФЕРЕНЦИАЛЬНЫХ И ЛИНЕЙНЫХ ВЕРОЯТНОСТЕЙ ШИФРОВ

Наши исследования с уменьшенными версиями многих шифров показали, что значения максимумов полных дифференциалов и линейных корпусов, которыми оцениваются показатели стойкости шифров к атакам дифференциального и линейного криптоанализа, зави-

сят не от показателей *S*-блоков, используемых в шифрах, а от дифференциальных и линейных показателей случайных подстановок соответствующей степени, к которым асимптотически приходят шифры после определенного начального числа циклов шифрования.

Для иллюстрации этого положения ниже предлагаются результаты исследований дифференциальных свойств 16-битной модели шифра Rijndael [5]. Для таких размеров входных блоков данных вычислительных ресурсов вполне достаточно, чтобы построить целиком таблицу XOR переходов (полных дифференциалов) сразу для всего шифра.

В табл. 1 представлены зависимости средних значений максимумов полных дифференциалов ($AMDP\times 2^{16}$) шифров, использующих *S*-блоки с различными значениями $DP^{s}_{\max} = p$ (δ-равномерности), от числа циклов *r* алгоритма Baby-Rijndael с операцией MixColumns на весь текст (как раз преобразование, являющееся основой структуры названной выше AES суперблоком).

Результаты, представленные в табл. 1, ярко иллюстрируют, что показатели стойкости шифров не зависят от применяемых в них *S*-блоков. Они определяются, как показано и в ряде других наших работ [6–8 и др.], значениями максимумов таблиц XOR разностей и смещений таблиц линейных аппроксимаций случайных подстановок соответствующей степени. У нас, правда, сразу нашлось много оппонентов, которые нас стали убеждать, что то, что свойственно малым шифрам, может не выполняться для их больших прототипов. Однако, последние наши исследования с большими шифрами [9–10] свидетельствуют о том, что и большие шифры также ведут себя как случайные подстановки, т.е. наша позиция является правильной.

В результате свойства AES суперблока не являются решающими для определения показателей доказуемой безопасности шифра Rijndael. Мы, тем не менее, далее рассмотрим дифференциальные свойства этого и других, близких к нему преобразований, с целью совершенствования и развития самой методики определения введенных выше новых показателей к оценке стойкости шифрующих преобразований (шифров) и сравнения их со старыми подходами.

2. ОЦЕНКА ЗНАЧЕНИЙ ДВУХЦИКЛОВОГО ДИФФЕРЕНЦИАЛА AES СУПЕРБЛОКА

Ниже предлагаются результаты вычислительных экспериментов по определению *AMDP* и *MADP* AES суперблока.

Конечно же, построить всю таблицу дифференциальных разностей для AES суперблока, также как и подстановки степени 2^{32}, не удается (не хватает вычислительных возможностей), но вполне достаточно имеющихся вычислительных ресурсов для построения закона распределения переходов отдельной строки таблицы XOR разностей.

Результаты решения этой задачи и представляются в табл. 2.

В правой колонке таблицы мы для сравнения представили закон распределения переходов в строке случайной подстановки степени 2^{32} (строка AES суперблока не «дотягивает» до строки случайной подстановки степени 2^{32}). Отметим здесь, что результаты для отдельных ключей практически не зависят от ключевого материала, т.е. в качестве оценки может выступать дифференциал, рассчитанный для отдельного ключа (это еще одно из достоинств развиваемого подхода).

Как следует из представленных данных значение максимума строки дифференциальной таблицы AES суперблока для выбранного входа равно 32. Это значит, что для всей дифференциальной таблицы ожидаемое значение максимума будет не менее 64-х, что существенно больше значения 12, 34, пропагандируемого в отмеченных ранее зарубежных публикациях (в последующих экспериментах нам удалось найти переход со значением 40).

Полученные результаты позволяют сделать вывод, что ожидаемое максимальное значение двухциклового

Таблица 2. Распределение переходов одной строки таблицы XOR-разностей AES суперблока ($AMDP\times 2^{16}$) для входа (в строку) 010101, безключевой вариант

Значение перехода	Число переходов в строке AES супер блока	Число переходов в строке подстановке степени 2^{32}
0	2605143438	2605070418
2	1302455376	1302484861
4	325637706	325626184
6	54254936	54271858
8	6794838	6784085
10	679254	678418
12	61352	56535
14	4021	4038
16	1543	252
18	13	14
20	291	1
24	52	
28	8	
32	4	

Таблица 1. Значения полного дифференциала ($AMDP\times 2^{16}$) для различных *S*-блоков и количества циклов алгоритма Rijndael с операцией MixColumns на весь текст

Sbox / *r*	Sbox, Сл *p*4F2	Sbox. *p*4 Лабир.	Sbox AES *p*4	Sbox *p*6F0	Sbox *p*6 F2	Sbox DES *p*8	Sbox *p*8 F0	Sbox *p*12 F0
1	16384,00	16384,00	16384,00	24576,00	24576,00	32768,00	32768,00	49152,00
2	83,87	132,00	132,00	490,87	230,40	1152,00	1536,00	5184,00
3	20,73	**19,47**	**18,80**	25,53	35,27	70,87	139,13	146,13
4	**19,60**	18,73	19,00	**19,20**	**18,93**	**19,27**	**23,93**	**19,07**
5	19,13	19,47	19,47	18,93	19,40	19,00	23,87	19,00

дифференциала большого AES супер блока ($AMDP\times 2^{32}$) должно быть больше максимального значения дифференциальной таблицы случайной подстановки степени 2^{32} равного 34.

В другом эксперименте мы для входа 010101 нашли максимальное значение строки дифференциальной таблицы AES суперблока. Оно оказалось равным 32. А затем для найденного максимального перехода $\Delta x = 10101 \rightarrow \Delta y = 661\text{E}0000$ были вычислены значения переходов при других значениях ключа. В табл. 3 представлены числа переходов, полученные для 30-ти случайно выбранных ключей зашифрования.

В соответствии с этими данными получено значение *MADP* для строки AES супер блока:

$$MADP(010101, 661\text{E}0000)\times 2^{16} = 7{,}86.$$

Для всей дифференциальной таблицы AES суперблока следует ожидать значение максимума в районе 15,72, что несколько больше значения 12,34, используемого в работах по оценке доказуемой безопасности шифра Rijndael (AES). Другое среднее значение $MADP\times 2^{16}$ максимального перехода для входа 010101 в AES получилось равным 8,76. Но дело не в этих небольших разницах в оценках значений *MADP* для AES суперблока. Получается, что приведенные в публикациях результаты являются, говоря мягко, не совсем точными. Самое главное это то, что эти значения не связаны с действительными значениями доказуемой стойкости шифров, как это считается в затронутых публикациях.

В табл. 4 мы приводим результаты исследования 16-битной версии SL преобразования шифра Мухомор [11] (практически изучаются показатели уменьшенной модели самого AES суперблока). В таблице представлены результаты экспериментов по построению законов распределения переходов дифференциальной таблицы SL преобразования.

Видно, что второй цикл является достаточно сложным для рассматриваемого преобразования. Приведем свои соображения по подсчету максимума дифференциальной таблицы для AES суперблока (для двух циклов шифрования AES).

Таблица 3. Числа переходов ($AMDP\times 2^{16}$) входа 010101 в один и тот же выход 661E0000 для 30-ти случайно выбранных ключей зашифрования

Ключ зашифрования	Значение перехода	Ключ зашифрования	Значение перехода
	32	7E0ACA68	8
10C9AA38	4	42DC38BF	0
EF34B4F6	16	F21B574C	8
522F3364	8	6F00601B	16
73B2CD8B	16	59ED7EE9	4
3BB11EC5	0	9F86B693	4
6C1A60C7	0	72569299	4
21F6E7E9	12	358F25B0	4
2FB26869	8	4848E2BE	4
3888589D	4	A0A2430D	16
27A47122	4	437C58F9	8
178448CA	16	3C30A2B6	4
C0D90AAE	4	ECA05DB8	12
7CCD5C0D	4	AEA79D44	8
B202E14F	0	DFE9D423	12
A5C7A90C	4		

При прохождении разностей пар входных блоков через первый цикл (*S*-блоки и преобразование MixColumn) наибольшая вероятность перехода $\Delta X \rightarrow \Delta Y$ обеспечивается при одном активном *S*-блоке. На его входе при прохождении по всем 2^{16} возможным значениям входных разностей каждая фиксированная разность повторяется $2^{16} / 2^4 = 2^{12}$ раз. Линейное преобразование тиражирует каждую разность на все четыре входа *S*-блоков следующего цикла. Если *S*-блок имеет значение δ-равномерности $\delta = 4$ (для *S*-блока AES), то на выходе первого цикла будет зафиксирован переход с максимальным значением $\delta \cdot 2^{12}$ (для AES это будет 2^{14}), причем если *S*-блок имеет 15 максимальных переходов $\delta = 4$, то на выходе первого цикла будет 60 значений $2^{14} = 16384$ (см. табл. 2).

На следующем цикле в прохождении разностей будут участвовать уже все четыре *S*-блока (второго цикла). Одна и та же разность на входе линейного преобразования сформирует повторяющиеся 16384 раза значения разностей (различных) на входах *S*-блоков второго цикла. А это значит, что, проходя *S*-блоки второго цикла, разные пары входов (после сложения с ключевыми битами) для разных *S*-блоков дадут разные значения выходных разностей со своими показателями прохождения (для AES *S*-блока это будут в подавляющем большинстве двойки). Заметим теперь, что ненулевые входные разности будут давать только ненулевые выходные разности. По статистике *S*-блоки имеют около 40 процентов ненулевых переходов (AES полубайтовый *S*-блок имеет 120 нулей в дифференциальной таблице без учета нулевой строки и нулевого столбца), т.е. из всего множества $2^4 - 1 = 15$ возможных ненулевых значений выходов для полубайтового *S*-блока в строке таблицы может быть реализовано только $15 \cdot 0{,}47 = 7$ различных ненулевых выходов.

Итак, нам нужно подсчитать число ситуаций, когда на выходах четырех *S*-блоков второго цикла будет одинаковое число совпадающих выходных разностей. Пусть мы зафиксировали одну (любую) из выходных (ненулевых) разностей первого *S*-блока. К этой разности мы можем выбрать одну из 6 возможных ненулевых разностей с выхода второго *S*-блока, так что вероятность получить набор из двух фиксированных значений разностей будет равна $\frac{1}{7}$. К этим двум разностям можно добавить еще одну из разностей с выхода третьего *S*-блока. Вероятность такой тройки (композиции) будет $\left(\frac{1}{7}\right)^2$. Наконец, к выбранной тройке можно добавить разность с выхода четвертого *S*-блока, и вероятность выбора этой четверки будет, по аналогии с предыдущим, равна $\left(\frac{1}{7}\right)^3$.

Таблица 4. Распределение числа переходов дифференциальной таблицы SL преобразования шифра Мухомор в зависимости от числа циклов шифрования

Количество переходов для ячейки	Число ячеек S_2(Baby$R$), 1 цикл	Количество переходов для ячейки	Число ячеек S_2(Baby$R$), 2 цикла	Количество переходов для ячейки	Число ячеек S_2(Baby$R$), 3 цикла
0	4168654065	**0**	2632290711	**0**	2605108264
16	65610000	**2**	1263628451	**2**	1302316781
32	43740000	**4**	329970420	**4**	325638830
64	10935000	**6**	56464541	**6**	54301413
128	4131000	**8**	10545896	**8**	6796804
256	1508625	**10**	1165323	**10**	678225
512	243000	**12**	324071	**12**	56663
1024	62100	**14**	20706	**14**	4390
2048	16200	**16**	379822	**16**	364
4096	1350	**18**	28307	**18**	21
8192	360	**20**	39641	**20**	5
16384	60	**22**	1296		
		24	7016		
		26	215		
		28	449		
		32	25940		
		34	3133		
		36	4032		
		38	176		
		40	442		
		44	36		
		48	4		
		64	790		
		66	144		
		68	166		
		72	20		
		128	8		
		132	4		
Время, с	192	**Время, с**	350	**Время, с**	509

Итак, с помощью четырех S-блоков мы можем получить фиксированный набор из четырех разностей (одинаковых или разных) с вероятностью $p=\left(\frac{1}{7}\right)^3$ и любой другой отличающийся от выбранной четверки набор из четырех разностей с вероятностью $p-1=1-\left(\frac{1}{7}\right)^3$. В результате можно считать, что мы имеем дело с двумя событиями, подчиняющимися биномиальному закону: одно событие – появление четверки разностей совпадающей с выбранной (вероятность такого события), другое – появление четверки разностей не совпадающей с выбранной (вероятность этого события). Для выборки $2^{14} = 16384$ таких независимых исходов среднее число совпадающих четверок выходных разностей в таком случайном эксперименте будет равно математическому ожиданию биномиального распределения, т. е.

$$2^{14} \cdot \left(\frac{1}{7}\right)^3 = 47{,}7.$$

Но этот результат является, конечно, оценкой снизу. Реальные значения (с учетом особенностей S-блоков, значений максимумов переходов, их распределения по таблице и других показателей) будут в общем случае существенно более высокими (в нашем примере имеется минимальное значение 83,87 и максимальное 5184).

3. СУПЕР БЛОК MISTY1

Мы выделили еще одну криптографическую функцию, заслуживающую внимания. Это FI подстановка в шифре MISTY1, являющегося еще одним из финалистов конкурса NESSIE.

Алгоритм MISTY1 разработан в 1995–1996 гг. командой специалистов под руководством известного криптолога Мицуру Мацуи (Mitsuru Matsui) из компании Mitsubishi Electric (Япония) [12]. Он имеет весьма необычную структуру – основан на «вложенных» сетях Фейстеля. Сначала 64-битный шифруемый блок данных разбивается на два 32-битных субблока, после чего выполняется r-циклов преобразований, имеющих ярко выраженную трехуровневую вложенную структуру. Рекомендуемым количеством раундов алгоритма является 8, но количество раундов алгоритма может быть любым, превышающим 8 и кратным четырем.

Мы не будем здесь приводить описание этой оригинальной конструкции, а интересующихся отправим к

оригинальной разработке [12]. Нас будет интересовать «кирпичики» – преобразования FI этой достаточно сложной конструкции, из которых строится цикловая функция. Ее структуру иллюстрирует рис. 1.

FI также (как и основная конструкция шифра) представляет собой сеть Фейстеля, но в шифре MISTY1 это преобразование осуществляет уже третий уровень вложенности. В отличие от сетей Фейстеля на двух верхних уровнях, данная сеть является несбалансированной: обрабатываемый 16-битный фрагмент делится на две части: 9-битную левую и 7-битную правую. Затем выполняются 3 раунда преобразований, которые состоят из следующих действий:

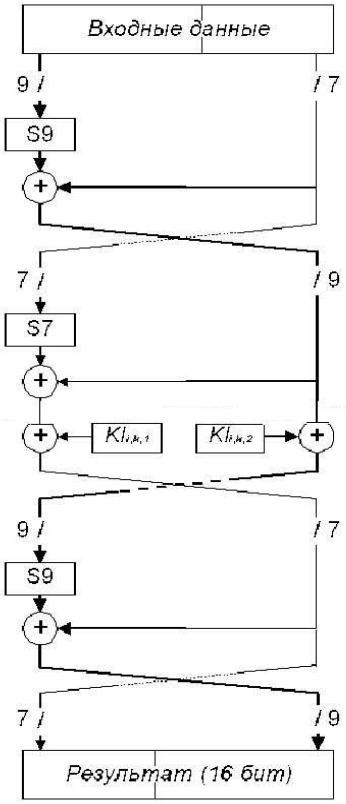

Рис. 1. Структура функции FI

1. Левая часть «прогоняется» через таблицу замен. 9-битная часть (в раундах 1 и 3) обрабатывается таблицей подстановки S_9, а 7-битная (в раунде 2) – таблицей подстановки S_7. Сами таблицы приведены в описании шифра [12].

2. На левую часть операцией XOR накладывается текущее значение правой части. При этом, если справа 7-битная часть, она дополняется нулями слева, а у 9-битной части удаляются слева два бита.

3. Во втором раунде на левую часть операцией XOR накладывается фрагмент ключа раунда $KI_{i,k,1}$, а на правую – фрагмент $KI_{i,k,2}$. В остальных раундах эти действия не выполняются.

4. Левая и правая части меняются местами.

Будем рассматривать функцию FI как суперблок. Сравним свойства этого суперблока с суперблоком AES рассмотренным ранее.

Как видно из представленных данных в рассматриваемом случае мы сразу (за один цикл) получаем закон распределения близкий к закону распределения переходов дифференциальной таблицы случайной подстановки 16-ой степени. Это преобразование на выходе сразу реализует асимптотическое значение максимума полного дифференциала (правда, это достигается внутренней трехцикловой структурой преобразования).

Отметим здесь, однако, что наши эксперименты с совершенными *S*-блоками, так мы назвали *S*-блоки, обладающими показателями случайных *S*-блоков (имеющих законы распределения числа инверсий, возрастаний и циклов, а также законы распределения переходов XOR таблиц и смещений таблиц линейных аппроксимаций, повторяющие соответствующие теоретические законы), показывают, что они ведут себя также как и другие применяемые в шифрах случайные или не случайные *S*-блоки, т.е. их применение не приводит к заметному улучшению характеристик сходимости шифров к асимптотическому значению максимума полного дифференциала. Поэтому вопрос об эффективности использования при

Таблица 5. Значения переходов дифференциальной таблицы супер блока MISTY1 для различных значений ключа зашифрования

Кол-во переходов в ячейке	Число ячеек Ключ 0x0000:	Число ячеек Ключ 0xFF00:	Число ячеек Ключ 0x0F0F:	Число ячеек Ключ 0x1234:	Число ячеек Ключ 0x1111:	Число ячеек Ключ 0xAAAA:
0	2605549364	2605492361	2605539766	2605527119	2605516029	2605520863
2	1300024352	1300109653	1300032540	1300064477	1300064802	1300060159
4	328372588	328366110	328380339	328359715	328384633	328378643
6	53631298	53614855	53627998	53624362	53618333	53624945
8	6564176	6560111	6562427	6566955	6558540	6557969
10	639805	638633	638937	639359	639510	639068
12	50994	50888	50481	50617	50780	50904
14	3430	3414	3517	3406	3374	3447
16	208	193	210	209	212	212
18	9	7	10	5	11	15
20	1	0	0	0	1	0
22				10	0	0

построении шифров преобразований, обладающих показателями более близкими к показателям случайных подстановок, остается пока открытым. Очевидно, что основная компонента обеспечения случайности преобразования все-таки связана с реализацией механизма достаточно глубокого перемешивания обрабатываемых блоков данных внутри «тела» всего шифра – достижения статистической инвариантности распределения разностей на выходе преобразования от ключевых и текстовых битов.

ВЫВОДЫ

Результатами работы следует считать выполненный анализ дифференциальных свойств суперблоков трех шифров: AES, мини Мухомора (SL преобразования этого шифра, как варианта уменьшенного AES суперблока) и шифра MISTY1.

И все же основным результатом является положение, в соответствии с которым свойства AES суперблока не являются решающими для определения показателей доказуемой безопасности шифра Rijndael.

Предложено вместо оценок максимумов средних значений дифференциальных и линейных вероятностей (*MADP* и *MALHP*) суперблоков и шифров рассматривать средние значения максимумов этих вероятностей (*AMDP* и *AMLHP*), как более адекватно характеризующих потенциальные возможности в реализации максимумов дифференциальных и линейных показателей шифрующих преобразований. Эти оценки в несколько раз превышают значения *MADP* и *MALHP* и позволяют получить белее точные результаты.

В процессе этого анализа разработана уточненная методика оценки максимального значения дифференциала ($AMDP \times 2^{-32}$) двухциклового AES суперблока. В качестве более точной оценки вероятности максимального значения двухциклового дифференциала (*AMDP*) обосновано значение $48/2^{32}$ (сегодня эксперименты уже дали результат $80/2^{32}$). Показано, что стойкость больших шифров и, в частности, шифра Rijndael (AES-a) не зависит от дифференциальных (и линейных) показателей *S*-блоков, используемых в шифрах. В соответствии с нашими результатами она определяется соответствующими характеристиками случайных подстановок, к которым приходит каждый шифр при увеличении числа циклов шифрования [13].

Представлено как одно из перспективных решений по построению суперблоков (криптографических примитивов) преобразование FI шифра MISTY1. Это преобразование реализует за один цикл (состоящий из последовательности трех простых преобразований) дифференциальные показатели, характерные для случайной подстановки соответствующей степени.

СПИСОК ЛИТЕРАТУРЫ

1. Computational aspects of the expected differential probability of 4-round AES and AES-like ciphers / M. Lamberger, J. Daemen, N. Pramstaller at al // Abstract – 8th Central European Conference on Cryptography 2008. Computing – 2009. – Pp. 85–104. DOI 10.1007/s00607-009-0034-y.
2. *Daemen, J.* 'Understanding two-round differentials in AES' / J. Daemen, V. Rijmen // Proc. Security and Cryptography for Networks (SCN 2006), LNCS, 4116, edited by De Prisco, R., and Yung, M., (Springer). – 2006. – Pp. 78–94.
3. *Keliher, L.* Exast maximum expected differential and linear probability for 2-round advanced encryption standard (AES) / L. Keliher, J. Sui // Cryptology ePrint archive Report 2005/ 321. –2005. – http://eprint.iacr.org.
4. *Sano, F.* On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis / Sano, K. Ohkuma, H. Shimizu, S. Kawamura / IEICE Trans. Fundamentals, January 2003. – vol. E86-a, NO.1. – Pp. 37–46.
5. *Долгов, В. И.* Вариации на тему шифра Rijndael / В. И. Долгов, И. В. Лисицкая, А. В. Казимиров // Прикладная радиоэлектроника. – 2010. – Т.9, №3. – С. 321–325.
6. Криптографические свойства уменьшенной версии шифра «Мухомор» / И. В. Лисицкая, О. И. Олешко, С. Н. Руденко [та ін.] // Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць. – Київ. – 2010. – Вип. 2(18). – С. 33–42.
7. *Кузнецов, А. А.* Линейные свойства блочных симметричных шифров, представленных на украинский конкурс / А. А. Кузнецов, И. В. Лисицкая, С. А. Исаев // Прикладная радиоэлектроника. – 2011. – Т. 10, № 2. – С. 135–140.
8. *Лисицкая, И. В.* Об участии *S*-блоков в формировании максимальных значений линейных вероятностей блочных симметричных шифров / И. В. Лисицкая, В. В. Ковтун // Межведомственный научн. технический сборник «Радиотехника». – 2011. – Вып. 166. – С. 17–25.
9. *Лисицкая, И. В.* Большие шифры - случайные подстановки / И. В. Лисицкая, А. А. Настенко // Межведомственный научн. технический сборник «Радиотехника». – 2011. – Вып. 166. –С. 50–55.
10. *Лисицкая, И. В.* Дифференциальные свойства шифра FOX / И. В. Лисицкая, Д. С. Кайдалов // Прикладная радиоэлектроника. – 2011. – Т. 10, № 2. – С. 122–126.
11. Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація / І. Д. Горбенко, М. Ф. Бондаренко, В. І. Долгов [та ін.] // Прикладная радиоэлектроника. – 2007. – Том. 6, №2. – С. 147–157.
12. *M. Matsui,* «New block encryption algorithm Misty», Fast Software Encryption '97, LNCS 1267, E. Biham, Ed., Springer-Verlag. – 1997. – Pp. 64–74.
13. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / И. Д. Горбенко, В. И. Долгов, И. В. Лисицкая, Р. В. Олейников // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 212–320.

Стаття надійшла до редакції 23.02.2011.
Після доробки 22.02.2012.

Лисицька І. В.

ПОРІВНЯННЯ ЗА ЕФЕКТИВНІСТЮ СУПЕРБЛОКІВ ДЕЯКИХ СУЧАСНИХ ШИФРІВ

Викладається нова методика оцінки показників доказової безпеки блокових симетричних шифрів. Із застосуванням цієї методики виконується аналіз диференціальних властивостей суперблоків трьох шифрів: шифру AES, зменшеної версії шифру Мухомор і шифру MISTY1. Викладаються результати обчислювальних експериментів по визначенню значень AMDP і MADP AES суперблоку. Демонструється, що стійкість великих шифрів і, зокрема шифру Rijndael (AES) не залежить від диференціальних показників S-блоків, використ-

товуваних у шифрах. Представляється як одне з перспективних рішень з побудови суперблоку перетворення FI шифру MISTY1, яке примітно тим, що реалізує за один цикл диференціальні показники випадкової підстановки відповідного степеня.

Ключові слова: доказова безпека, диференціал, суперблок, випадкова підстановка.

Lysytska I. V.

COMPARING oN EFFECTIVENESS OF SUPERBOXES some MODERN SIPHERS

New method of assessment indicators provable security block symmetric ciphers sets out. With application of this method are analyzed for differential properties superblock three ciphers: cipher AES, the reduced version cipher Muhomor and cipher MISTY1. The results of computational experiments to determine the values of AMDP and MADP AES superblock are presented. Demonstrated that the resistance of large ciphers and, in particular cipher Rijndael (AES) is independent of the differential properties of S-blocks used in the ciphers. It seems like one of the promising solutions for building superblocks transformation FI cipher MISTY1, which is noteworthy that sells for one cycle of differential performance random permutation corresponding degree.

Key words: of provable security, differential, superblock, random permutation.

УДК 004.3

Баркалов А. А.[1], Мальчева Р. В.[2], Солдатов К. А.[3]

[1]Д-р техн. наук, проф. Университета Зеленогурского (Польша)
[2]Канд. техн. наук, доцент Донецкого национального технического университета
[3]Аспирант Донецкого национального технического университета

ОПТИМИЗАЦИЯ СХЕМЫ АВТОМАТА МУРА, РЕАЛИЗУЕМОЙ В БАЗИСЕ ПЛИС

В статье предлагается метод, предназначенный для уменьшения числа входных переменных и промежуточных термов в реализуемых системах булевых функций. Предложенный метод основан на расширении кодов состояний перехода и замене логических условий. Применение предложенного метода позволяет до 20 % уменьшить общее число макроячеек в блоках БЛУ и БФП.

Ключевые слова: автомат Мура, ПЛИС, ГСА, псевдоэквивалентные состояния, замена логических условий.

ВВЕДЕНИЕ

Практически любая цифровая система включает в свой состав устройство управления (УУ) [1]. При реализации схем УУ часто используется модель микропрограммного автомата Мура [2]. В настоящее время программируемые логические интегральные схемы (ПЛИС) [3] широко применяются для реализации схем УУ. Существуют два основных класса ПЛИС: CPLD (Complex Programmable Logic Devices) и FPGA (Field-Programmable Gate Arrays) [4, 5]. Для уменьшения числа макроячеек ПЛИС в схеме УУ необходимо уменьшать число входных переменных и промежуточных термов в реализуемых системах булевских функций (СБФ) [6]. В настоящей работе предлагается метод решения этой задачи для микропрограммного автомата (МПА) Мура. Метод основан на расширении кодов состояний перехода и замене логических условий.

Целью исследований является оптимизация схемы МПА Мура за счет расширения кодов состояний перехода и замены логических условий.

Задачей исследований является разработка метода синтеза МПА Мура, позволяющего уменьшить число макроячеек ПЛИС в схеме автомата. При этом алгоритм управления представляется в виде граф-схемы алгоритма (ГСА) [1].

ОБЩИЕ ПОЛОЖЕНИЯ И ОСНОВНАЯ ИДЕЯ ПРЕДЛОЖЕННОГО МЕТОДА

Пусть автомат Мура задан прямой структурной таблицей (ПСТ) со столбцами [1]: a_m, $K(a_m)$, a_S, $K(a_S)$, X_h, Φ_h, h. Здесь a_m – исходное состояние МПА; $K(a_m)$ – код состояния $a_m \in A$ разрядности $R_A = \lceil \log_2 M \rceil$, для кодирования состояний используются внутренние переменные из множества $T = \{T_1,...,T_{R_A}\}$; a_S, $K(a_S)$ – соответственно состояние перехода и его код; X_h – входной сигнал, определяющий переход $< a_m, a_S >$, и равный конъюнкции некоторых элементов (или их отрицаний) множества логических условий $X = \{x_1,...,x_L\}$; Φ_h – набор функций возбуждения триггеров памяти МПА, принимающих единичное значение для переключения памяти из $K(a_m)$ в $K(a_S)$, $\Phi_h \subseteq \Phi = \{\varphi_1,...,\varphi_{R_A}\}$; $h = 1,...,H$ – номер перехода. В столбце a_m записывается набор микроопераций Y_q, формируемых в состоянии $a_m \in A$, где $Y_q \subseteq Y = \{y_1,...,y_N\}$, $q = 1,...,Q$. Эта таблица является основой для формирования систем функций:

$$\Phi = \Phi(T, X), \quad (1)$$

$$Y = Y(T), \quad (2)$$