УДК 681.3.06: 519.248.681

М. Ф. БОНДАРЕНКО, д-р техн. наук, А. С. КОРЯК, В. И. РУЖЕНЦЕВ

ПОВЫШЕНИЕ УСТОЙЧИВОСТИ ШИФРА DES К АТАКАМ ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА

В работе [1] изучаются и обсуждаются принципы построения таблиц подстановок (*S*-блоков) для шифра DES, использованные разработчиками. Показано, что на момент принятия стандарта предложенные разработчиками шифра ограничения действительно позволяли считать его достаточно надежным для практического применения. Сегодня, однако, найдены атаки на шифр, сложность которых оказалась меньше сложности прямого перебора всех возможных ключей (атаки грубой силой). Сначала Эли Бихамом и Ади Шамиром был разработан дифференциальный криптоанализ [2], а немного позже Мицуру Мацуи была обоснована атака на шифр DES, названная линейным криптоанализом [3]. Известно, что стойкость к названным атакам определяется свойствами таблиц *S*-блоков. Естественным, поэтому, является интерес, проявленный в последнее время к разработке подходов в том числе и методов отбора таблиц подстановок, позволяющих повысить показатели защищенности шифра DES [4-6 и др.].

В этой работе речь будет идти о защите от известной атаки на шифр DES, предложенной Э. Бихамом и А. Шамиром [2]. Она основана на использовании двухцикловых характеристик, допускающих итеративное продолжение. Центральная идея, использованная при обосновании излагаемого подхода, состоит в нахождении таких *S*-блоков, которые исключают всякую возможность (ненулевую вероятность) построения "обнуляющего" разностного преобразования (так в [1] названо выполнение одноциклового преобразования, при котором ненулевая разность на входе цикловой функции F преобразуется в нулевую разность на ее выходе).

Целесообразно будет начать с того, что напомнить методику построения трехблочных обнуляющих характеристик , изложенную в работе [1].

При построении трехблочных характеристик рассматриваются 14-битные входы цикловой функции вида (0, 0, x, y, z, 1, t, p, 1, q, l, m, 0, 0) трех смежных (соседних) *S*-блоков. При этом учет требований, предъявленных к *S*-блокам разработчиками стандарта [7], позволяет выделить два принципиальных момента:

- из всего множества входов (0, 0, x, y, z, 1, t, p, 1, q, l, m, 0, 0) трех (смежных) активных *S*-блоков реально могут быть использованы только те, у которых биты z и q одновременно не равны нулю (т.к. переход в 0 для входной разности вида (0, x, y, z, t, 0) в таблицах, составленных из перестановок, невозможен);

- в атаке, использующей несколько активных *S*-блоков в обнуляющем цикле, в принципе могут участвовать только связанные (смежные) *S*-блоки.

Все допустимые варианты входов *S*-блоков, которые могут участвовать в формировании трехблочных характеристик (характеристик с тремя активными *S*-блоками), представлены в табл. 1.

Напомним, что связь обозначений входов в *S*-блоки, представленных в табл.1, с таблицами стандарта определяется правилами, оговоренными в [8]: вход по строкам таблицы ab_x соответствует 6-битному вектору входной разности $\Delta=(\Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_5, \Delta_6)$, где a представляет собой шестнадцатеричную запись двоичного числа $\Delta_1\Delta_6$, а b – числа $\Delta_2\Delta_3\Delta_4\Delta_5$.

Анализ представленных в табл. 1 композиций входов в *S*-блоки позволяет заключить, что всего возможно 64×3=192 варианта атак для каждой тройки таблиц, а для шифра в целом 192×8=1536 вариантов.

Для перекрытия этих характеристик, как показано в [1], разработчики шифра DES пошли двумя путями. Основную массу трехблочных обнуляющих характеристик они просто запретили с помощью требования 6 (входы 28_x, $2A_x$, $2C_x$, $2E_x$ во всех таблицах побитовых разностей выбраны с нулевыми вероятностями переходов в выходную разность ноль) и требования 4 (для входов 10_x и 20_x нет переходов в ноль). В результате из общего числа 192 вариантов остается защититься от 48 оставшихся характеристик для каждой тройки смежных *S*-блоков. Разработчики постарались перекрыть их за счет ограничений на допустимые значения вероятностей одноблочных переходов, участвующих в формировании этих трехблочных характеристик [1]. Однако для защиты от атак, предложенных Э. Бихамом и А. Шамиром, этого оказалось недостаточно. Указанные атаки на 16-цикловый DES построены именно на возможности реализации трехблочных обнуляющих характеристик. Э. Бихам и А. Шамир используют две наиболее вероятные итерационные характеристики, в которых участвуют первые три

S-блока: одна – для входной разности 19 60 00 00 00 00 00 00_x (ей соответствует трехблочная входная разность 00001100101100 или входы таблиц разностей 11_x, 29_x, 26_x), вторая – для входной разности $1B$ 60 00 00 00 00 00 00_x (трехблочная входная разность 00001101101100 или, соответственно, входы таблицы разностей 11_x, $2B_x$, 26_x).

Таблица 1

Участие S-блоков в формировании входной разности (0, 0, x, y, z, 1, t, p, 1, q, l, m, 0, 0) при трехблочной характеристике					
z	Входные разности первого S-блока (0, 0, x, y, z, 1)	z q	Входные разности второго S-блока (z, 1, t, p, 1, q)	q	Входные разности третьего S-блока (1, q, l, m, 0, 0)
0	(0, 0, 0, 0, 0, 1) → 10_x		(0, 1, 0, 0, 1, 1) → 19_x		(1, 0, 0, 0, 0, 0) → 20_x
	(0, 0, 0, 1, 0, 1) → 12_x	0	(0, 1, 0, 1, 1, 1) → $1B_x$		(1, 0, 0, 1, 0, 0) → 22_x
	(0, 0, 1, 0, 0, 1) → 14_x	1	(0, 1, 1, 0, 1, 1) → $1D_x$	0	(1, 0, 1, 0, 0, 0) → 24_x
	(0, 0, 1, 1, 0, 1) → 16_x		(0, 1, 1, 1, 1, 1) → $1F_x$		(1, 0, 1, 1, 0, 0) → 26_x
1	(0, 0, 0, 0, 1, 1) → 11_x		(1, 1, 0, 0, 1, 0) → 29_x		(1, 1, 0, 0, 0, 0) → 28_x
	(0, 0, 0, 1, 1, 1) → 13_x	1	(1, 1, 0, 1, 1, 0) → $2B_x$		(1, 1, 0, 1, 0, 0) → $2A_x$
	(0, 0, 1, 0, 1, 1) → 15_x	0	(1, 1, 1, 0, 1, 0) → $2D_x$	1	(1, 1, 1, 0, 0, 0) → $2C_x$
	(0, 0, 1, 1, 1, 1) → 17_x		(1, 1, 1, 1, 1, 0) → $2F_x$		(1, 1, 1, 1, 0, 0) → $2E_x$
			(1, 1, 0, 0, 1, 1) → 39_x		
		1	(1, 1, 1, 0, 1, 1) → $3D_x$		
		1	(1, 1, 0, 1, 1, 1) → $3B_x$		
			(1, 1, 1, 1, 1, 1) → $3F_x$		

В то же время, анализ приведенных выше вариантов возможных входных разностей для трехблочной атаки и их распределения по S-блокам позволяет сделать вывод, что разработчики стандарта при формировании требований к отбору S-блоков, по-видимому, не ставили перед собой задачу добиться максимально возможной защищенности шифра от атак дифференциального криптоанализа, а стремились просто гарантировать некоторый уровень защиты, который, по их мнению, обеспечит достаточную его надежность, так как существуют возможности улучшения показателей надежности шифра. Легко убедиться, что на таблицы дифференциальных разностей, а соответственно, на таблицы S-блоков можно наложить дополнительные ограничения, которые делают шифр DES неуязвимым по крайней мере к дифференциальным атакам, использующим трехблочные обнуляющие характеристики. Для этого достаточно потребовать, например, чтобы в таблицах дифференциальных разностей дополнительно были запрещенными переходы в нуль еще для четырех входов, а именно, для входов 29_x, $2B_x$, $2D_x$, $2F_x$. Действительно, как уже отмечалось ранее, в стандарте DES S-блоки построены так, что для входных разностей 28_x, $2A_x$, $2C_x$, $2E_x$ не существует переходов в нуль. Это означает, что в соответствии с табл.1 в трехблочной характеристике для последнего (третьего в связке) S-блока "работают" только четыре входа, для которых $q = 0$. Этому же значению бита во входной разности соответствуют четыре значения входов для второго S-блока связки, а именно, входы 29_x, $2B_x$, $2D_x$, $2F_x$ (все другие входы срабатывают только при $q = 1$). Но тогда трехблочную обнуляющую характеристику можно сделать нереализуемой, если, как уже отмечалось выше, сделать запрещенными переходы в ноль для входов 29_x, $2B_x$, $2D_x$, $2F_x$. В результате, для повышения устойчивости к атакам дифференциального криптоанализа необходимо S-блоки строить так, чтобы в таблицах дифференциальных разностей отсутствовали нулевые выходные разности одновременно для восьми входов в эти таблицы: 28_x, 29_x, $2A_x$, $2B_x$, $2C_x$, $2D_x$, $2E_x$, $2F_x$.

Отметим здесь, что к этому же результату, как оказалось, раньше нас пришли и исследователи группы Кваджио Ким [5]. В их интерпретации изложенные выше дополнительные требования к отбору S-блоков сформулированы более компактно: необходимо чтобы для любого S-блока $S(\mathbf{x}) \neq S(\mathbf{x} \oplus 11ef10)$.

Здесь мы хотим привлечь внимание к тому, что представленный результат не является единственно возможным решением задачи перекрытия трехблочных обнуляющих характеристик. Можно предложить еще несколько вариантов правил отбора S-блоков, позволяющих защитить шифр DES от известных атак дифференциального криптоанализа (перекрыть наиболее вероятные атаки), чему и посвящаются дальнейшие результаты

Сразу можно отметить, что для наших целей подходят только таблицы S-блоков, для которых не "срабатывают" и двухблочные обнуляющие характеристики, а для этого, как показано в [1], должны быть равными нулю вероятности переходов в ноль (должны иметь нулевые значения ячейки таблиц дифференциальных разностей, соответствующие нулевым выходам) для входов S-блоков хотя бы одного из столбцов табл. 2. (В обозначениях корейских исследователей – это либо требование $S(\mathbf{x}) \neq S(\mathbf{x} \oplus 00ef11)$, либо требование $S(\mathbf{x}) \neq S(\mathbf{x} \oplus 11ef00)$).

Таблица 2

Участие S-блоков в формировании входной разности $(0, 0, x, y, 1, 1, t, p, 0, 0)$ при двухблочной характеристике	
Входные разности первого S-блока $(0, 0, x, y, 1, 1)$	Входные разности второго S-блока $(1, 1, t, p, 0, 0)$
$(0, 0, 0, 0, 1, 1) \rightarrow 11_x$	$(1, 1, 0, 0, 0, 0) \rightarrow 28_x$
$(0, 0, 0, 1, 1, 1) \rightarrow 13_x$	$(1, 1, 0, 1, 0, 0) \rightarrow 2A_x$
$(0, 0, 1, 0, 1, 1) \rightarrow 15_x$	$(1, 1, 1, 0, 0, 0) \rightarrow 2C_x$
$(0, 0, 1, 1, 1, 1) \rightarrow 17_x$	$(1, 1, 1, 1, 0, 0) \rightarrow 2E_x$

Кроме того, если идти дальше, введенные ограничения должны обеспечивать и невозможность построения "обнуляющего" разностного преобразования для большего количества активных S-блоков (многоблочных обнуляющих характеристик), так как для характеристики обнуляющего типа с 4-мя активными S-блоками при одноцикловом преобразовании с вероятностью $\frac{16}{64} = \frac{1}{4}$ на один S-блок (граничное значение, определяемое элементами таблиц дифференциальных разностей S-блоков, установленное требованием 7 разработчиков стандарта [1]), для вероятности результирующей 13-ти цикловой характеристики получаем оценку

$$\left(\frac{1}{4}\right)^{4\cdot 6} = \left(\frac{1}{4}\right)^{24} = 2^{-48},$$

что меньше, чем вероятность прямого перебора всех ключей (2^{-55}).

Участие S-блоков в формировании входной разности при построении четырехблочных характеристик иллюстрирует табл. 3.

Анализ представленных результатов позволяет заключить, что для всего набора возможных переходов, представленных в табл.1 и табл. 2, приведенным ограничениям удовлетворяют, включая отмеченный выше, пять вариантов задания нулевых вероятностей переходов в нулевую выходную разность (нас будут интересовать в первую очередь ограничения минимального типа, под которыми будем понимать минимальное число ячеек (выходов) таблиц дифференциальных разностей, нулевые значения которых обеспечивают нереализуемость многоцикловых обнуляющих характеристик). Они показаны входами в таблицы дифференциальных разностей, представленными в табл. 4.

Как показывает более тщательный анализ, из этих характеристик необходимо исключить последнюю, так как в отличие от остальных она не запрещает характеристики обнуляющего типа с числом активных S-блоков в каждом цикле, большем, чем три (см. табл. 3). Нулевые значения переходов в ноль для первых четырех сочетаний входов обеспечивают перекрытие не только всех двухблочных, трехблочных, но и всех других обнуляющих характеристик с числом активных S-блоков до 7 включительно в каждом цикле.

Заметим также, что во втором и четвертом случаях мы отходим от требования 6 стандарта, вводя вместо него другое (вместо $S(\mathbf{x}) \neq S(\mathbf{x} \oplus 11ef00)$ вводится требование $S(\mathbf{x}) \neq S(\mathbf{x} \oplus 00ef11)$ с дополнительным ограничением на еще одну четверку входов).

Таблица 3

Участие S-блоков в формировании входной разности (0, 0, x, y, z, 1, p, q, r, s, t, l, 1, m, n, k, 0, 0) при четырехблочной характеристике							
z	Входные разности первого S-блока (0, 0, x, y, z, 1)	z r s	Входные разности второго S-блока (z, 1, p, q, r, s),	r s m	Входные разноси третьего S-блока (r, s, t, l, 1, m)	m	Входные разности четвертого S-блока (1, m, n, k, 0, 0)
0	(0, 0, 0, 0, 0, 1) → 10_x		(1, 1, 0, 0, 0, 0) → 28_x		(0, 1, 0, 0, 1, 1) → 19_x	0	(1, 0, 0, 0, 0, 0) → 20_x
	(0, 0, 0, 1, 0, 1) → 12_x	1	(1, 1, 0, 1, 0, 0) → $2A_x$	0	(0, 1, 0, 1, 1, 1) → $1B_x$		(1, 0, 0, 1, 0, 0) → 22_x
	(0, 0, 1, 0, 0, 1) → 14_x	0	(1, 1, 1, 0, 0, 0) → $2C_x$	1	(0, 1, 1, 0, 1, 1) → $1D_x$		(1, 0, 1, 0, 0, 0) → 24_x
	(0, 0, 1, 1, 0, 1) → 16_x	0	(1, 1, 1, 1, 0, 0) → $2E_x$	1	(0, 1, 1, 1, 1, 1) → $1F_x$		(1, 0, 1, 1, 0, 0) → 26_x
1	(0, 0, 0, 0, 1, 1) → 11_x		(0, 1, 0, 0, 1, 1) → 19_x		(1, 1, 0, 0, 1, 0) → 29_x	1	(1, 1, 0, 0, 0, 0) → 28_x
	(0, 0, 0, 1, 1, 1) → 13_x	0	(0, 1, 0, 1, 1, 1) → $1B_x$	1	(1, 1, 0, 1, 1, 0) → $2B_x$		(1, 1, 0, 1, 0, 0) → $2A_x$
	(0, 0, 1, 0, 1, 1) → 15_x	1	(0, 1, 1, 0, 1, 1) → $1D_x$	1	(1, 1, 1, 0, 1, 0) → $2D_x$		(1, 1, 1, 0, 0, 0) → $2C_x$
	(0, 0, 1, 1, 1, 1) → 17_x	1	(0, 1, 1, 1, 1, 1) → $1F_x$	0	(1, 1, 1, 1, 1, 0) → $2F_x$		(1, 1, 1, 1, 0, 0) → $2E_x$
			(1, 1, 0, 0, 1, 1) → 39_x		(1, 1, 0, 0, 1, 1) → 39_x		
		1	(1, 1, 1, 0, 1, 1) → $3D_x$	1	(1, 1, 1, 0, 1, 1) → $3D_x$		
		1	(1, 1, 0, 1, 1, 1) → $3B_x$	1	(1, 1, 0, 1, 1, 1) → $3B_x$		
		1	(1, 1, 1, 1, 1, 1) → $3F_x$	1	(1, 1, 1, 1, 1, 1) → $3F_x$		
			(1, 1, 0, 0, 1, 0) → 29_x		(1, 0, 0, 0, 1, 0) → 21_x		
		1	(1, 1, 0, 1, 1, 0) → $2B_x$	1	(1, 0, 0, 1, 1, 0) → 23_x		
		1	(1, 1, 1, 0, 1, 0) → $2D_x$	0	(1, 0, 1, 0, 1, 0) → 25_x		
		0	(1, 1, 1, 1, 1, 0) → $2F_x$	0	(1, 0, 1, 1, 1, 0) → 27_x		
			(1, 1, 0, 0, 0, 1) → 38_x		(1, 0, 0, 0, 1, 1) → 31_x		
		1	(1, 1, 0, 1, 0, 1) → $3A_x$	1	(1, 0, 0, 1, 1, 1) → 33_x		
		0	(1, 1, 1, 0, 0, 1) → $3C_x$	0	(1, 0, 1, 0, 1, 1) → 35_x		
		1	(1, 1, 1, 1, 0, 1) → $3E_x$	1	(1, 0, 1, 1, 1, 1) → 37_x		
			(0, 1, 0, 0, 0, 1) → 18_x		(0, 0, 0, 0, 1, 1) → 11_x		
		0	(0, 1, 0, 1, 0, 1) → $1A_x$	0	(0, 0, 0, 1, 1, 1) → 13_x		
		0	(0, 1, 1, 0, 0, 1) → $1C_x$	0	(0, 0, 1, 0, 1, 1) → 15_x		
		1	(0, 1, 1, 1, 0, 1) → $1E_x$	1	(0, 0, 1, 1, 1, 1) → 17_x		

Таблица 4

1) Входы в таблицы дифференциальных разностей S-блоков	2) Входы в таблицы дифференциальных разностей S-блоков	3) Входы в таблицы дифференциальных разностей S-блоков	4) Входы в таблицы дифференциальных разностей S-блоков	5) Входы в таблицы дифференциальных разностей S-блоков
(1, 1, 0, 0, 0, 0)→28_x	(0, 0, 0, 0, 1, 1)→11_x	(1, 0, 0, 0, 0, 0)→20_x	(0, 0, 0, 0, 0, 1)→10_x	(0, 0, 0, 0, 1, 1)→11_x
(1, 1, 0, 1, 0, 0)→$2A_x$	(0, 0, 0, 1, 1, 1)→13_x	(1, 0, 0, 1, 0, 0)→22_x	(0, 0, 0, 1, 0, 1)→12_x	(0, 0, 0, 1, 1, 1)→13_x
(1, 1, 1, 0, 0, 0)→$2C_x$	(0, 0, 1, 0, 1, 1)→15_x	(1, 0, 1, 0, 0, 0)→24_x	(0, 0, 1, 0, 0, 1)→14_x	(0, 0, 1, 0, 1, 1)→15_x
(1, 1, 1, 1, 0, 0)→$2E_x$	(0, 0, 1, 1, 1, 1)→17_x	(1, 0, 1, 1, 0, 0)→26_x	(0, 0, 1, 1, 0, 1)→16_x	(0, 0, 1, 1, 1, 1)→17_x
(1, 1, 0, 0, 1, 0)→29_x	(0, 1, 0, 0, 1, 1)→19_x	(1, 1, 0, 0, 0, 0)→28_x	(0, 0, 0, 0, 1, 1)→11_x	(1, 1, 0, 0, 0, 0)→28_x
(1, 1, 0, 1, 1, 0)→$2B_x$	(0, 1, 0, 1, 1, 1)→$1B_x$	(1, 1, 0, 1, 0, 0)→$2A_x$	(0, 0, 0, 1, 1, 1)→13_x	(1, 1, 0, 1, 0, 0)→$2A_x$
(1, 1, 1, 0, 1, 0)→$2D_x$	(0, 1, 1, 0, 1, 1)→$1D_x$	(1, 1, 1, 0, 0, 0)→$2C_x$	(0, 0, 1, 0, 1, 1)→15_x	(1, 1, 1, 0, 0, 0)→$2C_x$
(1, 1, 1, 1, 1, 0)→$2F_x$	(0, 1, 1, 1, 1, 1)→$1F_x$	(1, 1, 1, 1, 0, 0)→$2E_x$	(0, 0, 1, 1, 1, 1)→17_x	(1, 1, 1, 1, 0, 0)→$2E_x$

Четыре отмеченные варианта ограничений были проверены моделированием и подтвердили свою эффективность. Как показывают результаты эксперимента, вычислительные затраты на построение таблиц подстановок для DES с дополнительными ограничениями 1 или 2 получаются на порядок меньшими, чем соответствующие затраты при использовании дополнительных ограничений 3 или 4 (в табл. 4 варианты 1-4 расположены в порядке увеличения вычислительной сложности процедуры построения таблиц подстановок). Поэтому ограничение в виде $S(\mathbf{x}) \neq S(\mathbf{x} \oplus 11ef10)$, на ко-

тором остановились и корейские ученые, можно действительно рассматривать в качестве одного из предпочтительных.

Отметим также, что дополнительное ограничение $S(\mathbf{x}) \neq S(\mathbf{x} \oplus 11ef10)$ рассматривается корейскими учеными как достаточное для полной защиты шифра DES от атак дифференциального криптоанализа. Вычислительные эксперименты, проведенные нами, подтверждают этот результат.

Список литературы: 1. *Долгов В.И., Лисицкая И.В., Олейников Р.В.* Принципы защиты алгоритма DES от атак дифференциального криптоанализа. // Радиотехника. 2000. Вып 113. С. 145-157. 2. *Biham E., Shamir A.* Differential Cryptanalysis of the DES- like Cryptosystems, Journal of Cryptology. Vol. 4. P. 3-72. 1991. 3. *Matsui M.* Linear Cryptanalysis Metod for DES Cipher // Pros. Eurocrypt'93. P. 386-397. Norway. 1993. 4. *Kim K.* Construction of DES-like S-boxes Based on Boolean Function Satisfying the SAK. Pros. Of Asiacrypt'91. P. 59-72. Fujiyoshida. Japan. 1991. 5. *Kim K., Park S., Lee S.* Reconstruction of s^2DES *S*-boxes and their Immunity to Differential Cryptanalysis. Pros. of 1993 Korea-Japan Joint Workshop on Information Security fnd Cryptology (JW-ISC'93). Oct. 24-36. Seoul. 1993. 6.. *Knudsen L* Iterative Characteristics of DES and s^2DES. Proc. of Crypto'92. UCSB. 1992. 7. *B. Schneier.* Applied Cryptography. *S*econd Edition: protocols, algorithms, and Source code in C. Published by John Wiley & *S*on*S*. Inc. New York: Chiche*S*ter Bri*S*bane Toronto *S*ingapore. 1996. 758 p. 8. *Барсуков В.С., Дворянкин С.В., Шеремет И.А.* Безопасность связи в каналах телекоммуникаций. М.: Россия. 1993. Т.20. 123 с.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 6.03.2001