УДК 681.3.06

С.А. ГОЛОВАШИЧ

КЛЮЧЕВЫЕ ГРУППЫ В АТАКАХ ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА DES-ПОДОБНЫХ ШИФРОВ

В данной работе нас будут интересовать только принципы построения характеристик, используемых в атаках дифференциального криптоанализа (далее дифференциальных характеристик либо просто характеристик) DES-подобных шифров (основанных на «подстановке с расширением»), и оценка вероятности их осуществления. Вначале дадим базовые определения и рассмотрим классический подход к построению и оценке вероятностей дифференциальных характеристик, предложенный в открытой печати Эли Бихамом. Изложение материала будет выполняться на примере алгоритма DES, так как он наиболее хорошо изучен, и успешная атака дифференциального криптоанализа впервые была предложена именно для этого криптоалгоритма. Заметим, однако, что предлагаемый подход может быть применён и к другим шифрам, имеющим сходную структуру

Алгоритм DES построен на базе 16-цикловой цепи Фестеля. Основу алгоритма составляет цикловая функция (F-функция), которая включает в себя последовательность из 4-х базовых операций: расширения E ($32 \rightarrow 48$), сложение по модулю 2 с 48-битным подключом, ключенезависимое нелинейное преобразование (табличная подстановка $8 \times S(6 \rightarrow 4)$), перестановка бит P [1].

Далее входные и выходные воздействия любого функционального блока шифра будем рассматривать как бинарные вектора, а под разностью этих векторов (либо их изменением) будем понимать операцию сложение по модулю 2 (XOR).

Введём ряд понятий и определений из теории дифференциального криптоанализа [2].

Взаимосвязь входной и выходной разностей вида: определённое изменение данных на входе некоторого функционального блока либо фрагмента шифра, с некоторой вероятностью, вызывает фиксированное изменение на выходе ($\Delta X \rightarrow \Delta Y$), будем называть дифференциальной характеристикой.

В зависимости от охватываемого функционального блока будем различать одноблочные (состоящие из одного S-блока), многоблочные (состоящие из группы смежных S-блоков), одноцикловые (охватывающие один цикл) и многоцикловые (охватывающие несколько смежных циклов) характеристики.

Под вероятностью одноцикловой дифференциальной характеристики $p(\Delta Y \setminus \Delta X)$ будем понимать вероятность перехода входной разности ΔX в выходную разность ΔY, т.е. вероятность выполнения соотношения $F(X \oplus \Delta X) = Y \oplus \Delta Y$, где $Y = F(X)$.

Под вероятностью n-цикловой дифференциальной характеристики будем понимать вероятность последовательного выполнения цепочки из n определённых одноцикловых характеристик. Вероятность многоцикловой характеристики определяется произведением вероятностей одноцикловых характеристик её составляющих.

Цикл шифрования либо отдельный S-блок считается активным, если на его вход подаётся разность отличная от нуля ($\Delta X \neq 0$), в противном случае цикл (либо S-блок) считается пассивным ($\Delta X = 0$) и с вероятностью $p = 1$ сохраняет значение своего выхода ($\Delta Y = 0$).

Стойкость DES-подобных шифров к атакам дифференциального криптоанализа определяется свойствами используемых нелинейных преобразований (S-блоков). Авторы дифференциального криптоанализа Ади Шамир и Эли Бихам предложили для оценки свойств каждого из 8 S-блоков, содержащихся в алгоритме, воспользоваться так называемой таблицей распределения битовых разностей. Эта таблица имеет организацию 64×16, где первая координата (номер строки) соответствует входной разности ΔX (каждый S-блок имеет 6-ти разрядный вход), а вторая (номер столбца) соответствует выходной разности ΔY (каждый S-блок имеет 4-х разрядный выход). Значение каждой ячейки таблицы равно количеству входных векторов X, для которых $S(X \oplus \Delta X) = Y \oplus \Delta Y$, где $Y = S(X)$, при вариации по всем возможным X. Отношение этого значения к общему числу возможных входных векторов ($2^6 = 64$) соответствует вероятности выполнения некоторой одноблочной характеристики $S(\Delta X) \rightarrow \Delta Y$. В свою очередь вероятность одноцикловой характеристики вычисляется как произведение вероятностей всех одноблочных характеристик её составляющих.

Атака дифференциального криптоанализа эффективна, если её сложность (величина обратная вероятности соответствующей полноцикловой характеристики) меньше чем сложность «силовой атаки» (прямого перебора ключей).

Рассмотрим правило «сшивки» (объединения) нескольких одноблочных характеристик в одноцикловую характеристику. Правило, использованное авторами дифференциального криптоанализа, учитывает только «сшиваемость» входных разностей. В соответствии с этим правилом для «сшивки» одноблочных характеристик двух соседних S-блоков необходимо чтобы два правых бита разности ΔX_1 левого S-блока совпадали с двумя левыми битами разности ΔX_2 правого S-блока: $\Delta X_1 = \{\Delta x_0, \Delta x_1, \Delta x_2, \Delta x_3, \Delta x_4, \Delta x_5\}$ $\Delta X_2 = \{\Delta x_4, \Delta x_5, \Delta x_6, \Delta x_7, \Delta x_8, \Delta x_9\}$. Это следует из того, что после выполнения расширения E и сложения с ключом (рис. 1), на входы каждой пары соседних S-блоков попадают два общих входных бита разности. Назовём это требование правилом «сшивки» по разности (или правилом динамической «сшивки»).

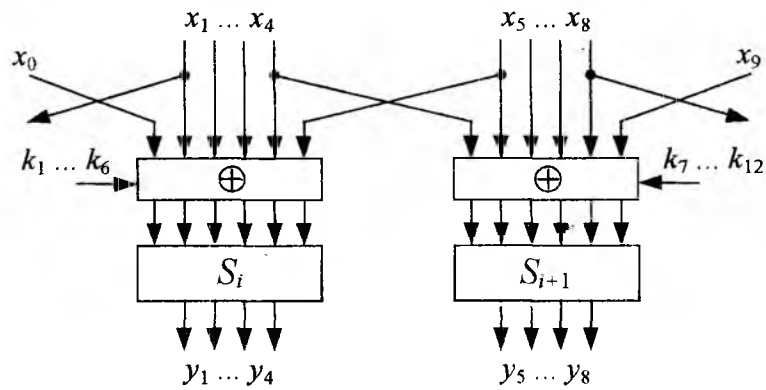

Рис. 1

Одноблочные характеристики, составляющие любую одноцикловую характеристику, всегда удовлетворяют указанному выше требованию. Вероятность результирующей одноцикловой характеристики авторы атаки вычисляют как произведение вероятностей всех одноблочных характеристик, участвующих в её построении, или как произведение вероятностей одноблочных характеристик активных S-блоков (на пассивных S-блоках происходит переход $0 \rightarrow 0$, вероятность которого всегда равна 1). Практически вероятность одноцикловой характеристики вычисляется как отношение произведения содержимого ячеек таблиц распределения дифференциальных разностей, соответствующих переходам (одноблочным характеристикам) активных S-блоков, к общему числу их возможных входных значений, т.е. 64^a, где a – количество активных S-блоков на данном цикле.

Приведенная методика вычисления вероятности одноцикловой характеристики, основана на допущении, что после сложения расширенного входного полублока данных с цикловым подключом (биты которого в пределах подключа независимы), входы любых двух S-блоков также становятся «статически» независимыми и поэтому на входах двух соседних S-блоков может возникнуть произвольное сочетание входных воздействий. Однако более тщательный анализ F-функции показывает, что использование в шифре DES сложения с подключом после E-расширения данных приводит к тому, что условия «сшивки» становятся зависимыми от ключевых битов. Далее будет показано, что в общем случае вероятность некоторой одноцикловой характеристики может принимать ряд дискретных значений, в зависимости от подключа шифрования, используемого в данном цикле, а величина, полученная по рассмотренной выше методике, соответствует среднему значению вероятности характеристики, при вариации по всем возможным вариантам подключа.

В первую очередь, отметим, что a соседних S-блоков имеют только $4 \times a + 2$ входных линий данных, и, следовательно, по ним можно подать только $2^{4 \times a + 2}$ (а не $2^{6 \times a}$) различных входных разностей. Далее нас будет интересовать характер взаимного влияния входов соседних S-блоков. Поэтому преобразуем классическую схему, приведенную на рис. 1 таким образом, чтобы сложение с ключом выполнялось до расширения E, как это показано на рис. 2, т.е. разделим преобразования, составляющие цикловую функцию F, на линейное (сложение входного блока с 32 битами подключа) и нелинейное (оставшаяся часть F-функции). Так как дифференциальные свойства алгоритма

пределяются соответствующими свойствами используемых нелинейных преобразований, то, ледовательно, нас будет интересовать «вторая» часть цикловой функции (перестановку P можно ключить из рассмотрения, так как её применение не влияет на ход дальнейших рассуждений).

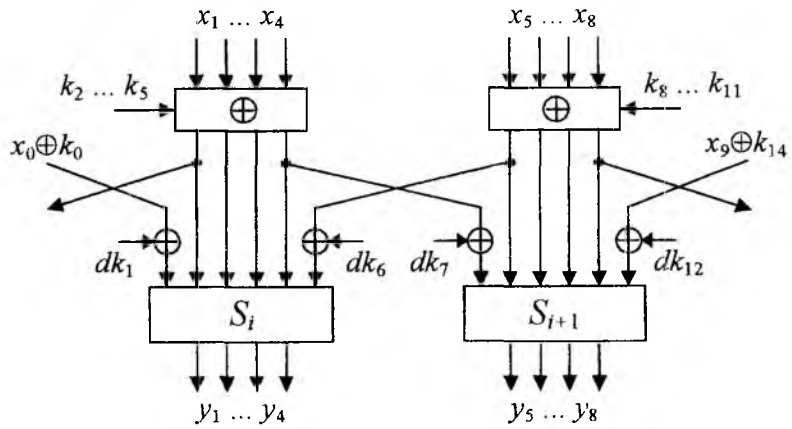

Рис. 2

В результате такого преобразования мы можем исключить из рассмотрения подключ в явном виде. Далее через x_i будем обозначать входные биты блока расширения E, полученные суммированием 32-х битного входного вектора с 32 битами подключа ($x_i := x_i \oplus k_j$). Оставшиеся 16 бит подключа будут участвовать в формировании 8 двухбитных векторов «ключевого смещения» dk – по одному вектору на каждую пару соседних S-блоков. Через dk_i обозначена сумма двух битов подключа, попадающих на входы соседних S-блоков, полученные (в результате расширения E) из одной линии данных, то есть:

$$dk_1 = k_1 \oplus k_0$$

$$dk_6 = k_6 \oplus k_8$$

$$dk_7 = k_7 \oplus k_5$$

$$dk_{12} = k_{12} \oplus k_{14}.$$

Из схемы, приведенной на рис. 2, видно, что если $X_1 = \{x_0, x_1, x_2, x_3, x_4, x_5\}$ и $X_2 = \{x_4', x_5', x_6, x_7, x_8, x_9\}$ – входные вектора соседних S-блоков, то

$$x_4' = x_4 \oplus dk_7$$

$$x_5' = x_5 \oplus dk_6$$

т.е. входные вектора двух соседних S-блоков по двум соответствующим разрядам всегда имеют фиксированную разность $\{dk_7, dk_6\} = \{k_7 \oplus k_5, k_6 \oplus k_8\}$, определяемую ключом шифрования. Назовём последнее свойство правилом «сшивки» по значению (или правилом статической «сшивки»).

Из последнего следует, что «сшивка» двух одноблочных характеристик возможна только в том случае, если пары одноблочных входных значений, участвующие в формировании одноблочных входных разностей, удовлетворяют правилу «сшивки» по значению, а, следовательно, и правилу «сшивки» по разности (правило динамической «сшивки» является частным случаем правила статической «сшивки»).

Исходя из всего выше сказанного, для вычисления вероятностей ключезависимых дифференциальных характеристик следует воспользоваться следующей методикой.

Значения в каждой ячейке «традиционной» таблицы дифференциальных разностей (описанной ранее), в общем случае, следует разбить на 2^4=16 ячеек соответствующих различным вариантам статической «сшивки», или, иначе говоря, к координатам входной ΔX и выходной ΔY разностей необходимо добавить координату X соответствующую фактическому значению 4 входных битов участвующих в «сшивке» (по 2 бита слева и справа).

Вероятность многоблочной характеристики, состоящей из a соседних S-блоков при некотором фиксированном ключе, может быть вычислена как сумма произведений вероятностей статически сшиваемых одноблочных характеристик, её составляющих:

$$p(k) = \sum_{x=0}^{4^{a-1}} \prod_{i=1}^{a} n[s_i, \Delta x, \Delta y, h(x, dk_i, i)] \Big/ 2^{4\times a+2}, \qquad (1)$$

где a – количество активных S-блоков в характеристике;

i – порядковый номер S-блока внутри многоблочной характеристики;

x – значение соответствующее двоичному представлению «статической сшивки»;

s_i – номер S-блока, имеющего в рассматриваемой характеристике индекс i;

$n[s_i, \Delta x, \Delta y, h]$ – количество входных значений S-блока s_i, для которых выполняется характеристика $\Delta x \rightarrow \Delta y$ и биты статической «сшивки» имеют значение h (т.е. элемент расширенной (новой) таблицы распределения дифференциальных разностей);

dk_i – вектор «ключевых смещений» между S-блоками s_i и s_{i-1} ($dk_0 = \{0,0\}$);

h – функция, возвращающая значения левого и правого «швов» для S-блока s_i, при котором его левый «шов» стыкуется с правым «швом» S-блока s_{i-1}.

Вероятность одноцикловой характеристики, состоящей из нескольких несвязанных (разделённых пассивным S-блоком) многоблочных характеристик будет равна произведению вероятностей многоблочных характеристик её составляющих.

В качестве примера рассмотрим две характеристики, предложенные Эли Бихамом для построения атаки с максимальной вероятностью, для стандартных таблиц DES [2]. В таблице 1 представлено разложение одноблочных обнуляющих характеристик, использованных в атаке Бихама по 16 «статическим швам» (верхняя строка). Каждый «шов» записан в 4-ричной системе счисления (старшая цифра соответствует левой паре входов S-блока, а младшая – правой паре); входные разности ΔX представлены в 16-ричном виде в виде индексов оригинальной таблицы, т.е. два старших бита определяют номер строки перестановки, а младшие четыре – номер элемента в этой строке.

Таблица 1

S	ΔX	00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33	Σ
S1	11	1	0	0	1	1	3	3	1	0	1	1	0	0	1	1	0	14
S2	29	0	0	0	2	0	1	0	1	0	1	0	1	0	2	0	0	8
	2B	2	0	0	0	0	0	2	0	2	0	0	0	0	0	2	0	8
S3	26	0	0	1	3	0	1	0	0	0	0	1	3	0	1	0	0	10

Для упрощения использования таблицы 1, её можно преобразовать следующим образом. Так как любая входная разность получается последовательным воздействием некоторой пары входных значений, то содержимое предыдущей таблицы можно представить в виде статистики распределения «переходов» по различным парам, в пределах некоторой входной дельты – получим таблицу 2. Значения в ячейках этой таблицы соответствуют количеству пар, для которых выполняется выбранная характеристика, в скобках в 4-ричной системе счисления указаны биты входной разности, соответствующие «швам».

Таблица 2

S1	00-03	01-02	10-13	11-12	20-23	21-22	30-33	31-32	Σ
ΔX = 11 (03)	1	0	1	3	0	1	0	1	7
S2	00-32	01-33	02-30	03-31	10-22	11-23	12-20	13-21	Σ
ΔX = 29 (32)	0	0	0	2	0	1	0	1	4
S2	00-32	01-33	02-30	03-31	10-22	11-23	12-20	13-21	Σ
ΔX = 2B (32)	2	0	0	0	0	0	2	0	4
S3	00-20	01-21	02-22	03-23	10-30	11-31	12-32	13-33	Σ
ΔX = 26 (20)	0	0	1	3	0	1	0	0	5

С целью дальнейшего сокращения количества значащих ячеек таблицы можно сгруппировать те из них, которые имеют идентичные наборы «статических швов», т.е. левая и правая двухбитные пары

которых совпадают. Полученная после такого преобразования таблица (см. строки блока S2 таблицы 3) может использоваться в качестве альтернативы таблицы 1. В такой таблице количество значащих ячеек для некоторого перехода (одноблочной характеристики) может принимать значения: 4 (входная разность по обоим «швам» отлична от 0), 8 (входная разность по одному из «швов» равна от 0), 16 (входная разность по обоим «швам» равна 0). Такое деление следует из того, что любая отличная от нуля 2-битная разность может быть получена из двух различных пар 2-битных значений. Таким образом, если разность по некоторому «шву» отлична от нуля, то по этому «шву» возможно только два варианта вероятности «сшивки», в противном случае - четыре.

При вычислении вероятности фиксированной многоблочной характеристики для крайних S-блоков можно объединить ячейки, отличающиеся только неиспользуемым «пассивным швом» (между активным и пассивным S-блоком). Получим таблицу 3.

Таблица 3

S1	00-03, 10-13, 20-23, 30-33		01-02, 11-12, 21-22, 31-32		Σ
ΔX = 11 (03)	1+1+0+0		0+3+1+1		7
S2	00-32, 02-30	01-33, 03-31	10-22, 12-20	11-23, 13-21	Σ
ΔX = 29 (32)	0+0	0+2	0+0	1+1	4
S2	00-32, 02-30	01-33, 03-31	10-22, 12-20	11-23, 13-21	Σ
ΔX = 2B (32)	2+0	0+0	0+2	0+0	4
S3	00-20, 01-21, 02-22, 03-23		10-30, 11-31, 12-32, 13-33		Σ
ΔX = 26 (20)	0+0+1+3		0+1+0+0		5

По таблице 3 легко рассчитать вероятность выполнения выбранной характеристики для произвольного подключа. В таблице 4 в столбце $p^{<1>}$ приведены вероятности выполнения двух рассматриваемых одноцикловых характеристик для различных вариантов вектора «ключевого смещения» (столбец *dk*), а в столбце keys указан процент подключей, для которых вероятность имеет указанное значение. В столбце $p^{<13>}$ приведены предельные значения вероятности осуществления атаки на полный вариант алгоритма (с помощью модифицированной 2R-атаки количество циклов понижается с 16 до 13 [2]). Предельное значение получается, если на всех активных циклах значения векторов «ключевого смещения» *dk* попадают в одну группу (принадлежат одной строке), т.е. если вероятность одноцикловой характеристики на всех активных циклах постоянна.

Таким образом, получаем, что вероятность лучшей дифференциальной криптоатаки на DES при стандартных таблицах подстановки для ряда ключей составит 2^{-43}, однако, для другой группы ключей (такой же размерности) вероятность снизится до 2^{-55}, т.е. будет соответствовать сложности «силовой атаки». В случае наиболее вероятной ситуации – когда для половины активных циклов (трёх) вероятность рассмотренной характеристики равна $112/2^{14}$, а для другой половины $28/2^{14}$ – вероятность полноцикловой характеристики будет равна 2^{-49}, что несколько ниже значения 2^{-47}, приведенного в работе Э. Бихама [2]. Значение 2^{-47} может быть получено, если вероятность одноцикловой характеристики принять равной среднему от двух фактически возможных значений: $112/2^{14} \times 8/16 + 28/2^{14} \times 8/16 = 70/2^{14}$.

Таблица 4

ΔX	$p^{<1>}$	$p^{<13>}$	keys	*dk*							
19600000	$28/2^{14}$	2^{-55}	8 / 16	00	02	10	12	20	22	30	32
	$112/2^{14}$	2^{-43}	8 / 16	01	03	11	13	21	23	31	33
1B600000	$112/2^{14}$	2^{-55}	8 / 16	00	02	10	12	20	22	30	32
	$28/2^{14}$	2^{-43}	8 / 16	01	03	11	13	21	23	31	33

Учитывая вид двух полученных групп «ключевого смещения», получим, что для обеих характеристик вероятность определяется одним битом вектора *dk*, т.е. только одной парой битов подключа (k_{12} и k_{14}). Анализ алгоритма развёртывания ключа показывает, что интересующие нас 6 пар битов ключа, соответствующих 6 активным циклам, формируются 11 битами ключа (разряды подключа k_{12} и k_{14} на 3 и 13 циклах соответственно, формируются одним 18-тым битом ключа,

остальные биты не повторяются), т.е. в каждой паре хотя бы один бит уникален. Таким образом, всего для анализируемой атаки возможно 7 вариантов вероятностей, в указанном выше диапазоне, а каждое из предельных значений вероятности возможно на 2^{50} ключей, т.е. на каждом 64-том ключе.

Следует отметить, что рассмотренное свойство было известно разработчикам стандарта (максимальная вероятность рассмотренных характеристик для 16 циклов равна $2^{-57,5}$), это подтверждает список требований к таблицам подстановки, приведенный в [3]. Рассмотрим два из них:

Для любых ненулевых 6-ти битовых различий входов не более чем 8 из 32 пар входов должны показывать одно и то же выходное различие.

Критерий, аналогичный вышеизложенному, но для случая трёх активных *S* блоков.

Первое требование вводит ограничение 8/32=16/64=1/4 на вероятность любой одноблочной характеристики, а второе - следует интерпретировать как ограничение равное $(1/4)^3$ на вероятность трехблочной характеристики для произвольного ключа шифрования, а, следовательно, и вектора «ключевого смещения», т.е. вероятность любой трёхблочной характеристики на произвольном ключе должна быть не хуже произведения предельных одноблочных вероятностей. Слово «аналогично» в последнем требовании можно интерпретировать как ограничение равное $2^{al/2}$ на количество пар, для которых выполняется выбранный переход, где $al = 4 \times a + 2$ – количество входных линий, способных активизировать a соседних S-блоков. Следовательно, предельная вероятность характеристики состоящей из a соседних S-блоков не должна превышать $2^{al/2} / 2^{al-1} = 2^{-2 \times a}$, что соответствует произведению ограничений a одноблочных характеристик.

Из всего выше изложенного следует, что традиционная методика оценки вероятностей дифференциальных атак не учитывает зависимость вероятностей характеристик от ключа шифрования, и поэтому не даёт возможность оценить реальную степень опасности отдельных характеристик, т.к. получаемая вероятность является усреднённым значением. Это связано с некоторым упрощением реальной схемы цикловой функции F, имевшем место при построении математической модели, удобной для описания дифференциального криптоанализа. Оригинальная методика игнорирует факт большей размерности циклового подключа по сравнению с размерностью входного блока данных и факт наличия «статической связи» между соседними S-блоками. Предложенная в статье методика свободна от этих недостатков и позволяет определить не только наиболее эффективную характеристику, но и множество ключей, на которых её вероятность будет максимальна.

Рассмотренное свойство дифференциальных характеристик (способность иметь вероятность, зависящую от применённого ключа шифрования) может проявляться и при других, отличных от DES, схемах цикловой функции. Это свойство может возникать в случае зависимости вида нелинейного преобразования от ключа шифрования. Также следует отметить другую важную особенность шифра DES – использование небиективных S-блоков (для которых пространство входных значений превышает пространство выходных значений), позволяет достигнуть меньших значений вероятностей дифференциальных характеристик, по сравнению с вариантом использования биективных S-блоков, т.к. в первом случае одноблочные характеристики отдельных S-блоков оказываются взаимосвязаны, и должны включаться в конечную характеристику одновременно.

Список литературы: **1.** *FIPS* PUB 46-2. Specifications for DATA ENCRYPTION STANDARD. U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 1993. **2.** *E. Biham, A. Shamir* Differential Cryptanalysis of the full 16-round DES. Technical Report - Computer Science Department, Technion, Israiel, 1993. **3.** *Schneier B.* 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.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 15.03.2000