УДК 681.3.06

В.И. ДОЛГОВ, д-р техн. наук, И.В. ЛИСИЦКАЯ, канд. техн. наук,
С.А. ГОЛОВАШИЧ, Р.В. ОЛЕЙНИКОВ

ПРИНЦИПЫ ЗАЩИТЫ АЛГОРИТМА DES ОТ АТАК ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА

Настоящая работа снова возвращается к стандарту шифрования DES. Этот алгоритм сегодня считается недостаточно надежным. Виной этому (кроме малой длины ключа и шифруемого блока) стали известные атаки дифференциального и линейного криптоанализа. Названные атаки, родившиеся при изучении стойкости DES, сегодня стали одним из основных инструментов проверки надежности и других используемых и разрабатываемых симметричных шифров. В этих условиях сохраняет значительный научный и практический интерес изучение особенностей и условий проведения успешных криптоаналитических атак в том числе и в уже известных случаях и применительно к известным алгоритмам с целью определения путей и изучения возможностей их перекрытия. В этой работе внимание сосредоточивается на принципах осуществления дифференциального криптоанализа шифра DES.

Известно, что показатели стойкости и возможности проведения криптоаналитических атак для шифра DES и ряда других DES-подобных шифров в первую очередь определяются свойствами используемых в них таблиц подстановок (*S* блоков). Известны также некоторые критерии отбора *S* блоков, которыми пользовались разработчики стандарта. Однако даже эти требования даны без разъяснений (разработчики стандарта считают их своим секретом).

Здесь мы хотим высказать свою версию обоснования требований к отбору *S* блоков, использованных разработчиками стандарта, так как считаем, что нам стали понятны "секреты" построения *S* блоков для этого шифра.

Поскольку изложение материала будет опираться на известные требования к отбору *S* блоков стандарта, полезно будет сразу их напомнить. Мы здесь сформулируем эти требования, опираясь на работу [1]. Критерии отбора *S* блоков здесь изложены в такой редакции:

1. Каждый *S* блок имеет 6 входных и 4 выходных бита.
2. Нет выходного бита *S*- блока, который может быть связан функцией, близкой к линейной с входными битами.
3. Если зафиксированы самый левый и самый правый биты в *S* блоке и меняется 4 средних бита, то каждый из возможных 4-х битовых выходов получается точно один раз.
4. Если два входа *S* блока отличаются точно одним битом, то выходы должны отличаться не менее чем в 2-х битах.
5. Если два входа *S* блока отличаются точно в двух средних битах, то выходные биты должны отличаться не менее чем двумя битами.
6. Если два входа *S* блока отличаются своими первыми двумя битами и имеют совпадающими 2 последних бита, то выходные биты не должны быть теми же самыми.
7. Для любых ненулевых 6-ти битовых различий между входами не более чем 8 из 32 пар входов могут показывать одни и те же выходные различия.
8. Критерий, подобный вышеизложенному, должен выполняться и в случае трех активных *S* блоков.

Будет показано, что подавляющее большинство из этих требований (шесть из восьми) подчинено именно стремлению обеспечить защиту от атак дифференциального криптоанализа.

Для более подробного знакомства с идеями дифференциального криптоанализа отошлем читателя к работам [1,2], а также некоторым разъяснениям [3,4,5]. Заострим сразу внимание на одном из принципиальных моментов: эффективность дифференциальной атаки для алгоритма DES в значительной мере определяются свойствами так называемых таблиц распределения побитовых разностей *S* блоков.

Для построения этих таблиц используется следующая методика: перебираются все возможные пары 6-битных чисел (от 0 до 63), которые подаются на вход *S* блока. Соответственно на выходе получаются различные комбинации 4-битных чисел от 0 до 15. Далее вычисляются поразрядные суммы по модулю 2 соответствующих пар входных и выходных значений. Полученные числа (входные и выходные разности) являются индексами входов в ячейки таблицы размером 64x16 соответственно по строкам и по столбцам. Сама таблица распределения побитовых разностей формируется заполне-

нием ячеек числами, соответствующими количествам попаданий в каждую из них при вариации по всему множеству значений входов S блока (для фиксированной входной разности).

Элемент таблицы характеризует вероятность появления некоторой побитовой разности на выходе S блока (разности для пары выходов) при поступлении на его вход фиксированной входной разности. А уже по вероятностям выходных разностей S блоков для каждой из них приписываются вероятности отдельным битам ключа (оказывается, что для любой заданной входной разности не все значения выходных разностей являются равновероятными [1]). В работах [1-5] взаимосвязь входов с выходами нескольких S блоков названа характеристикой, которая может быть распространена на несколько циклов (в последнем случае мы ее будем называть также дифференциальной характеристикой). Пока вероятность соответствующей характеристики меньше некоторого порогового значения, дифференциальный криптоанализ неэффективен (его сложность получается большей, чем прямой перебор всех ключей). Как только находится характеристика с вероятностью, большей пороговой, дифференциальный криптоанализ становится атакой, с которой уже надо считаться.

Дальнейшие рассуждения ведутся в предположении, что читатель знаком с отмеченными ранее работами. Основой развиваемого подхода станет детальное изучение самой техники реализации дифференциальных атак. Сейчас нас будет интересовать процесс построения дифференциальных характеристик для некоторого заданного набора S блоков.

Будем сразу ориентироваться на вариант атаки на 16-цикловый DES, описанной в [3]. Эта атака использует итеративную характеристику, строящуюся с помощью "обнуляющего" разностного преобразования. Так мы назвали выполнение одноциклового преобразования, при котором ненулевая разность на входе цикловой функции F преобразуется в нулевую разность на ее выходе. Если обозначить разность на входе S блока $\bar{\Delta}$, то речь идет о характеристиках, для которых входная разность $\bar{\Delta} \neq \bar{0}$ с некоторой вероятностью $p \neq 0$ преобразуется в выходную разность $F(\bar{\Delta}) = \bar{0}$. В сочетании с тривиальным циклом (в котором входная и выходная разности равны нулю) такое преобразование позволяет реализовать двухцикловую характеристику вида $\Omega_P = (\bar{\Delta},\bar{0}) \rightarrow \Omega_T = (\bar{0},\bar{\Delta})$, представленную на рис. 1. Здесь мы пользуемся символикой и обозначениями, введенными в работе [3]: Ω_P и Ω_T обозначены соответствующие значения разностей, а (x,y) – конкатенация разностей для левого и правого полублоков, данных на входе и выходе рассматриваемых циклов.

Приведенная характеристика может быть циклически продолжена необходимое количество раз. Именно в этом случае при проведении атаки удается реализовать максимально возможное число тривиальных циклов, что позволяет осуществить эффективную атаку на 16-цикловый DES (в атаке

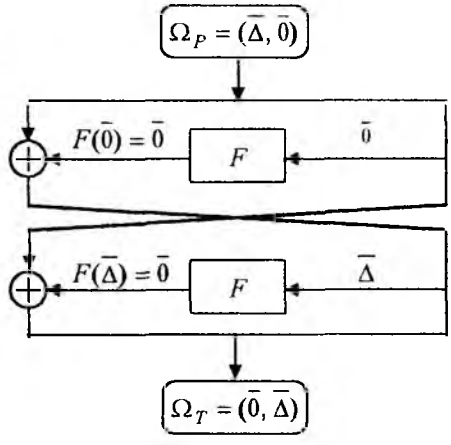


Рис.1

применяется 13-цикловая характеристика на циклах со 2-го по 14-й со специально подобранным первым циклом и последующая $2R$-атака на 15-м и 16-м циклах). Как уже отмечалось ранее в [5], в этой атаке на каждом цикле используется одновременно три активных S блока. Если вероятность трехблочной 2-цикловой (с учетом тривиального преобразования) характеристики обнуляющего типа обозначить p_T, то для вероятности 13-цикловой характеристики, получающейся в результате итеративного повторения трех-

блочной характеристики шесть с половиной раз при $p_T = \frac{1}{234}$, получается результат [3]

$$(p_T)^{\frac{n-4}{2}} = p_T^6 = 2^{-47,2}. \quad (1)$$

Этот результат позволяет Эли Бихаму, имея $\approx 2^{48}$ отобранных открытых текстов, предложить эффективную процедуру определения ключей шифрования, которая оказывается существенно менее сложной, чем их прямой перебор (заметим, что все расчеты здесь ведутся в предположении статистической независимости 6-битных входных разностей смежных S блоков).

Нашей ближайшей задачей и будет изучение свойств таблиц побитовых разностей для S блоков стандарта и установление связи их показателей с достижимыми вероятностями дифференциальных характеристик.

Покажем прежде всего, что для таблиц, использованных в DES, характеристики с меньшим числом активных S блоков, по мнению разработчиков (на момент создания стандарта), либо нереализуемы, либо сложность дифференциального криптоанализа превышает прямой перебор всех ключей.

Для большей наглядности изложения полезно будет сразу привязаться к реальному виду таблиц побитовых разностей S блоков для шифра DES. Ниже приведен пример построения такой таблицы для первого S блока стандарта (отметим, что расположение строк в нашей таблице несколько иное, чем в оригинальной работе [2]. Обозначения входов в таблицу представлены в шестнадцатеричной системе счисления, адаптированной к правилам пользования таблицами стандарта, описанным в [6]. Вход по строкам таблицы ab_x соответствует 6-битному вектору входной разности $\overline{\Delta} = (\Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_5, \Delta_6)$, где a представляет собой шестнадцатеричную запись двоичного числа $\Delta_1\Delta_6$, а b – числа $\Delta_2\Delta_3\Delta_4\Delta_5$.

Таблица 1

Входная разность	Выходная разность															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
2	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
3	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
4	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
5	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
6	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
7	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
8	0	0	0	0	0	0	2	14	0	6	6	12	4	6	8	6
9	0	8	4	2	6	6	4	6	6	4	2	6	6	0	4	0
a	0	8	8	0	10	0	4	2	8	2	2	4	4	8	4	0
b	0	8	10	8	0	2	2	6	10	2	0	2	0	6	2	6
c	0	6	6	0	8	4	2	2	2	4	6	8	6	6	2	2
d	0	6	4	0	4	6	6	6	6	2	2	0	4	4	6	8
e	0	10	10	6	6	0	0	12	6	4	0	0	2	4	4	0
f	0	2	6	0	14	2	0	0	6	4	10	8	2	2	6	2
10	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
11	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
12	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
13	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
14	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
15	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
16	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
17	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
18	6	8	2	4	6	4	8	6	4	0	6	6	0	4	0	0

Продолжение таблицы 1

Входная разность	Выходная разность															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
19	2	4	4	6	2	0	4	6	2	0	6	8	4	6	4	6
1a	0	4	6	4	2	2	4	10	6	2	0	10	0	4	6	4
1b	4	4	6	0	10	6	0	2	4	4	4	6	6	6	2	0
1c	2	6	2	4	0	8	4	6	10	4	0	4	2	8	4	0
1d	4	4	2	4	10	6	6	4	6	2	2	4	2	2	4	2
1e	4	2	4	0	8	0	0	2	10	0	2	6	6	6	14	0
1f	2	4	10	6	2	2	2	8	6	8	0	0	0	4	6	4
20	0	0	0	10	0	12	8	2	0	6	4	4	4	2	0	12
21	10	4	6	2	2	8	2	2	2	2	6	0	4	0	4	10
22	12	0	0	2	2	2	2	0	14	14	2	0	2	6	2	4
23	0	0	4	10	10	10	2	4	0	4	6	4	4	4	2	0
24	12	2	2	8	2	6	12	0	0	2	6	0	4	0	6	2
25	4	2	4	6	0	2	8	2	2	14	2	6	2	6	2	2
26	4	2	2	4	0	2	10	4	2	2	4	8	8	4	2	6
27	6	6	2	2	0	2	4	6	4	0	6	2	12	2	6	4
28	0	4	6	0	12	6	2	2	8	2	4	4	6	2	2	4
29	4	2	6	4	4	2	2	4	6	6	4	8	2	2	8	0
2a	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6
2b	2	6	2	2	8	0	2	2	4	2	6	8	6	4	10	0
2c	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10
2d	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	0
2e	0	10	4	0	12	0	4	2	6	0	4	12	4	4	2	0
2f	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
30	0	4	2	4	4	8	10	0	4	4	10	0	4	0	2	8
31	0	4	4	8	0	2	6	0	6	6	2	10	2	4	0	10
32	6	4	4	12	4	4	4	10	2	2	2	0	4	2	2	2
33	10	4	2	0	2	4	2	0	4	8	0	4	8	8	4	4
34	4	2	2	10	0	2	4	0	0	14	10	2	4	6	0	4
35	12	2	2	2	4	6	6	2	0	2	6	2	6	0	8	4
36	6	2	6	2	8	4	4	4	2	4	6	0	8	2	0	6
37	2	2	2	2	2	6	8	8	2	4	4	6	8	2	4	2
38	4	8	2	10	2	2	2	2	6	0	0	2	2	4	10	8
39	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4
3a	2	2	4	0	8	0	0	0	14	4	6	8	0	2	14	0
3b	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4
3c	6	2	2	4	12	6	4	8	4	0	2	4	2	4	4	0
3d	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2
3e	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4
3f	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

Рассмотрим некоторый произвольно взятый S блок. Пусть $\overline{\Delta} = (\Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_5, \Delta_6)$ – разность на входе S блока, где Δ_i, $i = \overline{1,6}$ – отдельные биты этой разности. Легко убедиться в том, что цикловая функция $F(\overline{\Delta}) = \overline{0}$ с одним активным S блоком для таблиц, составленных из перестановок (что гарантирует выполнение требования 3, использованного разработчиками стандарта), вообще неосуществима.

Действительно, в соответствии с таблицей расширения E первый, второй, пятый и шестой биты входов каждого из S блоков становятся входными битами и соседних S блоков, и их ненулевые значения всегда активизируют соседние S блоки. В результате можно сделать вывод, что одноблочную характеристику в рассматриваемом случае можно пытаться строить лишь для значений входных разностей (6 - битных входов S блоков) вида $\overline{\Delta} = (0, 0, x, y, 0, 0)$. Но входные разности этого вида определяются парами входов в таблицы S блоков, которые формируют их выходы путем выбора различных элементов из одной и той же строки таблицы подстановок (a = 0). Очевидно, что для строки в

виде перестановки (размещения без повторений элементов) все 64 возможные пары входов, формирующих разность $\bar{\Delta}$ (три допустимых варианта входных различий: (0, 0, 0, 1, 0, 0) $\rightarrow 2_x$, (0, 0, 1, 0, 0, 0) $\rightarrow 4_x$ и (0, 0, 1, 1, 0, 0) $\rightarrow 6_x$), будут давать несовпадающие выходы. Поэтому вероятности этих переходов для одного активного S блока равны нулю (в табл.1 для входных разностей 2_x, 4_x, 6_x число возможных нулевых выходных разностей равно 0). Следовательно, обнуляющую характеристику $F(\bar{\Delta}) = \bar{0}$ с одним активным S блоком и ненулевой вероятностью для таблиц, состоящих их перестановок, построить нельзя. Заметим, что использование числовых конструкций типа перестановок обеспечивает во всех таблицах побитовых разностей только ненулевые выходные разности для всех входных разностей от 1_x до F_x. Отметим также следствие из полученного результата: многоблочные характеристики, использующие "обнуляющее" разностное преобразование, могут строиться только из смежных или групп смежных S блоков.

Рассмотрим теперь возможность построения атаки, использующей один активный S блок при $F(\bar{\Delta}) \neq \bar{0}$. Опять нас должны интересовать входные разности S блоков вида $\bar{\Delta} = (0, 0, x, y, 0, 0)$. В этом случае снова возможны три ненулевых значения входов (опять это входы 2_x, 4_x, 6_x).

Очевидно, что во всех этих случаях для построения одноблочных характеристик допустимыми являются только однобитные переходы (переходы в однобитные выходные разности), так как из-за завершающей цикловую функцию P перестановки два и более битов на выходе любого S блока будут активизировать на следующем цикле сразу несколько S блоков. Причем этот один бит при проходе S блоков на разных циклах не должен попадать на входы, общие для двух соседних S блоков. Приведем для иллюстрации (см. рис. 2) возможные варианты прохождения битов через S блоки, учитывающие конкретный вид P перестановки [6] и отмеченное выше ограничение.

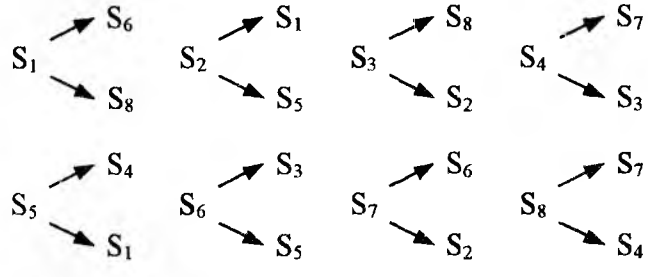


Рис. 2

Легко видеть, что для шифра DES характеристику с однобитными переходами построить не удается, так как однобитный выход текущего S блока, объединяясь через цепь Фестеля с однобитным входом S блока предыдущего цикла, всегда будет приводить к двухбитной разности на входе очередного цикла, т.е. будут активизироваться сразу два S блока.

Перейдем к изучению условий реализации двухблочных характеристик. Опять рассмотрим сначала характеристики, строящиеся с помощью "обнуляющего" разностного преобразования. Их, как уже отмечено выше, можно пытаться строить только для смежных S блоков. Для характеристики с двумя активными соседними S блоками необходимо уже рассматривать 10-битные входные разности

$$\bar{\Delta} = \left(\underbrace{\Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_5, \Delta_6}_{\text{входы левого } S \text{ блока}}, \underbrace{\Delta_7, \Delta_8, \Delta_9, \Delta_{10}}_{\text{входы правого S блока}} \right).$$

Здесь опять из условия сохранения на каждом цикле именно двух активных S блоков необходимо рассматривать входные разности, удовлетворяющие условию: $\Delta_1 = \Delta_2 = \Delta_9 = \Delta_{10} = 0$. Далее легко убедиться, что для получения двухблочной обнуляющей характеристики необходимо, чтобы $\Delta_5 = \Delta_6 = 1$, так как при одном из ненулевых значений этих битов вероятность дифференциальной обнуляющей характеристики одного из S блоков равна нулю (для таблиц дифференциальных разностей S блоков с перестановками вероятности переходов всех входов от 1_x до F_x в выходную разность 0_x равны нулю). Тогда для получения двухблочной характеристики можно использовать только входные разности вида (0, 0, x, y, 1, 1, z, t, 0, 0). Это будут 16 вариантов сочетаний двух входов (входных разностей), представленные в табл. 2.

Следовательно, для полного запрещения двухблочных характеристик, строящихся с помощью "обнуляющего" разностного преобразования, достаточно таблицы построить таким образом, чтобы по крайней мере для входных разностей 11_x, 13_x, 15_x, 17_x либо для входных разностей 28_x, $2A_x$, $2C_x$, $2E_x$ были запрещенными нулевые выходные разности. В стандарте *S* блоки как раз выбраны так, что для входных разностей 28_x, $2A_x$, $2C_x$, $2E_x$ нулевые выходные разности запрещены (соответствующие пары входов не имеют совпадающих выходов, см. требование 6). Поэтому двухблочных характеристик обнуляющего типа для шифра DES также построить нельзя.

Рассмотрим теперь процесс образования двухблочных характеристик при $F(\bar{\Delta}) \neq \bar{0}$. В этом случае удобно будет воспользоваться достаточно очевидным утверждением.

Таблица 2

Входные разности первого *S* блока	Входные разности второго *S* блока
$(0, 0, 0, 0, 1, 1) \rightarrow 11_x$	$(1, 1, 0, 0, 0, 0) \rightarrow 28_x$
$(0, 0, 0, 1, 1, 1) \rightarrow 13_x$	$(1, 1, 0, 1, 0, 0) \rightarrow 2A_x$
$(0, 0, 1, 0, 1, 1) \rightarrow 15_x$	$(1, 1, 1, 0, 0, 0) \rightarrow 2C_x$
$(0, 0, 1, 1, 1, 1) \rightarrow 17_x$	$(1, 1, 1, 1, 0, 0) \rightarrow 2E_x$

Утверждение. Пусть при построении дифференциальной характеристики на текущем цикле активизируется некоторое заданное число *S* блоков. Тогда для сохранения этого же числа активных *S* блоков на следующем цикле побитовая сумма по модулю два выходов *S* блоков текущего цикла со входами *S* блоков предыдущего цикла должна активизировать это же число *S* блоков.

Справедливость утверждения следует непосредственно из правил построения цикловой функции самого шифра DES (см. конструкцию цикловой функции шифра DES, например, [6]). Выходом цикловой функции шифра DES является сумма по модулю два результата шифрования на текущем цикле правого входного полублока (результата его сложения с ключом и последующего прохождения через *S* блоки и *P* перестановку) с левым полублоком, являющимся входом цикловой функции предыдущего цикла. Но это же правило будет справедливо и для разностей (побитовых сумм по модулю два) входных и выходных блоков цикловой функции (при этом исключается явная зависимость от битов ключа).

Из этого утверждения приходим к следствию: если на текущем цикле активизируется некоторое заданное число *S* блоков, то для того, чтобы на следующем цикле дифференциальной характеристики получить тривиальное преобразование, выходы активизированных *S* блоков текущего цикла должны совпадать со входами активизированных *S* блоков предыдущего цикла.

Пользуясь приведенными правилами, легко убедиться, что можно пытаться строить двухблочные дифференциальные характеристики двух типов:

– с использованием тривиальных переходов (переходов с вероятностью единица);

– без использования тривиальных переходов.

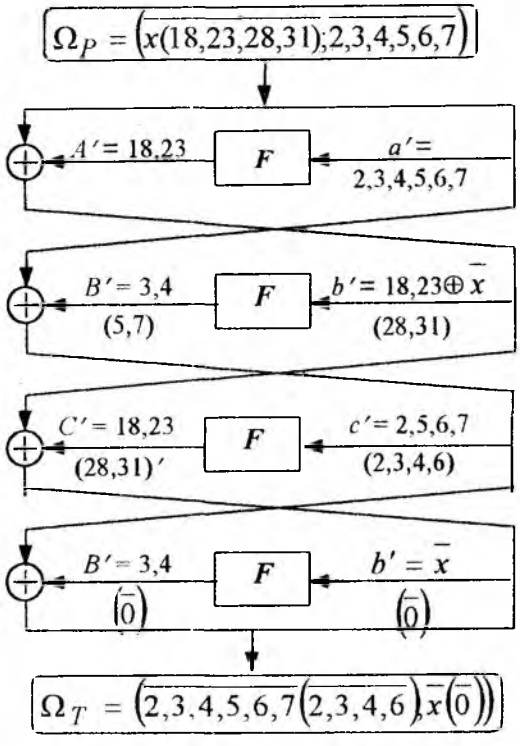
Действительно, рассмотрим процесс построения произвольной характеристики с двумя активными *S* блоками. Пусть для конкретности это будут два первых *S* блока S_1 и S_2, как это показано на рис. 3. Потенциально в активизации этих двух *S* блоков могут участвовать 2, 3, 4, 5, 6 и 7-ой биты 32-битной разности правых полублоков, участвующих в шифровании. На выходе этих *S* блоков (S_1 и S_2) в принципе могут быть задействованными 2, 9, 13, 17, 18, 23, 28, 31 биты (один или два, в зависимости от того,сколько *S* блоков следующего цикла активизирует каждый из них). В соответствии с правилами *P* и *E* преобразований DES из этих битов могут активизировать именно два первых *S* блока (если стремиться прийти к тривиальному преобразованию) только вполне определенные биты (9, 17, 18, 23, 28, 31).

Пусть для конкретности используются ненулевые выходы *S* блоков S_1 и S_2, формирующие 18 и 23 биты (на промежуточном цикле активизируются *S* блоки S_5 и S_6).

В соответствии с приведенным утверждением ненулевое значение $\bar{x}$ в данном случае может включать в себя либо биты, подтверждающие входы *S* блоков S_5 и S_6 (19, 20, 21 и 22 биты), либо биты, компенсирующие один из двух битов 18 или 23 или оба сразу и вводящие вместо них новые биты, активизирующих иную пару *S* блоков (например, 5, 6, 18, 23).

В первом случае на очередном цикле снова активизируются *S* блоки S_1 и S_2, и естественно получается подтверждение (или компенсация) входных битов предыдущих циклов. Во втором – активизируется новая пара *S* блоков (в рассмотренном примере *S* блоки S_7 и S_8). Видно также, что приведенная на рис. 3 характеристика во всех случаях допускает итеративное продолжение. Формированию тривиального перехода в рассматриваемом примере соответствуют условия: либо $\Omega_P = (\overline{0;3,4})$ и тогда

мы приходим к 6-цикловой итеративной характеристике с двумя тривиальными циклами (две различные 3-цикловые характеристики, каждая содержащая тривиальный цикл), либо для много битного входа $\Omega_P = \left(\overline{0};\overline{2,3,4,5,6,7}\right)$ мы приходим к 8-цикловой итеративной характеристике с двумя



Вероятность 16-цикловой характеристики:

$\left(p_Д\right)^{2\cdot 5} = \left(p_Д\right)^{10}$, если $\Omega_P = \left(\overline{0};\overline{3,4}\right)$

и

$\left(p_Д\right)^{3\cdot 4} = \left(p_Д\right)^{12}$, если $\Omega_P = \left(\overline{0};\ \overline{2,3,4,5,6,7}\right)$.

Для $p_Д = \left(\frac{16}{64}\right)^2$ имеем

$$\left(\left(\frac{16}{64}\right)^2\right)^{2\cdot 5} = 2^{-40}.$$

Рис. 3

тривиальными циклами (две 4-цикловых характеристики, содержащие тривиальный цикл каждая (для входа $\Omega_P = \left(\overline{18,23};\overline{2,3,4,5,6,7}\right)$ вторым можно получить тривиальный цикл, при этом вход следующего за тривиальным циклом будет $\Omega_{P'} = \left(\overline{0};\overline{2,3,4,5,6,7}\right)$ и далее ситуация сводится к рассмотренному выше случаю. Точнее, если правый полублок поступающий на вход цикловой функции, содержит более двух битов, инициирующих заданную пару S блоков, то, как следует из рис. 3, имеется возможность построить итеративную двухблочную характеристику с двумя тривиальными циклами.

Формирование тривиального цикла при $\overline{x} = \overline{0}$ (биты левого полублока являются нулями) констатирует приведенное выше следствие. Действительно, таблица P перестановки шифра DES разрешает в этом случае для входа в различные S блоки следующего цикла использовать только по одному выходному биту каждого из S блоков текущего цикла или два выходных бита одного из S блоков текущего цикла (каждый бит на выходе любого S блока попадает на входы различных S блоков следующего цикла). В результате на выходе двух S блоков можно использовать либо один бит (если он после E перестановки оказывается общим для входов сразу двух S блоков), либо два бита (если каждый их битов инициирует свой S блок). Условию подтверждения исходных входов S блоков S_1 и S_2 (входов предыдущего цикла) на выходе текущего цикла в рассматриваемом случае удовлетворяют только 18 и 23 биты (S блоки S_5 и S_6), и никакие другие биты этому условию не удовлетворяют. В результате формируется вход в S блоки очередного цикла, равный нулю, т.е. мы приходим на очередном цикле к использованию тривиального преобразования типа $F(\overline{0}) = \overline{0}$.

Как показывает анализ, главной особенностью характеристик первого типа является непременное использование при их построении циклов, у которых входы в пары активизируемых S блоков содержат не более двух отличающихся битов (иначе не получится эффект компенсации битов при получении тривиального цикла). При этом либо различия с однобитными переходами используются уже на первом (начальном) цикле (у каждого из активизированных S блоков начального цикла ис-

ользуется однобитное выходное различие), либо на первом цикле у одного из S блоков используется вухбитное выходное различие (а у второго используется переход в ноль), но эти два бита, поступают сегда на входы различных S блоков очередного цикла, а у тех в свою очередь активизируются одноитные выходы (выходные различия). В результате во всех случаях при построении двухблочных характеристик с тривиальными переходами используются циклы с однобитными переходами (переходами однобитных различий в однобитные).

Теперь становится понятным, что для того, чтобы сделать не реализуемыми двухблочные (на каждом икле) характеристики, содержащие тривиальные циклы, необходимо, чтобы были запрещены все одноитные переходы. Этому и служит требование 4, использованное разработчиками стандарта (если два вхоа S блока отличаются точно одним битом, то выходы должны отличаться не менее чем в 2-х битах).

Во втором случае двухблочные характеристики можно строить без тривиальных циклов, для чего достаочно использовать входы в S блоки (в два активизируемых S блока), содержащие более двух единичных битов при этом $\bar{x} \neq 0$ (тогда никогда не получится "компенсация" единичных битов на входе цикловой функции).

В рамках рассматриваемого примера на первом цикле уже используется многобитный вход. Для того гобы уйти от однобитного перехода на втором цикле, можно взять левый полублок $\bar{x}$, содержащий биты, опадающие на те же входы S блоков (S блоки S_5 и S_6), что и использованные ранее входы – 18 и 23 биты олжна сохраниться идея активизации на каждом цикле не более двух S блоков). Это могут быть 19, 20, 1, 22 биты. В итоге можно сформировать 3-цикловую характеристику с двумя активными S блоками $_P$ = 19,20,21,22, 2,3,4,5,6,7 $\rightarrow \Omega_T$ = 19,20,21,22, 2,5,6,7, которая также допускает "итеративное" продолжение (3, 4 и 18, 23 биты попарно то компенсируются, то возникают снова). Таким способом могут быть ализованы двухблочные характеристики с переходами $F(\bar{\Delta}) \neq \bar{0}$.

Разработчики стандарта ясно представляли опасность двухблочных характеристик второго типа для защиты шифра от атак, использующих эти характеристики, наложили ограничение на максимально возможное значение выходов таблиц побитовых разностей. Этому служит требование 7, в соответствии с которым допустимое значение выходов таблиц побитовых разностей ограничено значением 16 (не более 8 из 32-х пар 6-битных входов могут показывать одни и те же выходные различия). ледует однако заметить, что разработчики стандарта при разработке требований к отбору S блоков це не владели (либо считали, что другие не владеют) всеми тонкостями проведения дифференциального криптоанализа (речь идет об уменьшении числа циклов до 13, предложенном позднее в атаке ихама) и в своих расчетах ориентировались на 16-цикловые атаки. Именно этим можно объяснить ыбор максимально допустимого значения для таблиц побитовых разностей равного 16. Действиельно, если воспользоваться расчетом вероятности реализации двухблочной 16-цикловой характеригики для самого "благоприятного" с точки зрения криптоаналитика и практически невероятного лучая, когда в каждом цикле удается использовать характеристику с максимальной вероятностью, авной $\frac{8}{32} = \frac{16}{64}$, то для шифра DES можно прийти к оценке

$$\left(\frac{16}{64}\right)^{2\times 16} = \left(\frac{1}{2^2}\right)^{32} = 2^{-64},$$

его казалось бы вполне достаточно для запрещения двухблочных атак.

Однако, если ориентироваться на теперь уже отработанную атаку в виде 13-цикловой характеригики со специально подобранным первым циклом и последующей $2R$ атакой на последних двух иклах, то надо было бы вести расчет так:

$$\left(\frac{16}{64}\right)^{2\times 13} = \left(\frac{1}{2^2}\right)^{26} = 2^{-52}.$$

Это хуже, чем прямой перебор.

Теперь мы подошли к трехблочным характеристикам. Здесь должны рассматриваться 14-битные ходы цикловой функции вида (0, 0, x, y, z, 1, t, p, 1, q, l, m, 0, 0), причем биты z и q не могут быть дновременно равными нулю (т.к. переход в 0 для входной разности вида (0, x_1, x_2, x_3, x_4, 0) невозмоен). Заметим опять, что в атаке могут участвовать только связанные (смежные) S блоки. В табл. 3 представлены все возможные варианты входов S блоков и таблиц разностей, которые могут участво-

вать в формировании трехблочной характеристики (характеристики с тремя активными S блоками). Всего получается $64 \times 3 = 192$ варианта атаки для каждой тройки таблиц, а для шифра в целом $192 \times 8 = 1536$ вариантов.

Расчеты показывают, что необходимо "перекрыть" все трехблочные обнуляющие характеристики, так как при $p_T = \left(\frac{16}{64}\right)^3 = 2^{-6}$ вероятность 16-цикловой характеристики, составленной из 2-цикловых характеристик обнуляющего типа (см. рис. 1), получается равной $(p_T)^8 = 2^{-48}$.

Таблица 3

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

Для перекрытия этих характеристик разработчики шифра DES пошли двумя путями. Основную массу трехблочных обнуляющих характеристик они просто запретили с помощью требования 6 (входы 28_x, $2A_x$, $2C_x$, $2E_x$, 10_x и 20_x во всех таблицах побитовых разностей выбраны с нулевыми вероятностями переходов в выходную разность ноль). В результате из 192 вариантов осталось перекрыть 48 возможных характеристик для каждой тройки смежных таблиц.

Решению задачи перекрытия оставшихся 48 вариантов должно было служить требование ограничивающее число нулевых выходных разностей для трех активных S блоков. Конечно, это требование уже нужно относить не к 6-битным парам входов одного S блока, а к 14-битным парам входов сразу трех активных S блоков, и оно эквивалентно ограничению на максимально допустимое значение вероятностей хотя бы для одной из одноблочных характеристик, участвующих в формировании трехблочной 3-цикловой характеристики (рис. 1). Как показывает анализ таблиц побитовых разностей S блоков стандарта, при их построении выполнено дополнительное ограничение, в соответствии с которым вероятность хотя бы одного из одноблочных обнуляющих переходов, участвующих в формировании трехблочной характеристики, ограничена значением $\frac{8}{64} = \frac{1}{8}$. При этом значении для вероятности трехблочной 16-цикловой характеристики обнуляющего типа (опять для самого "благоприятного" с точки зрения криптоаналитика случая, когда в каждом цикле удается использовать характеристику с максимальной вероятностью), приходим к результату

$$\left(\left(\frac{16}{64}\right)^2 \cdot \frac{8}{64}\right)^8 = 2^{-56},$$

что сложнее прямого перебора ключей.

Это ограничение используется также для перекрытия трехблочных характеристик с переходами

$F(\bar{\Delta}) \neq \bar{0}$, причем речь идет о характеристиках смешанного типа, когда удается сформировать итеративную 3-цикловую характеристику, включающую один цикл с тремя активными S блоками, второй цикл с двумя активными S блоками и третий цикл тривиального типа. Расчет вероятности такой 15-цикловой характеристики при использовании только ограничения на максимальное значение вероятностей таблиц побитовых разностей приводит к оценочному результату

$$\left(\left(\frac{16}{64}\right)^3 \cdot \left(\frac{16}{64}\right)^2\right)^5 = 2^{-50},$$

т.е. от этих характеристик действительно тоже надо защищаться (анализ показывает, что с учетом ранее рассмотренных ограничений остается только две характеристики такого типа).

Таким образом, нам удалось объяснить практически все требования, использованные разработчиками при построении таблиц стандарта (имеющие отношение к дифференциальному криптоанализу), за исключением требований 5 и 8 (конечно, и они имеют непосредственное отношение к защите от атак дифференциального криптоанализа, но выходят за рамки настоящей работы).

В результате можно сделать вывод, что уже выполнение при построении S блоков требований 3, 4, 6 и 7 вместе с отмеченным дополнительным ограничением, позволяло на время появления стандарта считать его неуязвимым к атакам дифференциального криптоанализа.

Сегодня, однако, предложенных разработчиками стандарта ограничений к отбору S блоков (в том числе и требований 5 и 8) уже оказывается явно недостаточно для безопасности шифра DES, о чем и свидетельствуют расчеты, приведенные в начале статьи.

Понимая теперь слабости S блоков и критериев отбора, предложенных разработчиками стандарта, а также то, что эти слабости обусловлены субъективными причинами (уровнем владения техникой выполнения дифференциальных атак на момент разработки шифра DES, или желанием не делать таблицы с запасом на стойкость), безусловно можно теперь ставить и решать задачи дальнейшего совершенствования методики отбора таблиц S блоков, приведения ее к уровню современной техники выполнения дифференциальных атак.

Представленные в работе результаты позволяют наметить ряд направлений продвижения по этому пути. В качестве таковых видятся следующие:

– снижение допустимого (максимального) значения выходов таблиц побитовых разностей;
– полное запрещение трехблочных характеристик обнуляющего типа;
– введение дополнительных ограничений на трехблочные характеристики с тривиальными переходами;
– оценка дополнительных мер защиты для характеристик с четырьмя активными S блоками;
– учет при оценке опасности атак зависимости от ключевых битов.

Представляется, что исследования в отмеченных направлениях могут позволить повысить устойчивость шифра DES к атакам дифференциального криптоанализа.

Список литературы: 1. *Schneier B.* Applied Cryptography. Second Edition: protocols, algorithms, and Source code in C. Published by John Wiley & Sons. Inc, New York: Chichester Brisbane Toronto Singapore, 1996. 758 p. 2. *Biham E., Shamir A.* Differential Cryptanalysis of the Data Encryption Standard. Springler Verlag, Berlin. 1993. 3. *Biham E., ShamirA.* Differential Cryptoanalysis of the full 16-round DES. Technical Report-Computer Science Department, Technion, Israiel, 1993. 4. *Лисицкая И.В., Головашич С.А., Олешко О.И., Олейников Р.В., Коряк А.С.* Построение таблиц подстановок для стандарта шифрования данных // Проблемы бионики. Вып. 50. С. 185-194. 5. *Лисицкая, И.В., Олейников Р.В., Головашич С.А., Коряк А.С., Олешко О.И.* Анализ стойкости DES - подобных алгоритмов шифрования при использовании таблиц подстановок случайного типа. Радиоэлектроника и информатика 1999. С. 77–81. 6. *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 15.07.99