УДК 681.3.06: 519.248.681

И. В. ЛИСИЦКАЯ, канд. техн. наук, А. С. БОНДАРЕНКО, А. И. КОЛЫБЕЛЬНИКОВ

ОБЕСПЕЧЕНИЕ СТОЙКОСТИ ШИФРА DES К АТАКАМ ЛИНЕЙНОГО КРИПТОАНАЛИЗА. ТРЕБОВАНИЯ К ОТБОРУ S-БЛОКОВ, ЗАЩИЩЕННЫХ ОТ АТАК НА ХАРАКТЕРИСТИКИ ОБНУЛЯЮЩЕГО ТИПА, ЧЕТЫРЕХЦИКЛОВЫЕ И ШЕСТИЦИКЛОВЫЕ ИТЕРАТИВНЫЕ АППРОКСИМАЦИИ

Идея построения S-блоков для шифра DES с улучшенными показателями безопасности по сравнению с таблицами, предложенными разработчиками стандарта, и сегодня многими специалистами в Украине воспринимается с известной долей скептицизма. Вместе с тем, исследования, проведенные в научном коллективе АО Институт Информационных Технологий [1-4], показали, что разработчики стандарта реализовали в своих таблицах далеко не потенциальные характеристики защищенности как в отношении дифференциального (ДК), так и линейного криптоанализа (ЛК). Однако наши проработки по этим вопросам, как оказалось, не являются полностью оригинальными. Практически с момента опубликования идей ДК и ЛК подобные исследования начала вести группа корейских ученых [5-10]. Анализ результатов этих публикаций и сопоставление их с результатами наших исследований показывает, что они во многом пересекаются, хотя, как оказалось, при определении критериев отбора таблиц S-блоков, защищенных от атак ЛК, мы не смогли избежать погрешностей. В этой работе мы хотим возвратиться к анализу уже известных результатов в рассматриваемом направлении (по линейному криптоанализу) и привести наши аргументы по их обоснованию. В дальнейшем полагается, что читатель знаком с работами [11-13], в которых излагаются основополагающие идеи ДК и ЛК, а также с отмеченными выше работами корейских ученых.

Подчеркнем здесь, что общей методологической основой формирования корейскими учеными условий повышения сопротивляемости шифра DES к атакам ЛК, стало выполнение требований к S-блокам, сформулированных разработчиками стандарта [14,5], и решалась задача определения дополнительных ограничений к отбору таблиц подстановок для шифра DES. И мы придерживаемся этой же точки зрения.

В качестве основы дальнейших рассуждений приведем формулировки дополнительных требований к отбору S-блоков в редакции, предложенной корейскими учеными. В работах [7-9] предлагается пять дополнительных критериев (условий) обеспечения невосприимчивости шифра DES к атакам ЛК.

Условие *L*-1 (условие единообразия таблиц распределения линейных аппроксимаций): Значения выходов таблиц распределения линейных аппроксимаций (ТРЛА) для всех S-блоков должны быть меньше, чем 16;

Условие *L*-2 (условие перекрытия 3R итеративных аппроксимаций): $S(x) \neq S(x \oplus 11efg0)$ для любых *efg*.

Здесь $S(x)$ –значение 6-битного входа x произвольного S-блока;

Условие *L*-3 (условие перекрытия 4R итеративных аппроксимаций): Для ТРЛА S-блоков необходимо выполнить следующие (общее число 18 случаев) условия:

- *S*1-блок : $NS_1(4, 4) = NS_1(2, 2) = 0$,
- *S*2-блок : $NS_2(4, 4) = NS_2(2, 1) = 0$,
- *S*3-блок : $NS_3(8, 4) = NS_3(4, 8) = 0$,
- *S*4-блок : $NS_4(8, 4) = NS_4(2, 2) = 0$,
- *S*5-блок : $NS_5(16, 1) = NS_5(8, 8) = NS_5(2, 4) = 0$,
- *S*6-блок : $NS_6(16, 4) = NS_6(4, 8) = NS_6(2, 2) = 0$,
- *S*7-блок : $NS_7(4, 8) = NS_7(2, 1) = 0$,
- *S*8-блок : $NS_8(16, 1) = NS_8(2, 4) = 0$.

Здесь $NS(\alpha, \beta)$ – элементы ТРЛА, которые определяются следующим образом:

$$NS(\alpha,\beta) = \{x \in GF(2)^6 \mid x \bullet \alpha = S(x) \bullet \beta\} - 32,$$

где $\alpha \in GF(2)^6$; $NS(\alpha,\beta)$ – маски входов (по строкам и столбцам) в ТРЛА *S*-блока; # обозначает число раз выполнения соотношения в фигурных скобках. Для элементов $x, y \in GF(2)^n$, $x \bullet y$, обозначает скалярное произведение x и y.

Из остальных вариантов ограничений, рассмотренных корейскими учеными, мы представим их окончательные предложения.

Условие *L*-4 (условие не обнаружения 4R итеративных аппроксимаций): Для $W(\alpha)$, $W(\beta) \le 2$, необходимо, чтобы $|NS(\alpha,\beta)| \le 10$, где, как и ранее, $W(\alpha)$, и $\beta \in GF(2)^4$, $W(\alpha)$,-вес по Хэммингу α.

Условие *L*-5 (условие перекрытия 5R итеративных аппроксимаций): Если $\alpha \neq 10_x$, то для $W(\alpha) = 1$, и $W(\beta_1 \oplus \beta_2) = 1$:

$$|NS_k(\alpha,\beta_1) \cdot NS_k(\alpha,\beta_2)| \le 48$$

Если же $\alpha = 10_x$, то

$$|NS_k(\alpha,\beta_1) \cdot NS_k(\alpha,\beta_2)| \le 48 \text{ для } \beta_1 \oplus \beta_2 = 1,$$

$$|NS_k(\alpha,\beta_1) \cdot NS_k(\alpha,\beta_2)| \le 48, \text{ для } \beta_1 \oplus \beta_2 = 4$$

для $k = 5,8$ и $l = 6$.

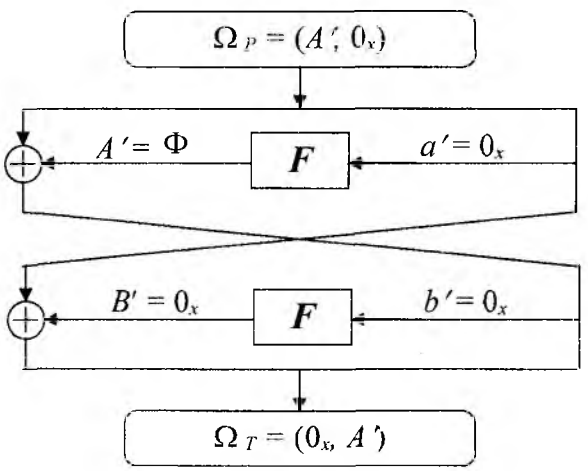
В этой статье мы остановимся на обосновании этих условий.

Прежде всего хотелось бы здесь отметить, что представленные в нашей работе [4] результаты не являются полным решением поставленной в ней задачи. Мы в целом правильно исходили из условия, что в аппроксимационные характеристики не должны входить цикловые преобразования, когда нулевая входная маска 0_x (здесь α_x: шестнадцатеричное значение α) сочетается с выходной маской ненулевого типа (вероятность перехода нулевого входа ТРЛА в ненулевой равна нулю). Но если для одноблочной характеристики это действительно справедливо, то для двух активных S-блоков (S-блоков с ненулевыми входными масками), участвующих в линейном соотношении, может возникнуть ситуация, когда входы соседних S-блоков, за счет расширяющей *E*-подстановки имеют совпадающие биты и тогда для масок, пропускающих эти биты, они в результирующем линейном соотношении будут компенсировать друг друга (входная маска будет эквивалентна нулевой). Именно этот эффект и использован в атаке Девиса, описанной в [12]. Но тогда можно говорить о формировании двухцикловой итеративной характеристики с нулевым входом активного цикла. В обозначениях корейских ученых речь идет об итеративной характеристике типа

$$\Phi \leftarrow 0_x,$$

которая названа ими одноцикловым итеративным линейным выражением. Ее лучше представить в естественном двухцикловом изображении (рис. 1), как это сделано в работе [12].

И здесь мы подходим к обоснованию одного из представленных выше дополнительных ограничений (условий). Нетрудно убедиться, что выполнение условия *L*-2 позволяет рассматривать эти характеристики как не реализуемые (имеющие нулевую вероятность).



$$\Phi \leftarrow 0_x$$
$$0_x \leftarrow 0_x$$

$$17 \oplus 18 \leftarrow 4 \oplus 5$$
$$0_x \leftarrow 0_x$$

Рис. 1

Действительно, в рассматриваемом случае речь идет об использовании трех сочетаний ненулевых входов двух смежных (соседних) S-блоков:

$$S_i(1_x,\beta'), S_{i+1}(10_x,\beta''),$$
$$S_i(2_x,\beta'), S_{i+1}(20_x,\beta''),$$
$$S_i(3_x,\beta'), S_{i+1}(30_x,\beta'').$$

Характеристики, использующие первые два варианта входов, нереализуемы ввиду того, что для ТРЛА всех S-блоков, отобранных по требованиям разработчиков стандарта, выполняется условие:

$$NS_i(1_x,\beta)=NS_i(20_x,\beta)=0 \qquad (1)$$

при любых β. Перекрытие третьей характеристики как раз и обеспечивается выполнением условия L-2, в котором наряду с отмеченными ограничениями разработчиков стандарта ТРЛА S-блоков удовлетворяют дополнительному условию:

$$NS_i(30_x,\beta)=0.$$

При выполнении указанных условий одновременно "перекрываются" и все другие характеристики, использующие нулевой вход активного цикла (для этих характеристик выходы (маски выходов) Г – это выходы S-блоков, формирующие общие входы смежных S-блоков очередного цикла). Четырехцикловая итеративная характеристика такого типа представлена на рис. 2 под номером 0. В результате итеративные характеристики с нулевым входом активного цикла при выполнении требования L-2 запрещены.

Отметим здесь, что рассмотренное ограничение использовалось и в наших исследованиях. Но даже, если исключать из рассмотрения характеристики с нулевым входом активного цикла, то утверждение в работе [4] о том, что в ней сформирована характеристика минимального типа в том смысле, что не существует итеративных характеристик, содержащих большее число циклов тождественного типа. все равно является неверным.

Действительно, кроме рассмотренных выше, существуют итеративные характеристики с числом циклов меньшим, чем 8, в том числе и характеристики, содержащие циклы тождественного типа. Возможные варианты таких характеристик, удовлетворяющие условиям сшивки аппроксимаций соседних циклов, изображенные в манере публикации [5], представлены на рис. 2. И здесь мы подходим к обоснованию одного из представленных выше дополнительных ограничений (условий). Нетрудно убедиться, что выполнение условия L-2 позволяет рассматривать эти характеристики как не реализуемые (имеющие нулевую вероятность).

1	2	3	4
$\Gamma \leftarrow \Phi$ $\Phi \leftarrow 0_x$ $\Gamma \leftarrow \Phi$ $0_x \leftarrow 0_x$	$\Gamma \leftarrow \Phi$ $\Phi \oplus \Theta \leftarrow \Gamma \oplus \Psi$ $\Psi \leftarrow \Phi$ $\Theta \leftarrow \Gamma \oplus \Psi$	$\Gamma \leftarrow \Phi$ $\Phi \leftarrow \Gamma$ $0_x \leftarrow 0_x$ $\Phi \leftarrow \Gamma$ $\Gamma \leftarrow \Phi$ $0_x \leftarrow 0_x$	$\Gamma \leftarrow \Phi$ $\Phi \oplus \Theta \leftarrow \Gamma \oplus \Psi$ $\Psi \leftarrow \Theta$ $\Phi \leftarrow \Gamma$ $\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$ $\Theta \leftarrow \Psi$
4-х цикловая итеративная характеристика	*4-х цикловая итеративная характеристика3*	*6-ти цикловая итеративная характеристика*	*6-ти цикловая итеративная характеристика*

Рис. 2

Предложенные в работе [4] ограничения касаются восьмицикловых итеративных характеристик. Они перекликаются с требованиями, предлагаемыми корейскими учеными, но являются, как теперь стало понятно, недостаточными. Необходимо еще защититься и от атак, построенных на использовании итеративных характеристик с меньшим числом циклов, которые не рассмотрены нами. Основной задачей этой работы и является изучение условий "перекрытия" характеристик, представленных на рис. 2.

Прежде всего заметим, что, как следует из рис. 2, в принципе возможны как итеративные характеристики, состоящие только из активных циклов, у которых S-блоки всех циклов участвуют в построении линейной аппроксимации, так и характеристики с переходами $0_x \leftarrow 0_x$, содержащие циклы "тождественного" типа. Другая особенность рассматриваемых характеристик заключается в том, что значения входов в циклы (левых частей характеристик) фиксированы, в то время, как значения

выходов (правых частей характеристик) являются свободными (в пределах используемой композиции выходов, задействованных S-блоков). Общим для всех итеративных характеристик с числом циклов большим 2, так как возможны линейные итеративные аппроксимационные характеристики только с четным числом циклов, является использование при их построении циклических переходов между одноименными S-блоками.

Изучим сначала возможности и требования по перекрытию четырехцикловой итеративной характеристики под номером 1 (рис. 2). Расчеты показывают, что необходимо "перекрыть" характеристики такого типа с числом активных S-блоков (приходящихся на четырехцикловую характеристику) меньшим семи (шесть и меньше):

$$\left[\left(\frac{16}{64}\right)^6 \cdot 2^5\right]^4 \cdot 2^3 = 2^{-25}, \left[\left(\frac{16}{64}\right)^7 \cdot 2^6\right]^4 \cdot 2^3 = 2^{-29}.$$

Как следует из рис. 2, главной особенностью четырехцикловых характеристик рассматриваемого типа является использование двух пар циклов с идентичными входами. Это значит, что нас должны интересовать итеративные характеристики 1 (рис. 1), составленные из двух пар одноблочных циклов или пары одноблочных и пары двухблочных циклов. Еще одной особенностью рассматриваемых характеристик следует считать то, что они допускают с точностью до порядка следования циклов еще два варианта представления, которые вместе с соответствующими им графами переходов приведены на рис. 3.

Рассмотрим сначала условия реализации характеристики 1.1 (рис. 3). Отметим, что для ее осуществления, как следует из рис. 3, одновременно должны выполняться два перехода: $\Phi \oplus \Theta \leftarrow \Gamma \oplus \Psi$ и $\Theta \leftarrow \Gamma \oplus \Psi$, а, следовательно, должен выполняться один из переходов $\Phi \leftarrow \Psi$ и $\Phi \leftarrow \Gamma$ или оба эти перехода должны выполняться вместе. В результате, с учетом существования для данной характеристики переходов $\Gamma \leftarrow \Phi$ и $\Psi \leftarrow \Phi$, приходим к выводу, что для получения ЛАХ рассматриваемого типа должен выполняться один из циклических переходов $\Phi \leftarrow \Gamma \leftarrow \Phi$, $\Phi \leftarrow \Psi \leftarrow \Phi$ или оба вместе, и при этом должны быть допустимыми переходы $\Theta \leftarrow \Gamma$ и $\Theta \leftarrow \Psi$ (Θ не входит в циклический переход и поэтому может выбираться из выходных битов S-блока, имеющего вход $\Gamma \oplus \Psi$). Именно из этих соображений построен граф переходов для этой характеристики, представленный под соответствующим номером на рис. 3.

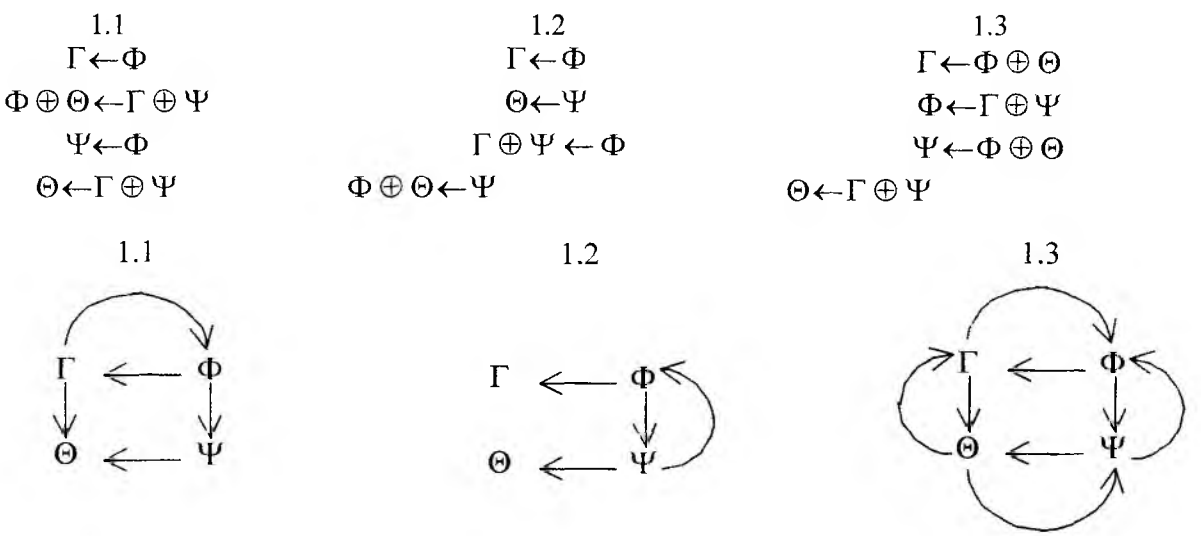


Рис. 3

Будем сначала считать, что каждый из символов в обозначении характеристик представляет собой один бит циклового входа или выхода. Назовем такие характеристики минимальными, только теперь в это понятие будем вкладывать тот смысл, что они формируются с помощью минимального числа ненулевых битов. Очевидно, что для характеристик минимального типа переходы $\Gamma \leftarrow \Phi$ и $\Psi \leftarrow \Phi$ одно-

блочные. Тогда, если Ф - это входы однотипных S-боков, то из-за *P*-перестановки, использованной в шифре DES, выходы Г и Ψ могут стать входами только разных S-блоков, и, следовательно, переходы $\Theta \leftarrow \Gamma \oplus \Psi$ и $\Phi \oplus \Theta \leftarrow \Gamma \oplus \Psi$ являются двухблочными. Получается, что должен быть справедливым двухблочный переход (цикл) $\Theta \leftarrow \Gamma \oplus \Psi$, для которого два различных (разнесенных) S-блока имеют общий однобитный выход Θ, что для шифра DES может быть только в том случае, если Θ – это выход одного из S-блоков, а выход второго S-блока имеет нулевое значение. Такие переходы для шифра DES имеют вероятность, равную нулю. Но выход Θ в рассматриваемой характеристике имеет свободу выбора, и поэтому он может быть выбран многобитным (для характеристики не минимального типа). Отметим теперь, что многобитными (в пределах выходов задействованных S-блоков) могут быть и выходы (маски выходов) одноблочных циклов. Результирующая характеристика получается шестиблочной и, следовательно, должна быть запрещена. Примеры построения четырехцикловых характеристик типа 1.1 приведены на рис. 4. Справа для каждой из характеристик построчно приведены значения числа активных S-блоков, участвующих в формировании цикла.

1.1.1

(14,25),3 ← 17 1

(2,9,13,18,23,31),17,28,31 ← 3,8 2

(14,25),8 ← 17 1

(2,9,13,18,23,31),17,28,31 ← 3,8 2

1.1.2

(14,25),3 ← 17,18 1

(2,9,13,23,31),17,18,28,31 ← 3,8 2

(14,25),8 ← 17,18 1

(2,9,13,23,31),28,31 ← 3,8 2

1.1.3

28 ← 5 1

(21,27),5,15 ← 28,31 1

31 ← 5 1

(21,27),15 ← 28,31 1

1.1.4

(2,9,13,17,18,23),28 ← 5 2

(21,27),5,15 ← 28,31 1

(2,9,13,17,18,23),31 ← 5 2

(21,27),15 ← 28,31 1

1.2.1

(9,31),23 ← 3 1

(14,25),8 ← 17 1

(9,31),17,23 ← 3 1

(14,25),3,8 ← 17 1

1.2.2

(9,31),23 ← 3 1

(1,10,14,20,25,26),8 ← 17 2

(9,31),17,23 ← 3 1

(1,10,14,20,25,26),3,8 ← 17 2

1.2.3

4 ⊕11 ⊕ 19 ← 21 1

5 ⊕ 15 ⊕ 27 ← 29 1

4 ⊕11 ⊕ 19 ⊕ 29 ← 21 1

5 ⊕ 15 ⊕ 21 ⊕27 ← 29 1

1.2.4

4 ⊕11 ⊕ 19 ← 21 (20.22,23,24,25) 1

5 ⊕ 15 ⊕ 27 ← 29 1

4 ⊕11 ⊕ 19 ⊕ 29 ← 21 1

5 ⊕ 15 ⊕ 21 ⊕27 ← 29 (28,30,31,32,1)1

Рис. 4

Если Ф – это входы разных S-боков, где Ф – это общий бит входа двух смежных S-блоков, то выходы Г и Ψ могут быть только входами в однотипные S-блоки и тогда четырехцикловая характеристика минимального типа будет одноблочной. В этом случае при построении характеристик используются пары циклических (однобитных) переходов, имеющих общий бит (Ф). Пример построения такой характеристики также приведен на рис. 4 (см. пример 1.1.3). При использовании для построения характеристик циклических переходов с большим, чем в случае однобитного циклического перехода числом S-блоков, они могут содержать и больше четырех задействованных S-блоков (см. пример 1.1.4).

Рассмотрим теперь условия реализации характеристики 1.2 (рис. 3). Из графа переходов, соответствующего этой характеристике, также представленного на рис. 3, следует, что эта характеристика строится с использованием циклического перехода $\Phi \leftarrow \Psi \leftarrow \Phi$. Легко убедиться, что для однобитного циклического перехода $\Phi \leftarrow \Psi \leftarrow \Phi$ существует характеристика минимального типа, которая будет одноблочной. Примеры построения подобных характеристик также приведены на рис. 4.

Именно одноблочные характеристики будут представлять наибольшую опасность во всех рассмотренных случаях, и поэтому они должны быть перекрыты в первую очередь. Как показывает анализ, ограничения, предложенные корейскими учеными, не учитывают рассмотренные характеристики. Некоторые из возможных характеристик, правда, попадают под ограничение *L*-5, которое введено для 10-цикловых характеристик.

Для перекрытия указанных выше четырехцикловых итеративных характеристик минимального и не минимального типа можно воспользоваться тем, что все они, как уже было отмечено выше, состоят из двух пар циклов с идентичными входами. Причем, как следует из приведенных рассуждений и примеров (рис.4), входы в пары циклов могут быть как однобитными, так и двухбитными. С учетом принципа формирования линейных аппроксимаций для перекрытия таких характеристик можно воспользоваться ограничением, подобным первой части Условия *L*-5, которое предлагается корейскими учеными для перекрытия десятицикловых характеристик (5R итеративных линейных аппроксимаций). Это условие, однако, мы переформулируем в виде двух новых. В дальнейшем будем пользоваться обозначениями дополнительных условий в виде символов У (Условие) со своими порядковыми номерами в отличии от символов *L*, использованных корейскими учеными. Считая, что первые два условия полностью повторяют предложения корейских ученых, закрепим за ними номера У-1 (*L*-1) и У-2 (*L*-2). Тогда для последующих двух ограничений, относящихся к четырехцикловым итеративным характеристикам, пользуясь оговоренной символикой, можем записать:

Условие У-3′ - условие перекрытия четырехцикловых итеративных характеристик с однобитными входами в однотипные S-блоки. Элементы ТРЛА для пар S-блоков, имеющих входные и выходные маски, удовлетворяющие условию $W(\alpha) = 1$, $W(\beta_1 \oplus \beta_2) = 1$, должны подчиняться ограничению:

$$\left|NS_k(\alpha,\beta_1)\cdot NS_k(\alpha,\beta_2)\right| \le 96.$$

Это условие практически только по форме напоминает условие *L*-5, однако по содержанию является совершенно другим.

Условие У-3″ (условие перекрытия четырехцикловых итеративных характеристик с однобитными входами в различные S-блоки). S-блоки для шифра DES должны выбираться так, чтобы пары элементов ТРЛА, имеющих входные и выходные маски, удовлетворяющие условию $W(\alpha) = 2$, $W(\beta_1 \oplus \beta_2) = 2$, подчинялись ограничению:

$$\left|NS_k(\alpha,\beta_1)\cdot NS_k(\alpha,\beta_2)\right| \le 96.$$

При выполнении указанных условий оценка максимального значения вероятности для 16-ти цикловой характеристики, использующей одноблочные четырехцикловые характеристики рассматриваемого типа, приводит к результату:

$$\left[\left(\frac{96}{64^2}\right)^2\cdot 2^3\right]^4\cdot 2^3 = 2^{-28,3}.$$

Но здесь рассмотрен случай, когда итеративная характеристика повторяется соответствующее число раз без изменений. В то же время в приведенных расчетах не учтена возможность свободного выбора значений правой части ЛАХ для ее начального и заключительного циклов.

Действительно, шестнадцатицикловая характеристика (первая и последняя четырехцикловые характеристики) допускает свободу выбора правой части (входа и выхода), как это проиллюстрировано характеристикой 1.2.4 на рис. 4. Здесь одновременно в одной четырехцикловой характеристике в скобках учтены возможности произвольного задания начального и конечного циклов всей шестнадцатицикловой характеристики и, следовательно, приведенное выше ограничение для первого и последнего циклов не "сработает".

Расчет вероятности такой 16-ти цикловой характеристики (с учетом свободного выбора значений ее входа и выхода) приводит к результату:

$$\left[\left(\frac{96}{64^2}\right)^2\cdot 2^3\right]^3\cdot\left[\left(\frac{96}{64^2}\right)\cdot\left(\frac{16}{64}\right)^2\cdot 2^3\right]\cdot 2^3 = 2^{-26,9},$$

чего уже оказывается недостаточным для защиты от атак на подобные характеристики. Поэтому условия У-3′ и У-3″ необходимо ужесточить. Вместо этих условий предлагается воспользоваться ограничением вида:

Условие У-3 (условие перекрытия четырехцикловых итеративных характеристик). S-блоки для шифра DES должны выбираться таким образом, чтобы для пары элементов ТРЛА, имеющих входные и выходные маски, удовлетворяющие условиям $W(\alpha) = 1$, $W(\beta_1 \oplus \beta_2) = 1$ или $W(\alpha) = 2$, $W(\beta_1 \oplus \beta_2) = 2$, подчинялись ограничению:

$$\left|NS_k(\alpha,\beta_1) \cdot NS_k(\alpha,\beta_2)\right| \le 80.$$

В этом случае, учитывая свободу в выборе значений ЛАХ на ее начальном и заключительном циклах, приходим к оценке вероятности результирующей характеристики:

$$\left[\left(\frac{80}{64^2}\right)^2 \cdot 2^3\right]^3 \cdot \left[\left(\frac{80}{64^2}\right) \cdot \left(\frac{16}{64}\right)^2 \cdot 2^3\right] \cdot 2^3 = 2^{-28,7}.$$

Этот результат уже является вполне приемлемым.

Что касается четырехцикловой характеристики под номером 3 на рис. 3, то здесь не возникает проблем. Из графа ее переходов, приведенного на этом же рисунке, видно, что она для шифра DES не реализуема (для нее нужно, чтобы одновременно выполнялись четыре однобитных циклических перехода с общими битами).

Перейдем к изучению условий перекрытия шестицикловых характеристик, представленных на рис. 2 под номерами 2 и 3.

Легко убедиться, что в этом случае представляют интерес характеристики с числом активных S-блоков, приходящихся на трехцикловую характеристику (половину шестицикловой итеративной характеристики), не превышающем шести (пять и меньше).

И здесь мы приходим к одному из вариантов обоснования условия L-1.

Действительно, трехблочные переходы в каждом из активных циклов не опасны, так как даже при максимально возможном значении вероятности перехода (значения элемента ТРЛА) для каждого из задействованных S-блоков, равном $\frac{16}{64}$, для вероятности всей 15-цикловой характеристики (пятикратном повторе трехцикловой характеристики, а еще более точно – двухкратном повторе шестицикловой итеративной характеристики, продолженной еще на три цикла) имеем:

$$2^4 \cdot \left[2^5 \cdot \left(\frac{16}{64^2}\right)^6\right]^5 = 2^{-7 \cdot 5 + 4} = 2^{-31}$$

в то время как для пятиблочной трехцикловой характеристики рассматриваемого типа соответственно получим:

$$2^4 \cdot \left[2^4 \cdot \left(\frac{16}{64^2}\right)^5\right]^5 = 2^{-6 \cdot 5 + 4} = 2^{-26},$$

что уже является недопустимым значением. Как известно [13], граничным значением вероятности результирующей характеристики, обеспечивающим более высокую эффективность линейного криптоанализа по сравнению с переборной атакой, является $\sqrt{2^{-56}} = 2^{-28}$.

Заметим далее, что при значении вероятности перехода (значения элемента ТРЛА) для каждого из задействованных S-блоков, равном $\frac{18}{64}$, для 16-цикловой характеристики (пятикратном повторении трехцикловой характеристики, а более точно – двукратном повторении шестицикловой итеративной характеристики, продолженной еще на три цикла с дополнительным циклом тождественного типа) с тремя S-блоками в каждом из активных циклов, имеем:

$$2^4 \cdot \left[2^5 \cdot \left(\frac{18}{64}\right)^6\right]^5 = 2^{-25,9}.$$

Это значение уже следует рассматривать как превышающее допустимое (т.е. значение вероятности $\frac{16}{64} = \frac{1}{4}$ для элементов ТРЛА в этом случае действительно является граничным).

Отметим, наконец, что при использовании одноблочной 16-цикловой характеристики рассматриваемого вида для максимально допустимых значений соответствующих элементов ТРЛА S-блоков можно получить оценку:

$$2^4\left[2(p)^2\right]^5 \le 2^{-28} \rightarrow p \le \sqrt[10]{2^{-37}} = 2^{-3,7}. \qquad (2)$$

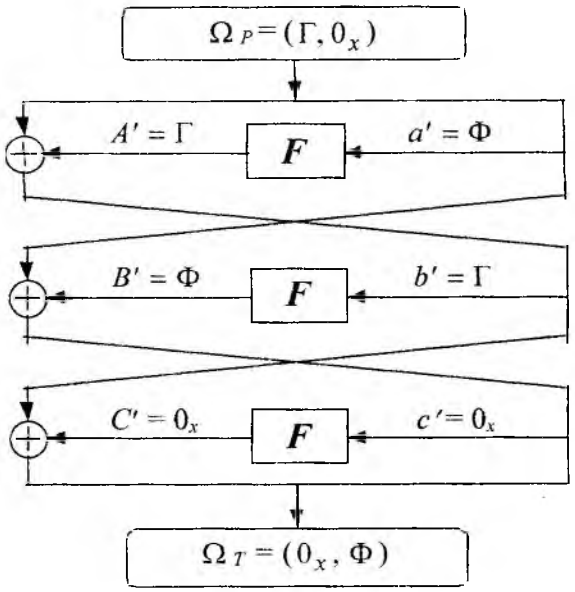
Это значит, что вероятность одноцикловой одноблочной характеристики в рассматриваемом случае ограничена значением 4.

Изучение возможностей атак, строящихся с использованием шестицикловых итеративных характеристик, начнем с рассмотрения трехцикловой характеристики под номером 2 на рис. 2 (половину шестицикловой характеристики). Графическое представление этой характеристики и варианты ее компактного изображения приведены на рис. 5. Сначала рассмотрим характеристики минимального типа, под которыми будем, как уже говорилось ранее, понимать характеристики, использующие для своего построения минимальное число битов (каждый символ – один бит входа или выхода). При такой договоренности характеристика под номером 2.1, рис. 5 будет состоять из одноблочных ненулевых циклов (1+1+0), характеристика 2 имеет вид 1+2+0, т.е. один из активных циклов является одноблочным, а второй – двухблочным, а характеристика 3 может включать 3 или четыре S-блока (имеет вид 1+2+0, 2+1+0 или 2+2+0). Естественно, существуют трехцикловые (шестицикловые) характеристики и с большим числом S-блоков, которые мы рассмотрим позднее.

Прежде всего отметим, что характеристики, интересующего нас типа, могут быть построены на основе использования однобитных переходов S-блоков (переходов одного входного бита маски в один выходной). Напомним, что из-за *P*-перестановки, используемой в шифре DES каждый S-блок может сформировать (инициировать) только однобитные входы S-блоков очередного цикла. Эти S-блоки, в свою очередь, могут только своими однобитными выходами сформировать двухбитный вход исходного (одного) S-блока (сформировать переход $\Gamma \oplus \Psi \leftarrow \Phi$ или переход $\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$).

На рис. 6 приведено распределение битов 32-битного полублока в каждом из циклов преобразования шифра DES, а возможные варианты однобитных переходов, построенных на основе изучения распределения битов рис. 6, перечислены в табл. 1.Пользуясь данными табл. 1 можно рассмотреть для каждого S-блока все переходы, которые могут быть задействованы при построении трехцикловых (шестицикловых) итеративных характеристик. Заметим далее, что переходы с входными масками 1_x и 20_x могут быть сразу исключены из рассмотрения, так как для S-блоков, отобранных по требованиям разработчиков, выполняется условие (1). Тогда для первого S- блока возможны три однобитных перехода $S_1 \Leftrightarrow S_1$:

$$3 \rightarrow 17 \rightarrow 3 : S_1(4_x, 4_x) \Leftrightarrow S_5(10_x, 1_x),$$
$$4 \rightarrow 23 \rightarrow 4 : S_1(2_x, 2_x) \Leftrightarrow S_6(4_x, 8_x),$$
$$5 \rightarrow 31 \rightarrow 5 : S_1(1_x, 1_x) \Leftrightarrow S_8(4_x, 8_x).$$



2.1

$\Gamma \leftarrow \Phi$

$\Phi \leftarrow \Gamma$

$0_x \leftarrow 0_x$

2.2

$\Gamma \oplus \Psi \leftarrow \Phi$

$\Phi \leftarrow \Gamma \oplus \Psi$

$0_x \leftarrow 0_x$

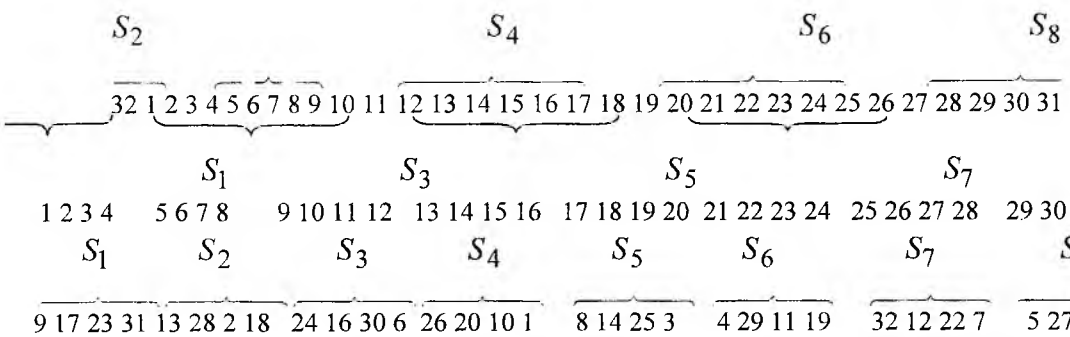
2.3

$\Phi \oplus \Theta \leftarrow \Gamma \oplus \Psi$

$\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$

$0_x \leftarrow 0_x$

Рис. 5



Биты на входах S-блоков и после расширения E

Биты на выходах S-блоков

P- перестановка

Рис. 6

Таблица 1

S-блок S_1	Задействованные переходы	S-блок S_2	Задействованные переходы	S-блок S_3	Задействованные переходы	S-блок S_4	Задействованные переходы
17→1	$S_4(1_x,1_x)$	13→6	$S_3(1_x,1_x)$	16→8	$S_5(20_x,8_x)$	26→12	$S_7(8_x,4_x)$
9→2	$S_2(1_x,2_x)$	28→7	$S_7(2_x,1_x)$	16→10	$S_4(2_x,2_x)$	20→14	$S_5(2_x,4_x)$
17→3	$S_5(10_x,1_x)$	28→5	$S_8(20_x,8_x)$	24→11	$S_6(2_x,2_x)$	1→15	$S_8(1_x,2_x)$
23→4	$S_6(4_x,8_x)$	18→8	$S_5(8_x,8_x)$	24→12	$S_7(20_x,4_x)$	10→16	$S_3(8_x,4_x)$
31→5	$S_8(4_x,8_x)$	2→9	$S_1(8_x,8_x)$	6→13	$S_2(8_x,8_x)$	1→17	$S_1(10_x,4_x)$
S-блок S_5	Задействованные переходы	S-блок S_6	Задействованные переходы	S-блок S_7	Задействованные переходы	S-блок S_8	Задействованные переходы
8→16	$S_3(20_x,4_x)$	29→21	$S_8(10_x,1_x)$	12→24	$S_3(2_x,8_x)$	5→28	$S_2(10_x,4_x)$
3→17	$S_1(4_x,4_x)$	29→22	$S_7(1_x,2_x)$	12→26	$S_4(20_x,8_x)$	21→29	$S_6(10_x,4_x)$
8→18	$S_2(2_x,1_x)$	4→23	$S_1(2_x,2_x)$	32→27	$S_8(2_x,4_x)$	5→31	$S_1(1_x,1_x)$
25→19	$S_6(1_x,1_x)$	11→24	$S_3(4_x,8_x)$	7→28	$S_2(4_x,4_x)$	27→32	$S_7(4_x,8_x)$
14→20	$S_4(8_x,4_x)$	19→25	$S_5(4_x,2_x)$	22→29	$S_6(8_x,4_x)$	15→1	$S_4(4_x,1_x)$

Для того, чтобы сделать одноблочные и двухблочные характеристики, построенные с помощью этих переходов не опасными, достаточно наложить ограничения на два перехода: $S_5(10_x,1_x)$, $S_6(4_x,8_x)$. Остающиеся однобитные переходы включают в себя вход в S-блок с маской 1_x и, следовательно, как уже отмечалось выше, вероятность этого перехода равна нулю.

Для второго S-блока остаются три однобитных перехода $S_2 \Leftrightarrow S_2$:

$$7 \to 28 \to 7: S_2(4_x,4_x) \Leftrightarrow S_7(2_x,1_x),$$
$$8 \to 18 \to 8: S_2(2_x,1_x) \Leftrightarrow S_5(8_x,8_x),$$
$$9 \to 2 \to 9: S_2(1_x,2_x) \Leftrightarrow S_1(8_x,8_x),$$

и здесь по аналогии с предыдущим случаем достаточно наложить ограничения (запретить) на два перехода $S_7(2_x,1_x)$, $S_5(8_x,8_x)$.

Аналогично для переходов $S_3 \Leftrightarrow S_3$ имеем:

$$10 \to 16 \to 10: S_3(8_x,4_x) \Leftrightarrow S_4(2_x,2_x),$$
$$11 \to 24 \to 11: S_3(4_x,8_x) \Leftrightarrow S_6(2_x,2_x),$$
$$13 \to 6 \to 13: S_3(1_x,1_x) \Leftrightarrow S_2(8_x,8_x),$$

и здесь достаточно наложить ограничения на переходы $S_4(2_x,2_x)$, $S_6(2_x,2_x)$.

В случае $S_4 \Leftrightarrow S_4$ получаем четыре варианта переходов:

$$12 \to 26 \to 12: S_4(20_x,8_x) \Leftrightarrow S_7(8_x,4_x),$$
$$14 \to 20 \to 14: S_4(8_x,4_x) \Leftrightarrow S_5(2_x,4_x),$$
$$16 \to 10 \to 16: S_4(2_x,2_x) \Leftrightarrow S_3(8_x,4_x),$$
$$17 \to 1 \to 17: S_4(1_x,1_x) \Leftrightarrow S_1(10_x,4_x).$$

Здесь опять достаточно наложить ограничения на два перехода: $S_5(2_x,4_x)$ и $S_3(8_x,4_x)$.

Действительно, оставшиеся два перехода имеют нулевые вероятности (содержат переходы с входными масками 1_x и 20_x), если их рассматривать как однобитные. Если эти однобитные переходы рассматривать совместно как двухбитный вход $S_4(21_x,8_x)$, то легко убедиться, что для таблиц стандарта выполняется условие: $NS_4(21_x,\beta_x) = 0$, т.е. эта характеристика для S-блоков, отобранных по требованиям разработчиков стандарта, также не реализуема.

Для пятого S-блока $S_5 \Leftrightarrow S_5$ имеем:

$$17 \to 3 \to 17: S_5(10_x,1_x) \Leftrightarrow S_1(4_x,4_x),$$
$$18 \to 8 \to 18: S_5(8_x,8_x) \Leftrightarrow S_2(2_x,1_x),$$
$$20 \to 14 \to 20: S_5(2_x,4_x) \Leftrightarrow S_4(8_x,4_x),$$

Возможные варианты однобитных переходов S-блоков и здесь должны быть перекрыты все три перехода $S_1(4_x,4_x)$, $S_2(2_x,1_x)$ и $S_4(8_x,4_x)$.

Для шестого S-блока получаем однобитные переходы $S_6 \Leftrightarrow S_6$:

$$19 \to 25 \to 19: S_6(1_x,1_x) \Leftrightarrow S_5(4_x,2_x),$$
$$21 \to 29 \to 21: S_6(10_x,4_x) \Leftrightarrow S_8(10_x,1_x),$$
$$23 \to 4 \to 23: S_6(4_x,8_x) \Leftrightarrow S_1(2_x,2_x),$$
$$24 \to 11 \to 24: S_6(2_x,2_x) \Leftrightarrow S_3(4_x,8_x).$$

Достаточно наложить ограничения на три перехода $S_3(4_x,8_x)$, $S_1(2_x,2_x)$ и $S_8(10_x,1_x)$ (оставшийся переход не реализуем).

Для седьмого S-блока однобитные переходы $S_7 \Leftrightarrow S_7$:

$$24 \to 12 \to 24: S_7(20_x,4_x) \Leftrightarrow S_3(2_x,8_x),$$
$$27 \to 32 \to 32: S_7(4_x,8_x) \Leftrightarrow S_8(2_x,4_x),$$
$$28 \to 7 \to 28: S_7(2_x,1_x) \Leftrightarrow S_2(4_x,4_x),$$
$$29 \to 22 \to 29: S_7(1_x,2_x) \Leftrightarrow S_6(8_x,4_x).$$

Достаточно наложить ограничения на два перехода $S_8(2_x,4_x)$ и $S_2(4_x,4_x)$ (по аналогии с четвертым S-блоком).

Совершенно аналогичная ситуация возникает для восьмого S-блока с однобитными переходами $S_8 \Leftrightarrow S_8$:

$$28 \to 5 \to 28: S_8(20_x,8_x) \Leftrightarrow S_2(10_x,4_x),$$
$$29 \to 21 \to 29: S_8(10_x,1_x) \Leftrightarrow S_6(10_x,4_x),$$
$$32 \to 27 \to 32: S_8(2_x,4_x) \Leftrightarrow S_7(4_x,8_x),$$
$$1 \to 15 \to 1: S_8(1_x,2_x) \Leftrightarrow S_4(4_x,1_x).$$

Здесь достаточно наложить ограничения на два перехода $S_6(10_x,4_x)$ и $S_7(4_x,8_x)$ (правда, эти переходы уже защищены введенным ранее ограничением на переходы $S_8(10_x,1_x)$ и $S_8(2_x,4_x)$).

Упорядочивая эти переходы по S-блокам, получим список из 18 значений переходов, подлежащих ограничению:

$$S_1(4_x,4_x),\ S_1(2_x,2_x);\quad S_2(4_x,4_x),\ S_2(2_x,1_x);$$
$$S_3(8_x,4_x),\ S_3(4_x,8_x);\quad S_4(8_x,4_x),\ S_4(2_x,2_x);$$
$$S_5(10_x,1_x),\ S_5(8_x,8_x),\ S_5(2_x,4_x);$$
$$S_6(2_x,2_x),\ S_6(4_x,8_x),\ S_6(10_x,4_x);$$
$$S_7(2_x,1_x),\ S_7(4_x,8_x);\quad S_8(2_x,4_x),\ S_8(10_x,1_x).$$

Нетрудно убедиться, что он полностью совпадает со списком элементов ТРЛА, представленным в Условии *L*-3. Приведенный список, однако, характеризует условия перекрытия характеристик, содержащих и одноблочные и двухблочные циклы. Так, если интересоваться характеристиками, содержащими только один активный S блок в каждом цикле, то, как легко видеть, все используемые в этом случае варианты однобитных переходов содержатся в приведенном списке. Если далее считать, что вероятности этих переходов ограничены значением 4, то для результирующей вероятности 16-цикловой характеристики, составленной из таких однобитных переходов, приходим к оценке:

$$2^4 \cdot \left[\left(\frac{4}{64}\right)^2 \cdot 2\right]^5 \cdot \left(\frac{4}{64}\right) \cdot 2 = 2^{-33}, \qquad 2^3 \cdot \left[\left(\frac{4}{64}\right)^2 \cdot 2\right]^4 \cdot \left(\frac{4}{64}\right) \cdot \left(\frac{16}{64}\right)^2 \cdot 2^3 = 2^{-30}$$

и, следовательно, эти характеристики действительно становятся не опасными (правое выражение учитывает произвол в выборе значений входа и выхода характеристики).

Корейские ученые, задавая нулевые значения вероятностей однобитных переходов (Условием *L*-3), полностью запретили все характеристики рассмотренного типа. Однако реальные ограничения для этих характеристик, как следует из приведенных выше расчетов (2), можно сделать менее жесткими (вместо нуля достаточно ограничиться значением 4).

Если теперь рассматривать характеристики с двухблочными циклами (1+2+0), реализующими переходы $\Phi \oplus \Theta \leftarrow \Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$ (переходы $\Phi \leftarrow \Gamma \oplus \Psi \leftarrow \Phi$ для шифра DES не реализуемы), то при вероятности ЛАХ одноблочного цикла, равной максимально возможному значению $\left(\frac{16}{64}\right)$, для 16-цикловой характеристики, построенной из шестицикловых характеристик рассматриваемого типа, получим результирующее значение вероятности равное:

$$2^4 \cdot \left[2^2 \cdot \left(\frac{16}{64}\right) \cdot \left(\frac{4}{64}\right)^2\right]^5 = 2^{-8 \cdot 5+4} = 2^{-36},$$

что является уже достаточным (если также учитывать особенности в начале и конце характеристики).

Полученное нами ограничение с измененным по отношению к условию L-3 граничным значением мы определим как условие У-4.

Условие У-4 (условие перекрытия шестицикловых итеративных аппроксимаций с однобитными переходами): Для ТРЛА S-блоков необходимо выполнить следующие (общее число 18 случаев) условия:

- $S1$-блок: $|NS_1(4_x, 4_x)| \le 4$, $|NS_1(2_x, 2_x)| \le 4$,
- $S2$-блок: $|NS_2(4_x, 4_x)| \le 4$, $|NS_2(2_x, 1_x)| \le 4$,
- $S3$-блок: $|NS_3(8_x, 4_x)| \le 4$, $|NS_3(4_x, 8_x)| \le 4$,
- $S4$-блок: $|NS_4(8_x, 4_x)| \le 4$, $|NS_4(2_x, 2_x)| \le 4$,
- $S5$-блок: $|NS_5(16_x, 1_x)| \le 4$, $|NS_5(8_x, 8_x)| \le 4$, $|NS_5(2, 4)| \le 4$,
- $S6$-блок: $|NS_6(16_x, 4_x)| \le 4$, $|NS_6(4_x, 8_x)| \le 4$, $|NS_6(2_x, 2_x)| \le 4$,
- $S7$-блок: $|NS_7(4_x, 8_x)| \le 4$, $|NS_7(2_x, 1_x)| \le 4$,
- $S8$-блок: $|NS_8(16_x, 1_x)| \le 4$, $|NS_8(2_x, 4_x)| \le 4$.

Трехцикловые характеристики с двумя двухблочными циклами получаются при использовании для их построения двух циклических однобитных переходов, связывающих различные S-блоки, и поэтому сразу становится очевидным, что здесь также "сработает" введенное выше ограничение на однобитные переходы. Они будут включать в себя однобитные переходы из списка ограничений Условия L-3 или нереализуемые переходы.

Особого внимания заслуживают трехцикловые (шестицикловые) характеристики, которые могут быть построены без использования S-блоков с однобитными переходами. Анализ показывает, что существует только два варианта характеристик с пятью S-блоками типа 3+2+0, которые строятся без однобитных переходов: это циклический переход 3,4,8,11 ← 18,23,(24) ← 3,4,8,11 и циклический переход 7,8,12,14 ← 18,(20),26 ← 7,8,12,14. Характеристики с большим числом S-блоков, как указано выше, для атак ЛК уже не опасны.

Для перекрытия этих характеристик можно воспользоваться условием L-4 корейских ученых, которое они предложили для защиты от атак на восьмицикловых характеристик. В новых обозначениях это будет условие У-5.

Условие У-5 (условие защищенности от атак ЛК на шестицикловые итеративные аппроксимации без однобитных переходов): Для $W(\alpha)$, $W(\beta) \le 2$ необходимо, чтобы $|NS(\alpha,\beta)| \le 10$, где, как и ранее, $\alpha \in GF(2)^6$ и $\beta \in GF(2)^4$, $W(\alpha)$ – вес битового входа, а $W(\beta)$ – вес битового выхода S-блока.

Это ограничение здесь даже является черезчур уж жестким, так как для вероятности пятнадцатицикловой характеристики, составленной из трехцикловых аппроксимаций рассматриваемого вида, получаем оценку

$$2^4 \cdot \left\lceil 2^4 \cdot \left(\frac{10}{64}\right)^5 \right\rceil^5 = 2^{-42,9}.$$

Осталось рассмотреть последнюю характеристику под номером 3 (рис. 2). Легко убедиться, что эта характеристика допускает многовариантное представление. Некоторые из возможных вариантов шестицикловых характеристик, содержащих все циклы активного типа, вместе с исходной характеристикой (рис. 2), приведены на рис. 7. Несмотря на их значительное многообразие, они с точностью до обозначений входов и выходов описываются тремя различными графами переходов, которые под номерами, соответствующими характеристикам рис. 7, приведены на рис. 8.

Характеристика с графом переходов 3.1 использует два независимых циклических перехода $\Phi \leftarrow \Gamma \leftarrow \Phi$, $\Psi \leftarrow \Theta \leftarrow \Psi$. Если символы Φ, Θ, Γ и Ψ в обозначениях характеристики – это однобитные входы и выходы различных S-блоков, то получается шестицикловая характеристика (по числу активных S-блоков каждого цикла) типа 1+2+1+1+2+1. Пары однобитных входов Φ, Θ и Γ, Ψ – входы в различные S-блоки и, следовательно, выходы соответствующих пар S-блоков не могут принимать свободные значения. В итоге, рассматриваемые шестицикловые характеристик содержат по четыре однобитных перехода, которые либо содержатся в списке ограничений У-4, либо хотя бы один из переходов является для шифра DES нереализуемым (использует входы в S-блоки с нулевой вероятностью). Для шестицикловых итеративных характеристик рассматриваемого типа достаточно защититься от атак на характеристики с числом активных S-блоков, приходящихся на шестицикловую характеристику, не превышающим десяти:

$$\left[\left(\frac{16}{64}\right)^4 \cdot 2^2\right]^5 \cdot 2^4 \cdot \left(\frac{16}{64}\right) \cdot 2 = 2^{-27}$$

3,1

$\Gamma \leftarrow \Phi$

$\Phi \oplus \Theta \leftarrow \Gamma \oplus \Psi$

$\Psi \leftarrow \Theta$

$\Phi \leftarrow \Gamma$

$\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$

$\Theta \leftarrow \Psi$

3.2

$\Gamma \leftarrow \Phi$

$\Theta \leftarrow \Psi$

$\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$

$\Theta \leftarrow \Gamma$

$\Psi \leftarrow \Phi$

$\Phi \oplus \Theta \leftarrow \Gamma \oplus \Psi$

3.4

$\Gamma \leftarrow \Phi$

$\Phi \oplus \Theta \leftarrow \Gamma \oplus \Psi$

$\Psi \leftarrow \Phi$

$\Theta \leftarrow \Gamma$

$\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$

$\Theta \leftarrow \Psi$

3.5

$\Gamma \leftarrow \Phi$

$\Theta \leftarrow \Psi$

$\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$

$\Phi \leftarrow \Gamma$

$\Psi \leftarrow \Theta$

$\Phi \oplus \Theta \leftarrow \Gamma \oplus \Psi$

Рис. 7

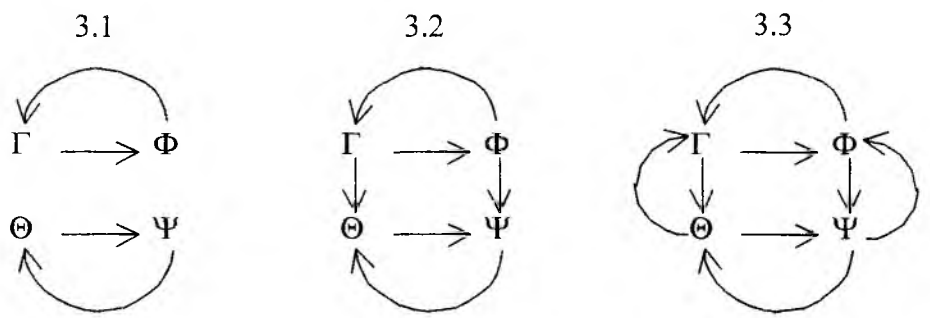


Рис. 8

Если символы Φ, Θ и Γ, Ψ в обозначениях характеристик – это однобитные входы и выходы однотипных S-блоков, то получается шестицикловая характеристика типа 1+1+1+1+2+1 или 1+2+1+1+2+1. В этом случае имеются пары однобитных входов Φ и Θ, Γ и Ψ, которые являются входами в различные S-блоки и, следовательно, только два или три выхода разнесенных циклов может принимать свободные значения. Но все равно и в этих характеристиках сохраняются минимум три однобитных перехода, которые делают ее с при выполнении ограничения У-4 неуязвимой для атак линейного криптоанализа. Примеры построения рассмотренных выше шестицикловых итеративных характеристик иллюстрирует рис. 9.

Если при построении характеристики используется хотя бы один циклический двухбитный переход (см. пример в нижней части рис.9), то и в этом случае оказывается, что в ее формировании принимает участие минимум два однобитных (одноблочных) перехода (выходы соответствующих S-блоков не являются свободными). В результате во всех рассмотренных случаях для вероятности результирующей пятнадцатицикловой характеристики приходим к оценке

$$\left[\left(\frac{4}{64}\right) \cdot \left(\frac{16}{64}\right)^3 \cdot 2^2\right]^5 \cdot 2^4 = 2^{-36},$$

т.е. эти характеристики не подвержены атакам ЛК. Заметим, что при получении последнего результата полагалось, что на каждые три цикла шестицикловой характеристики приходится не менее одного S-блока, удовлетворяющего условию У-4, и трех S-блоков, не попадающих под какие-либо ограничения, кроме максимально допустимого значения элементов ТРЛА. Естественно, что при использова-

нии ограничения L-3, предложенного корейскими учеными, все рассмотренные выше шестицикловые характеристики становятся просто не реализуемыми.

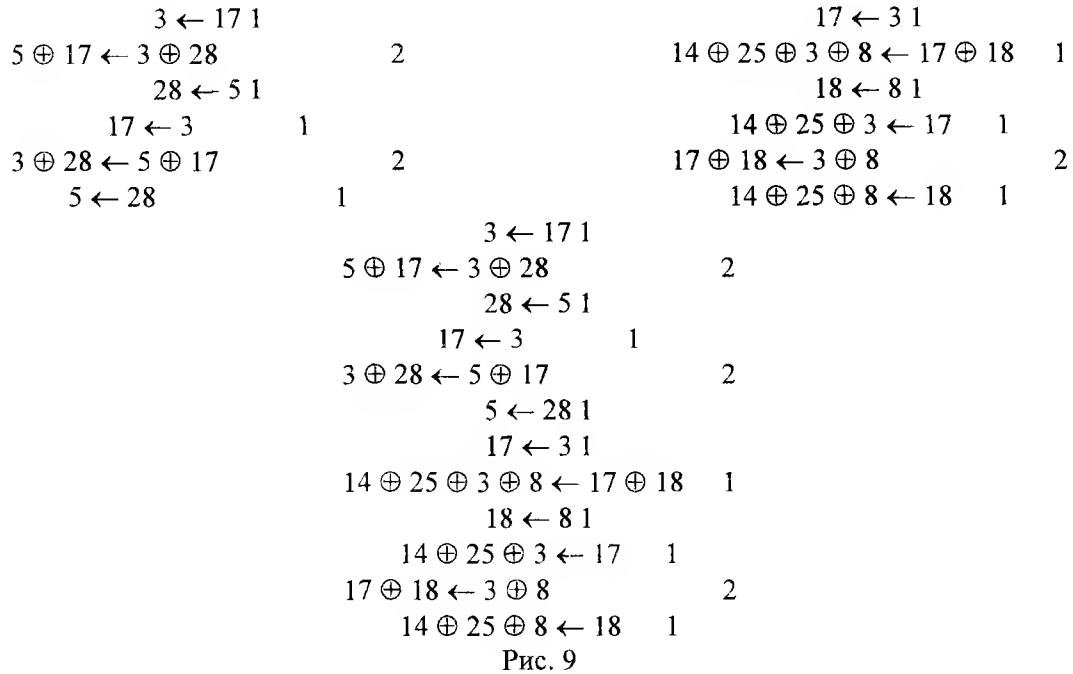


Рис. 9

Что касается характеристик с графами переходов 3.4 и 3.5, рис. 8, то все они, как показывает анализ, для шифра DES не осуществимы.

Таким образом, нам удалось обосновать три первых (L-1÷L-3) условия отбора S-блоков для шифра DES, которые корейскими учеными рассматривались как необходимые и достаточные для защиты четырехцикловых и шестицикловых ЛАХ от атак линейного криптоанализа. Вместе с тем показано, что рассмотренных трех ограничений явно недостаточно для решения этой задачи. Имеются четырехцикловые характеристики, не рассмотренные корейскими учеными, которые требуют использования дополнительного ограничения, сформулированного в виде Условия У-4. Кроме того, для защиты шестицикловых характеристик обосновано Условие У-5. В очередной работе мы рассмотрим условия обеспечения защищенности от атак линейного криптоанализа для итеративных характеристик с большим числом циклов.

Список литературы: 1. Построение таблиц подстановок для стандарта шифрования данных / *И.В. Лисицкая, С.А. Головашич, Р.В. Олейников и др.* // Проблемы бионики. 1999. Вып 50. С. 185–194. 2. Анализ стойкости DES подобных алгоритмов шифрования при использовании таблиц подстановок случайного типа / *И.В. Лисицкая, А.С. Коряк, Р.В. Олейников и др.* // Радиоэлектроника и информатика. 1999. № 1. С. 111-115. 3. The selection criteria of random substitution tables for symmetric enciphering algorithms / *I.V. Lysytska, A.S. Koriak, S.A. Golovashich, O.I. Oleshko, R.V. Oleinik* // Abstracts of XXVIth General Assembly. Toronto, Ontario Canada. 1999. P. 204. 4. Обеспечение стойкости DES-подобных алгоритмов шифрования к атакам линейного криптоанализа при использовании подстановок случайного типа / *В.И. Долгов, И.В. Лисицкая, С.А. Головашич и др.* // Радиотехника. 2000. Вып 114. С. 39-46. 5. *Kim K., Park S., Lee S.* Reconstruction of s^{2}DES 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. *Lars Ramkilde Knudsen.* Iterative Characteristics of DES and s^{2}DES, Proc. of Crypto'92. UCSB. 1992. 7. *Kim K., Lee S., Park S.* Necessary Conditions to Strengthen DES S-boxes against Linear Cryptanalysis. Pros. of SCIS'94, Biwako, Japan, Pp.15D. 1-11. 1994. 8. *Kim K.* Construction of DES-like S-boxes Based on Boolean Function Satisfying the SAK, Pros. Of Asiacrypt'91, Pp. 59-72, Fujiyoshida, Japan, 1991. 9. *Kim K., Lee S., Park S., Lee D.* DES can be Immune to Linear Cryptanalysis, Workshop Record of SAC '94 (Selected Areas in Cryptography) May 5-6. Queen's Univ. Canada. 1994. 10. *Kim K., Lee S., Park S., Lee D.* How to Strengthen DES against Two Robust Attacks, Joint Workshop on Information Security and Cryptology Inuyata. Japan. January 24-25, 1995. 11. *Biham E., Shamir A.* . Differential Cryptanalysis of the Data Encryption Standard. Springler Verlag. Berlin. 1993. 12. *Biham E., Shamir A.* Differential Cryptoanalysis of the full 16-round DES. Technical Report - Computer Science Department. Technion. Israiel. 1993. 13. *Mitsuru Matsui* Linear Cryptanalysis Method for DES Cipher. Proc. of Eurocrypt'93, Norway, 1993. 14. *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.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 6.03.2001