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 ВОСЬМИЦИКЛОВЫЕ ЛИНЕЙНЫЕ ИТЕРАТИВНЫЕ АППРОКСИМАЦИИ

В предыдущей нашей работе [1] рассмотрены требования к отбору S-блоков, защищенных от атак линейного криптоанализа на характеристики обнуляющего типа и четырехцикловые характеристики. В этой работе будет продолжено изучение условий отбора S-блоков, защищенных от атак линейного криптоанализа теперь уже на восьмицикловые характеристики.

На рис.1 представлены линейные итеративные характеристики для числа циклов большего двух вплоть до десятицикловых. Нас сейчас будут интересовать характеристики по номерами 4 и 5.

Особенностью характеристик рассматриваемого типа является то, что они включают в себя пары циклов с идентичными входами (масками входов). Это позволяет заключить, что для восьмицикловых характеристик, использующих пары S-блоков с идентичными входами, анализу подлежат линейные аппроксимации с 12-ю и меньшим числом S-блоков, так как для конфигурации из 14-ти S-блоков имеем

$$\left[\left(\frac{16}{64}\right)^{14}\cdot 2^{13}\right]^2\cdot 2 = 2^{-29}.$$

Рассмотрим более детально характеристику под номером 4. Можно убедиться, что если в характеристике 4(рис.1) каждый из символов в обозначении представляет собой один бит входа или выхода (масок входа и выхода) соответствующего цикла (такие характеристики в [1] названы характеристиками минимального типа), то она уже содержит не менее 12 S-блоков. Покажем сразу, что характеристика 4(рис.1) и не минимального типа для шифра DES в принципе не осуществима.

Действительно, глядя на эту характеристику, легко прийти к выводу, что наряду с переходами $\Phi \oplus \Theta \leftarrow \Psi$ и $\Theta \leftarrow \Psi$ для нее следует считать допустимым и переход $\Phi \leftarrow \Psi$. Аналогично, из существования для этой характеристики переходов $\Gamma\oplus\Psi \leftarrow \Phi$ и $\Gamma \leftarrow \Phi$ следует выполнимость и перехода $\Psi \leftarrow \Phi$. Но тогда из справедливости перехода $\Phi \oplus \Theta \leftarrow \Gamma\oplus\Psi$ при условии, что допустимы переходы $\Phi \leftarrow \Psi$ и $\Theta \leftarrow \Psi$, следует считать допустимыми переходы $\Theta \leftarrow \Gamma$ и $\Phi \leftarrow \Gamma$. Именно из этих соображений построен граф переходов для характеристики 4(рис.1) приведенный под соответствующим номером на (рис.2). Как уже отмечалось в предыдущей нашей работе [1], такая комбинация циклических переходов для шифра DES совместно не осуществима. Можно убедиться в нереализуемости характеристики 4(рис.1) (и других, полученных на основе комбинирования композициями входов и выходов циклов характеристики 4) сразу рассматривая переходы $\Phi \oplus \Theta \leftarrow \Gamma\oplus\Psi$ и $\Gamma\oplus\Psi \leftarrow \Phi$. Из справедливости этих двух переходов, очевидно, следует считать допустимым и циклический переход $\Phi\oplus\Theta \leftarrow \Gamma\oplus\Psi \leftarrow \Phi \oplus \Theta$.

При этом, как следует из рассматриваемой характеристики, одновременно должны выполняться однобитные переходы $\Gamma \leftarrow \Phi$, $\Psi \leftarrow \Theta$, $\Gamma \leftarrow \Theta$, $\Theta \leftarrow \Psi$. Но для *P*-перестановки, использованной в шифре DES, циклический двухбитный переход $\Phi \oplus \Theta \leftarrow \Gamma\oplus\Psi \leftarrow \Phi \oplus \Theta$ с одновременным выполнением условий $\Gamma \leftarrow \Phi$, $\Psi \leftarrow \Theta$, $\Gamma \leftarrow \Theta$, $\Theta \leftarrow \Psi$ является не осуществимым. Таким образом, восьмицикловая характеристика под номером 4(рис.1) не может быть использована для атак линейного криптоанализа.

Рассмотрим теперь восьмицикловую итеративную характеристику представленную на рис.1 под номером 5. Как нетрудно убедиться, особенностью и этой характеристики является внутренний циклический характер ее переходов. Он проявляется в том, что одни и те же значения входов (масок входов) Ф в разнесенные на один "этаж" циклы формируют выходы (маски) Г и Г⊕Ψ, побитное различие которых Ψ задает вход (маску входа) промежуточного цикла. Выходом промежуточного цикла снова является исходное значение Ф совпадающих входов (масок входов) разнесенных циклов. Если при этом вход и выход (соответствующие маски) внутреннего цикла Ф← Г⊕Ψ являются фиксированными, то маски выходов разнесенных циклов (с одинаковыми входами) могут быть произвольными (лишь бы побитовая сумма по модулю 2 формировала соответствующий вход промежуточного цикла Ψ.

1

Г ←Ф
Ф ⊕ Θ← Г⊕Ψ
Ψ ← Ф
Θ← Г⊕Ψ

4-х цикловая итеративная характеристика

2

Г ←Ф
Ф ← Г.
0_x←0_x
Ф ← Г
Г ←Ф
0_x←0_x

6-ти цикловая итеративная характеристика

3

Г ←Ф
Ф ⊕ Θ← Г⊕Ψ
Ψ ← Θ
Ф ← Г.
Г⊕Ψ ←Ф ⊕ Θ.
Θ ← Ψ

6-ти цикловая итеративная характеристика

4

Г ←Ф
Ф ⊕ Θ← Г⊕Ψ
Ψ ← Θ
Ф ← Г⊕Ψ
Г ← Θ
Ф ⊕ Θ← Ψ
Г⊕Ψ ←Ф
Θ ← Ψ

8-ми цикловая итеративная характеристика

5

Г ←Ф
Ф ← Г⊕Ψ
Ψ ←Ф
0_x ← 0_x
Ψ ←Ф
Ф ← Г⊕Ψ
Г ←Ф
0_x ← 0_x

8-ми цикловая итеративная характеристика

6

Г ←Ф
Ф ← Ψ
Г⊕Ψ ← Θ
Ф ⊕ Θ← Г⊕Ψ
0_x←0_x
Ф ⊕ Θ← Г⊕Ψ
Г⊕Ψ ← Θ
Ф ← Ψ
Г ←Ф
0_x←0_x

10-ти цикловая итеративная характеристика

7

Г ←Ф
Ф⊕ Θ ← Ψ
Г⊕Ψ ←Ф
Ф ← Г.
Ψ ←Ф⊕ Θ
Θ← Г⊕Ψ
Г ←Ф
Ф⊕ Θ ← Ψ
Г⊕Ψ ←Ф
Θ ← Ψ

10-ти цикловая итеративная характеристика

Рис.1

Это значит, что мы практически снова имеем дело с характеристиками, строящимися с использованием однобитных переходов, которые мы рассматривали при построении шестицикловых итеративных характеристик в предыдущей нашей работе [1] (по крайней мере для промежуточного цикла Ф ← Ψ).

Как уже было показано выше, перекрытию подлежат все характеристики с числом S-блоков, приходящихся на симметричную половину восьмицикловой характеристики, меньшим шести. Рассмотрим характеристику 5(рис.2), представленную в более естественном виде на рис.3. На этом же рисунке приведены также еще два возможных варианта компактного изображения симметричной половины восьмицикловой характеристики, получающиеся при других композициях входов и выходов задействованных S блоков. Переход Ф← Г⊕Ψ

для характеристики 5.1, Рис.3 означает, что одновременно выполняются и переходы Ф← Г и Ф ← Ψ. С учетом выполнения для этой характеристики и переходов Г ←Ф и Ψ ←Ф приходим к графу ее переходов, представленному под соответствующим номером на рис.2.

Для характеристики 5.2 из выполнимости перехода ГФΨ ← Ф следует справедливость перехода Ψ ← Ф, и граф ее переходов принимает вид 5.2, Рис.2. Аналогичные рассуждения приводят к графу переходов характеристики 5.3 также представленному на рис.2. Как следует из графа 5.1 на рис.2, восьмицикловая итеративная характеристика рассматриваемого типа основывается на использовании сразу двух однобитных циклических переходов

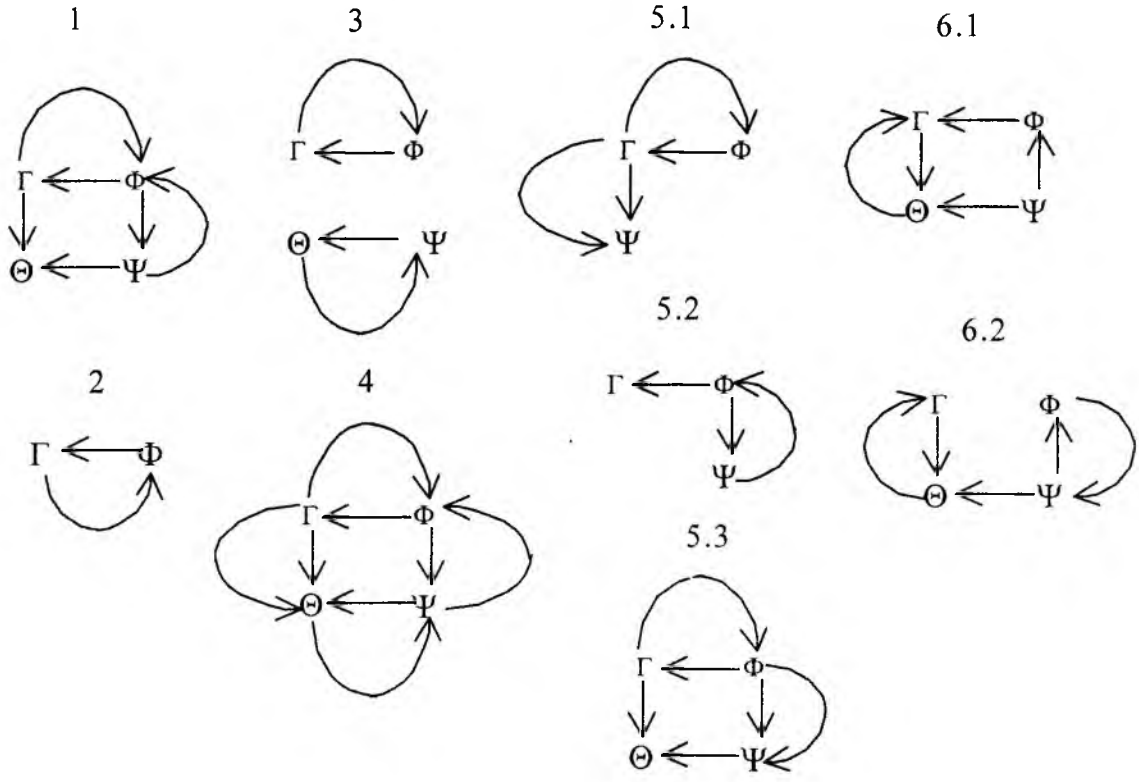

Рис.2

Ф←Г←Ф и Ф ←Ψ←Ф, имеющих общий бит Ф. Здесь полезно будет привести свойство, характеризующее однобитные циклические переходы шифра DES, которое мы сформулируем в виде утверждения. Его справедливость легко проверяется непосредственной проверкой (см. распределение битов 32-битного полублока для одного цикла преобразования DES [1]).

Утверждение 1. Для *P*-подстановки, использованной в шифре DES, циклические переходы Г←Ф←Г и Ψ←Ф←Ψ с общим элементом Ф могут быть только однобитными, при этом Г и Ψ являются входами одного и того же S-блока.

Из приведенного утверждения следует, что промежуточный цикл Ф ← ГФΨ для характеристики 5.1 является одноблочным, в то время как Ф является однобитным входом в разные (смежные) S-блоки. Шифр DES позволяет построить 7 пар однобитных циклических переходов с общим битом. Так как все они без исключения образуют циклы с однобитными входами в разные S блоки, то это означает, что разнесенные одноблочные циклы не имеют свободы в выборе своих масок выходов, при этом, как показывает анализ, один из двух

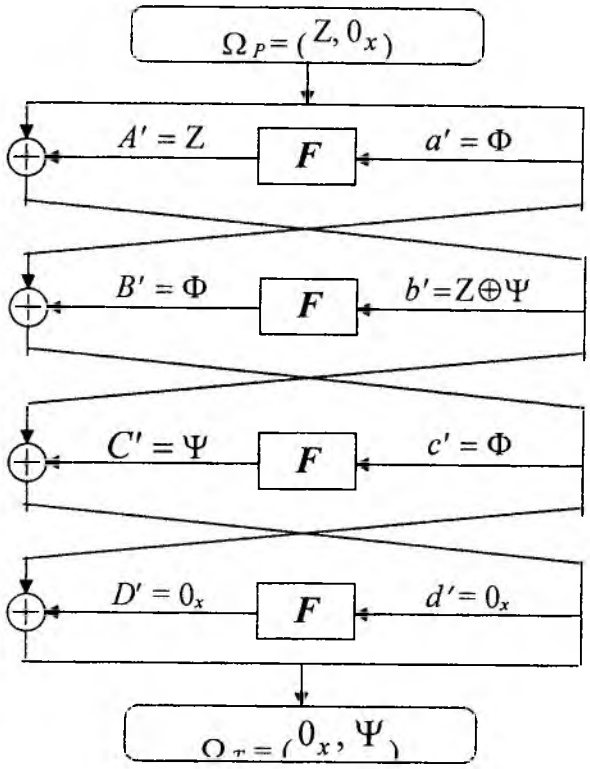

Рис.3

5.1
$\Gamma \leftarrow \Phi$
$\Phi \leftarrow \Gamma \oplus \Psi$
$\Psi \leftarrow \Phi$
$0_x \leftarrow 0_x$

5.2
$\Gamma \leftarrow \Phi$
$\Phi \leftarrow \Psi$
$\Gamma \oplus \Psi \leftarrow \Phi$
$0_x \leftarrow 0_x$

5.3
$\Phi \leftarrow \Gamma \oplus \Psi$
$\Gamma \oplus \Psi \leftarrow \Phi$
$\Phi \oplus \Theta \leftarrow \Gamma \oplus \Psi$
$0_x \leftarrow 0_x$

5.1.1
$28 \leftarrow 5$ 1
$5 \leftarrow 28 \oplus 31$ 1
$31 \leftarrow 5$ 1
$0_x \leftarrow 0_x$

5.1.2
$(2,9,13,17,18,23),28 \leftarrow 5$ 2
$5 \leftarrow 28 \oplus 31$ 1
$(2,9,13,17,18,23),31 \leftarrow 5$ 2
$0_x \leftarrow 0_x$

5.1.3
$(14,25),8 \leftarrow 17 \oplus 18$ 1
$17 \oplus 18 \leftarrow 3 \oplus 8$ 2
$(14,25),3 \leftarrow 17 \oplus 18$ 1
$0_x \leftarrow 0_x$

5.2.1
$(1,26),20 \leftarrow 16$ 1
$16 \leftarrow 10$ 1
$(1,26),10 \oplus 20 \leftarrow 16$ 1
$0_x \leftarrow 0_x$

5.3.1
$(15,21),27 \leftarrow 28,31$ 1
$28,31 \leftarrow 5$ 2
$(15,21),27 \oplus 5 \leftarrow 28,31$ 1
$0_x \leftarrow 0_x$

5.3.2
$(3,22,25,32),7,8 \leftarrow 18,26$ 2
$18,26 \leftarrow 7,8,12,14$ 2
$(3,22,25,32),12,14 \leftarrow 18,26$ 2
$0_x \leftarrow 0_x$

Рис.4

однобитных входов (масок входов) в эти S-блоки для всех без исключения вариантов восьмицикловых характеристик принимает значение или 1_x, или 20_x. Но, как известно, для этих входов значения ТРЛА S блоков, отобранных по требованиям разработчиков стандарта, удовлетворяют условию

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

При построении характеристик 5.1, использующих двухблочные циклы, появляется возможность за счет свободного выбора значений выходов уйти от однобитных переходов в циклах $\Gamma \leftarrow \Phi$ и $\Psi \leftarrow \Phi$, как это показано на рис.4, для характеристики 5.1.2 (в этом случае циклы $\Gamma \leftarrow \Phi$ и $\Psi \leftarrow \Phi$ уже двухблочные). Для перекрытия подобных характеристик можно

воспользоваться условием У-5 (L-4), как раз предложенным корейскими учеными для перекрытия именно восьмицикловых характеристик. Напомним здесь его

Условие У-5 (условие защиты от атак ЛК на восьмицикловые итеративные аппроксимации). Элементы ТРЛА S-блоков, удовлетворяющие условиям $W(\beta)\leq 2$, должны подчиняться ограничению

$$|\mathrm{NS}(\alpha,\beta)|\leq 10$$

при любых β. Поэтому одноблочные характеристики типа 5.1 для шифра DES не реализуем

Этому условию подчиняется S-блок внутреннего (промежуточного) цикла характеристики 5.1.2 (и всех других характеристик, в том числе и характеристик с двумя S-блоками промежуточного цикла), который не имеет свободы в выборе значений выходов (из-за необходимости обеспечения тождественного перехода). Но этого ограничения, как показывают расчеты, здесь (для характеристик из одноблочных циклов) оказывается недостаточно. Необходимо дополнительное ограничение и на циклы со свободными выходами. Можно, однако, убедиться в том, что для этих циклов мы находимся в условиях выполнения ограничения, У-3, введенного ранее в [1] для перекрытия одного из типов четырехцикловых итеративных характеристик. Напомним это условие (его часть).

Условие У-3 (условие перекрытия теперь уже восьмицикловых итеративных характеристик) Элементы ТРЛА пар S-блоков, имеющие входные и выходные маски, удовлетворяющие условию $W(\alpha)=1, W(\beta_1 \oplus \beta_2)=1$, должны подчиняться ограничению

$$|NS_k(\alpha,\beta_1)\bullet NS_k(\alpha,\beta_2)|\leq 80\ .$$

Условию У-3 подчиняются все четыре S-блока двухблочных циклов. В итоге для вероятности 16-цикловой характеристики, построенной из пятиблочных итеративных линейных аппроксимаций вида 5.1.2, получим оценку

$$\left[\left(\frac{80}{64^2}\right)^2\cdot\left(\frac{10}{64}\right)\cdot 2^4\right]^4\cdot 2^3=2^{-37}.$$

Можно, конечно, рассматривать и характеристики, полученные на основе объединения простейших (минимального типа). Все они, как показывает анализ, попадают под рассмотренные выше ограничения (для половинок восьмицикловых характеристик, состоящих из пяти и более S-блоков). Исключение составляет только характеристика вида

$$\begin{gathered}21,5\leftarrow 28\oplus 29 \quad 1\\ 28\oplus 29\leftarrow 5\oplus 7\oplus 21\oplus 22 \quad 2\\ 22,27\leftarrow 28\oplus 29 \quad 1\\ 0_x\leftarrow 0_x\end{gathered}$$

Эта характеристика содержит 4 S-блока, и все они попадают под ограничение У-5. Одного этого ограничения, однако, для перекрытия рассматриваемой характеристики оказывается недостаточно:

$$\left[\left(\frac{10}{64}\right)^4\cdot 2^3\right]^4\cdot 2^3=2^{-27,8}.$$

Зато ее одноблочные циклы с совпадающими входами (28-й и 29-й биты) – это переходы через седьмой и восьмой S-блоки, причем восьмой S-блок имеет вход (маску) 30_x, а в соответствии с условием У-2 (L-2) [1] ТРЛА S-блоков должны удовлетворять дополнительному ограничению $NS_i(30_x,\beta)=0$ для всех значений β и всех i. Это значит, что рассматриваемая характеристика при выполнении условия У-2 (L-2) для шифра DES просто не реализуема.

Характеристика 5.1.3(рис.4) построена с использовании двухбитного циклического перехода 3,8 ← 17,18 ← 3,8. В этом случае промежуточный цикл оказывается двухблочным. Он состоит из S блоков с однобитными переходами и потому попадает под ограничение, использованное в условии У-4 [1], но теперь это ограничение можно применить для перекрытия и восьмицикловых характеристик.

При построении восьмицикловых характеристик с графом переходов 5.2(рис.2) используется циклический однобитный переход Ф ←Г←Ф (для характеристики минимального типа). Компактное изображение этой характеристики приведено также под соответствующим номером на рис.3. Здесь значения выходов циклов с идентичными входами Г←Ф и Г⊕Ψ←Ф являются свободными (в пределах выходных битов S-блока). Поэтому в принципе могут быть построены характеристики, в которых на промежуточном цикле используется однобитный переход, который может и не быть в списке элементов ТРЛА условия У-4 - правда, этот однобитный переход попадает под ограничение У-5. Но зато два цикла с совпадающими входами, состоящие из однотипных S-блоков, удовлетворяют условию: $W(\alpha)=1$, $W(\beta_1 \oplus \beta_2)=1$ и, следовательно, в этом случае будет "работать" и ограничение У-3. Этих ограничений, однако, для перекрытия характеристик 5.2 (см. пример 5.2.1) оказывается также явно недостаточно. После введения всех предыдущих дополнительных ограничений одноблочные характеристики рассматриваемого типа, по-видимому, оказываются для шифра DES наиболее уязвимыми. Поэтому для защиты от атак на эти характеристики предлагается ввести дополнительные ограничения на все оставшиеся 11 ненулевых однобитных переходов. Представим это ограничение в виде условия У-6.

Условие У-6 (условие перекрытия восьмицикловых итеративных аппроксимаций с однобитными переходами) Для ТРЛА S-блоков необходимо выполнить следующие (общее число 11 случаев) условия:

- $S1$-блок: $|NS_1(8_x, 8_x)| \le 4$, $|NS_1(10_x, 4_x)| \le 4$;
- $S2$-блок: $|NS_2(8_x, 8_x)| \le 4$, $|NS_2(10_x, 4_x)| \le 4$;
- $S3$-блок: $|NS_3(2_x, 8_x)| \le 4$; $S4$-блок: $|NS_4(4_x, 1_x)| \le 4$,
- $S5$-блок: $|NS_5(4_x, 2_x)| \le 4$, $|NS_5(2_x, 4_x)| \le 4$; $S6$-блок: $|NS_6(8_x, 4_x)| \le 4$;
- $S7$-блок: $|NS_7(8_x, 4_x)| \le 4$; $S8$-блок: $|NS_8(4_x, 8_x)| \le 4$.

При выполнении этого условия и условия У-3 для одноблочной характеристики типа 5.2.1 получим оценку

$$\left[\left(\frac{80}{64^2}\right)\cdot\left(\frac{4}{64}\right)\cdot 2^2\right]^4 \cdot 2^3 = 2^{-27,7}.$$

Как видно, этого также оказывается недостаточно. Поэтому усилим ограничение У-3, разделив его на две части. Одну обозначим прежним номером У-3, а второй присвоим новый номер У-7.

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

$$|NS_k(\alpha, \beta_1) \bullet NS_k(\alpha, \beta_2)| \le 80 .$$

Условие У-7 (условие перекрытия восьмицикловых итеративных характеристик) Элементы ТРЛА пар S блоков, имеющие входные и выходные маски, удовлетворяющие условию $W(\alpha)=1, W(\beta_1 \oplus \beta_2)=1$, должны подчиняться ограничению

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

При выполнении условий У-4 либо У-6 и У-7 для характеристики 5.2.1 приходим к результату.

$$\left[\left(\frac{48}{64^2}\right)\cdot\left(\frac{4}{64}\right)\cdot 2^2\right]^4\cdot 2^3 = 2^{-30}.$$

Рассмотрим теперь характеристику 5.3(рис.3) (минимального типа).Она строится с использованием двухбитных входов в одноблочные циклы $\Phi \leftarrow \Gamma\oplus\Psi$ и $\Phi \oplus \Theta \leftarrow \Gamma\oplus\Psi$. Граф переходов для этой характеристики представлен под соответствующим номером на рис.2. По виду он повторяет граф переходов для четырехцикловой итеративной характеристики под номером 1, рис.2. Примеры построения характеристик вида 5.3 приведены под соответствующими номерами на рис.4. Характеристика 5.3.1 состоит из минимально возможного для нее числа активных S-блоков (четырех), а характеристика 5.3.2 – из шести (построена на основе использования циклического двухблочного перехода 7,8,12,14 ← 18,26 ← 7,8,12,14, включающего в себя два циклических однобитных перехода: 8 ← 18 ← 8 и 12 ← 26 ← 12). Покажем, что для перекрытия и этих характеристик достаточно будет воспользоваться рассмотренными выше ограничениями. Приведем здесь аргументы, касающиеся всех рассматриваемых характеристик в более общем виде.

Прежде всего заметим, что особенностью последних и всех других уже рассмотренных характеристик является использование при их построении циклических переходов между разнесенными циклами. Поэтому здесь будут уместно сформулировать еще два утверждения, касающиеся циклических переходов шифра DES.

Утверждение 2. Если в формировании циклического перехода шифра DES используется одноблочный цикл, то как минимум один из его переходов является однобитным (состоит из однобитного прохода).

Справедливость этих утверждений следует из самого принципа построения примененной в шифре DES *P*-подстановки, в соответствии с которым выходные биты каждого (одного) S-блока распределяются по одному по входам различных S-блоков [3], и поэтому замыкание циклического перехода при двух исходных битах будет происходить с использованием однобитных (одноблочных) переходов.

Утверждение 3. Любой двухбитный циклический переход (два бита переходят в два бита) шифра DES содержит минимум два S-блока с однобитными переходами.

Для того чтобы убедиться в справедливости этого утверждения, рассмотрим характеристики, использующие для своего построения циклические переходы двухблочных циклов в одноблочные и наоборот, одноблочных циклов в двублочные.

Анализ показывает, что всего возможно 80 характеристик с переходами типа 2→1. Из их общего числа 80 имеется 22 характеристики подобные такой, как

$$\begin{matrix} S_1(4_x,4_x) \\ S_2(2_x,1_x) \end{matrix} \Rightarrow S_5(18_x,9_x).$$

Их особенностью является то, что один из однобитных переходов в цикле с двумя активными S-блоками (в данном примере $S_1(4_x,4_x)$) имеется в списке ограничений условия У-4 [1], а второй – в списке ограничений условия У-6.

11 характеристик используют оба однобитных перехода из списка У-4.

Имеется 4 характеристики вида:

$$\begin{matrix} S_1(10_x,4_x) \\ S_7(8_x,4_x) \end{matrix} \Rightarrow S_4(21_x,9_x),$$

в которых входами в циклы с одним активным S блоком являются маски 21_x, а, как известно [3,4], для таблиц стандарта $NS_i(21_x,\beta)=0$ для всех возможных значений β и для всех S-блоков (заметим, что в представленном варианте "характеристики"оба однобитных перехода отсутствуют в списке ограничений У-4, но зато имеются в списке ограничений У-6). В то же время среди четырех вариантов этого типа имеется и характеристика такого вида:

$$\begin{matrix} S_2(8_x,8_x) \\ S_5(20_x,8_x) \end{matrix} \Rightarrow S_3(21_x,5_x).$$

Здесь, очевидно, с учетом $NS_i(20_x,\beta)=0$ оба перехода для соседних циклов становятся однобитными $S_2(8_x,8_x)\Rightarrow S_3(1_x,1_x)$, и здесь снова с учетом выполнения требований разработчиков к таблицам стандарта ($NS_i(1_x,\beta)=0$ для всех значений β и всех S блоков) приходим к выводу, что вероятность и этой характеристики равна нулю.

Имеется также 4 характеристики типа

$$\begin{matrix} S_2(1_x,2_x) \\ S_4(1_x,1_x) \end{matrix} \Rightarrow S_1(18_x,C_x), \text{ либо } \begin{matrix} S_3(20_x,4_x) \\ S_6(1_x,1_x) \end{matrix} \Rightarrow S_5(24_x,A_x),$$

вероятности которых также равны нулю

Остальные характеристики имеют вид

$$\begin{matrix} S_1(4_x,4_x) \\ S_3(20_x,4_x) \end{matrix} \Rightarrow S_5(30_x,9_x) \text{ либо } \begin{matrix} S_1(8_x,8_x) \\ S_3(1_x,1_x) \end{matrix} \Rightarrow S_2(9_x,A_x).$$

В этих характеристиках один из однобитных переходов нулевой (имеет нулевую вероятность), т.е. здесь снова приходим к одноблочным характеристикам, причем либо один из оставшихся переходов имеется в списке ограничений У-4 (таких характеристик 27), либо оставшийся переход содержится в списке ограничений У-6 (таких 12 характеристик). Однако, как показывает анализ, даже в этом случае все однобитные переходы Г←Ф и Г⊕Ψ←Ф, формирующие путем суммирования по модулю двух своих выходов и вход в промежуточный цикл (например, для характеристики 5.2), имеют входы вида $S_i(1_x,\beta)$ либо $S_i(20_x,\beta)$, Для этих значений входов элементы ТРЛА S блоков соответственно равны $NS_i(1_x,\beta)=0$ и $NS_i(20_x,\beta)=0$.

Приведенные результаты позволяют заключить, что в качестве условий перекрытия восьмицикловых характеристик минимального типа можно рассматривать выполнение ограничений на однобитные переходы У-4 [1].

Действительно, в этом случае все характеристики типа 5.1 (не одноблочные), содержат циклы с однобитными переходами (минимум два однобитных перехода). Тогда, с учетом выполнения ограничений на однобитные переходы У-4, У-6 для результирующей вероятности одноблочных характеристик (содержащих минимум два однобитных перехода на три активных S-блока), получим оценку (не учитывая, что здесь будет "работать" и ограничение У-5):

$$\left[\left(\frac{16}{64}\right)\cdot\left(\frac{4}{64}\right)^2\cdot 2^2\right]^4\cdot 2^3 = 2^{-32+3} = 2^{-29}.$$

Характеристики минимального типа 5.2.1, как показано выше, могут строиться без однобитных переходов из списка ограничений У-4, и здесь пришлось ввести дополнительные ограничения У-6 и У-7.

Для характеристик 5.3.1 это уже будет два однобитных перехода из списка ограничений У-4 на четыре S блока, причем оставшиеся два S-блока не попадают под ограничение У-5. Но ограничения У-4 здесь уже оказывается достаточным для защиты этих характеристик от атак ЛК. Действительно,

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

Очевидно, что приведенное ограничение будет достаточным для характеристик 5.3.1 и не минимального типа.

Для характеристики 5.3.2 в качестве необходимого дополнительного ограничения выступает приведенное выше условие У-4, примененное корейскими учеными как раз для защиты от атак ЛК именно восьмицикловых характеристик.

При выполнении этого ограничения для шестиблочной половины восьмицикловой характеристики (при шести активных S блоках, приходящихся на симметричную половину восьмицикловой характеристики) при условии, что два S блока из шести удовлетворяют ограничению У-5 (L-4), приходим к оценке результирующей вероятности шестнадцатицикловой характеристики

$$\left[\left(\frac{10}{64}\right)^2 \cdot \left(\frac{16}{64}\right)^4 \cdot 2^5\right]^4 \cdot 2^3 = 2^{-30}.$$

Это значение является уже вполне достаточным.

Список литературы: 1. *Лисицкая И.В., Бондаренко А. С., Колыбельников А. И.* 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 // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып 119. С.177-190. 2. *Долгов В.И., Лисицкая И.В., С.А.Головашич, А.С.Бондаренко* Обеспечение стойкости DES-подобных алгоритмов шифрования к атакам линейного криптоанализа при использовании подстановок случайного типа // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2000. Вып. 114. С. 39-46. 3. *Schneier B.* Applied Cryptography. *S*econd Edition: protocols, algorithms, and Source code in C. Published by John Wiley & *Son*S. Inc, New York: Chiche*S*ter Bri*S*bane Toronto *S*ingapore, 1996 – 758 p. 4. *Mitsuru* Matsui Linear Cryptanalysis Method for DES Cipher. Proc. of Eurocrypt'93, Norway, 1993. 5. *K. Kim, S. Lee and S Park.* Necessary Conditions to Strengthen DES S-boxes against Linear Cryptanalysis, Pros. of SCIS'94, Biwako, Japan, pp.15D. 1-11, Jan.27-29,1994.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 13.07.2001