УДК 681.3.06: 519.248.681

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

ОБЕСПЕЧЕНИЕ СТОЙКОСТИ ШИФРА DES К АТАКАМ ЛИНЕЙНОГО КРИПТОАНАЛИЗА. ТРЕБОВАНИЯ К ОТБОРУ S-БЛОКОВ, ЗАЩИЩЕННЫХ ОТ АТАК НА ДЕСЯТИЦИКЛОВЫЕ ИТЕРАТИВНЫЕ ЛИНЕЙНЫЕ АППРОКСИМАЦИОННЫЕ ХАРАКТЕРИСТИКИ.

Продолжим обсуждение условий отбора таблиц S-блоков стандарта DES, защищенных от атак линейного криптоанализа, начатое в работе [1]. Рассмотрим теперь возможные атаки на десятицикловую характеристику с тождественными циклами, представленную на рис. 1 под номером 6(десятицикловая характеристика под номером 7 рис.1, составленная только из активных S-блоков, описывается графом переходов под номером 4 на рис.2, а такой граф переходов, как уже было показано выше, для шифра DES не реализуем).

Нас будут интересовать характеристики, каждая из симметричных половинок которых содержат общее число активных S-блоков, не превышающее восьми:

$$\left[\left(\frac{16}{64}\right)^8 \cdot 2^7\right]^3 \cdot 2^2 = 2^{-25}, \left[\left(\frac{16}{64}\right)^9 \cdot 2^6\right]^3 \cdot 2^2 = 2^{-34}.$$

Будем сначала рассматривать характеристики, в которых каждый из символов, использованных при их описании, обозначает однобитный вход или выход S-блока, участвующего в их образовании. Пусть будет допустимой характеристика 6, рис. 1. Из этой характеристики следует, что выполняются переходы $Z \leftarrow \Phi$, $\Phi \leftarrow \Psi$, $Z \oplus \Psi \leftarrow \Theta$ и $\Phi \oplus \Theta \leftarrow Z \oplus \Psi$. Для шифра DES (для однобитных значений Γ, Ψ, Φ и Θ) это обозначает, что не выполняются обратные переходы $\Phi \leftarrow \Gamma$ и $\Theta \leftarrow \Psi$. Но тогда из выполнимости перехода $\Phi \oplus \Theta \leftarrow Z \oplus \Psi$ в нижней части характеристики при условии, что существует переход $\Phi \leftarrow \Psi$, следует, что должен выполняться и переход $\Theta \leftarrow Z$ (так как $\Phi \neq \Theta$). Выполнение же перехода $Z \oplus \Psi \leftarrow \Theta$ (при однобитных входах и выходах S-блоков первые три цикла рассматриваемой характеристики будут одноблочными) обязывает, чтобы существовали одновременно раздельные переходы $\Gamma \leftarrow \Theta$ и $\Psi \leftarrow \Theta$.

Приведенные соображения позволяют имеющиеся и установленные связи между входами и выходами S-блоков представить в виде графа переходов, изображенного под номером 6.1 на рис. 2.

Но характеристика вида 6, рис. 1 и соответствующий ей граф переходов не являются единственно возможными для десятицикловых характеристик. Наряду с рассматриваемой допустимыми будут еще несколько вариантов характеристик, получающихся путем варьирования допустимыми композициями входов и выходов S-блоков, задействованных при построении характеристики. Симметричные половины некоторых из них без своих зеркальных дополнений представлены вместе с "исходной" на рис. 3.

Заметим теперь, что, например, характеристики 2, 4 и 6 могут быть получены соответственно из характеристик 1, 2 и 3, если символы Ψ заменить на символы Γ, а символы Θ заменить на символы Φ, и поэтому в данном случае можно рассматривать только характеристики трех типов. Анализ и других возможных вариантов характеристик

1

$Z \leftarrow \Phi$

$\Phi \oplus \Theta \leftarrow Z \oplus \Psi$

$\Psi \leftarrow \Phi$

$\Theta \leftarrow Z \oplus \Psi$

4-х цикловая итеративная характеристика

2

$Z \leftarrow \Phi$

$\Phi \leftarrow Z$

$0_x \leftarrow 0_x$

$\Phi \leftarrow Z$

$Z \leftarrow \Phi$

$0_x \leftarrow 0_x$

6-ти цикловая итеративная характеристика

3

$Z \leftarrow \Phi$

$\Phi \oplus \Theta \leftarrow Z \oplus \Psi$

$\Psi \leftarrow \Theta$

$\Phi \leftarrow Z$

$Z \oplus \Psi \leftarrow \Phi \oplus \Theta$

$\Theta \leftarrow \Psi$

6-ти цикловая итеративная характеристика

4

$Z \leftarrow \Phi$

$\Phi \oplus \Theta \leftarrow Z \oplus \Psi$

$\Psi \leftarrow \Theta$

$\Phi \leftarrow Z \oplus \Psi$

$Z \leftarrow \Theta$

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

$Z \oplus \Psi \leftarrow \Phi$

$\Theta \leftarrow \Psi$

8-ми цикловая итеративная характеристика

5

$Z \leftarrow \Phi$

$\Phi \leftarrow Z \oplus \Psi$

$\Psi \leftarrow \Phi$

$0_x \leftarrow 0_x$

$\Psi \leftarrow \Phi$

$\Phi \leftarrow Z \oplus \Psi$

$Z \leftarrow \Phi$

$0_x \leftarrow 0_x$

8-ми цикловая итеративная характеристика

6

$Z \leftarrow \Phi$

$\Phi \leftarrow \Psi$

$Z \oplus \Psi \leftarrow \Theta$

$\Phi \oplus \Theta \leftarrow Z \oplus \Psi$

$0_x \leftarrow 0_x$

$\Phi \oplus \Theta \leftarrow Z \oplus \Psi$

$Z \oplus \Psi \leftarrow \Theta$

$\Phi \leftarrow \Psi$

$Z \leftarrow \Phi$

$0_x \leftarrow 0_x$

10-ти цикловая итеративная характеристика

7

$Z \leftarrow \Phi$

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

$Z \oplus \Psi \leftarrow \Phi$

$\Phi \leftarrow Z$

$\Psi \leftarrow \Theta \oplus k$

$\Theta \leftarrow Z \oplus \Psi$

$Z \leftarrow \Phi$

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

$Z \oplus \Psi \leftarrow \Phi$

$\Theta \leftarrow \Psi$

10-ти цикловая итеративная характеристика

Рис.1

на рис. 2. Что касается характеристик с графом переходов 6,1, который построен с использованием одного циклического перехода, то при однобитной интерпретации символов обозначений в соответствии с реальным видом характеристики следует считать, что Φ и Θ – это входные биты одного и того же S-блока, точнее, одноименных S-блоков, в то время как Γ и Ψ – это входные биты разных S-блоков. Поэтому речь должна идти не об однобитном циклическом переходе между двумя одноименными S-блоками, а о циклическом переходе $\Phi \oplus \Theta \leftarrow Z \oplus \Psi \leftarrow \Phi \oplus \Theta$, который может и не быть объединением однобитных циклических переходов $\Phi \leftarrow \Gamma$ и $\Theta \leftarrow \Psi$ (в нем отсутствуют переходы, но может существовать переход $\Psi \leftarrow \Phi$, так как при наличии еще хотя бы одного из переходов $\Phi \leftarrow \Gamma$ или $\Theta \leftarrow \Psi$ результирующая характеристика для шифра DES становится нереализуемой).

Переход $\Phi \oplus \Theta \leftarrow Z \oplus \Psi \leftarrow \Phi \oplus \Theta$ для шифра DES может состояться лишь с использованием трех различных S-блоков, при этом один из его полупереходов должен

быть одноблочным ("зайти" в один и тот же S-блок, т.е. попасть в одну и ту же вершину графа,

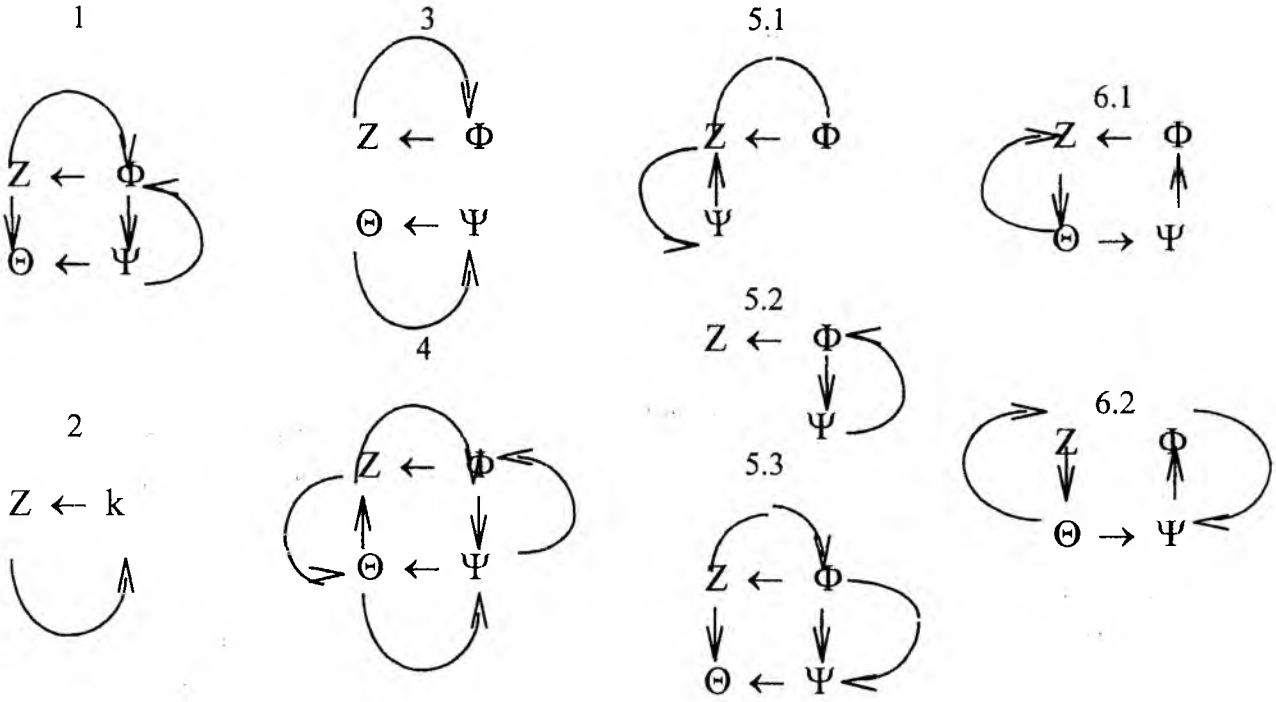


Рис.2

1

$Z \leftarrow \Phi$

$\Phi \leftarrow \Psi$

$Z \oplus \Psi \leftarrow \Theta$

$\Phi \oplus \Theta \leftarrow Z \oplus \Psi$

$0_x \leftarrow 0_x$

2

$\Psi \leftarrow \Theta$

$\Theta \leftarrow Z$

$Z \oplus \Psi \leftarrow \Phi$

$\Phi \oplus \Theta \leftarrow Z \oplus \Psi$

$0_x \leftarrow 0_x$

3

$\Phi \leftarrow \Psi$

$\Psi \leftarrow \Theta$

$\Phi \oplus \Theta \leftarrow Z \oplus \Psi$

$Z \leftarrow \Phi \oplus \Theta$

$0_x \leftarrow 0_x$

4

$\Theta \leftarrow Z,$

$Z \leftarrow \Phi,$

$\Phi \oplus \Theta \leftarrow Z \oplus \Psi$

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

$0_x \leftarrow 0_x$

5

$\Phi \leftarrow \Psi$

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

$\Theta \leftarrow Z$

$Z \oplus \Psi \leftarrow \Theta$

$0_x \leftarrow 0_x$

6

$\Theta \leftarrow \Gamma$

$Z \leftarrow \Phi \oplus \Theta$

$\Phi \leftarrow \Psi$

$Z \oplus \Psi \leftarrow \Phi$

$0_x \leftarrow 0_x$

Рис. 3

можно только из вершин, "принадлежащих" разным S-блокам). Для иллюстрации на рис. 4 представлены различные варианты построения таких характеристик при использовании трех S-блоков S_1, S_2 и S_5:

$$\left.\begin{matrix} S_1(4_x, 4_x) \\ S_2(2_x, 1_x) \end{matrix}\right\} \Leftrightarrow S_5(18_x, 9_x)$$ или в побитовой записи $\begin{matrix} 3 \leftarrow 17 \\ 8 \leftarrow 18 \end{matrix} \Leftrightarrow 17,18 \leftarrow 3,8.$

1

$8 \leftarrow 17$ 1

$17 \leftarrow 3$ 1

$3 \oplus 8 \leftarrow 18$ 1

$17 \oplus 18 \leftarrow 3 \oplus 8$ 2

$0_x \leftarrow 0_x$

2

$3 \leftarrow 18$ 1

$18 \leftarrow 8$ 1

$3 \oplus 8 \leftarrow 17$ 1

$17 \oplus 18 \leftarrow 3 \oplus 8$ 2

$0_x \leftarrow 0_x$

3

$17 \leftarrow 3$ 1

$3 \leftarrow 18$ 1

$17 \oplus 18 \leftarrow 3 \oplus 8$ 2

$8 \leftarrow 17 \oplus 18$ 1

$0_x \leftarrow 0_x$

4

$18 \leftarrow 8$ 1

$8 \leftarrow 17$ 1

$17 \oplus 18 \leftarrow 3 \oplus 8$ 2

$3 \leftarrow 17 \oplus 18$ 1

$0_x \leftarrow 0_x$

5

$17 \leftarrow 3$ 1

$3 \leftarrow 17 \oplus 18$ 1

$18 \leftarrow 8$ 1

$3 \oplus 8 \leftarrow 18$ 1

$0_x \leftarrow 0_x$

6

$18 \leftarrow 8$ 1

$8 \leftarrow 17 \oplus 18$ 1

$17 \leftarrow 3$ 1

$3 \oplus 8 \leftarrow 17$ 1

$0_x \leftarrow 0_x$

Рис. 4

Здесь задействованы циклические однобитные переходы $18 \leftarrow 8 \leftarrow 18$, $17 \leftarrow 3 \leftarrow 17$ и циклический двубитный переход $3,8 \leftarrow 17,18 \leftarrow 3,8$, при этом допустимыми являются также переходы $18 \leftarrow 3$ и $8 \leftarrow 17$, в то время как переходы $17 \leftarrow 8$ и $18 \leftarrow 3$ являются нереализуемыми. Четыре первых характеристики рис. 4 состоят из трех одноблочных циклов и одного двухблочного, остальные – являются одноблочными. Первые четыре характеристики кроме двух одноблочных циклов с однобитными переходами также включают двублочный цикл с однобитными переходами. При этом минимум два однобитных перехода для этих характеристик имеются в списке ограничений У-4, что и обеспечивает их "неуязвимость" атакам линейного криптоанализа (если один из однобитных переходов не из списка ограничений У-4, то второй однобитный переход для шифра DES нереализуем):

$$\left[\left(\frac{16}{64}\right)^3 \cdot \left(\frac{4}{64}\right)^2 \cdot 2^4\right]^3 \cdot 2^2 = 2^{-28}.$$

В одноблочных характеристиках под номерами 5 и 6, рис.4 сохраняются однобитными одновременно два перехода. Они попадают в циклы без свободных выходов, и поэтому даже если один из переходов оказывается не из списка ограничений У-4, то второй непременно имеет вероятность, равную нулю - задействуются входы S-блоков 1_x или 20_x. Если оба эти однобитных перехода оказываются из списка ограничений У-4, то тогда ограничений У-4 для перекрытия подобных характеристик оказывается уже недостаточно. Действительно, в этом случае для вероятности пятнадцатицикловой характеристики приходим к оценке:

$$\left[\left(\frac{4}{64}\right)^2 \cdot \left(\frac{16}{64}\right)^2 \cdot 2^3\right]^3 \cdot 2^2 = 2^{-25}, \qquad (1)$$

чего для перекрытия подобных характеристик явно недостаточно.

Заметим, однако, что эти две характеристики (как и предыдущие) удовлетворяют также введенному ранее ограничение У-5.

Условие У-5 (условие защиты от атак ЛК теперь уже на десятицикловые итеративные аппроксимации). Элементы ТРЛА S-блоков, удовлетворяющие условиям $W(\alpha)$, $W(\beta) \le 2$, должны подчиняться ограничению $|NS(\alpha,\beta)| \le 10$.

С учетом этого ограничения приходим к результату

$$\left[\left(\frac{4}{64}\right)^2 \cdot \left(\frac{10}{64}\right)^2 \cdot 2^3\right]^3 \cdot 2^2 = 2^{-29}.$$

Заметим, однако, что ограничение на однобитные переходы, введенное корейскими учеными, обеспечивает перекрытие всех рассмотренных выше десятицикловых характеристик.

Если идти дальше, то на основе конкатенации (объединения) характеристик простейшего типа, рассмотренных выше, могут быть построены характеристики, использующие большее число циклических переходов между S-блоками. Пример построения таких характеристик иллюстрирует рис. 5.

1

$22 \oplus 32 \leftarrow 24 \oplus 28$

$24 \oplus 28 \leftarrow 7 \oplus 12$

$7 \oplus 12 \oplus 22 \oplus 32 \leftarrow 27 \oplus 29$

$24 \oplus 27 \oplus 28 \oplus 29 \leftarrow 7 \oplus 12 \oplus 22 \oplus 32$

$0_x \leftarrow 0_x$

2

$7 \oplus 12 \leftarrow 27 \oplus 29$

$27 \oplus 29 \leftarrow 22 \oplus 32$

$7 \oplus 12 \oplus 22 \oplus 32 \leftarrow 24 \oplus 28$

$24 \oplus 27 \oplus 28 \oplus 29 \leftarrow 7 \oplus 12 \oplus 22 \oplus 32$

$0_x \leftarrow 0_x$

3

$24 \oplus 28 \leftarrow 7 \oplus 12$

$7 \oplus 12 \leftarrow 27 \oplus 29$

$24 \oplus 27 \oplus 28 \oplus 29 \leftarrow 7 \oplus 12 \oplus 22 \oplus 32$

$22 \oplus 32 \leftarrow 24 \oplus 27 \oplus 28 \oplus 29$

$0_x \leftarrow 0_x$

4

$27 \oplus 29 \leftarrow 22 \oplus 32$

$22,32 \leftarrow 24 \oplus 28$

$24 \oplus 27 \oplus 28 \oplus 29 \leftarrow 7 \oplus 12 \oplus 22 \oplus 32$

$7 \oplus 12 \leftarrow 24 \oplus 27 \oplus 28 \oplus 29$

$0_x \leftarrow 0_x$

5

$27 \oplus 29 \leftarrow 22 \oplus 32$

$22 \oplus 32 \leftarrow 24 \oplus 27 \oplus 28 \oplus 29$

$24 \oplus 28 \leftarrow 7 \oplus 12$

$7 \oplus 12 \oplus 22 \oplus 32 \leftarrow 24 \oplus 28$

$0_x \leftarrow 0_x$

6

$24 \oplus 28 \leftarrow 7 \oplus 12$

$7 \oplus 12 \leftarrow 24 \oplus 27 \oplus 28 \oplus 29$

$27 \oplus 29 \leftarrow 22 \oplus 32$

$7 \oplus 12 \oplus 22 \oplus 32 \leftarrow 27 \oplus 29$

$0_x \leftarrow 0_x$

Рис. 5

Из приведенных на рис. 5 характеристик четыре: 1, 2, 3 и 4–содержат восемь активных S-блоков, а 5 и 6 – шесть. Все шестиблочные характеристики имеют двублочные циклы, которые состоят из однобитных переходов, причем, хотя бы три из этих переходов имеются в списке ограничений условий У-4. Легко убедиться, что использование при построении таких характеристик хотя бы двух однобитных переходов из списка ограничений У-4 уже обеспечивает полную их безопасность для атак линейного криптоанализа:

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

Но все же существуют десятицикловые характеристики, которые требуют дополнительных ограничений. Они могут быть построены на основе использования циклических двубитных переходов. Условием их образования является использование S- блоков, выходы которых инициируют входы двух смежных S-блоков очередного цикла. Таких S-блоков три: S_5 (3 и 8 биты), S_6 (4 и 11 биты), и S_7 (7 и 12 биты). Примеры построения таких характеристик представлены на Рис. 6.

1	3	5
17,18 ← 5 2	5 ← 28,31 1	5 ← 28,31 1
5 ← 28,31 1	28,31 ← 3,8 2	28,31 ← 3,5,8 2
17,18,28,31 ← 3,8 2	3,5,8 ← 17,18,28,31 2	3,8 ← 17,18 1
3,5,8 ← 17,18,28,31 2	17,18 ← 3,5,8 2	17,18,28,31 ← 3,8 2
$0_x \leftarrow 0_x$	$0_x \leftarrow 0_x$	$0_x \leftarrow 0_x$
2	4	6
28,31 ← 3,8 2	3,8 ← 17,18 1	3,8 ← 17,18 1
3,8 ← 17,18 1	17,18 ← 5 2	17,18 ← 3,5,8 2
17,18,28,31 ← 5 2	3,5,8 ← 17,18,28,31 2	5 ← 28,31 1
3,5,8 ← 17,18,28,31 2	28,31 ← 3,5,8 2	17,18,28,31 ← 5 2
$0_x \leftarrow 0_x$	$0_x \leftarrow 0_x$	$0_x \leftarrow 0_x$

Рис. 6

Действительно, как показывает анализ завершающей цикловую функцию *P*-подстановки, существуют пары смежных S-блоков, входящие в двублочный циклический переход, которые можно активизировать дополнительным входным битом (одним), входящим в еще один одноблочный циклический переход, причем последний имеет общие биты с исходным двублочным циклическим переходом. Всего существует три S-блока, выходы которых активизируют одновременно два смежных S-блока: S_5 (выходные биты *P*-подстановки 3,8 – входы S-блоков S_1, S_2), S_6 (выходные биты *P*-подстановки 4,11 – входы S блоков S_2, S_3) и S_7 (выходные биты *P*-подстановки 7,12 – входы S-блоков S_3, S_4). В первом случае возникает дополнительные циклические переходы 5 ← 28,31 ← 5, во втором – 8 ← 16,18 ← 8 и в третьем – 8 ← 16,18 ← 8, причем, нас интересуют только характеристики, при построении которых используются одноблочные циклы. Для десятицикловой характеристики из двублочных циклов хотя бы один будет состоять из S- блоков с однобитными переходами.

Характеристики под номерами 1 и 2 содержат по два однобитных перехода, а для характеристики 1 один из переходов имеет нулевую вероятность. И тогда для вероятности пятнадцатицикловой характеристики получаем оценку

$$\left[\left(\frac{4}{64}\right)^2 \cdot \left(\frac{16}{64}\right)^5 \cdot 2^6\right]^3 \cdot 2^2 = 2^{-34}.$$

Но зато все другие характеристики действительно строятся или могут быть построены без однобитных переходов. Следовательно, здесь уже ограничение У-4 не работает. В то же время рассматриваемые характеристики гарантированно имеют минимум два

цикла с двубитными входами, при этом выходы S-блоков этих циклов могут иметь не более чем двубитные выходы. Общее число активных S-блоков, приходящееся на симметричную половину такой характеристики, равно 6 или 7. Здесь можно воспользоваться условием L-4, введенным корейскими учеными для перекрытия восьмицикловых характеристик (в наших обозначениях – это условие У-5, введенное для перекрытия шестицикловых характеристик и уже использованное выше для перекрытия десятицикловых характеристик).

Для характеристик 3-6, рис.7, все S-блоки удовлетворяют условию У-5. В этом случае для вероятности пятнадцатицикловой характеристики получим оценку

$$\left[\left(\frac{10}{64}\right)^7 \cdot 2^6\right]^3 \cdot 2^2 = 2^{-36}.$$

В приведенных выше расчетах не учитывается еще один дополнительный цикл и возможность свободного выбора начального и заключительного циклов линейной аппроксимации. Однако во всех рассмотренных случаях имеется запас, позволяющий заключить, что десятицикловые характеристики являются защищенными от атаки линейного криптоанализа.

Других дополнительных ограничений в виде Условия L-5, использованного корейскими учеными, здесь уже не требуется.

Требования к отбору S-блоков, защищенных от атак ЛК на двенадцатицикловые итеративные линейные аппроксимационные характеристики

В этом случае анализу подлежат характеристики с общим число S-блоков, приходящихся на двенадцать, четырнадцать и шестнадцать циклов меньшее 17, 19,22 соответственно

$$\left(\frac{16}{64}\right)^{22} \cdot 2^{15} = 2^{-29}.$$

Для этих характеристик выполняется циклический переход $Z \oplus \Psi \leftarrow \Phi \oplus \Theta \leftarrow Z \oplus \Psi$, при этом для первой из них являются допустимыми переходы $Z \leftarrow \Phi$, $Z \leftarrow \Theta$, $\Phi \leftarrow \Psi$ и $\Theta \leftarrow \Psi$. Но тогда являются допустимыми переходы $\Psi \leftarrow \Phi$ и $\Psi \leftarrow \Theta$. Граф переходов для этой характеристики представлен под соответствующим номером на рис.8. Из этого графа следует, что рассматриваемая характеристика может быть построена на основе двух однобитных переходов с общим битом. Все такие пары циклических однобитных переходов (их всего семь) имеют несовпадающие биты, принадлежащие входам одного и того же S-блока, и, следовательно, в этом случае переход $Z \oplus \Psi \leftarrow \Phi \oplus \Theta$ является одноблочным. В результате рассматриваемая двенадцатицикловая харктеристика является одноблочной – ее т.е. и характеристики этого типа оказываются не опасными для атак ЛК.

Пример характеристики второго типа также приведен на рис.8, а на рис.7 под соответствующим номером приведен ее граф переходов.

Симметричная половина содержит 5 S-блоков. Ограничение У-4 на однобитные переходы в этом случае обеспечивает полное перекрытие таких характеристик.

Понятно, что если хотя бы один из однобитных переходов имеет нулевую вероятность, то такая характеристика нереализуема. Пример построения характеристики рассматриваемого вида приведен на рис. 8.

$$\left(\frac{4}{64}\right)^{21} \cdot 2^{15} = 2^{-69}.$$

Подчеркнем, что и в характеристиках неминимального типа (использующих свободу в выборе выходов S-блоков) имеются однобитные переходы (обеспечивающие согласование с тождественными циклами). Их сохраняется четыре на двенадцатицикловую характеристику, что приводит к оценке

$$\left(\frac{16}{64}\right)^{12}\cdot\left(\frac{4}{64}\right)^{9}\cdot 2^{15}=2^{-45},$$

1

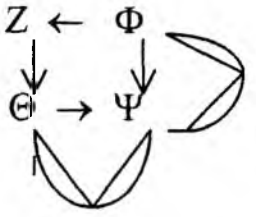
$$Z \leftarrow \Phi$$
$$\Phi \leftarrow \Psi$$
$$Z\oplus\Psi \leftarrow \Phi\oplus\Theta$$
$$\Theta \leftarrow \Psi$$
$$Z \leftarrow \Theta$$
$$0_x \leftarrow 0_x$$
$$Z \leftarrow \Theta$$
$$\Theta \leftarrow \Psi$$
$$Z\oplus\Psi \leftarrow \Phi\oplus\Theta$$
$$\Phi \leftarrow \Psi$$
$$Z \leftarrow \Phi$$
$$0_x \leftarrow 0_x$$

12-цикловая итеративная характеристика 1

2

$$Z \leftarrow \Phi$$
$$\Phi \leftarrow \Psi$$
$$Z\oplus\Psi \leftarrow \Phi\oplus\Theta$$
$$\Theta \leftarrow Z$$
$$\Psi \leftarrow \Theta$$
$$0_x \leftarrow 0_x$$
$$\Psi \leftarrow \Theta$$
$$\Theta \leftarrow Z$$
$$Z\oplus\Psi \leftarrow \Phi\oplus\Theta$$
$$\Phi \leftarrow \Psi$$
$$Z \leftarrow \Phi$$
$$0_x \leftarrow 0_x$$

12-цикловая итеративная характеристика 2



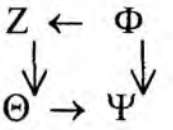


Рис. 7

Для этой характеристики оказываются в силе все высказанные выше соображения, и она также оказывается не опасной для атак ЛК.

Остается заметить, что в принципе можно построить двенадцатицикловую итеративную характеристику и без тождественных циклов, но она попадает в число нереализуемых – содержит нереализуемую композицию циклических однобитных переходов. Подобные же общие соображения можно высказать и об итеративных четырнадцатицикловых и шестнадцатицикловых характеристиках, и, значит, никаких дополнительных ограничений для итеративных характеристик с числом циклов превышающем десять не требуется.

Подводя итоги результатам исследований, представленных в этой и предшествующих работах [1,2], можно прийти к общему выводу, состоящему в том, что конечный набор критериев для отбора таблиц подстановок шифра DES,

1
$23 \leftarrow 1\ 1$

$1 \leftarrow 17$ 1
$17,23 \leftarrow 1,3$ 1

$3 \leftarrow 17$ 1
$23 \leftarrow 3$ 1

$0_x \leftarrow 0_x$

2.1

$17 \leftarrow 3$ 1

$3 \leftarrow 18$ 1

$17,18 \leftarrow 3,8$ 2

$8 \leftarrow 17$ 1

$18 \leftarrow 8$ 1

$0_x \leftarrow 0_x$

2.2

$8 \leftarrow 17$ 1

$17 \leftarrow 3$ 1

$3,8 \leftarrow 17,18$ 1

$18 \leftarrow 8$ 1

$8 \leftarrow 18$ 1

$0_x \leftarrow 0_x$

Рис. 8

устойчивых к атакам линейного криптоанализа, кроме требований разработчиков, на наш взгляд, должен включать в себя также следующие дополнительные ограничения:

Условие У-1′ (объединенные У-4 и У-6; условие перекрытия шестицикловых и восьмицикловых итеративных аппроксимаций с однобитными переходами). Для ТРЛА S -блоков необходимо выполнить следующие (общее число 28 случаев) условия:

- *S*1-блок: $|NS_1(4_x, 4_x)| \le 4$, $|NS_1(2_x, 2_x)| \le 4$, $|NS_1(8_x, 8_x)| \le 4$ $|NS_1(10_x, 4_x)| \le 4$;
- *S*2-блок: $|NS_2(4_x, 4_x)| \le 4$, $|NS_2(2_x, 1_x)| \le 4$, $|NS_2(8_x, 8_x)| \le 4$ $|NS_2(10_x, 4_x)| \le 4$;
- *S*3-блок: $|NS_3(8_x, 4_x)| \le 4$, $|NS_3(4_x, 8_x)| \le 4$, $|NS_3(2_x, 8_x)| \le 4$;
- *S*4-блок: $|NS_4(8_x, 4_x)| \le 4$, $|NS_4(2_x, 2_x)| \le 4$, $|NS_4(4_x, 1_x)| \le 4$;
- *S*5-блок: $|NS_5(16_x, 1_x)| \le 4$, $|NS_5(8_x, 8_x)| \le 4$, $|NS_5(2, 4)| \le 4$ $|NS_5(4_x, 2_x)| \le 4$;
- *S*6-блок: $|NS_6(16_x, 4_x)| \le 4$, $|NS_6(4_x, 8_x)| \le 4$, $|NS_6(2_x, 2_x)| \le 4$ $|NS_6(8_x, 4_x)| \le 4$;
- *S*7-блок: $|NS_7(4_x, 8_x)| \le 4$, $|NS_7(2_x, 1_x)| \le 4$, $|NS_7(8_x, 4_x)| \le 4$;
- *S*8-блок: $|NS_8(16_x, 1_x)| \le 4$, $|NS_8(2_x, 4_x)| \le 4$, $|NS_8(4_x, 8_x)| \le 4$.

Условие У-2′ (условие У-7 перекрытия восьмицикловых итеративных характеристик). Элементы ТРЛА пар S-блоков со выходными масками, удовлетворяющие условию $W(\alpha) = 1$, $W(\beta_1 \oplus \beta_2) = 1$, должны подчиняться ограничению:

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

Условие У-3' (условие У-3; условие защиты от атак на четырехцикловые и восьмицикловые итеративные характеристики). Элементы ТРЛА пар S-блоков, имеющие входные и выходные маски, удовлетворяющие условию $W(\alpha) \le 2$, $W(\beta_1 \oplus \beta_2) \le 2$, кроме ситуации $W(\alpha) = 2$, $W(\beta_1 \oplus \beta_2) = 2$ должны подчиняться ограничению:

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

Условие У-4′ (условие У-5 защиты от атак ЛК на шестицикловые, восьмицикловые и десятицикловые итеративные аппроксимации). Элементы ТРЛА S-блоков, удовлетворяющие условиям $W(\alpha)$, $W(\beta) \le 2$, должны подчиняться ограничению $|NS(\alpha, \beta)| \le 10$.

В приведенных соотношениях $\alpha \in GF(2)^6$, $\beta \in GF(2)^4$, $W(\alpha)$ – вес битового входа, а $W(\beta)$ – вес битового выхода S блока.

Список литературы: 1. *И .В. Лисицкая, 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 // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып 119. С. 117-190. 2. *И. В. Лисицкая, 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 // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2002. Вып 124. С. - .

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 19.03.2002