УДК 681.3.06: 519.248.681

В.И. ДОЛГОВ, д-р техн. наук, И.В. ЛИСИЦКАЯ, канд. техн. наук, В.И. РУЖЕНЦЕВ

ОБЕСПЕЧЕНИЕ СТОЙКОСТИ ШИФРА DES К АТАКАМ ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА. ПЕРЕКРЫТИЕ ШЕСТИ-, ВОСЬМИ- И ДЕСЯТИЦИКЛОВЫХ ИТЕРАТИВНЫХ ХАРАКТЕРИСТИК

В этой работе мы продолжим обсуждение требований к отбору S-блоков для шифра DES, устойчивых к атакам дифференциального криптоанализа, начатое в предыдущей публикации [1]. Теперь нас будут интересовать шести-, восьми- и десятицикловые итеративные характеристики, представленные на рис. 1 под номерами 4-9.

1

$0_x \leftarrow \Gamma$

$0_x \leftarrow 0_x$

2-х цикловая итеративная характеристика

2

$\Phi \leftarrow \Gamma$

$0_x \leftarrow \Phi$

$\Phi \leftarrow \Gamma$

$0_x \leftarrow 0_x$

4-х цикловая итеративная характеристика

3

$\Phi \leftarrow \Gamma$

$\Gamma \oplus \Psi \leftarrow \circledcirc$

$\Phi \leftarrow \Psi$

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

4-х цикловая итеративная характеристика

4

$\Phi \leftarrow \Gamma$

$\Gamma \leftarrow \Phi$

$0_x \leftarrow 0_x$

$\Gamma \leftarrow \Phi$

$\Phi \leftarrow \Gamma$

$0_x \leftarrow 0_x$

6-ти цикловая итеративная характеристика

5

$\Phi \leftarrow \Gamma$

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

$\circledcirc \leftarrow \Psi$

$\Gamma \leftarrow \Phi$

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

$\Psi \leftarrow \circledcirc$

6-ти цикловая итеративная характеристика

6

$\Phi \leftarrow \Gamma$

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

$\circledcirc \leftarrow \Psi$

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

$\circledcirc \leftarrow \Gamma$

$\Psi \leftarrow \Phi \oplus \circledcirc$

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

$\Psi \leftarrow \circledcirc$

8-ми цикловая итеративная характеристика

7

$\Phi \leftarrow \Gamma$

$\Psi \leftarrow \Phi$

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

$0_x \leftarrow 0_x$

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

$\Psi \leftarrow \Phi$

$\Phi \leftarrow \Gamma$

$0_x \leftarrow 0_x$

8-ми цикловая итеративная характеристика

8

$\Phi \leftarrow \Gamma$

$\Psi \leftarrow \Phi$

$\circledcirc \leftarrow \Gamma \oplus \Psi$

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

$0_x \leftarrow 0_x$

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

$\circledcirc \leftarrow \Gamma \oplus \Psi$

$\Psi \leftarrow \Phi$

$\Phi \leftarrow \Gamma$

$0_y \leftarrow 0_y$

10-ти цикловая итеративная характеристика

9

$\Phi \leftarrow \Gamma$

$\Psi \leftarrow \Phi \oplus \circledcirc$

$\circledcirc \leftarrow \Gamma \oplus \Psi$

$\Gamma \leftarrow \Phi$

$\Phi \oplus \circledcirc \leftarrow \Psi$

$\Gamma \oplus \Psi \leftarrow \circledcirc$

$\Phi \leftarrow \Gamma$

$\Psi \leftarrow \Phi \oplus \circledcirc$

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

$\Psi \leftarrow \circledcirc$

10-ти цикловая итеративная характеристика

Рис. 1

На рис. 2 под соответствующими номерами приведены графы переходов рассматриваемых итеративных дифференциальных характеристик.

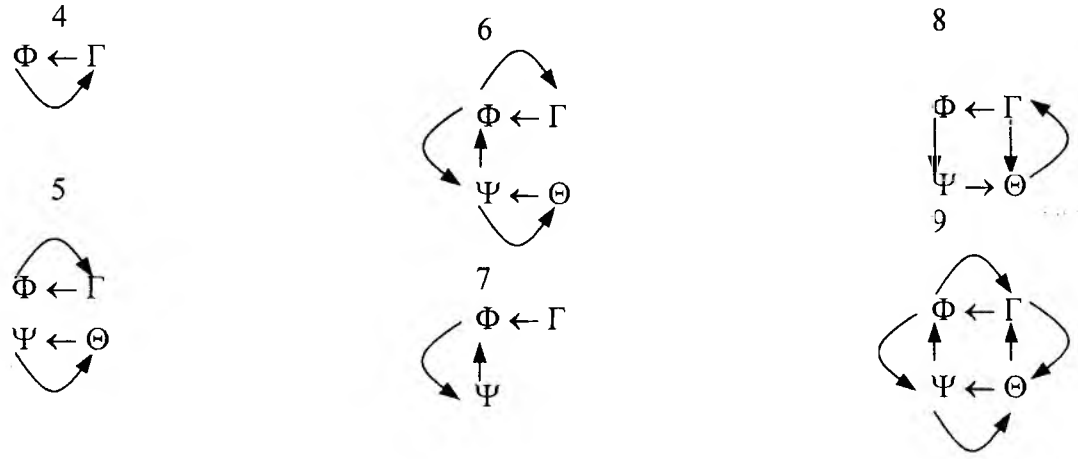

Рис. 2

Перекрытие атак, использующих шестицикловые итеративные характеристики

Рассмотрим первую из шестицикловых итеративных характеристик с очень простым графом переходов, представленным под номером 4 на рис. 2. Эта характеристика, как следует из графа, строится с использование одного циклического перехода Г ← Ф ← Г. Расчеты показывают, что перекрытию подлежат все подобные характеристики, имеющие менее семи S-блоков на каждую свою симметричную половину (два активных цикла)

$$\left[\left(\frac{16}{64}\right)^{n}\right]^{4} = 2^{-8n} > 2^{-56} \Rightarrow n \le 6.$$

Главной особенностью шестицикловых характеристик этого типа является то, что они не допускают свободных значений входов и выходов S-блоков, участвующих в их построении. Поэтому здесь достаточно будет рассмотреть только условия перекрытия собственно циклических переходов шифра DES. Представим эти условия в виде утверждений, приведенных ниже.

Утверждение 1. Циклический переход, содержащий одноблочный цикл, строится с использованием однобитных переходов.

Справедливость этого утверждение следует из самого принципа построения примененной в шифре DES *P*-подстановки, в соответствии с которым выходные биты каждого (одного) S-блока распределяются по одному на входы различных S-блоков [2], и поэтому замыкание циклического перехода и при двух исходных битах (в одном отдельном активном S-блоке могут инициироваться только два внутренних бита) будет происходить с использованием однобитных переходов.

Заметим также, что примененная в шифре DES расширяющая *E*-перестановка позволяет одному (отдельному) S-блоку войти в циклический переход только двумя своими внутренними битами. Последующая *P*-подстановка приводит к тому, что в циклический переход, использующий внутренний бит любого S-блока, всегда содержит и бит, инициирующий два смежных S-блока. Кроме того, все полученные активные S-блоки будут однобитными, и каждый из них обязательно активизирует минимум 2 S-блока, т.е. возврат к единственному начальному активному S-блоку невозможен. Поэтому для шифра DES справедливо утверждение 2.

Утверждение 2. В шифре DES циклические переходы с использованием одноблочных циклов невозможны.

Утверждение 3. Любой циклический переход, содержащий два активных S-блока в каждом цикле, строится с использованием однобитных переходов.

Справедливость этого утверждения вытекает из того, что один из 2-х активных S-блоков на 2-м цикле всегда будет однобитным, следовательно, без использования однобитных переходов исключается возможность активизации на следующем цикле исходных 2-х S-блоков (будет активизировано либо три S-блока, либо два, но других).

Очевидно, что, учитывая утверждения 2 и 3, можно считать одноблочно-*n*-блочные (1+1, 1+2, 1+3, 1+4, 1+5) и двублочные (2+2) шестицикловые характеристики защищенными от атак дифференциального криптоанализа (во всех этих случаях характеристики строятся с использованием однобитных переходов, а они по требованиям разработчиков стандарта запрещены).

В результате остается рассмотреть характеристики вида 4, которые строятся без использования однобитных переходов и переходов 6_x в однобитный выход (см. требование 5 разработчиков стандарта [1]), с числом S-блоков, приходящихся на четыре активных цикла (шестицикловой характеристики), большим четырех. Анализ показывает, что существует две такие характеристики с пятью S-блоками типа 3+2+0: это циклический переход 3,4,8,11 ← 18,23 ← 3,4,8,11 и циклический переход 7,8,12,14 ← 18,26 ← 7,8,12,14, девять характеристик типа 3+3+0:

3,4,8,10,11 ← 16,17,18,23 ← 3,4,8,10,11;
4,5,7,11 ← 23,24,28,31 ← 4,5,7,11;
1,3,6,30 ← 13,17,18 ← 1,3,6,30;
3,4,7,32 ← 18,21,23,27 ← 3,4,7,32;
1,2,26,30 ← 7,9,12,15 ← 1,2,26,30;
1,3,26,29 ← 15,17,21,22,23 ← 1,3,26,29;
7,8,11,12,13 ← 18,20,24,26 ← 7,8,11,12,13;
7,8,12,14,15 ← 18,26,28,30 ← 7,8,12,14,15;
11,19,21,22 ← 24,25,29,30 ← 11,19,21,22,

а также характеристики типа 4+2+0.

Что касается характеристик типа 4+2+0, то можно легко убедиться, что и они для шифра DES нереализуемы. Для этого рассмотрим примеры таких характеристик.

3,10,11 ← 16,17,23,24; 30_x в 0; 6,8,14,16 ← 10,18; 30_x в 0, 30_x в 0;
22,24,30,32 ← 11,27;30_x в 0, 4_x в 0.

Все они при своем построении используют обнуляющий переход S-блоков со входами 30_x, который в соответствии с условием У-1([1]) имеет вероятность перехода в ноль равную нулю.

Для перекрытия характеристик типа 3+2+0 и 3+3+0 можно воспользоваться ограничением, рассмотренным в [3], в соответствии с которым вероятности переходов активных S-блоков, участвующих в формировании трехблочного цикла, ограничиваются значением $\frac{1}{8}$. В этом случае значение вероятности 13-ти цикловой характеристики типа 3+2+0 будет не больше чем

$$\left[\left(\frac{8}{64}\right)^3 \cdot \left(\frac{16}{64}\right)^2\right]^4 \cdot \left(\frac{16}{64}\right)^2 = 2^{-56}.$$

Это ограничение по своему смыслу представляется в каком-то смысле похожим на требование 8 разработчиков стандарта, хотя и подходя строго, точный смысл этого требования из доступных публикаций нам выяснить так и не удалось. Мы обозначим здесь это ограничение условием 3, которое представим в следующем "усиленном" виде.

Условие 3 (У-3). Для трех одновременно активных *S*-блоков со значениями весов выходов таблиц распределения разностей $W(\beta) \le 2$, должно выполняться ограничение

$$\left|NS_i(\alpha,\beta) \cdot NS_{i+1}(\alpha,\beta) \cdot NS_{i+2}(\alpha,\beta)\right| \le 8^3,$$

где, как и ранее, $\alpha \in GF(2)^6$, $\beta \in GF(2)^4$ – значения входов в таблицы разностей по строкам и столбцам.

Очевидно, что это ограничение делает неопасными для атак ДК и характеристики типа 3+3+0.

Что касается шестицикловой итеративной характеристики под номером 5 на рис. 1, то, как следует из ее графа переходов (см. рис.2), для этой характеристики необходимо, чтобы одновременно выполнялось два не связанных между собой циклических перехода. Очевидно, что здесь применимы все рассуждения, которые были изложены при изучении реализуемости характеристики под номером 4. Это позволяет прийти к выводу, что характеристика 5 для шифра DES при выполнении всех рассмотренных выше ограничений также будет нереализуемой.

Перекрытие атак, использующих восьмицикловые итеративные характеристики

К итеративным характеристикам этого типа относятся характеристики под номерами 6 и 7 на рис. 1. Характеристику 6 (рис. 1) сразу следует отнести к числу нереализуемых, что следует из вида ее графа переходов, приведенного под соответствующим номером на рис. 2. Это еще более усложненный вариант графа 3 рис. 2 из работы [1], рассмотренного ранее при изучении четырехцикловых итеративных характеристик.

Внимания по обеспечению защищенности шифра DES от атак дифференциального криптоанализа, безусловно, заслуживают дифференциальные характеристики, строящиеся с использованием восьмицикловых итеративных характеристик 7 (рис. 1). Граф переходов для характеристики 7 представлен под соответствующим номером на рис. 2. Как следует из графа этой характеристики, она повторяет характеристику под номером 4 с одним циклическим переходом, рассмотренную ранее, только теперь в графе появился свободный переход из дополнительной его вершины Г в одну из его вершин ($\Phi \leftarrow \Gamma \oplus \Psi$). Переход свободный в том смысле, что вершина Г не входит ни в какой циклический переход, и ее значение может выбираться произвольным (в пределах возможностей варьирования входными битами S-блоков, определяемых входом Ψ).

Если идти дальше, то можно убедиться, что характеристика типа 7 допускает еще один вариант представления, который вместе с исходным изображен (без зеркальных половинок) на рис. 3. На этом же рисунке приведены графы переходов характеристик обоих типов, из которых следует их основное различие: во втором случае граф строится с использованием двух циклических переходов с общей вершиной Ф.

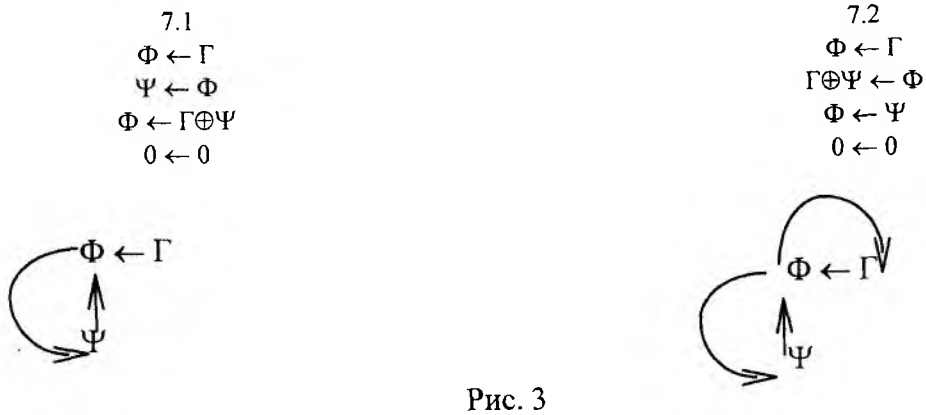

Рис. 3

На рис. 4 представлены примеры построения таких характеристики для обоих вариантов.

7.1.1

8 ← 17 (14,15,16,18,19) 2
18 ← 8 2
8 ← 17,18 (14,15,16,18,19) 2
0 ← 0

Здесь входы F_x и 20_x переходят в ноль

7.1.2.

17,18 ← 4 (2,5,6,7,9,10,11) 2(3)
3,8 ← 17,18 2
17,18 ← 3,4,8 (2,5,6,7,9,10,11) 3
0 ← 0

Здесь входы 1_x, $1C_x$ и $3C_x$ переходят в ноль

7.1.3

3,4,8,11 ← 18,23 (19,20,21,22) 2
18,23 ← 3,4,8,11 3
3,4,8,11 ← (19,20,21,22) 2
0 ← 0

Здесь вход 24_x, переходит в ноль

7.2.1

1 ← 17 (14,16,18,19)2
15,17 ← 1 2
1 ← 15 (14,16,18,19)2
0 ← 0

Здесь входы 10_x, $3C_x$ и $2C_x$ переходят в ноль

7.2.2

28,31 ← (2,3,4,6,7) 2
5 ← 28,31 2
28,31 ← 5 (2,3,4,6,7) 2
0 ← 0

Здесь вход 2_x переходит в ноль

7.2.3

3,8 ← 18 (14,15,16,19) 1(2)
17,18 ← 3,8 2
3,8 ← 17 (14,15,16,19) 2
0 ← 0

Здесь вход E_x, 1_x, F_x и 20_x переходят в ноль

Рис. 4

Заметим, что для шифра DES необходимо перекрыть восьмицикловые характеристики с общим числом S-блоков, приходящихся на симметричную половину восьмицикловой характеристики, не превышающим 8. На рис. 4 представлены примеры построения характеристик с шестью и семью S-блоками.

Очевидно, что восьмицикловые характеристики этого типа, независимо от того используются ли при их построении однобитные переходы или переходы обнуляющего типа, попадают под ограничение У-2 [1] (наличие двух пар S-блоков, удовлетворяющих ограничению У-2, как показано ранее, уже обеспечивает защиту восмицикловых характеристик от атак ДК). Характеристик вида 7.1 и 7.2 с числом S-блоков, меньшим восьми и не содержащих запрещенных переходов, нам просто не удалось найти.

В результате можно сделать вывод, что для перекрытия восьмицикловых итеративных характеристик оказывается вполне достаточным ограничений на отбор S-блоков, использованных разработчиками стандарта и ранее введенного ограничения У-2 [1].

Анализ десятицикловых итеративных характеристик и характеристик с бо́льшим числом циклов

Здесь нас будут интересовать десятицикловые итеративные характеристики. Теоретически возможные варианты таких характеристик (их половинки без зеркальных дополнений), построенные для различных композиций входов и выходов итеративных характеристик с тождественными циклами, представлены на рис. 5.

Расчеты показывают, что перекрытию подлежат все подобные характеристики, имеющие менее двенадцати (одиннадцать и менее) S-блоков на каждую из симметричных половинок:

$$\left(\frac{16}{64}\right)^{12\cdot2+2\cdot2} = 2^{-56}, \left(\frac{16}{64}\right)^{11\cdot2+2\cdot2} = 2^{-52}.$$

Покажем, что характеристики типа 1 (рис. 5) минимального и неминимального типов для шифра DES нереализуемы только за счет ограничений разработчиков стандарта. Изучим для этого особенности построения этих характеристик в зависимости от числа S-блоков последнего цикла (цикла $\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$).

1	3	5
$\Phi \leftarrow \Gamma$	$\Psi \leftarrow \Phi$	$\Psi \leftarrow \Phi$
$\Psi \leftarrow \Phi$	$\Theta \leftarrow \Psi$	$\Phi\oplus\Theta \leftarrow \Psi$
$\Theta \leftarrow \Gamma\oplus\Psi$	$\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$	$\Gamma \leftarrow \Theta$
$\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$	$\Phi\oplus\Theta \leftarrow \Gamma$	$\Theta \leftarrow \Gamma\oplus\Psi$
$0 \leftarrow 0$	$0 \leftarrow 0$	$0 \leftarrow 0$
2	4	6
$\Theta \leftarrow \Psi$	$\Gamma \leftarrow \Theta$	$\Gamma \leftarrow \Theta$
$\Gamma \leftarrow \Theta$	$\Phi \leftarrow \Gamma$	$\Phi\oplus\Theta \leftarrow \Gamma$
$\Phi \leftarrow \Gamma\oplus\Psi$	$\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$	$\Psi \leftarrow \Phi$
$\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$	$\Phi\oplus\Theta \leftarrow \Psi$	$\Phi \leftarrow \Gamma\oplus\Psi$
$0 \leftarrow 0$	$0 \leftarrow 0$	$0 \leftarrow 0$

Рис. 5

Сначала рассмотрим вариант, когда входы Φ и Θ являются входами в одноблочный цикл. Тогда они должны быть внутренними битами входов S-блока, причем в этом случае один из этих внутренних битов – бит Φ входит в циклический переход $\Phi \leftarrow \Gamma \leftarrow \Phi$ (из самого вида характеристики 1 следует, что одновременно справедливы два перехода: переход $\Phi \leftarrow \Gamma$ и для одноблочного перехода $\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$ следует справедливость перехода $\Gamma \leftarrow \Phi$). В результате справедлив циклический переход $\Phi \leftarrow \Gamma\oplus\Psi \leftarrow \Phi$. С другой стороны, справедлив и переход $\Theta \leftarrow \Gamma\oplus\Psi$, а значит, выполняется и циклический переход $\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta \leftarrow \Gamma\oplus\Psi$. Из восьми вариантов внутренних битов S-блоков шифра DES только шесть могут образовать двухбитные циклические переходы. Это 2,3 ← 9,17 ← 2,3; 10,11 ← 16,24 ← 10,11; 18,19 ← 8,25 ← 18,19; 22,23 ← 4,29 ←22,23; 6,27 ← 12,32 ← 26,27. Все они, как показывает анализ, имеют вторую пару бит, которые являются входным битом в два смежных S-блока, так что цикл $\Theta \leftarrow \Gamma\oplus\Psi$ должен быть четырехблочным, а цикл $\Phi \leftarrow \Gamma$ – двублочным. Если теперь вспомнить, что в четырехблочном цикле $\Theta \leftarrow \Gamma\oplus\Psi$ (содержащим две пары смежных S-блоков) три S-блока из четырех имеют нулевые выходы и один из входов в пару S-блоков (вход Ψ) не имеет свободы выбора своих значений (в пределах значений входов S-блока), т.е. является однобитным, то можно прийти к выводу, что характеристики рассмотренного типа (когда цикл $\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$ – одноблочный) в условиях выполнения ограничений разработчиков стандарта на переходы S-блоков в ноль нереализуемы.

Если цикл $\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta$ – двухблочный, то здесь могут представиться два случая:

- Φ и Θ – это однобитные входы разных (разнесенных) S-блоков;
- Φ и Θ – двубитный вход в два смежных S-блока.

Если Φ и Θ – однобитные входы разных (разнесенных) S-блоков, то это опять внутренние биты, но теперь уже разных S-блоков. И в этом случае должен выполняться циклический двубитный переход $\Gamma\oplus\Psi \leftarrow \Phi\oplus\Theta \leftarrow \Gamma\oplus\Psi$. Обратим теперь внимание на то, что циклические переходы (двухбитные), составленные только из внутренних битов различных S-блоков, для шифра DES невозможны (приведем здесь список переходов внутренних битов входов S-блоков во внутренние: 2,3 → 23,31; 6,7 → 2,18; 10,11 → 6,30; 14,15 → 10,26; 18,19 → 3,14; 22,23 → 11,19; 26,27 → 7,22; 30,31 → 15,27). Это означает, что в рассматриваемом случае один из битов входов Γ или Ψ цикла $\Theta \leftarrow \Gamma\oplus\Psi$ (или оба вместе) не будет внутренним битом входа S-блока, а будет входным битом одновременно в два S-блока. Но тогда цикл $\Theta \leftarrow \Gamma\oplus\Psi$ будет как минимум двублочным (см. характеристику 1.1, рис. 6). В этом цикле в соответствии с *видом характеристики один из входов (вход Ψ) является несвободным. Но тогда, так как выходом этого цикла является один (единственный) бит, а цикл как минимум двублочный, этот цикл* будет содержать хотя бы один S-блок с однобитным переходом или переходом одного бита входа в ноль. Следовательно, и характеристики этого типа для шифра DES нереализуемы.

1.1		1.2		1.3	
14 ← 17 (18,19)	2	18 ← 8 (6,7,9,10,11)	2	4 ← 20 (18,19,21,22)	2
10 ← 14 (15)	1	3 ← 18 (19)	1	23 ← 4 (2,3,5,6,7)	2
3 ← 10,17 (18,19)	3	17 ← 3,8 (6,7,9,10,11)	3	14 ← 20,23 (18,19,21,22)	2
10,17 ← 3,14 (15)	2	3,8 ← 17,18 (19)	2	20,23 ← 4,14 (2,3,5,6,7)	3
0 ← 0		0 ← 0		0 ← 0	
Есть однобитный переход		Есть однобитный переход		Есть однобитный переход	

Рис. 6

Эти же условия (наличие в цикле $\Theta \leftarrow \Gamma \oplus \Psi$ S-блока с однобитным переходом, либо пе реходом одного бита входа в ноль) сохраняются и во втором случае, когда Ф и Θ – это дву битный вход в два смежных S-блока (см. характеристику 1.2 (рис. 6)).

Если цикл $\Gamma \oplus \Psi \leftarrow \Phi \oplus \Theta$ трехблочный, то хотя бы один вход Ф или Θ в этот цикл – эт общий бит входа в два смежных S-блока. В этом случае для одноблочного цикла $\Psi \leftarrow \Phi$ од нобитный вход Θ является входом в два смежных S-блока, который для этой характеристик не является свободным. В результате мы снова приходим к S-блокам с однобитными перехо дами и (или) переходами одного бита входа в ноль.

Если, наконец, цикл $\Psi \leftarrow \Phi$ – двублочный, то одноблочным (однобитным) является пе реход $\Gamma \leftarrow \Theta$, где внутренний бит входа в S-блок Θ для рассматриваемой характеристики н является свободным, и, следовательно, и в этом случае десятицикловые характеристики пе рекрываются за счет ограничений, использованных разработчиками стандарта (см. характе ристику 1.3, (рис. 6)).

Во всех рассмотренных случаях характеристики содержат также и переходы обнуляю щего типа (с однобитными входами).

Возможны также характеристики с дополнительными битами выходов S-блоков и харак теристики, использующие циклические переходы с числом битов, большим двух. Примерь построения таких характеристик также представлены на рис. 7.

1		3	
8 ← 17 (14,15,(16),19)	2	24 ← 11	1
(16)18 ← 8 (6,7,9,10,11)	2	11,19,22 ← 24	2
(1)3 ← 17,18 (14,15,19)	2	25,30 ← 11,19,21,22	3
17,18 ← (1),3,8 (6,7,9,10,11)	3	11,19,21,22 ← 24,25,30	3
0 ← 0		0 ← 0	
S-блоков больше 8		S-блоков больше 8	

2		4	
7 ← 26 (27)	1	4 ← 23 (22)	1
18 ← 7 (6)	1	18 ← 4 (2,5,6,7)	2
8,12,14 ← 18,26 (27)	2	3,8,11 ← 18,23 (22)	2
18,26 ← 7,8,12,14 (6)	3	18,23 ← 3,4,8,11 (2,5,6,7)	3
0 ← 0		0 ← 0	
Здесь вход 22_x, переходит в ноль и однобит- ные переходы (переходы 6_x в один бит)		Здесь вход 24_x, переходит в ноль и однобит- ные переходы (переходы 6_x в один бит)	

Рис. 7

В случае использования циклических переходов с бо́льшим числом активизируемых S блоков возможны и ситуации, когда обнуляющие переходы выходят за рамки ограничени разработчиков стандарта (см. примеры 2 и 4 (рис. 7)). Но зато для этих характеристик оказы вается характерным использование циклов со входами, которые включают внутренние бит S-блоков, и однобитными выходами. Такие переходы, как известно, запрещены разработчи ками стандарта.

Отмеченное позволяет сделать общий вывод о том, что десятицикловые характеристики типа 1 (рис. 5) для шифра DES нереализуемы.

Анализ показывает, что приведенные выше рассуждения полностью оказываются применимыми и для десятицикловой характеристики, представленной на рис. 5 под номером 2 (эта характеристика получается из 1, если символы Ф, Θ и Г, Ψ поменять местами).

Отмеченный дуализм характерен и для характеристик с номерами 3 и 4, а также 5 и 6 на рис. 5. Более того, для всех остальных характеристик, в том числе и для характеристик с числом S-блоков, большим десяти, оказываются справедливыми приведенные выше рассуждения, что позволяет их также считать неопасными для использования в атаках ДК.

Таким образом, обоснован набор требований к S-блокам, позволяющих решить задачу создания стойкого к дифференциальным атакам шифра DES. При этом уточнены критерии отбора S-блоков, разработанные ранее корейскими учеными [4]. Итоговый набор требований к отбору S-блоков, устойчивых к атакам дифференциального криптоанализа, включает в себя все требования разработчиков и следующие дополнительные условия:

Условие 1 (У-1). Для защиты от атак ДК на основе использования итеративных двухцикловых ДХ обнуляющего типа с числом активных S-блоков в двух циклах, меньшем восьми, необходимо и достаточно, чтобы дополнительно к требованию 6 разработчиков стандарта S-блоки не имели переходов в ноль еще для четырех входов: 32_x, 36_x, $3A_x$, $3E_x$ ($S(\mathbf{x}) \neq S(\mathbf{x} \oplus 11ef10)$).

Условие 2 (У-2) (условие перекрытия четырехцикловых итеративных характеристик). Элементы таблиц дифференциальных разностей каждого S-блоков, для которых $W(\alpha_1 \oplus \alpha_2) = 1$ или $W(\alpha_1 \oplus \alpha_2) = 2$, при этом $\beta_1 = \beta_2 = \beta$, должны подчиняться следующему ограничению:

$$NS_k(\alpha_1,\beta) \cdot NS_k(\alpha_2,\beta) \leq 160,$$

где $W(a)$ – вес по Хэммингу числа a; β – выходная 4-битная разность; α_1,α_2 – входные 6-битные разности; $NS_k(a,b)$ – число случаев, когда разность a на входе k-го S-блока переходит в выходную разность b.

Условие 3 (У-3). Для трех одновременно активных S-блоков со значениями весов выходов таблиц распределения разностей $W(\beta) \leq 2$ должно выполняться ограничение

$$\left| NS_i(\alpha, \beta) \cdot NS_{i+1}(\alpha, \beta) \cdot NS_{i+2}(\alpha, \beta) \right| \leq 8^3,$$

где, как и ранее, $\alpha \in GF(2)^6$, $\beta \in GF(2)^4$– значения входов в таблицы разностей по строкам и столбцам.

Как видно из представленного списка дополнительных требований, сохранено и единственное требование У-1, которое предложено корейскими учеными в [4]. В то же время, добавлены два дополнительных требования, без которых, по нашему мнению, нельзя с уверенностью говорить о стойкости шифра DES к атакам дифференциального криптоанализа.

Использование предложенного набора требований позволяет при необходимости повысить характеристики безопасности шифра DES, однако все равно сохраняет практическую необходимость увеличение длины шифруемого блока и длины ключа, что и объясняет интенсивные исследования, проводимые в рамках мирового сообщества по разработке новых стандартов шифрования.

Список литературы: 1. *Долгов В.И., Лисицкая И.В., Руженцев В.И.* Обеспечение стойкостии шифра DES к атакам дифференциального криптоанализа. Перекрытие итеративных характеристик обнуляющего типа и четырехцикловых итеративных характеристик // Радиотехника. 2001. № 120. С. 192-198. 2. *Долгов В.И., Лисицкая И.В., Головашич Р.В., Олейников С.А.* Принципы защиты алгоритма DES отатак дифференциального криптоанализа // Радиотехника. 2000. № 113. С. 148-157. 3. *Lysytska I.V., Koriak A.S., Golovashich S.A., Oleshko O.I., Oleinik R.V.* The selection criteria of random substitution tables for symmetric enciphering algorithms // Abstracts of XXVIth General Assembly. Toronto, Ontario Canada, August 13-21, 1999. P. 204. 4. *K. Kim, S. Lee, S. Park.* How to Strengthen DES against Two Robust Attacks // Joint Workshop on Information Security and Cryptology Inuyata. Japan. January 24-25. 1995.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 16.10.2001