1. P.709-710. 29. *Bocchieri P., Loinger A.* Energy, equipartition and classical electrodynamics //Lett. Nuovo Cimento. - 1971. Vol. 2. P.41-42. 30. *Bocchieri P., Vaz-Griz F.* Dynamical study of an anharmonic crystal interacting with an ideal gas/ /Lett. Nuovo Cimento. 1972. Vol. 4. P.685-689. 31. *Cercignani C., Galgani L., Scotti A.* Zoro-point energy in classical nonlinear mechanics // Phys. Lett. 1972. Vol. 38A. P.403-404. 32. Galgani L., Scotti A. Plank-like distributions in nonlinear mechanics // Phys. Rev. Lett. 1972. Vol. 28. P.1173-1176. 33. *Galgani L., Scotti A.* Recent progress in classical nonlinear dynamics //Lett. Nuovo Cimento. 1972. Vol. 2. P.189-209. 34. *Zabusky N.J.* A synergetic approach to problems of nonlinear dispersive wave propagation and interaction // In Nonlinear Partical Differential Equations, W.Ames, Ed. - New York: Academic Press, 1967. P.223-258. 35. *Zabusky N.J.* Solitons and energy transport in nonlinear lattices // Comput. Phys. Comumn. 1973. Vol. 5. P.1-10.

Поступила в редколлегию 07.07.99

Рецензент: д-р физ.-мат. наук Ляшенко Н.И.

Рудько Борис Федорович, канд. физ.-мат. наук, старший научный сотрудник, заведующий отделом специальных измерений Научно-исследовательского центра квантовой медицины "ВІДГУК" Министерства здравоохранения Украины. Адрес: Украина, 252033, Киев, ул. Владимирская, 61-б, тел. 244-44-58.

Човнюк Юрий Васильевич, канд. техн. наук., доцент, профессор Высшей школы экономики и деловой администрации "АЖИО-КОЛЛЕДЖ" (г.Киев, Украина), Научно-исследовательский центр квантовой медицины "ВІДГУК" Министерства здравоохранения Украины. Адрес: Украина, 252033, Киев, ул. Владимирская, 61-б, тел. 244-44-39, занимаемая должность- старший научный сотрудник.

Овсянникова Татьяна Николаевна, канд. техн. наук, старший научный сотрудник. Научно-исследовательского центра квантовой медицины "ВІДГУК" Министерства здравоохранения Украины. Адрес: Украина, 252033, Киев, ул.Владимирская, 61-б, тел. 244-44-39.

Ивановская Алла Владимировна, младший научный сотрудник Научно-исследовательского центра квантовой медицины "ВІДГУК" Министерства здравоохранения Украины. Адрес: Украина, 252033, Киев, ул.Владимирская, 61-б, тел. 244-44-39.

УДК 681.3.06: 519.248.681

К ВОПРОСУ ПОСТРОЕНИЯ СЛУЧАЙНЫХ *S* БЛОКОВ ДЛЯ АЛГОРИТМА DES. КРИТЕРИИ ОТБОРА *S* БЛОКОВ

ЛИСИЦКАЯ И.В., КОРЯК А.С., ОЛЕЙНИКОВ Р.В., ГОЛОВАШИЧ С.А.

Обсуждаются известные требования к отбору *S* блоков для алгоритма шифрования DES. Приводятся результаты статистической проверки применения этих критериев отбора к таблицам стандарта и случайным таблицам, построенным по предлагаемым правилам. Детально изучаются реализационные возможности выполнения при формировании случайных *S* блоков требования об исключении однобитных переходов.

В предыдущих наших работах [1,2] рассматривается задача построения *S*блоков для алгоритма DEA (так мы назвали алгоритмическую часть стандарта DES), устойчивых к атакам дифференциального и линейного криптоанализа. Обосновывается идея интерпретации *S*блоков как 8 полиподстановок фиксированного вида, каждая из которых в свою очередь состоит из 4-х подстановок 16-й степени. Предлагается при построении таблиц требование к *S*блокам разработчиков стандарта, в соответствии с которым однобитное различие на входе *S* блока должно приводить к изменению более чем одного бита на выходе [3], заменить проверкой выполнения критериев случайности [4]. Дальнейшие наши исследования, однако, свидетельствуют о том, что выполнение отмеченного требования при отборе *S* блоков для шифра DES является одним из принципиальнейших моментов. В этой работе изучаются реализационные возможности выполнения при формировании случайных *S*блоков требования об исключении однобитных переходов, а также излагаются результаты проверки выполнения для таблиц случайного типа и других известных требований к *S*блокам стандарта.

Прежде всего, остановимся на свойствах *S*блоков шифра DES, которые считаются уникальными на протяжении вот уже более двадцати лет его существования. Для этого следует напомнить критерии отбора *S* блоков. Они уже не раз становились предметом изложения и обсуждения многих работ [3,5,6 и др.]. Здесь мы их приведем, опираясь на работу [6], в которой они представлены в интерпретации самих разработчиков. Критерии для *S*блоков в этой работе изложены в такой редакции:

1. Каждый *S*блок имеет 6 входных и 4 выходных бита.

2. Нет выходного бита *S* блока, который может быть связан с входными битами функцией, близкой к линейной.

3. Если зафиксированы самый левый и самый правый входные биты *S* блока и меняются 4 его средних бита, то каждый из возможных 4-битовых выходов получается точно один раз.

4. Если два входа *S*блока отличаются точно одним битом, то выходы должны отличаться не менее чем в двух битах.

5. Если два входа *S* блока отличаются точно в двух средних битах, то выходные биты должны отличаться не менее чем двумя битами.

6. Если два входа *S* блока отличаются своими первыми двумя битами и имеют совпадающими 2 последних бита, то выходные биты не должны быть теми же самыми.

7. Для любых ненулевых 6-битовых различий входов не более чем 8 из 32 пар входов должны показывать одни и те же выходные различия.

8. Критерий, подобный предыдущему, должен выполняться и в случае трех активных *S* блоков.

Некоторые результаты статистической проверки выполнения изложенных выше требований применительно к *S*блокам, предложенным разработчиками стандарта, и "случайным" *S*блокам из работы [2], представлены в табл. 1-6.

Следует сразу обратить внимание на то, что не все из перечисленных требований полностью реализованы в таблицах *S*блоков самого стандарта. Приведем нашу версию ряда соображений, использованных при их формировании.

Первое из приведенных требований отражает специфику построения шифра DES. В [6] причиной выбора таких параметров S блоков называется ограничение на размер таблиц, которые могли быть размещены в одном чипе технологии 1974 года. Мы, однако, видим в использовании именно такой конструкции S блоков более глубокий смысл. Представляется, что их выбор в DES подчинен прежде всего стремлению обеспечить одно из основных свойств шифра - лавинного эффекта и на это направлена структура всего алгоритма шифрования в целом. Использование именно 8 S блоков, выполняющих отображение $GF(2^6) \rightarrow GF(2^4)$, в сочетании с таблицей расширения E в алгоритме DES позволяет добиться того, что изменение любого из 6-битных входов S блока с большой вероятностью (в 60 случаях из 63) сопровождается изменением уже на текущем цикле преобразования состояний входов (и соответственно выходов) соседних (одного или двух сразу) S блоков. Выходы любого из S блоков (4 бита) с помощью последующей P подстановки снова распределяются так, что воздействуют по одному (снова за счет расширяющей подстановки E) на входы сразу 6-ти S блоков следующего цикла, усиливая лавинный эффект.

Второе требование в такой общей формулировке можно считать подчиненным стремлению обеспечить защищенность от атак линейного криптоанализа; как оно учитывалось при формировании таблиц стандарта, нам осталось неясным. Известно мнение [6 и др.], что S блоки стандарта по этому требованию не оптимизированы, что следует из результатов, представленных в табл. 1.

Самым "смещенным" в стандарте является 5-й S блок. Его (максимальное) смещение равно -20. Оно и использовано Мацуи для осуществления успешной атаки на DES [6].

Характеристики альтернативных S блоков приведены в табл. 2. При получении этих S блоков, как уже отмечалось в работе [1], были наложены ограничения на максимально допустимое значение смещения линейных аппроксимационных характеристик, и в этом отношении альтернативные таблицы выглядят предпочтительней. Но это лишь поверхностное суждение. Конечно, здесь требуется более детальное обсуждение связи приведенных показателей с эффективностью проведения линейного криптоанализа, которое мы отложим для отдельного рассмотрения.

Выполнение третьего требования приводит к использованию в качестве строк таблиц S блоков числовых конструкций типа подстановок (перестановок, не имеющих совпадающих элементов). Это требование представляется вполне естественным, поскольку направлено на реализацию одного из главных свойств рассматриваемой процедуры шифрования – максимального перепутывания (перемешивания) элементов исходного текста. Практически, как отмечено в [1], каждый из S блоков представляет собой таблицу из четырех перестановок степени $n = 16$, и ее применение в алгоритме можно интерпретировать как полиподстановку – процедуру криптографического преобразования, которая из числа известных простейших считается одной из эффективных.

Все остальные требования в той или иной мере также направлены на быстрое приобретение шифруемым текстом свойств чисто случайного двоичного блока символов, что имеет самое непосредственное отношение и к защите от атак дифференциального криптоанализа. Незначительное изменение открытого текста при неизменном ключе должно приводить к существенному изменению соответствующего шифрованного текста (близкие по структуре тексты при шифровании должны превращаться в статистически не связанные блоки). Это же относится и к небольшим изменениям ключа при шифровании одного и того же текста.

Здесь возможны две крайние ситуации.

В одном случае открытые тексты (блоки двоичных символов) могут быть близкими друг к другу (совпадать в большом числе битов). Но тогда небольшие отличия в отдельных битах (а в пределе - отличие в одном бите) должны усиливаться (подчеркиваться) на каждом этапе криптопреобразования (однобитные и двухбитные различия на входе должны приводить к изменению более одного выходного бита).

Таблица 1. Характеристики линейных аппроксимационных таблиц S блоков стандарта

Проверяемый параметр	S блоки							
	S1	S2	S3	S4	S5	S6	S7	S8
Максимальное (по модулю) значение смещения	-18	-16	16	-16	-20	-14	-18	-16
Процент элементов таблицы, имеющих ненулевые значения	70	65	71	54	70	70	70	68
Число ненулевых элементов таблицы	718	662	730	557	717	724	715	692
Дисбаланс однобитных переходов	-6	-4	6	4	4	-4	4	2

Таблица 2. Характеристики линейных аппроксимационных таблиц для случайных S блоков

Проверяемый параметр	S блоки							
	S1	S2	S3	S4	S5	S6	S7	S8
Максимальное по модулю значение смещения	-10	10	-10	10	10	10	-10	-10
Процент элементов таблицы, имеющих ненулевые значения	72	72	74	71	71	72	71	72
Число ненулевых элементов таблицы	736	741	754	726	730	738	728	741
Дисбаланс однобитных переходов	-6	-6	-8	-8	-8	-6	-8	-6

Как раз это и сформулировано в требованиях 4 и 5 (по требованию 4 запрещены совпадающие выходы и однобитные выходные разности для входных разностей 000001, 000010, 000100, 001000, 010000, 100000; по требованию 5 запрещены совпадающие выходы и однобитные выходные разности для входной разности 001100). Отметим, что эти требования учитывают специфику алгоритма DES - использование расширяющей подстановки E, в соответствии с которой два первых и два последних входных бита каждого Sблока становятся также входными битами соседних Sблоков. В частности, один общий бит двух смежных S блоков без выполнения требования 4 может перейти в единственный выходной бит одного из S блоков.

В другом крайнем случае тексты могут отличаться большим числом битов (быть близкими к противоположным текстам). Здесь уже речь должна идти об исключении (ограничении) на каждом этапе процедуры криптопреобразования и, в частности, при проходе S блоков, одновременно возникающего большого числа переходов с одинаковыми изменениями противоположных (совпадающих с точностью до наоборот) групп символов шифруемых текстов. На это как раз и направлены требование 7 и 8 (как мы их поняли). В итоге в обоих случаях криптографическое преобразование должно превращать различия между текстами (как предельно малые, так и предельно большие) в сбалансированную двоичную последовательность).

Выполнение рассмотренных требований трактуется в литературе как реализация одного из основных свойств любого шифра – лавинного эффекта.

Отметим еще раз, что именно лавинный эффект играет основную роль и в обеспечении защиты от атак дифференциального криптоанализа, однако это положение – предмет отдельного обсуждения.

Мы здесь не приводим результаты проверки требования 8 (так как мы его поняли), но, как показывает анализ, оно в одинаковой мере не выполняется как для таблиц стандарта, так и для случайных таблиц.

Заметим, наконец, что требование 6 также имеет самое непосредственное отношение к защите от атак дифференциального криптоанализа.

В соответствии с этим требованием 6-битные входы в таблицы S блоков, имеющие между собой различия (поразрядные суммы по модулю два), равные 110000, 110100, 111000, 111100, не должны приводить к совпадающим выходам. Значение этого условия мы обсудим в следующей публикации.

Как видно из представленных результатов, разработчиками стандарта в полном объеме выполнены требования 1, 3, 4, 5, 6 и 7. Требования 2 и 8 практически не выполняются (в той или иной мере) как для таблиц стандарта, так и для случайных таблиц

Таблица 3. Результаты проверки S блоков стандарта DES и случайных S блоков по критерию 4

Тест 1. Если два входа S блока отличаются точно одним битом, то выходы должны отличаться не меньше чем в двух битах (384 возможных вариации для каждого S блока)									
Число отличий в выходных битах S блоков стандарта					Число отличий в выходных битах случайных S блоков				
S блоки	Мин.	Макс.	Средн.	Тест не прошли	S блоки	Мин.	Макс.	Средн.	Тест не прошли
S1	2	4	2.48	0	S1	1	4	2.05	120
S2	2	4	2.53	0	S2	1	4	2.13	104
S3	2	4	2.64	0	S3	1	4	2.13	90
S4	2	4	2.46	0	S4	1	4	2.04	112
S5	2	4	2.53	0	S5	1	4	2.09	112
S6	2	4	2.60	0	S6	1	4	2.19	104
S7	2	4	2.62	0	S7	1	4	2.25	76
S8	2	4	2.50	0	S8	1	4	2.06	108

Таблица 4. Результаты проверки S блоков стандарта DES и случайных S блоков по критерию 5

Тест 2. Если два входа S блока отличаются в двух средних битах, то выходы должны отличаться не меньше чем в двух битах. (64 возможных вариации для каждого S блока)									
Число отличий в выходных битах S блоков стандарта					Число отличий в выходных битах случайных S блоков				
S блоки	Мин.	Макс.	Средн.	Тест не прошли	S блоки	Мин.	Макс.	Средн.	Тест не прошли
S1	2	4	2.44	0	S1	1	4	2.00	36
S2	2	4	2.62	0	S2	1	4	2.31	14
S3	2	4	2.37	0	S3	1	4	2.00	22
S4	2	3	2.5	0	S4	1	4	2.19	14
S5	2	4	2.37	0	S5	1	4	2.31	10
S6	2	3	2.37	0	S6	1	4	2.00	20
S7	2	4	2.44	0	S7	1	4	2.12	18
S8	2	3	2.44	0	S8	1	4	1.94	22

(ограничение на максимальное значение асимметрии линейных характеристик еще не гарантирует защиту от атак линейного криптоанализа). Здесь требуется провести дополнительный предметный анализ сущности самих этих требований и оценки возможностей их реализации в алгоритме шифрования.

В то же время случайные таблицы подстановок не удовлетворяют критериям 4, 5 и 6, хотя и в статистическом смысле эти отличия от свойств таблиц стандарта можно считать не столь существенными. Они касаются некоторого уменьшения для случайных таблиц среднего значения числа битовых отличий на выходах S блоков при однобитных отличиях на их входах (см. табл. 3, 4)

В этой работе мы уделим основное внимание анализу 4-го требования В соответствии с этим требованием любое однобитное изменение на входе S блока должно приводить к изменению двух и более символов (битов) на выходе. Рассмотрим в связи с этим задачу оценки числа допустимого множества таблиц подстановок, удовлетворяющих требованию 4.

Воспользуемся для решения поставленной задачи правилами записи и представления таблиц S блоков, изложенными в работе [7]. Напомним кратко их сущность. Пусть $b_1 \ldots b_6$ – 6-битный вектор, поступающий на вход некоторого S блока S_i. Образуем два десятичных числа k и l, двоичная запись первого из которых есть $b_1 b_6$, а второго – $b_2 b_3 b_4 b_5$. Тогда результатом работы S блока S_i, соответствующим входу $b_1 \ldots b_6$, является 4-битовая двоичная запись десятичного числа, стоящего в i-й матрице на пересечении k-й строки и l-го столбца.

Именно исходя из приведенного правила пользования таблицами, каждый S блок действительно является полиподстановкой, которую математически будем представлять в виде расширения стандартной записи подстановки [8] путем дописывания дополнительных трех строк, т.е. в виде матрицы

$$S_{4,16} = \begin{bmatrix} 1 & 2 & 3 & \ldots & 16 \\ i_{11} & i_{12} & i_{13} & \ldots & i_{116} \\ i_{21} & i_{22} & i_{23} & \ldots & i_{216} \\ i_{31} & i_{32} & i_{33} & \ldots & i_{316} \\ i_{41} & i_{42} & i_{43} & \ldots & i_{416} \end{bmatrix}. \qquad (1)$$

Верхнюю строку, как и ранее [4], будем называть нулевой, а остальные нумеровать от 1-й до 4-й.

Рассмотрим решение задачи с некоторыми упрощениями. Будем сначала интересоваться выполнением требования о запрещении однобитных и нулевых выходных различий для однобитных различий на входе S блока, создаваемых только внутренними символами $b_2 b_3 b_4 b_5$ его 6-битных входов.

В соответствии с правилами построения таблицы, оговоренными выше, требование отсутствия однобитных и нулевых разностей (различий) выходов при изменении одного (любого) из четырех символов $b_2 b_3 b_4 b_5$ сводится к однобитным и нулевым различиям (расстояниям по Хэммингу) между элементами подстановок, попавшими в столбцы, для которых побитовая сумма 4-битных входов $b_2 b_3 b_4 b_5$ (внутренних символов нулевой строки) содержит только один ненулевой бит.

Таблица 5. Результаты проверки S блоков стандарта DES и случайных S блоков по критерию 6

Тест 3. Если два входа S блока отличаются двумя первыми битами и совпадают в двух последних битах, то выходы должны быть отличными друг от друга									
Число отличий в выходных битах S блоков стандарта					Число отличий в выходных битах случайных S блоков				
Средние два бита не отличаются 110000 (64 возможных варианта)									
S блоки	Мин.	Макс.	Средн.	Тест не прошли	S блоки	Мин.	Макс.	Средн.	Тест не прошли
S1	1	4	1.81	0	S1	0	4	1.75	8
S2	1	4	2.19	0	S2	0	4	2.1	2
S3	1	3	1.68	0	S3	0	4	2.00	4
S4	1	3	2.00	0	S4	0	4	1.94	6
S5	1	3	1.86	0	S5	0	4	2.18	4
S6	1	4	1.94	0	S6	0	4	2.00	6
S7	1	4	1.81	0	S7	0	4	2.06	6
S8	1	4	1.81	0	S8	0	4	1.94	2
Средние два бита отличаются одним битом 110100, 111000 (128 возможных вариантов)									
S блоки	Мин.	Макс.	Средн.	Тест не прошли	S блоки	Мин.	Макс.	Средн.	Тест не прошли
S1	1	4	2.22	0	S1	0	4	2.00	4
S2	1	4	1.97	0	S2	0	4	1.98	2
S3	1	4	1.90	0	S3	0	4	2.06	8
S4	1	4	1.87	0	S4	0	4	2.03	4
S5	1	4	1.94	0	S5	0	4	2.21	4
S6	1	4	2.12	0	S6	0	4	2.03	8
S7	1	4	1.83	0	S7	0	4	1.98	8
S8	1	4	1.93	0	S8	0	4	2.02	4

Это значит, что запрещены все нулевые и однобитные (с одним отличным от нуля битом) различия для всех столбцов, у которых входы $b_2b_3b_4b_5$ имеют однобитные различия.

Для иллюстрации в табл. 7 представлены двоичные эквиваленты всех возможных 16 значений элементов подстановки-строки вместе с подмножествами однобитных переходов для каждого из чисел.

Рассмотрим сначала процесс получения отдельной подстановки, удовлетворяющей оговоренным выше условиям. Пусть в качестве первого элемента подстановки-строки начального (нулевого) столбца взят произвольный элемент (один из 16 возможных). В этом случае столбцами, для которых нужно контролировать однобитные различия в соответствии с табл.7, выступают 1, 2, 4 и 8-й столбцы. В этих столбцах должны разместиться элементы, отличающиеся от исходного более чем одним битом. Но в соответствии с этой же таблицей для любого элемента имеется ровно 5 чисел, которые являются запрещенными для размещения в 1, 2, 4 и 8-м столбцах. Остаются разрешенными для размещения на этих позициях $16-5=11$ элементов. В результате можно сделать вывод, что выбрать пять элементов (0, 1, 2, 4 и 8-й) для рассматриваемой строки таблицы подстановок можно

$$16\cdot A_{11}^4 = 16\cdot 11\cdot 10\cdot 9\cdot 8 = 126720$$

способами (A_n^m – число размещений из n элементов по m).

Рассмотрим задачу выбора еще пяти элементов этой строки, но теперь пусть следующим (определяющим пятерку) будет последний (15-й, если отсчет вести с нуля) элемент строки. Поскольку пять элементов строки уже выбрано, то для назначения очередных пяти элементов остается 11 вариантов чисел. С другой стороны, для 15-го элемента столбцами, которые надо контролировать, выступают 7, 11, 13 и 14 столбцы. Они не пересекаются с ранее выбранными и, следовательно, здесь снова можно воспользоваться примененной выше методикой. Отличие состоит лишь в том, что пять элементов перестановки уже выбраны, и теперь в распоряжении для выбора 15-го элемента рассматриваемой строки имеется лишь 11 различных чисел. После выбора этого 15-го элемента для размещения на четырех из пяти рассматриваемых позиций этой строки, как показывает анализ, можно размещать в зависимости от ситуации от 6 до 10 чисел (множество чисел, отличающихся от выбранного 15-го более чем одним битом, из которого исключены числа, совпадающие с уже выбранными пятью для размещения на 0, 1, 2, 4 и 8-й позициях подстановки) Среднее по множеству возможных значение числа размещений меньше 8 (близко к 7). Поэтому для числа вариантов размещений пяти очередных чисел на позициях 7, 11, 13, 14, 15 получаем оценку

$$11\cdot A_8^4 = 11\cdot 8\cdot 7\cdot 6\cdot 5 = 18480\cdot$$

Остается еще разместить на шести не занятых позициях 3, 5, 6, 9, 10 и 12-й шесть оставшихся чисел. Анализ показывает, что с учетом запретов, создаваемых однобитными переходами и уже выбранными числами, все оставшиеся случаи могут дать для каждого из вариантов задания десяти рассмотренных выше элементов первой строки (0, 1, 2, 4, 7, 8, 11, 13, 14 и 15-го элементов) не более трех вариантов размещения оставшихся шести элементов.

Для иллюстрации в табл. 8 приведены возможные варианты разрешенных значений шести оставшихся элементов первой строки для ряда примеров задания нулевого и пятнадцатого ее элементов вместе с четверками сопутствующих им элементов этой строки.

Таблица 6. Результаты проверки *S* блоков стандарта DES и случайных *S* блоков по критерию 7

Тест 4 . Для ненулевых 6- битовых различий входов не более чем 8 из 32 пар входов должны показывать одинаковые выходные различия									
Число пар входов с одинаковыми выходными различиями для S блоков стандарта					Число пар входов с одинаковыми выходными различиями для случайных S блоков				
S блоки	Число 0-разл.	Мин.	Макс.	Тест не прошли	S блоки	Число 0-разл.	Мин.	Макс.	Тест не прошли
S1	2	0	4	0	S1	3	0	5	0
S2	2	0	7	0	S2	2	0	4	0
S3	1	0	5	0	S3	1	0	6	0
S4	4	0	8	0	S4	1	0	5	0
S5	4	0	4	0	S5	1	0	4	0
S6	0	0	4	0	S6	2	0	4	0
S7	7	0	7	0	S7	0	1	5	0
S8	0	0	5	0	S8	1	0	4	0

Таблица 7

4-х битные выходы S блока и соответствующие им значения других выходов, имеющих с ними однобитные различия

Элементы подстановки - строки S блока															
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
1000	1001	1010	1011	1100	1101	1110	1111	0000	0001	0010	0011	0100	0101	0110	0111
0100	0101	0110	0111	0000	0001	0010	0011	1100	1101	1110	1111	1000	1001	1010	1011
0010	0011	0000	0001	0110	0111	0100	0101	1010	1011	1000	1001	1110	1111	1100	1101
0001	0000	0011	0010	0101	0100	0111	0110	1001	1000	1011	1110	1101	1100	1111	1110

Как следует из приведенных примеров, действительно выбор десяти "исходных" элементов строки практически уже почти полностью определяет вид перестановки. В результате для общего числа вариантов построения одной строки матрицы (1) (числа подстановок, удовлетворяющих рассматриваемому ограничению) можно получить оценку

$$16 \cdot A_{11}^4 \cdot 11 \cdot A_8^4 \cdot 3 = 7 \cdot 10^9 .$$

Чтобы выполнить требование 4 в полном объеме, необходимо удовлетворить ограничению еще одного типа – дополнительно обеспечить отсутствие тождественных и однобитных переходов на выходах S блоков при изменении одного бита на их входах в композициях символов $b_1 b_6$. Это значит, что должны выполняться определенные соотношения и между элементами каждой подстановки, находящимися в различных столбцах матрицы (1).

В соответствии с правилами построения таблицы, оговоренными выше, требование отсутствия однобитных и нулевых разностей (различий) выходов при изменении одного (любого) из двух символов $b_1 b_6$, как видно из рисунка 1, сводится к запрещению однобитных и нулевых различий по всем столбцам между двоичными представлениями элементов первой и второй, первой и третьей, а также между двоичными эквивалентами элементов четвертой, второй и четвертой и третьей подстановок, входящих в каждую из таблиц S блоков. В то же время разрешаются произвольные (в том числе и совпадающие) значения элементов, попавших в один и тот же столбец, для первой и четвертой или (и) второй и третьей подстановок (строк матрицы). Поэтому сформулированная задача сводится к выбору (отбору) 4-х подстановок, которые имеют в каждом столбце этой таблицы элементы (двоичные векторы), находящиеся в метрике Хэмминга на определенных взаимных расстояниях друг от друга.

Число возможных (допустимых) подстановок, удовлетворяющих сразу двум ограничениям, может быть оценено путем модификации ранее приведенных рассуждений следующим образом.

Пусть каким-либо способом уже построены (выбраны) две строки матрицы (1), удовлетворяющие первому из рассмотренных нами ограничений (это в соответствии с рисунком 1 могут быть либо первая и четвертая строки, либо вторая и третья, так как на указанные пары строк не распространяется ограничение второго типа). Пусть для конкретности это будут первая и четвертая строки матрицы (1). Ставится задача построить (выбрать) вторую и третью строки-перестановки этой матрицы, каждая из которых должна удовлетворять первому из рассмотренных ограничений и при этом еще в пределах каждого из столбцов для каждой из перестановок должно исключаться также множество однобитных переходов (выходов), которое задается первым и четвертым элементами этого столбца (элементами уже выбранных первой и четвертой строки). Поскольку на эти строки не распространяется ограничение второго типа, то можно рассматривать только одну из строк (все рассуждения относительно одной строки будут справедливы и для другой).

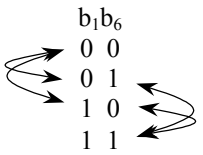

Рис.1. Возможные однобитные переходы при изменении символов $b_1 b_6$

Рассмотрим нулевой столбец матрицы (1) (соответствующий нулевому элементу нулевой строки). Очевидно, что если уже выбраны первый и четвертый элементы столбца, то для выбора второго и третьего элементов этого столбца, которые отстоят от первого и четвертого элементов на минимальное расстояние по Хеммингу, не меньшее единицы, получаем множество, являющееся пересечением множеств, состоящих из 11 элементов каждое, определяемых исключением из полного множества элементов перестановки пяти чисел, которые включают соответственно числа, занявшие первую и четвертую позиции в рассматриваемом столбце, и относящиеся к ним четверки чисел, представляющих в соответствии с табл.7 их однобитные переходы. Непосредственной проверкой можно легко убедиться, что пересечение рассматриваемых множеств будет содержать не более 8 элементов. Если быть более точным, то из 256 возможных пар выбора нулевых элементов первой и четвертой строки 11 пар (совпадающие элементы первой и четвертой строки) будут давать разрешенное множество для выбора нулевого элемента второй (третьей) строки, состоящее из 11 элементов, остальные (пары несовпадающих элементов) дают: 160 пар – множества из 8 элементов и 80 пар – множества из 6 элементов.

При рассмотрении элементов второй строки, занимающих позиции, которые соответствуют четверкам элементов первой и четвертой строки, сопровождающих выбранные нулевые элементы этих строк, нужно уже рассматривать пересечение множества элементов, задаваемого выбранным нулевым элементом второй строки (находящимся на заданном

Таблица 8

Распределение числа возможных значений разрешенного множества элементов в зависимости от булевой побитовой суммы предыдущих двух элементов столбца

Нулевая строка															
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Варианты первых строк (цветом выделены поля с разрешенными значениями элементов)															
4	1	14	2, 8	13	6	2, 8	11	15	12	8, 9	7	3, 6	10	5	0
11	8	12	2, 7	1	2, 14	2, 10	13	6	15	0, 10, 15	9	10, 15	4	5	3
14	4	13	1, 11	2	14, 15	11, 14	8	3	10, 15	6, 10	12	5, 15	9	0	7
13	2	8	4, 11	6	15	11, 15	1	10	5, 9	3, 5	14	3 ,5, 9, 15	0	12	7

Хэммингов расстоянии от нулевого элемента), и пересечения множеств разрешенных элементов, соответствующих элементам первой и четвертой строки, попавшим в рассматриваемый столбец. Здесь под разрешенным понимается множество элементов, находящихся на заданном Хэммингов расстоянии от заданного (выбранного) элемента.

Здесь также возможны различные размерности разрешенных множеств, зависящие от того, совпадает ли выбранный нулевой элемент второй строки с одним или сразу с двумя (одинаковыми) элементами первой и четвертой строки, попавшими в рассматриваемый столбец (получаются значения 11, 8, 5). Воспользуемся для расчетов значением размера разрешенного множества элементов для всех четырех возможных столбцов, равным 6 (реальное среднее значение меньше этого числа). В результате для оценочного (оценки сверху) значения числа вариантов выбора первых пяти элементов второй строки можем записать выражение

$$8 \cdot 6^4 = 10368.$$

Аналогичные рассуждения можно сделать и относительно выбора элементов второй и третьей строки для пятнадцатого столбца матрицы (1), только нужно учесть дополнительное усечение разрешенных множеств элементов за счет исключения из рассматриваемых множеств пяти уже выбранных элементов.

Для оценки числа вариантов выбора вторых пяти элементов второй (третьей) строки можно предложить оценочное выражение (с завышением) в виде

$$6 \cdot 3^4 = 486.$$

Тогда для общего числа таблиц подстановок, удовлетворяющих требованию 4 о запрещении однобитных переходов, можно предложить оценочное выражение в виде

$$\widetilde{W}_{4,16} \le$$

$$\le \left(16 \cdot A_{11}^4 \cdot 11 \cdot A_8^4 \cdot 3\right)^2 \times$$

$$\times \left(8 \cdot 6^4 \cdot 6 \cdot 3^4 \cdot 3\right)^2 = 1{,}1 \cdot 10^{34}.$$

Реальное число таблиц подстановок, удовлетворяющих требованию 4, очевидно будет существенно меньше этого числа.

Если бы таблицы строились без всяких ограничений, то это число получилось бы близким к

$$\widetilde{W}_{4,\,16} = \left(2 \cdot 10^{13}\right)^4 \approx 1{,}6 \cdot 10^{53}.$$

Это позволяет заключить, что порождать подходящие таблицы подстановок случайным образом практически безнадежно.

Таким образом, таблицы подстановок, удовлетворяющие требованию 4, действительно можно считать "уникальными" в том смысле, что по сравнению с общим множеством таблиц подстановок их количество ничтожно малое. Конечно, можно предложить вполне практичные процедуры генерации подстановок, сразу исключающих нулевые и однобитные переходы на выходах S блоков при однобитных изменениях на их входах.

Здесь мы, однако, заострим внимание на возможностях применения таблиц подстановок случайного типа, о которых говорилось в предыдущих наших работах, при использовании менее жестких ограничений требование 4.

Наши исследования показывают, что при генерировании случайных таблиц подстановок можно ввести дополнительные ограничения на допустимое число однобитных разностей на выходах S блоков при фиксированных однобитных разностях на входах. Естественно, что по мере уменьшения допустимого числа однобитных разностей быстродействие вероятностной процедуры отбора замедляется. Для проверки были построены таблицы случайных S блоков с ограничением на допустимое число однобитных разностей, равное 6.

Дальнейшее ужесточение требований к числу однобитных переходов ведет уже к практически неприемлемым временным показателям алгоритма отбора случайных таблиц подстановок. В этих условиях более эффективным путем отбора Sблоков для шифра DES по-видимому действительно является создание специализированных программных методов.

Литература: 1. *Лисицкая И.В.*, *Головашич С.А.*, *Олешко О.И., Олейников Р.В., Коряк А.С.* Построение таблиц подстановок для стандарта шифрования данных // Проблемы бионики. 1999. Вып 50. С. 185−194 2. *Лисицкая И.В.*, *Олейников Р.В., Головашич С.А.*, *Коряк А.С.* Анализ стойкости DES подобных алгоритмов шифрования при использовании таблиц подстановок случайного типа // Радиоэлектроника и информатика. 1999. № 1. С 111 − 115. 3. *Konheim A.G.* Cryptography: A primer. I. Wiley, New York. 1981. 4. *Горбенко И.Д., Лисицкая И.В.* Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 2847-89 // Радиотехника. 1997. Вып. 103. С. 121-130. 5. *Davio Mark et oll.* Analitical characteristics of the DES Proceedings ÌCRYPTOÿ83Ì. London. 1983. P. 171-202. 6. *Sheier B.* Applied Cryptography. Second Edition: protocols, algorithms, and source code in C. Published by John Wiley & Sons. Inc, New York, 1996. 158 p. 7. *Барсуков В.С., Дворянкин С.В., Шеремет И.А.* Безопасность связи в каналах телекоммуникаций. М.: Россия, 1993. Т.20, 123 с. 8. *Скачков В.Н.* Введение в комбинаторные методы дискретной математики. Наука. 1982. 384с 9. *Кононова И.В.* Противоречивые подстановки в алгоритме ГОСТ 28147-89 // Информационные системы: Сб. научн. тр. Харьков: НАНУ. 1995. Вып. 2. С. 71-77.

Поступила в редколлегию 12.09.99

Рецензент: д-р техн. наук Стасев Ю. В.

Лисицкая Ирина Викторовна, канд. техн. наук, доцент ХТУРЭ. Научные интересы: вероятностно-статистические методы и методы теории чисел в задачах криптографических преобразований и защиты информации. Адрес: Украина, 310180, Харьков, пер. Шекспира, 7, кв. 84, тел. 32-44-60.

Коряк Алексей Сергеевич, аспирант кафедры ПО ЭВМ ХТУРЭ. Научные интересы: криптография. Адрес: Украина, 310166, Харьков, пр. Ленина 14, ХТУРЭ, e-mail: AlecKoryak@yahoo.com

Олейников Роман Васильевич, аспирант кафедры ЭВМ. Научные интересы: криптография. Адрес: Адрес: Украина, 310166, Харьков, пр. Ленина, 14, тел.40-93-33.

Головашич Сергей Александрович, стажер исследователь кафедры ЭВМ. Научные интересы: криптография. Адрес: Адрес: Украина, 310166, Харьков, пр. Ленина, 14, тел.40-93-33.