Список литературы

1. *Свердлов Л.М., Ковнер М.А., Крайнов Е.П.* Колебательные спектры многоатомных молекул. М.: Наука, 1970. 560 с.

2. *Березин В.И.* Прямые и обратные задачи спектроскопии циклических и комплексных соединений: Дис. ... д-ра физ.-мат. наук. Саратов, 1983. 336 с.

3. *Минкин В.И.* Теория строения молекул. Ростов н/Д: Феникс, 1997. 386 с.

4. *Yoshida H., Takeda K., Okamura J. et al.* New Approach to Vibrational Analysis of Large Molecules by Density Functional Theory: Wavenumber-Linear Scaling Method // J. Phys. Chem. A. 2002. Vol.106, №14. P.3580–3586.

5. *Frisch M.J., Trucks G.W., Schlegel H.B. et al.* Revision A.7. Gaussian. Inc., Pittsburgh (PA), 2003.

6. *Элькин М.Д.* Кинематическая ангармоничность в электронно-графических исследованиях геометрии молекул // Журн. структ. химии. 1986. Т.27. С.42–46.

7. *Элькин М.Д.* К вопросу об использовании функции плотности вероятности в ангармонической теории рассеяния электронов молекулами // Журн. структ. химии. 1989. Т.30, №6. С.33–37.

8. *Элькин М.Д., Костерина Э.К.* Внутримолекулярная динамика и её математическое описание в задачах молекулярной спектроскопии и газовой электронографии // Хим. физика. 1994. Т.10, №1. С.38–42.

9. *Березин К.В.* Квантово-механические модели и решение на их основе прямых и обратных спектральных задач для многоатомных молекул: Дис. ... д-ра физ.-мат. наук. Саратов, 2004. 264 с.

10. *Краснощеков С.В., Степанов Н.Ф.* Масштабирующие множители как эффективные параметры для коррекции неэмпирического силового поля // Журн. физ. химии. 2007. Т.81, №4. С.680–689.

11. *Элькин М.Д., Эрман М.А., Пулин В.Ф.* Структурно-динамические модели и ангармонический анализ колебательных состояний пятичленных циклических соединений // Вестн. Сарат. гос. техн. ун-та. 2006. №4, вып.4.С.38–44.

12. *Элькин П.М. Эрман М.А.* Структурно-динамические модели и ангармонический анализ колебательных состояний полихлорзамещенных дибензо-п-диоксинов // Журн. прикл. спектроскопии. 2007. Т.74, №1. С.21–24.

13. *Элькин М.Д., Эрман Е.А., Пулин В.Ф.* Колебательные спектры конформеров бензофенона // Журн. прикл. спектроскопии. 2007. Т.74, №5. С.563–568.

14. *Элькин М.Д., Джалмухамбетова Е.А., Гречухина О.Н.* Проявление межмолекулярного взаимодействия в димерах урацила // Изв. Сарат. ун-та. Нов. сер. 2008. Сер. Физика. Т.8, №2. С.24–30.

15. *Элькин П.М., Пулин О.В., Джалмухамбетова Е.А.* Теоретический анализ таутомерных форм пурина // Журн. прикл. спектроскопии. 2008. Т.75, №1. С.23–27.

16. *Элькин П.М., Эрман Е.А., Пулин О.В.* Квантово-химический расчет нормальных колебаний молекул замещенных пятичленных халькоген-гетероциклических соединений с учетом ангармонизма анализ структуры и спектров пятичленных циклических соединений // Журн. прикл. спектроскопии. 2009. Т.76, №2. С.170–175.

17. *Amat G., Nielsen H.H., Torrago G.* Rotation-vibration of polyatomic molecules. N.Y.: Pergamon Press, 1971. 580 с.

18. *Герцберг Г.* Электронные спектры и строение многоатомных молекул. М.: Мир, 1969. 772 с.

УДК 530.182

КРИПТОГРАФИЯ ГЛАЗАМИ ФИЗИКА

Ю.Н. Зайко

ФГОУ ВПО Поволжская академия государственной службы им. П.А. Столыпина
E-mail: zymick@rambler.ru

Приведены результаты исследования криптоалгоритмов DES (США) и ГОСТ 28147-89 (Россия) методами нелинейной динамики. Исследуются точечные отображения, задаваемые важными элементами криптоалгоритмов – блоками подстановок (S-блоками). Продемонстрировано явление возврата. Исследована эргодичность рассматриваемых отображений. Оценка качества S-блока может быть выполнена с помощью отображения первого возвращения. Приведены результаты статистического исследования S-блоков. Показано, что отбор S-блоков ГОСТ из всего множества подстановок не связан с их случайным и равновероятным выбором из указанного множества.

Ключевые слова: криптография, подстановка, отображение, цикл, нелинейная динамика, явление возврата, эргодичность, ключ, S-блок, динамический хаос, лавинный эффект, перестановка.

Cryptography from the Physicist's Point of View

Yu.N. Zayko

The results of treating of crypto algorithms such as DES (USA) and GOST 28147-89 (Russia) with the help of nonlinear dynamics methods are presented. Point maps which are generated by the blocks of substitutions (S-blocks) are investigated. The phenomenon of return is demonstrated. The ergodicity of these maps are treated. An estimation of quality of S-block could be made by maps of first return. The results of statistical treating of S-blocks are presented.

Key words: cryptography, substitution, mapping, cycle, nonlinear dynamics, return, ergodicity, key, S-box, dynamical chaos, avalanche effect, permutation.

Введение

Криптография является одним из основных средств защиты информации. Зашифровать информацию можно легко и, самое главное, быстро – сейчас для этого могут быть использованы различные алгоритмы как в программном, так и в аппаратном исполнении (о некоторых оговорках сказано ниже). Выполнить обратное преобразование без знания секретной информации – ключа,

т.е. взломать шифр при современном состоянии криптоанализа, значительно сложнее. Например, для взлома блочного симметричного криптоалгоритма DES (Data Encryption Standard, США, длина ключа 56 бит) методом распределенных вычислений по данным конкурса компании RSA Data Security, проведенного в 1997 г., потребовалось 140 дней, а для криптоалгоритма RC5 с той же длиной ключа – 210 дней. С деталями подобных атак можно познакомиться в [1, 2]. Там же приведены результаты и прогнозы аналогичных атак на асимметричные криптосистемы, требующие значительно больших временных и вычислительных ресурсов.

Если оценивать степень защиты информации по отношению (стоимость взлома)/(стоимость защиты), то криптографические методы далеко превосходят все прочие.

Правительства всех стран давно используют криптографию для защиты дипломатической и военной информации. Что же касается коммерческой, и, особенно, частной информации, то здесь правительства проявляют сдержанность, предлагая для использования криптосистемы с явно заниженными криптографическими свойствами, например понижая длину ключа. Есть и другие способы затормозить широкое использование криптографии. Билль Сената США № 266, требующий предоставления правительству права получать простое текстовое содержание разговора, данных и других видов связи и Указ Президента РФ № 334 [3] о необходимости использования только сертифицированных криптографических средств, по сути дела, являются только разными по форме мерами установления государственного контроля за использованием криптографии в целях защиты конфиденциальной, и в том числе личной, информации.

1. Сертифицированные криптографические средства

В США к таким средствам относился уже упоминавшийся выше криптоалгоритм DES, разработанный в IBM под руководством Х. Фейстеля под названием Lucifer в 1976 г. и опубликованный в 1977 г. [4][1], а в России – криптоалгоритм ГОСТ 28147 – 89, разработанный в 1989 г. [5]. Они достаточно подробно описаны, например в [1, 2]. Оба являются симметричными блочными шифрами, т.е. совершают криптографические преобразования с блоками текста длиной 64 бита и имеют ключи длиной 64 (эффективно 56) и 256 бит соответственно. Оба используют схему преобразования, разработанную Фейстелем, заключающуюся в циклической перестановке правой и левой частей блока с одновременным побитовым сложением по модулю 2 очередной правой части и текущего ключа. Отличие только в числе циклов: у DES 16 циклов, а у ГОСТ 32 цикла. Другие детали преобразований мы опустим (они подробно описаны в [1, 2]). Остановимся только на преобразованиях 32-битных отрезков шифртекста с помощью подстановок, реализуемых с помощью S-блоков (S – substitution). К. Шеннон доказал [7], что эффективное преобразование блоков шифртекста может быть достигнуто путем чередования линейных операций перестановок битов, сохраняющих число значащих битов, и нелинейных операций, размножающих значащие биты, и реализуемых S-блоками[2]. Для линейных операций в DES используются P-блоки (P – permutation), а в ГОСТе – циклический сдвиг [2]. Из сказанного следует, что между двумя криптоалгоритмами много общего, что неудивительно, если учесть, что ГОСТ являлся российским ответом на DES [8, 9].

Целью криптопреобразований, примененных в обоих алгоритмах, является достижение лавинного эффекта, заключающегося в том, что каждый бит шифртекста зависит от каждого бита открытого текста и каждого бита ключа. В DES для этого нужно 5 циклов, тогда как в ГОСТ – 8. Однако ГОСТ состоит из 32 циклов, а DES – только из 16. После 8-ми циклов в DES наблюдается пик лавинного эффекта – каждый бит шифртекста является случайной функцией всех битов открытого текста и ключа. Успешные атаки на DES с тремя, четырьмя и шестью циклами подтвердили значение лавинного эффекта [2].

[1] В 2000 г. ему на смену пришел AES (Advanced Encryption Standard) [6].

[2] В книге Н. Дж. А. Слоана «Коды, исправляющие ошибки, и криптография» (М.: Мир, 1983) отмечается, что подобное чередование операций эквивалентно «преобразованию пекаря», широко известному в нелинейной динамике.

Выше уже приводились данные результатов атак на блочные криптоалгоритмы, в том числе и на алгоритм RC5, отличающийся от DES длиной блока (от 32 до 128 бит), ключа (от 0 до 2048 бит) и числом циклов преобразований (от 0 до 255), а также другими деталями [2]. По этим же данным можно сделать заключение о значительном влиянии на криптостойкость длины ключа. Продолжительность атаки на RC5 с длиной блока 32 бита и числом циклов 12 варьировалась от 313 ч (длина ключа 48 бит) до 3.5 ч (длина ключа 40 бит).

Итак, криптостойкость алгоритма шифрования определяется в основном двумя элементами: ключом и таблицами подстановок [2], исследованию которых и будет посвящено дальнейшее изложение.

2. Блоки подстановок

Блоки подстановок или S-блоки представляют собой таблицы десятичных чисел от 0 до 15 размером 1x16 (ГОСТ) или 4x16 (DES). Это связано с особенностями преобразований. В ГОСТ на вход S-блоков поступает 32-битный отрезок шифртекста, который разбивается на восемь 4-битных отрезков по числу S-блоков, которые затем каждый по отдельности преобразуются на своем блоке и на выходе снова собираются в 32-битный отрезок. На вход S-блоков DES поступает не 32, а 48-битный отрезок шифртекста, полученный из 32-битного после перестановки с расширением [2]. Он разбивается на восемь 6-битных отрезков, каждый из которых поступает на вход одного из восьми S-блоков, представляющих аналогичные таблицы размером 4×16. Два крайних бита 0-й и 5-й, записанные в десятичной системе, определяют номер строки таблицы, по которой преобразуются биты с 1-го по 4-й. Объединенные преобразованные 32-битные отрезки поступают на вход P-блоков.

Отличие S-блоков DES и ГОСТ еще и в том, что для DES S-блоки являются частью стандарта, т.е. не меняются от сеанса к сеансу, тогда как стандарт ГОСТ не определяет способ генерации S-блоков. Однако общим для обоих криптоалгоритмов является то, что способ составления S-блоков является их секретной частью.

Очевидно, что от качества S-блоков зависит качество всего криптоалгоритма и, в первую очередь, его криптостойкость.

Приведем для дальнейшего исследования S-блоки ГОСТ [1, 2] (табл. 1), используемые в приложениях ЦБ РФ [1].

Таблица 1

S1	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3
S2	14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9
S3	5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11
S4	7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3
S5	6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2
S6	4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14
S7	13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12
S8	1	5	13	0	5	7	10	4	9	2	3	14	6	11	8	12

Целью настоящей публикации является попытка выяснить, почему S-блоки, реализуемые криптоалгоритмами DES и ГОСТ, имеют именно такой вид, а не какой-либо другой, иными словами, попытаться хотя бы в общих чертах охарактеризовать алгоритм их выбора из множества всех возможных подстановок из 16-ти элементов.

Долгое время эта тема была предметом многочисленных обсуждений, и в 1992 г. IBM раскрыла секрет конструирования S-блоков. Однако указанные попытки не прекращались даже после этого, поскольку рекомендации IBM носили эвристический характер [1]. В [1] рассматриваются различные предложения по выработке S-блоков – от «ручного» конструирования на основе интуиции до случайного выбора или выбора на основе строгой математической теории. Анализ S-блоков, основанный на предположении об их случайном выборе, таит опасность, связанную с тем, что «*проблема усложняется из-за способности человеческого сознания находить в случайных данных структуры, которые в действительности не являются структурами*» [1].

В любом случае создатели криптоалгоритмов исходили из условия их устойчивости против известных методов криптоанализа и возможностей вычислительной техники [1].

В литературе [1, 2] встречаются утверждения, что выбор S-блоков ГОСТ осуществляется случайным образом. Как показано ниже, есть определенные свидетельства против этого.

Другой не менее важной целью является оценка качества S-блоков. Общепризнано, что существуют «слабые» S-блоки. Тривиальный пример – тождественная подстановка, не меняющая 4-битный отрезок шифртекста. Другой не столь очевидный пример приведен в статье [10]:

$$S = (9, 8, 3, 10, 12, 13, 7, 14, 0, 1, 11, 2, 4, 5, 15, 6). \quad (1)$$

Его слабость становится явной, если записать его в двоичном виде в форме таблицы (табл.2).

Таблица 2

i	0000	0001	0010	0011	0100	0101	0110	0111
S(i)	1001	1000	0011	1010	1100	1101	0111	1110
i	1000	1001	1010	1011	1100	1101	1110	1111
S(i)	0000	0001	1011	0010	0100	0101	1111	0110

Здесь i – двоичное значение преобразуемого элемента, S(i) – его значение после подстановки. Из табл. 2 видно, что преобразование оставляет два бита из четырех неизменными[3]. Кроме этого таблица замен может содержать обходные пути других типов, позволяющие расшифровать сообщение более эффективным образом, чем полным перебором по возможным значениям ключа. Автор [10] высказывает пессимистическое утверждение о том, что не существует способа отсеять слабые таблицы подстановок.

3. Некоторые физические аналогии. Явление возврата

В дальнейшем мы будем рассматривать только S-блоки сами по себе безо всякой связи с криптоалгоритмами. Для этого есть все основания, поскольку подстановки – один из объектов дискретной математики и всегда представляли интерес для исследователей. Спектр приложений этих исследований весьма обширен [11].

Подстановка на множестве N элементов – это отображение данного множества на себя, и нас будут интересовать свойства этого отображения. Для того чтобы не погрязнуть в абстракциях, мы будем, по возможности, прибегать к геометрическим иллюстрациям. Первое понятие из теории отображений, которое мы проиллюстрируем на примере S-блоков, это понятие возврата. А. Пуанкаре доказал теорему о возврате для непрерывных отображений [12], из которой следует, что с течением времени траектория динамической системы, совершающей движение в ограниченной области фазового пространства, вернется в сколь угодно малую окрестность начальной точки. Для дискретных систем это утверждение становится очевидным, поскольку точки фазового пространства характеризуются конечным объемом V и число шагов (аналог времени) до возврата оценивается сверху как отношение объема фазового пространства системы (многомерного в общем случае) к V. Проиллюстрируем это явление на примере отображения последовательности натуральных чисел от 0 до 15 с помощью слабого S-блока (1) (рис. 1). Программа выполняет итерации отображения (1), т.е $y_i = S^i(x)$, $x = \{0, 1, \ldots, 15\}$, i – номер итерации.

Из рис. 1 видно, что через 4 шага итераций отображаемая последовательность пришла в исходное состояние, т.е. произошло явление возврата. Легко понять, что это связано с тем, что максимальная длина циклов, на которые может быть разложена подстановка (1), равна 4, а длины остальных циклов являются делителями 4. Приведем полное разложение подстановки (1) на циклы:

$$S = C_4(9,8,1,0); C_4(3,10,11,2); C_4(7,14,15,6); C_2(12,4); C_2(13,5). \quad (2)$$

Здесь индекс означает длину цикла, а числа в скобках – элементы S-блока, преобразующиеся по данному циклу. Таким образом, мы показали, что слабость данного S-блока связана с небольшой длиной циклов, на которые он разлагается, точнее, с небольшой величиной их наименьшего общего кратного (НОК).

Представление подстановок с помощью циклов хорошо изучено [11]. Ниже мы еще воспользуемся этими результатами. Отметим, что в криптографической литературе им уделяется меньше внимания, чем они заслуживают.

[3] Само по себе число неизменных битов ни о чем не говорит. Например, для приведенной далее подстановки (2) число неизменных битов может достигать 3. Гораздо важнее, что это фиксированные биты (1-й и 2-й), а также то, что подстановка (1) не обладает свойством размешивания: группы 4, 5; 8, 9 и 12, 13 переходят в другие компактные группы.

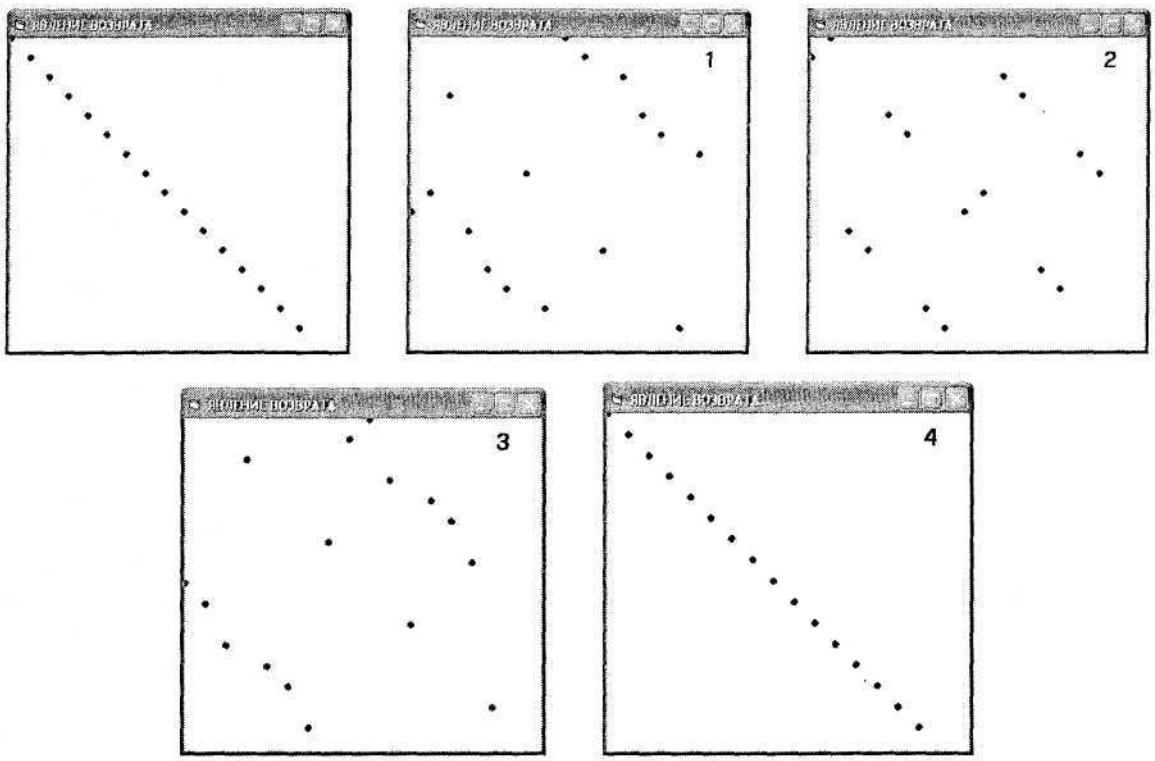


Рис. 1. Демонстрация явления возврата. Число в правом верхнем углу – номер итерации

4. Некоторые физические аналогии. Эргодичность

Эргодичность – это свойство отображений, приводящее к равномерному заполнению траекторией всего фазового объема. В дальнейшем мы будем рассматривать отображения в фазовом пространстве, представляющем гиперкуб в восьмимерном пространстве с длиной ребра 15.

Существует еще одна характеристика отображений – перемешивание, которая оценивает степень разбегания траекторий динамической системы. В нелинейной динамике она оценивается с помощью так называемых показателей Ляпунова [12], характеризующих скорость разбегания двух изначально близких траекторий. Можно усмотреть аналогию между понятием перемешивания в динамике и понятием размешивающего преобразования в криптографии. Приведем цитату из [13]:

«*Под размешивающим преобразованием Шеннон понимает некоторое отображение векторного пространства на себя, при котором каждая или почти каждая его компактная область в отображении распределяется в большую, некомпактную с точки зрения метрики, область...*

Рассматривая вектора как числа и применив подстановку:

0 1 2 3 4 5 6 7

7 3 1 5 4 2 3 0

мы видим, что данное преобразование с большим основанием можно назвать размешивающим, т.к. компактная область 0 1 2 отображается в 7 3 1».

Перемешивание – более сильное свойство динамической системы, чем эргодичность, в частности, система, обладающая перемешиванием, всегда эргодична. Системы с перемешиванием демонстрируют хаотическое, непредсказуемое поведение. В поисках аналогий можно было бы пойти еще дальше и сопоставить понятия динамического хаоса в динамике и лавинного эффекта в криптографии. Однако следует сказать, что прямой аналогии здесь нет, хотя бы потому, что отображения, реализуемые подстановками в криптографии и рассматриваемые здесь, всегда обратимы, тогда как хаотические системы в динамике демонстрируют необратимость.

В дискретных системах понятие ляпуновских показателей перестает работать. Если рассмотреть две изначально близкие тра-

ектории, принадлежащие одному циклу, то с ростом номера итерации расстояние между соответственными точками траекторий ведет себя случайным образом[4]. Поэтому вместо ляпуновских показателей можно характеризовать степень разбегания траекторий, а точнее, степень скорости, с которой стирается информация об их начальной близости с помощью автокорреляционной функции [14], вычисляя ее для зависимости расстояния от номера итерации (приложение).

Вернемся к эргодичности. Приведем ее определение [14]: «*Если движение динамической системы эргодично, то относительное время, проведенное фазовой траекторией внутри любой области Г фазового пространства, равно относительному объёму этой области и не зависит от выбора начальных условий. Иными словами, фазовая траектория эргодической системы будет равномерно и плотно заполнять всю область Г*».

Ниже приведены результаты расчета траектории отображения, реализуемого итерациями S-блоков DAS в проекции на грани, соответствующие первым трем S-блокам (U = S11, V = S21, S = S31) (рис. 2).

На рис. 3, *а*, *б* показаны результаты расчета числа точек траектории, попавших в измерительный 8-мерный куб с центром, совпадающим с центром фазовой области в зависимости от L – размера половины ребра измерительного куба. Слева показаны объем измерительного куба (плавная кривая) и число точек траектории в нем (ломаная) в зависимости от L, а справа – их отношение. Начальная точка отображения имеет координаты 4, 15, 10, 7, 2, 12, 4, 2. Это соответствует длине траектории возврата C = 16016[5].

Из полученных результатов следует, что точки траектории распределены не равномерно, а слоями, параллельными граням кубического фазового объема. Слабая зависимость результата от числа итераций (за исключением числа точек отображения) позволяет говорить о равномерном заполнении точками всего фазового пространства, т.е. эргодичности S-блоков DES (по крайней мере, выбранных) (табл. 3).

Таблица 3

S-блоки DES

S11	S21	S31	S41	S51	S61	S71	S81
14	15	10	7	2	12	4	13
4	1	0	13	12	1	11	2
13	8	9	14	4	10	2	8
1	14	14	3	1	15	14	4
2	6	6	0	7	9	15	6
15	11	3	6	10	2	0	15
11	3	15	9	11	6	8	11
8	4	5	10	6	8	13	1
3	9	1	1	8	0	3	10
10	7	13	2	5	13	12	9
6	2	12	8	3	3	9	3
12	13	7	5	15	4	7	14
5	12	11	11	13	14	5	5
9	0	4	12	0	7	10	0
0	5	2	4	14	5	6	12
7	10	8	15	9	11	1	7

Примечание. Использованы первые строки каждого S-блока.

[4] Если соответствующий S-блок достаточно велик, например имеет число входов-выходов равное 256 (см. приложение), и обладает хорошим рассеиванием, то этим свойством можно воспользоваться для генерации псевдослучайных последовательностей.

[5] Чтобы сравнивать число точек и объем гиперкуба, каждой точке отображения приписывается «объем» $15^8/(C+1)$. На рисунках видны следствия этой довольно произвольной процедуры – ломаная кривая пересекает плавную кривую и может сложиться впечатление, что суммарный «объем» точек в гиперкубе превосходит объем всего гиперкуба.

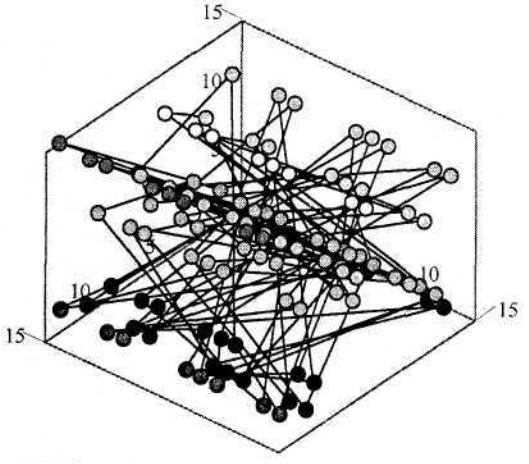
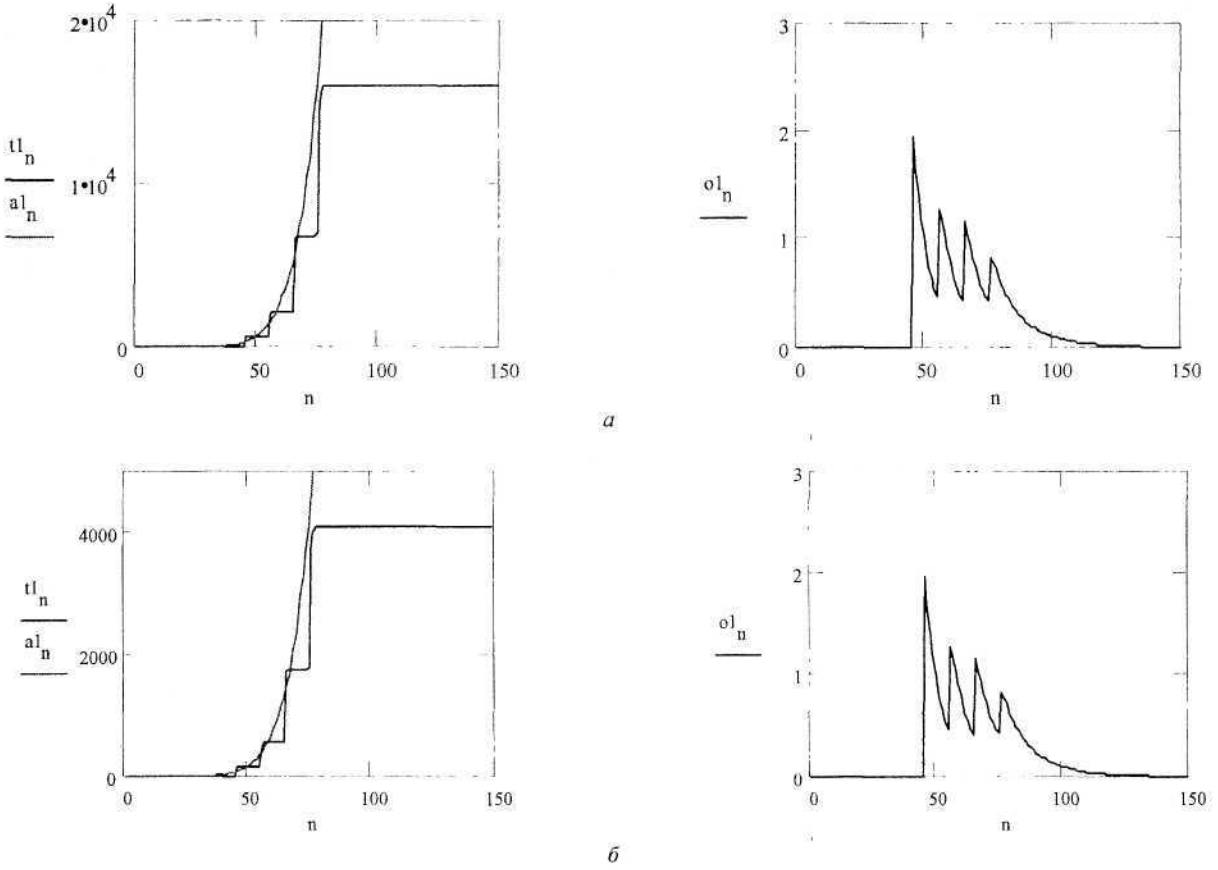


Рис. 2. Трехмерная проекция фазовой траектории для элементов S-блоков с номерами (1 0 0 0 0 0 0 1). Длина траектории возврата равна 16016

На рис. 4, *а*, *б* показаны результаты расчета для тех же S-блоков, но для другой начальной точки с координатами 14, 15, 10, 7, 2, 12, 4, 13, которой соответствует траектория возврата с длиной C = 1232.

Сравнение рис. 3, *а* и 4, *а* позволяет утверждать, что сказанное выше о равномерности заполнения точками отображения фазового пространства не зависит от конкретной траектории отображения и, в частности, от длины траектории возврата[6].

Другая особенность отображения – отсутствие точек в центре куба, связана с многомерным характером траектории и согласуется с известной особенностью многомерных объектов – вклад в их полный объем дают в основном периферические области.



а

б

Рис. 3. Результаты исследования эргодичности для S-блоков DES. Длина ребра измерительного куба равна 2L, L = n/10, 0 < n < 150. Точки перестают накапливаться при n > 75, т.е. после прохождения границы фазового объема. Число итераций C = 16016 (*а*) и C = 4096 (*б*)

[6] Необходимо помнить, что каждая данная совокупность S-блоков генерирует разные траектории. Исключение составляет случай, когда все подстановки в S-блоках полноцикловые.

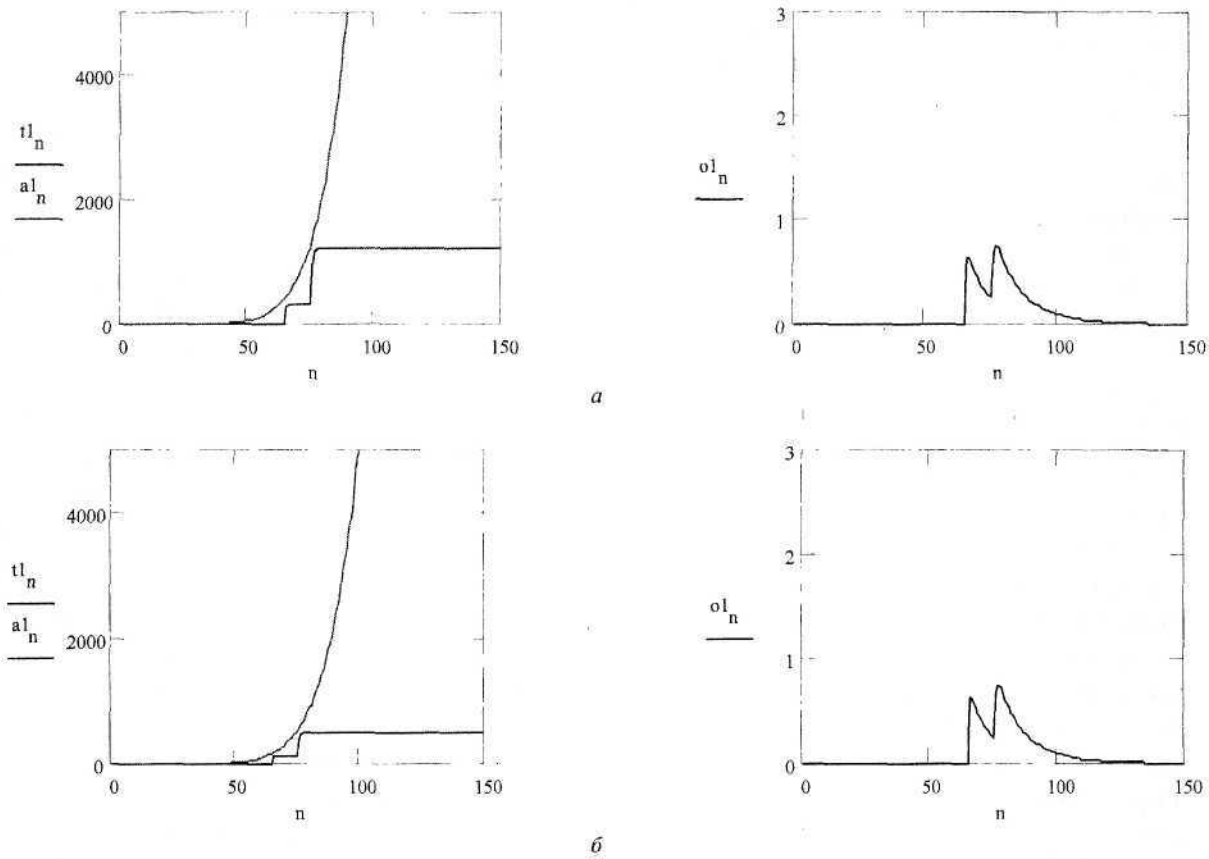


Рис. 4. Расчет для тех же S-блоков DES с начальной точкой, соответствующей номерам элементов (0 0 0 0 0 0 0 0). Число итераций C = 1232 (*а*) и C = 512 (*б*)

Для сравнения на рис. 5 приведем результаты аналогичного расчета для одного S-блока – S31, реализующего полноцикловую подстановку с длиной траектории возврата 16.

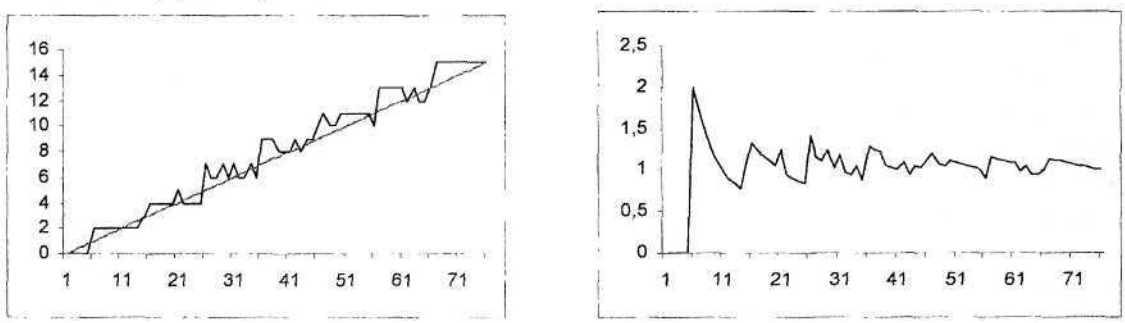


Рис. 5. Результаты исследования эргодичности для блока S31: *а* – 2L – длина ребра измерительного куба (отрезка) – прямая; N – число точек в кубе – ломаная; *б* – N/2L – их отношение. По оси абсцисс отложена величина L/10

5. Качество подстановок

Вопрос о качестве подстановок, реализуемых S-блоками блочных шифров, является одним из основных. Хороший S-блок (наряду с хорошим ключом) должен обеспечивать выполнение требований, предъявляемых к криптостойкости шифра. Очевидно, в шифросистемы ГОСТ 28147-89 и DES заложены алгоритмы выработки S-блоков, удовлетворяющие этим требованиям. Однако они

не раскрываются. Вместе с тем нет гарантии, что в некоторых реализациях упомянутых криптосистем не используются ослабленные S-блоки, наподобие (1). Поэтому исследователи-криптографы пытаются найти правила, позволяющие a priori оценивать качество подстановок, используемых в S-блоках.

В [9] приводятся некоторые, достаточно сложные, рассуждения, целью которых является нахождение лучших возможных подстановок. Для 16-ти элементов приведен явный вид подстановки, названной логарифмической:

14 12 3 7 9 15 8 13 0 6 2 10 5 4 1 1 (3)

Приведем цитату из [9]:

«Это был, пожалуй, мой самый красивый математический результат. Но, к большому сожалению, логарифмические подстановки так и не нашли достойного применения в криптографии. Почему? Да очень просто – их мало. Помните фразу про долговременные ключи-подстановки в дисковых шифраторах: "Их не опробуют. Их покупают". Если в схемы типа "Ангстрем-3" мы будем ставить только логарифмические подстановки, то опробование всевозможных вариантов подобных подстановок сведется к опробованию всего лишь трех элементов: q – примитивного элемента в поле Галуа GF(257), r – произвольного ненулевого элемента поля GF(257) и r – произвольного элемента из Z/256. Это – копейки, совершенно ничтожная, по криптографическим меркам, величина. Если же выбирать подстановку случайно и равновероятно из всей симметрической группы S_{256} (т.е. группы подстановок на множестве из 256 элементов. – *Ю.З.*), *то общее число опробуемых вариантов будет совершенно астрономической величиной 256!, намного превосходящей психологически недосягаемую в криптографии величину* 10^{100}.

Но для шифров на новой элементной базе логарифмические подстановки позволили полнее представить общую картину того "лавинного эффекта", к достижению которого так стремятся криптографы всего мира».

Эта цитата позволяет хотя бы приблизительно оценить сложность поставленной задачи и получить представление о методах, которые применяют специалисты-криптографы для ее решения.

Выше приводился пример слабого S-блока (1) и было высказано соображение, что его слабость связана с наличием коротких циклов, на которые разлагается реализуемая им подстановка. Можно было бы предположить, что полноцикловые подстановки, т.е. подстановки, состоящие из одного цикла максимальной длины, заведомо не будут слабыми и будут приводить к преобразованиям с хорошими размешивающими свойствами. То, что это не так, легко видно из простого примера полноцикловой подстановки, не удовлетворяющей требованию размешивания:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 0

Другой пример связан с упоминавшимися выше логарифмическими подстановками. Среди них могут быть полноцикловые, как, например, (3), и состоящие из более чем одного цикла (М. Масленников, частное сообщение).

Логарифмические подстановки, как уже было сказано, не находят широкого применения из-за того, что их мало и, следовательно, они могут быть легко вычислены.

Полноцикловые подстановки даже с хорошим размешиванием опасно применять еще и по следующим соображениям. Рассмотрим набор из восьми S-блоков, реализующих исключительно полноцикловые подстановки. Поскольку они оперируют независимо друг от друга, естественно перенести рассмотрение в восьмимерное пространство. Поставим вопрос о длине траектории возврата для данного варианта. Ответ очевиден – 16. Т.е. через 16, 32 и т.д. итераций преобразуемый текст восстановится. Конечно, этот результат получен в пренебрежении всеми остальными деталями криптоалгоритма, но это и позволило подчеркнуть слабую сторону полноцикловых подстановок.

Теперь посмотрим, какие подстановки применяют на практике (на примере ГОСТа). Для этого разложим S-блоки ГОСТ на циклы:

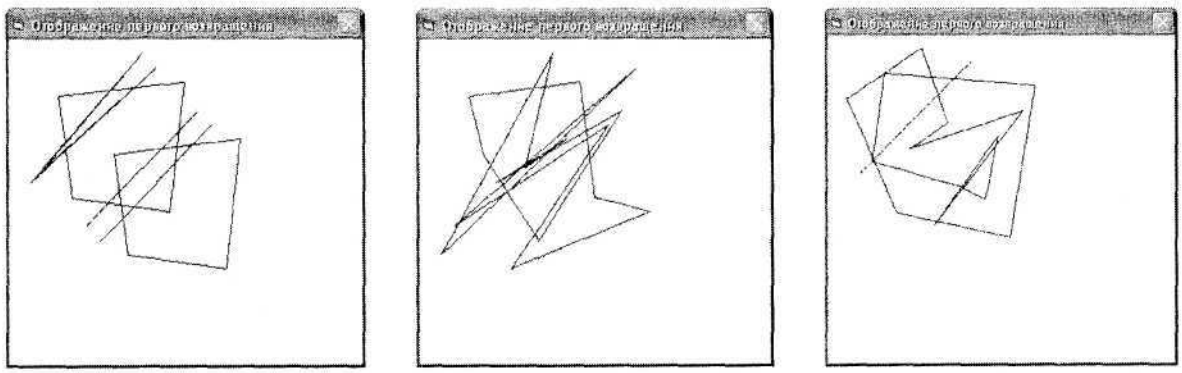
$S1 \rightarrow C_2(10, 1); C_{14}(0, 4, 13, 15, 3, 2, 9, 11, 12, 7, 14, 5, 8, 6)$

$S2 \rightarrow C_2(1, 11); C_{14}(0, 14, 5, 13, 7, 10, 8, 2, 4, 6, 15, 9, 3, 12)$

$S3 \to C_4(0, 5, 3, 13); C_4(4, 10, 12, 6);$
$C_8(8, 14, 9, 15, 11, 7, 2, 1)$
$S4 \to C_2(11, 12); C_3(8, 14, 5);$
$C_{11}(7, 15, 3, 1, 13, 2, 10, 6, 9, 4, 0)$ (4)
$S5 \to C_2(11, 14); C_2(9, 10); C_6(5, 15, 2,$
$7, 8, 4); C_6(6, 13, 3, 1, 12, 0)$
$S6 \to C_2(14, 15); C_{14}(4, 7, 13, 12, 9, 6, 1,$
$11, 5, 2, 10, 8, 3, 0)$
$S7 \to C_3(13, 8, 0); C_4(15, 12, 6, 5);$
$C_9(11, 7, 9, 10, 14, 2, 4, 3, 1)$
$S8 \to C_3(5, 7, 4); C_6(13, 11, 14, 8, 9, 2);$
$C_7(1, 15, 12, 6, 10, 3, 0)$

Видно, что создатели алгоритма использовали самые разные подстановки. Причина этого уже понятна. Отметим, что, в отличие от DES, среди циклов ГОСТ нет единичных, что, конечно, усиливает криптоалгоритм. Попытаемся оценить длину траектории возврата. Для этого найдем НОК длин всех входящих в разложение (4) циклов. Полученное число равно 5544 – это верхняя граница искомой величины. Представляется разумным предположить, что разработчики шифра стремились выбирать подстановки так, чтобы сделать это число максимально большим. Однако вопрос, каким образом они этого достигали, остается открытым.

Наконец, попытаемся представить качество подстановок визуально с помощью отображения первого возвращения, демонстрирующего зависимость S(S(i)) от S(i) (i – номер элемента) для двух представленных выше подстановок и реального S-блока (рис. 6).



а *б* *в*

Рис. 6. Отображение первого возвращения: *а* – для подстановки (1); *б* – для (2); *в* – для S1-блока ГОСТ

Отличие отображений бросается в глаза. Отображение *а* резко отличается от отображений *б* и *в* своей регулярностью, связанной с плохими криптографическими свойствами подстановки (1). С другой стороны, на каждом отображении четко просматривается цикловая структура соответствующей подстановки. Особенно четко она просматривается на рис. 6, *а*. Две прямые соответствуют двум циклам длины 2, три четырехугольника – трем циклам длины 4. На основании рис. 6 можно попытаться сформулировать геометрический критерий отбора «хороших» S-блоков.

6. Статистика S-блоков

Представление подстановок с помощью циклов позволяет исследовать их статистические характеристики и сопоставить с характеристиками реальных S-блоков. Результаты статистического исследования подстановок мы заимствуем у Д. Кнута [11].

Если A – число циклов в подстановке[7] из n элементов, то его средние характеристики суть:

$$\min A = 1, \quad \text{ave}\, A = H_n, \qquad \max A = n, \quad \text{dev}\, A = (H_n - H_n^2)^{1/2}. \tag{5}$$

Здесь ave и dev – среднее значение и среднеквадратичное отклонение соответственно (в обозначениях Д. Кнута) и

$$H_n^m = \sum_{1 \le k \le n} \frac{1}{k^m}, H_n = H_n^1. \tag{6}$$

Кроме того, подстановка из n предметов имеет k циклов с вероятностью, равной

[7] Д. Кнут называет их перестановками.

$|S(n, k)| / n!$, где $(-1)^{n-k}S(n, k)$ – числа Стирлинга первого рода.

Можно также задать вопрос о средней длине одного цикла. Согласно (5), общее число циклов во всех $n!$ перестановках есть $n!H_n$ (поскольку оно равно среднему числу циклов, взятому $n!$ раз). Отсюда можно получить выражение для средней длины произвольного цикла в виде n/H_n.

Отсюда же следует выражение для вероятности появления цикла длины k в подстановке из n элементов. Поскольку общее число циклов длины k в подстановке из n элементов равно $n!/k$, а общее число циклов есть $n!H_n$, то искомая вероятность равна их отношению, т.е. $1/kH_n$.

Подсчитаем вероятность появления полноцикловых подстановок на множестве из 16 элементов. Она равна $1/16H_{16} = 0.0185$.

На рис. 7 представлены статистические результаты по длинам циклов. На их основе можно решить вопрос о характере отбора S-блоков из всего множества подстановок. Уже беглого взгляда достаточно, чтобы понять, что для ГОСТ отбор делался не случайно и не равновероятно. Чтобы получить точный ответ, приведем результаты корреляционного анализа представленных данных.

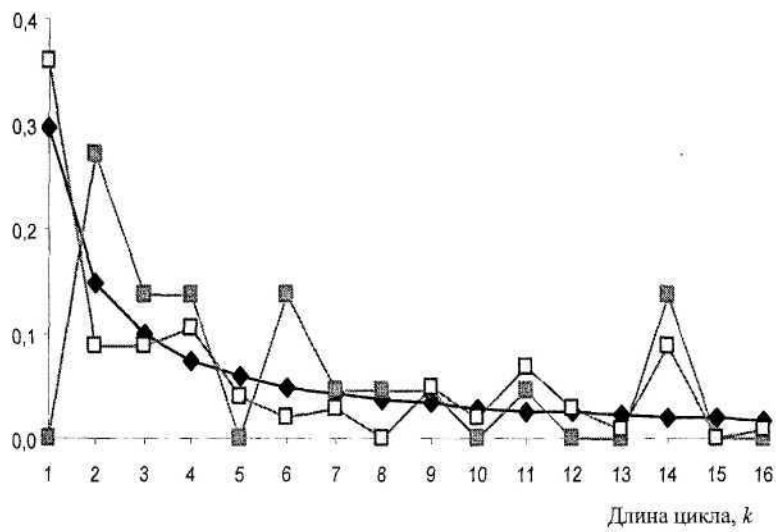


Рис. 7. Статистические характеристики длин циклов: –◆– вероятность $P(k)$; –■– частота ГОСТ; –□– частота DES

Формула для оценки коэффициента корреляции двух случайных величин x и y имеет вид [15]:

$$r_{xy} = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\left[\sum_{i=1}^{N}(x_i - \bar{x})^2 \sum_{i=1}^{N}(y_i - \bar{y})^2\right]^{1/2}} = \frac{\sum_{i=1}^{N} x_i y_i - N\bar{x}\bar{y}}{\left[\left(\sum_{i=1}^{N} x_i^2 - N\bar{x}^2\right)\left(\sum_{i=1}^{N} y_i^2 - N\bar{y}^2\right)\right]^{1/2}}. \quad (7)$$

Здесь x_i и y_i – вероятность появления в подстановке цикла длиной i и частота этого события для конкретного криптоалгоритма (DES или ГОСТ), $\bar{x}$ и $\bar{y}$ – их среднее и выборочное среднее значения, $N = 16$ – число испытаний (т.е. различных циклов) в выборке.

Область принятия гипотезы о нулевой корреляции (т.е. отсутствии корреляции) имеет вид [15]:

$$-z_{\alpha/2} \le \sqrt{N-3}\cdot w \le z_{\alpha/2}, w = \frac{1}{2}\ln\frac{1+r_{xy}}{1-r_{xy}}, \quad (8)$$

где z – стандартная, нормально распределенная величина. Если значение окажется вне этого интервала, то это будет признаком наличия статистической корреляции с уровнем значимости α.

Выполняя расчеты, получаем следующие значения. Для ГОСТ: $r_{xy} = 0.203783$ и $w = 0.206676$, а для DES – $r_{xy} = 0.916768$ и $w = 1.568383$. Сразу бросается в глаза, что значение коэффициента корреляции для DES более чем в четыре раза превышает аналогичное значение для ГОСТ. Задавая уровень значимости $\alpha = 5\%$ и беря значение $z_{\alpha/2}$ из таблиц [15, с.500] равным 1.96, получим, что гипотеза о нулевой корреляции с указанным уровнем значимости должна быть отвергнута для DES, поскольку $w(N-3)^{1/2}$, равное 5.6549, не попадает в интервал ±1.96. В то же время для ГОСТ эта гипотеза с тем же уровнем значимости должна быть принята, так как значение $w(N-3)^{1/2}$, равное 0.7452, оказывается внутри этого интервала.

Проделаем аналогичные расчеты для распределения S-блоков по числу циклов, на которые они разлагаются, исходя из публикуемых данных (рис.8).

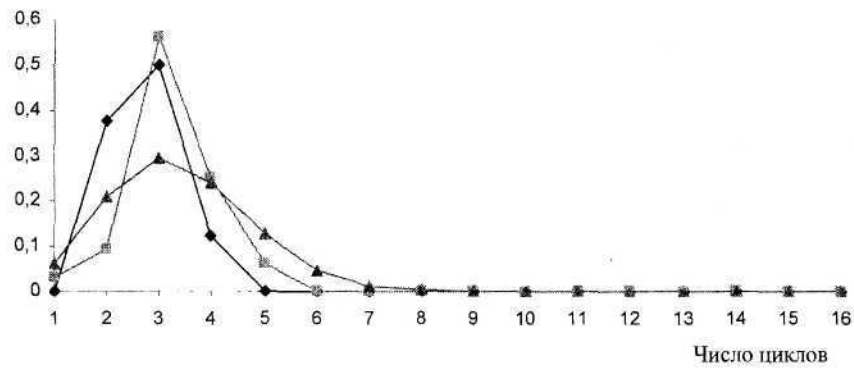


Рис. 8. Статистические данные по числу циклов в S-блоках: –♦– ГОСТ; –■– DES; –▲– вероятность

Выполняя расчеты по формулам (7) и (8), получим: для ГОСТ – коэффициент корреляции $r_{xy} = 0.852265$, $w = 1.264372$ и $w(N-3)^{1/2} = 4.558759$, а для DES – $r_{xy} = 0.804818$, $w = 1.112141$ и $w(N-3)^{1/2} = 4.009883$. Задавая тот же уровень значимости 5%, получим, что гипотеза о нулевой корреляции как для ГОСТ, так и для DES должна быть отвергнута, поскольку полученные значения не попадают в интервал ±1.96. Говоря другими словами, если за фактор оценки выбора S-блоков взять число циклов в них, то полученный результат говорит в пользу случайного и равновероятного отбора S-блоков из множества всех подстановок.

Следует сказать, что этот результат, как и приведенный выше, не вносит окончательной ясности в вопрос о случайности (или неслучайности) выбора S-блоков. В литературе встречаются утверждения обоего толка [1, 2]. Ввиду того что упомянутые утверждения представляют собой мнения, не подкрепленные ссылками на иные источники, кроме других мнений [16] (Бёрд Киви, частное сообщение), следует, по-видимому, относиться к ним с осторожностью, по крайней мере, в отношении публикуемых S-блоков.

Можно привести некоторые дополнительные соображения о неслучайности выбора S-блоков, привлекая для этой цели закон больших чисел [15]. Согласно ему разности выборочных средних случайной величины, взятые по некоторым выборкам мощности N_1 и N_2, и математического ожидания этой величины относятся как $(N_1/N_2)^{-1/2}$. Чтобы применить закон больших чисел к данной ситуации, надо пренебречь отличиями алгоритмов выбора S-блоков DES и ГОСТ и считать их наборы двумя случайными выборками разной мощности $N_2 = 32$ и $N_1 = 8$. Тогда вышеупомянутое отношение должно быть равно 2. Однако в действительности, как легко проверить с помощью вышеприведенных формул, оно близко к 4, причем это справедливо как для числа циклов в перестановках, так и для их длин.

Следует сказать, что высказывание А. Чморы [2] о случайном выборе S-блоков ГОСТ заимствовано им у Б. Шнайера [1], что снимает с него ответственность за необоснованные «домыслы» (Бёрд Киви, частное сообщение). Что же касается первоисточника [1], то, скорее всего, это утверждение – результат слишком вольного перевода.

Заключение

В статье представлены некоторые результаты исследования важных элементов блочных криптографических систем – блоков подстановок, так называемых S-блоков, методами, которые заимствованы из нелинейной динамики сложных систем. Эти методы используют понятия точечного отображения, эргодичности, перемешивания и др. Сами эти понятия не являются чем-то чуждым в криптографии, например, понятие отображения с перемешиванием близко к понятию размешивающего преобразования. Новым является использование визуального представления преобразований, осуществляемых S-блоками, что позволяет наглядно представить процесс оценки качества и отбора «хороших» с криптографической точки зрения подстановок.

Другим результатом статьи является статистический анализ S-блоков, выполненный на основе разложения их на циклы. Это позволяет более обоснованно, чем это делалось ранее, решить вопрос о выборе S-блоков из всего множества подстановок.

Возможно, в дальнейшем этот подход в сочетании с традиционными для криптографии методами позволит по-новому взглянуть на проблемы блочных криптографических систем и получить новые полезные результаты.

Автор выражает благодарность М. Масленникову за обсуждения статьи, а также студентам ФГОУ ВПО ПАГС им. П.А. Столыпина и филиала в г. Балакове, обучающимся по специальности «Прикладная информатика», О. Елистратовой и М. Конинской за активное и полезное участие в работе.

Список литературы

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С / Пер. с англ. М.: Триумф, 2002. 816 с.

2. *Чмора А.Л.* Современная прикладная криптография. М.: Гелиос АРВ, 2002.

3. Указ Президента РФ № 334 от 05.04.95 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставление услуг в области шифрования информации» // Собрание законодательства РФ. 1995. №29.

4. Federal Information Processing Standards Publication (FIPS PUB) 46-1, Data Encryption Standard, Reaffirmed 1988 Jan 22 (supersedes FIPS PUB 46, 1977 Jan 15).

5. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». М.: Госстандарт СССР, 1989.

6. *Бернет С., Пэйн С.* Криптография. Официальное руководство RSA Security / Пер. с англ.; Под ред. А.И. Тихонова. М.: Бином, 2002.

7. *Шеннон К.* Работы по теории связи и кибернетике. М.: Иностр. лит., 1963. 830 с.

8. *Масленников М.* Практическая криптография. СПб.: БХВ-Петербург, 2003.

9. *Масленников М.* Криптография и свобода // http://mikhailmasl.livejournal.com/4852.html

10. *Винокуров А.Ю.* Как устроен блочный шифр // http://algolist.manual.ru/defence/index.php

11. *Кнут Д.* Искусство программирования: В 4 т. Т.1. Основные алгоритмы. М.: Мир, 1976.

12. *Заславский Г.М.* Стохастичность динамических систем. М.: Наука, 1984.

13. *Щербаков А.Ю., Домашев А.В.* Прикладная криптография. Использование и синтез криптографических интерфейсов. М.: Русская редакция, 2003.

14. *Лоскутов А.Ю., Михайлов А.С.* Введение в синергетику. М.: Наука, 1990.

15. *Бендат Дж., Пирсол А.* Прикладной анализ случайных данных. М.: Мир, 1989.

16. http://en.wikipedia.org/wiki/Data_Encryption_Standard (англоязычная версия), http://ru.wikipedia.org/wiki/DES (русскоязычная версия).

Приложение

Тестирование S-блоков хеш-функций методами нелинейной динамики

Хеш-функции применяются в криптографии для целей шифрования паролей, создания цифровой подписи и т.д. [17]. Среди направлений разработки стойких хеш-функций можно выделить использование симметричных блочных алгоритмов [18], одним из основных элементов алгоритма которых является преобразование подстановки, выполняемое с помощью S-блоков, подобных рассмотренным в настоящей статье. Применим изложенную выше методику для оценки качества используемых в реальных алгоритмах хеширования S-блоков, исследуя эргодичность реализуемых ими преобразований. Для этого рассмотрим несколько заявок конкурса, проводимого Национальным институтом стандартов США (NIST), информация о котором была помещена на официальном сайте NIST [19] в декабре 2008 г.

Одна из заявок зарегистрирована под кодовым именем Abacus (заявитель – Neil Sholer). Не вдаваясь в детали, отметим, что в предлагаемом алгоритме используется S-блок 256*256, преобразующий входные байты в выходные (256 – число входов и выходов). S-блок представлен в табл. П.1 (в шестнадцатеричной системе).

Таблица П.1

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	e3	84	f0	d6	f9	f6	bc	90	85	7d	28	43	12	c0	e1	b4
10	55	c7	8c	87	42	e0	d9	27	78	ec	cb	07	aa	95	c1	3f
20	b2	dc	26	a7	1f	df	f3	54	d2	e7	24	3e	32	d1	56	c6
30	35	73	f7	7b	62	29	52	80	a9	ba	ab	e9	02	53	6a	e4
40	67	a0	8e	fb	9a	79	4e	8d	e5	4a	41	af	5a	5c	a6	6b
50	16	5e	e8	3c	9c	5b	88	76	15	f4	60	bd	83	98	8f	c8
60	09	68	0d	18	65	45	04	ce	7a	f2	39	c5	9e	f1	17	ef
70	38	21	94	86	69	37	f5	ed	36	66	cf	3b	63	4b	33	b6
80	ff	bc	11	5d	b3	2b	d3	d0	3a	96	77	7c	1c	c2	fe	0a
90	c3	25	4d	fc	89	de	30	23	64	81	d5	ac	70	db	e6	7e
a0	b0	6f	0f	d7	bf	9b	c4	74	b7	57	4f	58	10	2d	a4	b9
b0	a2	ad	61	eb	ac	1a	a3	d8	2c	5f	91	2f	72	31	b1	82
c0	49	da	0c	ca	00	a1	b5	75	6e	47	6d	13	19	93	20	05
d0	01	9f	1d	44	8a	1e	50	34	fa	9d	a8	8b	0b	4c	a5	2e
e0	71	f8	40	cd	99	fd	51	59	0e	2a	3d	92	14	48	6c	ea
f0	46	22	cc	06	d4	97	e2	1b	dd	7f	bb	c9	b8	03	ee	08

Старшие значащие биты расположены слева. S-блок читается слева направо и сверху вниз. Например, входу 02 соответствует выход f0, а входу 7e – выход 33. Ниже представлены результаты исследования эргодичности S-блока.

На рис. П.1 показана зависимость отношения числа точек в измерительном кубе n (отрезке) к длине отрезка 2L в зависимости от L, $1 \le L \le 127$. Центр куба расположен в точке 127. Кроме того, там же представлены результаты расчета автокорреляционной функции для расстояния двух изначально близких точек, принадлежащих одному циклу по формуле

$$Corr(j) = \frac{1}{C}\sum_{i=0}^{C-1}\left[r(i) - < r >\right]\cdot\left[r(i+j) - < r >\right], \quad (9)$$

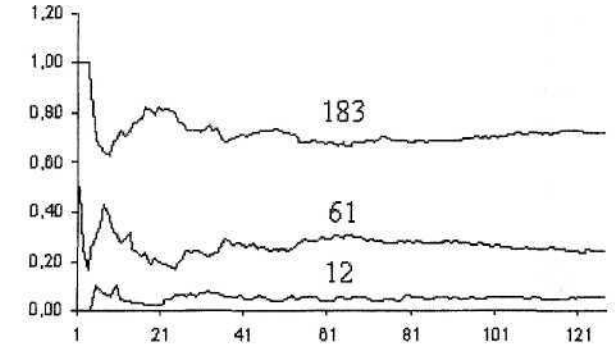
где r – расстояние между точками, $< r >$ – среднее расстояние (по итерациям), i, j – номер итерации, C – длина цикла (траектории возврата). Начальные точки выбраны так, что $r(0) = 1$.

S-блок имеет три цикла (подстановка разлагается на три цикла) длиной C = 12, 61 и 183 (12 + 63 + 183 = 256). Для каждого из них получается своя характеристика эргодичности. Для цикла длиной 12 график показывает насыщение величины n/2L порядка $0.05 \approx 12/256 = 0.046875$. Для цикла длиной 61 – насыщение порядка $0.25 \approx 61/256 = 0.23828$. Для цикла длиной 183 насыщение порядка $0.7 \approx 183/256 = 0.71484$.

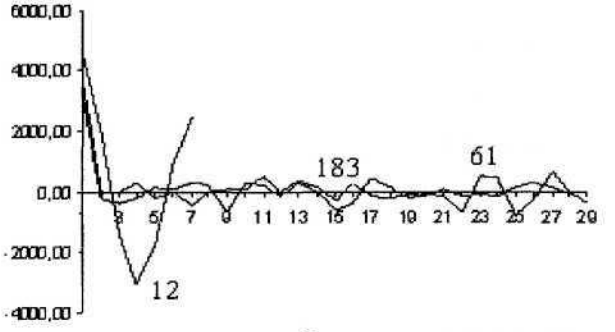
Эти значения представляют собой не что иное, как значения инвариантной меры на соответствующих подмножествах, совпадающих с циклами подстановки. Это следует из определения понятия инвариантной меры [20], позволяющей выразить среднее значение произвольной функции $g(x)$ на множестве элементов подстановки как среднее значение относительно инвариантной меры

$$\frac{1}{N}\sum_{i=0}^{N-1} g(x_i) = \frac{1}{N}\sum_j\sum_{i=0}^{N-1} g(f^i(x_{oj})) = \sum_j \rho_j \sum_{i=0}^{N_j-1} g(x_i). \quad (10)$$

Здесь $N = 256$ – полное число элементов подстановки f, N_j = 12, 61, 183 (j = 1, 2, 3) – число элементов каждого из циклов, на которые распадается подстановка f; f^i – i-я итерация подстановки f, x_{0j} – произвольный элемент подстановки, принадлежащий j-му подмножеству (циклу); $\rho_j = N_j / N$ – значения инвариантной меры ρ на j-м подмножестве.



а



б

Рис. П.1. Результаты тестирования S-блока Abacus: *а* – результаты расчета эргодичности; *б* – автокорреляционная функция. Число у кривой означает длину соответствующей траектории возврата. По оси абсцисс отложена величина L/2 (*а*) и номер итерации j (*б*)

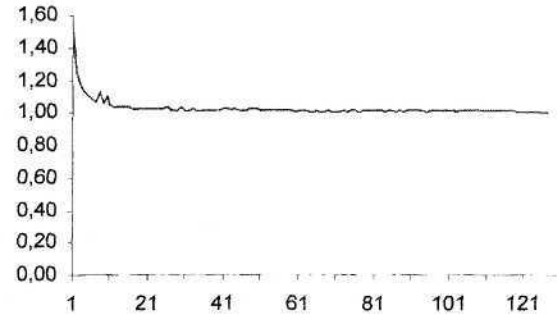
Из анализа поведения автокорреляционной функции можно заключить, что переход от цикла длиной 183 к циклу длиной 61 приводит к значительному росту ее значений на итерациях с большим номером. Для цикла длиной 12 рост значений автокорреляционной функции имеет место при любых итерациях.

Рассмотрим характеристики другого кандидата – MCSSHA-3 (заявитель М. Масленников). Соответствующий S-блок представлен в табл. П.2

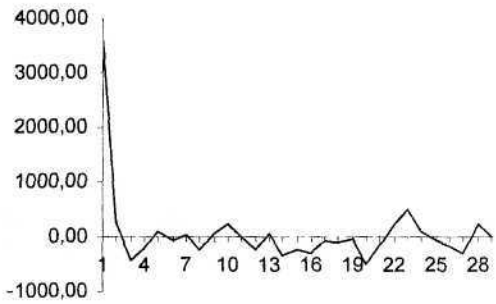
Таблица П.2

30 60 67 B5 43 EA 93 25 48 0D 18 6F 28 7A FE B6
D5 9C 23 86 52 42 F7 FD F6 9B EE 99 91 BC 2A 63
A1 A0 57 3C 39 D2 EC 71 45 CB 41 DC 0B 5B C2 36
01 55 7D FB ED 83 8F 31 C0 4C 08 E3 9D C1 D3 E9
B8 BD AE 0F E7 70 5A EB 4D 29 F9 A9 3D 26 46 06
D0 50 A5 BE 66 90 F4 20 E4 33 27 E2 AB EF 68 54
37 6A DB BB D8 7B 69 C4 F2 BF 85 C7 A6 B4 9A DD
72 34 E8 FC D6 21 98 96 32 CA 49 B3 F3 97 8E 2F
00 B0 10 1A 77 38 CF 51 BA 1F 22 AC 62 89 76 C3
02 6E 2C 47 3A 5C 1B 56 8A 5D 03 16 74 58 79 09
D7 F5 0A 92 4F 87 CD DA 8C C9 9E 3B 12 6B 53 FF
80 B7 F8 D9 F1 5E AF E0 05 A4 14 2B A3 CC 6C 7C
78 AA 95 84 61 A8 CE 13 88 FA 59 4E B9 C8 4B 24
D1 07 94 2E DF B1 17 A2 1D 4A C6 AD 15 19 35 7F
81 44 0C 9F 75 7E D4 82 DE E6 E1 2D 3E 73 11 8B
C5 A7 F0 6D 1C 64 0E 04 40 1E 8D E5 3F B2 65 5F

Результаты анализа показали, что подстановка имеет один цикл длиной 256. Это хорошо видно на рис. П.2.



а



б

Рис. П.2. Результаты тестирования S-блока MCSSHA-3: *а* – результаты расчета эргодичности; *б* – автокорреляционная функция. По оси абсцисс отложена величина L/2 (*а*) и номер итерации *j* (*б*)

Из сравнения рис. П.1 и П.2 можно сделать вывод о преимуществах полноцикловых подстановок перед прочими подстановками с достаточно большой длиной цикла. Это видно из того, что точки отображения, генерируемого полноцикловой подстановкой, равномернее заполняют фазовое пространство. Очевидно, что уменьшение длины цикла ведет к снижению криптографических свойств S-блока и, как следствие, алгоритма хеширования в целом.

По характеру поведения кривой на рис. П.2, *а* можно заключить, что данная подстановка (MCSSHA-3) обладает хорошими размешивающими свойствами, поскольку кривая достаточно быстро выходит на значение соответствующей инвариантной меры $\rho = 1$ (чего нельзя сказать о подстановке Abacus).

Список литературы

17. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. М.: Кудиц-Образ, 2001.

18. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хеширования.

19. http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html

20. *Шустер Г.* Детерминированный хаос / Пер. с англ.; Под ред. А.В. Гапонова-Грехова, М.И. Рабиновича. М.: Мир, 1988.

УДК 530.182:577.3

ОБ ОБУСЛОВЛЕННОСТИ НЕПЕРИОДИЧЕСКИХ АВТОКОЛЕБАНИЙ ПРОКСИМАЛЬНОГО ДАВЛЕНИЯ В НЕФРОНЕ НЕЛИНЕЙНЫМ ОТКЛИКОМ СОКРАТИТЕЛЬНОГО МЕХАНИЗМА АФФЕРЕНТНОЙ АРТЕРИОЛЫ

О.Н. Павлова, Д.Э. Постнов

Саратовский государственный университет
E-mail: pavlova_olga@yahoo.ru

Методами нелинейной динамики и анализа временных рядов исследуется вопрос о механизме возникновения хаотических автоколебаний, экспериментально наблюдаемых в физиологических экспериментах по исследованию процесса авторегуляции почечного кровотока в нефронах почки млекопитающих. Полученные результаты говорят в пользу гипотезы, согласно которой сложные колебательные режимы возникают за счет нелинейных характеристик сократительного механизма малого кровеносного сосуда (афферентной артериолы) на входе в нефрон.

Ключевые слова: нефрон, автоколебания, хаос, артериола, гипертензия, вейвлет.

About Conditionality of Nonlinear Responce of Miogenic Response of Afferent Arteriola for Irregular Self-Sustained Oscillations of Nephron Proximal Pressure

O.N. Pavlova, D.E. Postnov

By means of nonlinear dynamics and time series analysis we investigate the possible mechanisms for the onset of chaotic self-sustained dynamics in nephron tubular pressure that is observed experimentally. Our results suggests that the miogenic constriction mechanism of afferent arteriola plays the key role providing the nonlinear response on temporal variation of filtration rate.

Key words: nephron, self-oscillation, chaos, hypertensia, wavelet.