Радиофизика и радиоастрономия, 2004, т. 9, №2, с. 208-213

УДК 681.3.06:519.248.681

Криптографический анализ случайных последовательностей, генерируемых системами с хаотическим поведением

Д. Д. Ваврив

Харьковский национальный университет имени В. Н. Каразина,
Украина, 61077, г. Харьков, пл. Свободы, 4.
E-mail: vavriv@ukrpost.net

Статья поступила в редакцию 31 марта 2004 г.

Исследована возможность использования детерминированных нелинейных динамических систем с хаотическим поведением в роли генераторов случайных последовательностей. Найдены статистические характеристики последовательностей, генерируемых системой Макея-Гласса. Установлено, что в широкой области управляющих параметров эти последовательности проходят тесты FIPS 140-1. Тем самым показано, что формирование случайных последовательностей путем использования детерминированных систем с хаотическим поведением является перспективным для криптографических задач.

Досліджено можливість використання детермінованих нелінійних динамічних систем з хаотичною поведінкою як генераторів випадкових послідовностей. Вивчено статистичні характеристики послідовностей, генерованих системою Макея-Гласса. Встановлено, що в широкій області керуючих параметрів ці послідовності проходять тест FIPS 140-1. Тим самим показано, що формування випадкових послідовностей шляхом використання детермінованих систем з хаотичною поведінкою є перспертивним для криптографічних задач.

1. Введение

В последнее время широкое распространение получают системы электронных платежей через Интернет и другие системы неограниченного доступа, в которых требуется обеспечить конфиденциальность передаваемой информации. В связи с этим все более актуальной становится задача создания надежных и одновременно удобных средств защиты сигналов и сообщений от несанкционированного доступа. Разработка методов защиты информации на основе применения хаотических колебаний, генерируемых системами с детерминированным поведением, является одним из наиболее перспективных направлений в этой области. Существует несколько возможных подходов к применению хаотических сигналов для этих целей, в частности, методы, основанные на использовании явления взаимной синхронизации хаотических систем [1, 2] или на обращении динамических систем [3, 4]. Общим для этих методов является то, что при их реализации в качестве кодирующей и декодирующей систем используются детерминированные (аналоговые или цифровые) хаотические динамические системы. Вместе с тем хаотические колебания могут применяться непосредственно в классических криптографических схемах в качестве источников случайных последовательностей, которые необходимы для реализации таких схем.

Известно, что проблема генерации истинно случайных последовательностей остается достаточно серьезной. Например, стандартные генераторы случайных чисел, встроенные в программное обеспечение компьютера, в действительности являются

псевдослучайными и мало подходят для криптографических целей. Наиболее подходящими генераторами случайных последовательностей считаются генераторы, основанные на физических источниках, например, шумовые диоды. Недостатками таких генераторов являются относительная сложность получения случайных последовательностей, неудобства, связанные с интеграцией этих генераторов с остальными подсистемами, а также невозможность воспроизведения случайных последовательностей с помощью этого же источника.

Исходя из общих соображений, генераторы случайных последовательностей на основе хаотических систем могут объединять преимущества стандартных компьютерных генераторов случайных чисел и физических источников шумовых колебаний. Вместе с тем статистические характеристики хаотических колебаний с точки зрения криптографических приложений изучены мало. В настоящей работе проведен такой анализ бинарных последовательностей хаотических колебаний, получаемых из решения уравнения Макея-Гласса и неавтономного уравнения маятника. Для проверки статистических характеристик последовательностей и их пригодности для криптографических применений использовался американский федеральный стандарт FIPS 140-1 [5].

2. Генераторы случайных битовых последовательностей на основе систем с хаотическим поведением

Существует достаточно много динамических систем, которые демонстрируют хаотическое поведение [6]. В настоящей работе в качестве генераторов случайных последовательностей изучались классические динамические системы, описываемые уравнением Макея-Гласса и неавтономным уравнением маятника. Уравнение Макея-Гласса имеет следующий вид:

$$\frac{dx}{dt} = -bx + a\frac{x(t-\tau)}{1+x^n(t-\tau)}. \qquad (1)$$

Здесь n – целое число, t – параметр запаздывания, a и b – действительные параметры. Это уравнение впервые было предложено в работе [7] для описания процесса регенерации белых кровяных шариков. В последующих работах было показано (см. [8]), что подобное уравнение является распространенной моделью разнообразных процессов с запаздыванием.

В качестве неавтономного уравнения маятника исследовалось следующее уравнение:

$$\frac{d^2x}{dt^2} + \delta\frac{dx}{dt} + \alpha\sin x = F\cos\omega t. \qquad (2)$$

Это уравнение описывает колебания маятника с учетом силы трения, задаваемой нормированным коэффициентом δ, и при наличии внешней силы с нормированной амплитудой F; x – отклонение маятника от вертикали, α – квадрат собственной частоты.

Приведенные уравнения решались численно с помощью метода Рунге-Кутта четвертого порядка. При проведении таких расчетов предполагалось, что все величины в уравнениях (1), (2) являются безразмерными. В результате определялись временные реализации состояний динамических систем $x(t)$. Исследовавшиеся динамические системы в зависимости от значения управляющих параметров могут демонстрировать как регулярное, так и хаотическое поведение. Пример хаотического решения уравнения (1) приведен на рис. 1. Это решение представляет собой случайную функцию $x(t)$.

Для формирования случайной последовательности нулей и единиц использовалась известная пороговая методика, в соответствии с которой сначала формировалась дискретная последовательность $x_i = x(t_0 + i\Delta t)$ из временной реализации $x(t)$. Здесь t_0 – начальный момент времени, Δt – шаг дискретизации по времени, $i = 0, 1, 2, \ldots$. Далее выбиралась не-

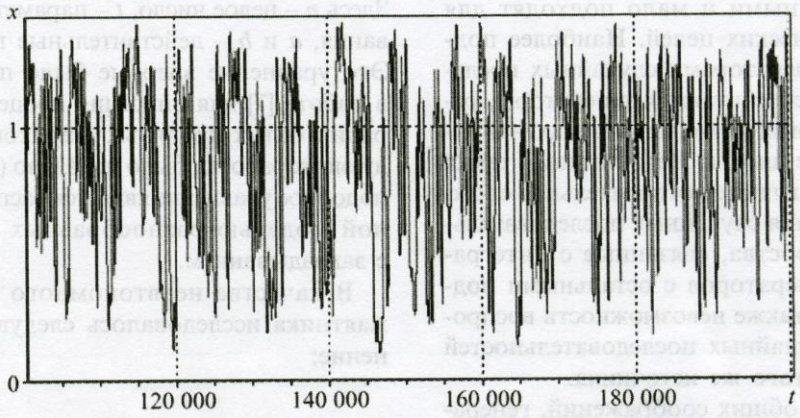

Рис. 1. *Пример решения уравнения Макея-Гласса*

которая пороговая величина $x_{\text{пор}}$ и формировалась последовательность нулей и единиц n_i в соответствии со следующим правилом:

$$n_i = \begin{cases} 0, & x_i \le x_{\text{пор}}, \\ 1, & x_i > x_{\text{пор}}. \end{cases} \qquad (3)$$

Таким образом, значение n_i равняется нулю, если значение функции $x(t)$ при $t = t_0 + i\Delta t$ не превосходит некоторого заданного порогового значения. В противном случае n_i присваивается значение единица.

Полученные последовательности анализировались на их соответствие американскому федеральному стандарту FIPS 140-1.

3. Структура стандарта FIPS-140-1

Стандарт FIPS 140-1 предписывает набор тестов, которые должны пройти битовые последовательности для признания их пригодными к применению в системах кодирования информации [5]. Этот набор включает в себя четыре независимых статистических теста на случайность: монобитный тест, тест Покера, тест серий, тест длин серий. Отдельная битовая строка длиной 20000 битов, получаемая из генератора случайных чисел, подвергается каждому из четырех перечисленных тестов. Если какой-нибудь из тестов не пройден, то считается, что последовательность не прошла весь комплекс проверок.

Монобитный тест. Суть теста заключается в том, что подсчитывается количество единиц (нулей) битовой последовательности X. Если полученное значение X удовлетворяет критерию $9654 < X < 10346$, то считается, что тест пройден.

Тест Покера. Последовательность длиной в 20 000 битов разделяется на 5 000 последовательностей по 4 бита. Затем считается количество повторений каждой из возможных 16 различных комбинаций 4-битовых последовательностей $f(i)$, где i – номер одной из 16 комбинаций. Подсчитывается число X по формуле

$$X = (16/5000)\left(\sum_{i=0}^{15}[f(i)]^2\right) - 5000.$$

Если последовательность случайна, то значение X должно удовлетворять условию $1.03 < X < 57.4$.

Тест серий. Тест подсчитывает количество встречающихся серий длиной от 1 до 6 бит. Под серией понимается непрерывающаяся последовательность нулей или единиц (серии с длиной более 6 бит принимаются за серию с длиной в 6 бит). Тест считается пройденным, если количество серий как

нулей, так и единиц удовлетворяет требованиям, приведенным в таблице.

Таблица.

Длина серий	Требуемый интервал
1	2267 ÷ 2733
2	1079 ÷ 1421
3	502 ÷ 748
4	223 ÷ 402
5	90 ÷ 223
6	90 ÷ 223

Тест длин серий. Определяет наличие длинных серий в тестируемой последовательности. Длинной считается серия длиной 34 бита и более (как для нулей, так и для единиц). Считается, что тест пройден, если в 20 000-битовой последовательности не встречаются длинные серии.

4. Результаты тестирования

Битовые строки длиной 20 000 битов, получаемые с помощью уравнения Макея-Гласса и неавтономного уравнения маятника, подвергались каждому из четырех приведенных тестов. Проведенные исследования выявили следующие закономерности. Оказалось, что области существования хаотических колебаний в пространстве управляющих параметров шире, чем области параметров, в которых генерируются истинно случайные битовые последовательности. Области существования хаотических колебаний определялись по таким признакам, как положительное значение показателей Ляпунова и наличие сплошного спектра колебаний, а под термином "истинно случайные" мы здесь понимаем такие последовательности, которые проходят указанные тесты. В случае неавтономного уравнения маятника нам не удалось обнаружить области параметров, при которых удается генерировать указанные последовательности. Таким образом, наличие хаотических колебаний еще не гарантирует, что на их основе можно сформировать истинно случайные битовые последовательности.

В случае уравнения Макея-Гласса существуют конечные по размерам области параметров, в которых генерируются случайные последовательности, удовлетворяющие стандарту FIPS-140-1. На рис 2. приведен пример такой плоскости параметров уравнения *a, b*. Уравнение Макея-Гласса решалось для каждого набора парамет-

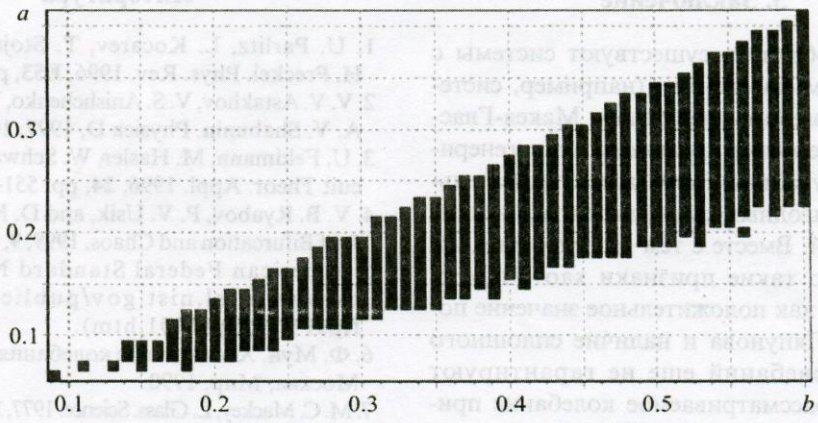

Рис. 2. *Область прохождения теста на случайность на плоскости параметров a и b*

ров, далее генерировалась битовая последовательность в соответствии с указанным выше правилом и проверялась тестом на случайность. В случае прохождения теста, исследуемая точка на плоскости параметров отмечалась квадратиком. Видно, что область параметров, где тест пройден, достаточно большая, что говорит о "грубости" рассматриваемого алгоритма генерирования случайной последовательности для данной динамической системы.

Это относится и к другим плоскостям параметров. Например, на рис. 3 приведена плоскость параметров высота порога – время задержки ($x_{пор}$, τ). Это те параметры, которые непосредственно управляют процессом формирования случайной последовательности. Видно, что и здесь область параметров, где пройден тест, достаточно большая.

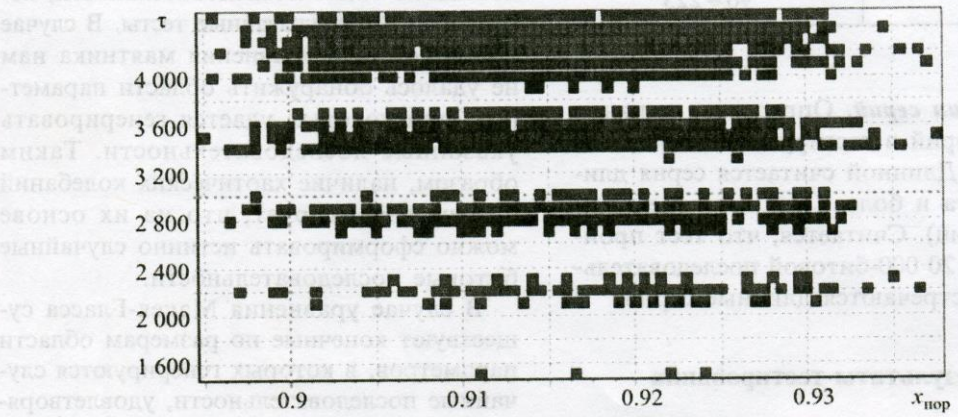

Рис. 3. *Область прохождения теста на случайность на плоскости параметров величина порога – время задержки*

5. Заключение

Таким образом, существуют системы с хаотическим поведением (например, системы, описываемые уравнением Макея-Гласса), которые могут применяться для генерирования случайных битовых последовательностей, пригодных для криптографических приложений. Вместе с тем исследования показали, что такие признаки хаотичности колебаний, как положительное значение показателей Ляпунова и наличие сплошного спектра колебаний еще не гарантируют того, что рассматриваемое колебание пригодно для генерирования истинно случайных битовых последовательностей.

Литература

1. U. Parlitz, L. Kocarev, T. Stojanovsky, and H. Preckel. Phys. Rev. 1996, **E53**, pp. 4351-4361.
2. V. V. Astakhov, V. S. Anishchenko, T. Kapitaniak, A. V. Shabunin. Physica D, 1997, **109**, pp. 11-16.
3. U. Feldmann, M. Hasler, W. Schwarz. Int. J. Circuit Theor. Appl. 1996, **24**, pp. 551-579.
4. V. B. Ryabov, P. V. Usik, and D. M. Vavriv. Int. J. of Bifurcation and Chaos. 1999, **9**, pp. 1181-1187.
5. American Federal Standard NIST (http://cs-www.ncsl.nist.gov/publications/fips/fips140-1/fips1401.htm).
6. Ф. Мун. Хаотические колебания. Пер. с англ., Москва, Мир, 1990.
7. M. C. Mackey, L. Glass. Science. 1977, **197**, pp. 287-289.
8. Ю. И. Неймарк, П. С. Ланда. Стохастические и хаотические колебания. Москва, Наука, 1987.

Cryptographic Analysis of Random Sequences Generated by System with Chaotic Behavior

D. D. Vavriv

A possibility of using determinate nonlinear dynamic systems with chaotic behavior as generators of random sequences has been investigated. Statistical characteristics of sequences generated by Makea-Glass system have been analyzed. For a wide range of control parameters this system has shown to generate sequences which pass the tests FIPS-140-1. Thus the formation of random sequences by using determinate systems with chaotic behavior has been shown rather promising for cryptography problems.