ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

УДК 004.421.5 + 517.938
https://doi.org/10.37661/1816-0301-2020-17-4-36-47

Поступила в редакцию 06.11.2020
Received 06.11.2020

Принята к публикации 23.11.2020
Accepted 23.11.2020

Цифровая модель генератора псевдослучайных чисел на основе непрерывной хаотической системы

Е. А. Дрыбин, С. В. Садов, В. С. Садов✉

Белорусский государственный университет, Минск, Беларусь
✉*E-mail: sadov@bsu.by*

Аннотация. Показано, что выбор параметра временной дискретизации цифровой модели непрерывной динамической системы с хаотическими режимами на основе ее динамики позволяет управлять характеристиками выходной последовательности, в том числе избегать коротких циклов и периодических режимов поведения. На примере системы Лоренца проведен анализ закона движения хаотической системы, линеаризованной в окрестностях точек устойчивого и неустойчивого равновесия. На основании этого закона выбраны параметры математической модели генератора псевдослучайных чисел. Выходная последовательность чисел, порождаемая предложенным в работе подходом, подвергнута статистическому и корреляционному анализам. Согласно результатам проведенных тестов полученные псевдослучайные последовательности на основе непрерывных хаотических систем обладают статистически случайными свойствами и могут быть использованы в системах стеганографической и криптографической защиты данных.

Ключевые слова: временная дискретизация, детерминированный хаос, система Лоренца, случайные последовательности, цифровая модель

Для цитирования. Дрыбин, Е. А. Цифровая модель генератора псевдослучайных чисел на основе непрерывной хаотической системы / Е. А. Дрыбин, С. В. Садов, В. С. Садов // Информатика. – 2020. − Т. 17, № 4. – С. 36–47. https://doi.org/10.37661/1816-0301-2020-17-4-36-47

Digital model of a pseudo-random number generator based on a continuous chaotic system

Yaugen A. Drybin, Siarhei V. Sadau, Vasili S. Sadau ✉

Belarussian State University, Minsk, Belarus
✉*E-mail: sadov@bsu.by*

Abstract. It is shown that the choice of the time sampling parameter of the digital model of a continuous dynamic system with chaotic modes based on its dynamics makes it possible to control the characteristics of the output sequence, including avoiding short cycles and periodic behavior modes. On the example of the Lorentz system, the analysis of the law of motion of a chaotic system, linearized in the vicinity of points of stable and unstable equilibrium, is carried out, on the basis of which the parameters of the mathematical model of the generator of pseudo-random numbers are selected. The output sequence of numbers generated in proposed way is subjected to statistical and correlation analysis. Based on the results of the tests carried out, we can say that the obtained pseudo-random sequences based on continuous chaotic systems have statistically random properties and can be used in steganographic and cryptographic systems.

Keywords: time sampling, deterministic chaos, Lorentz system, random sequences, digital model

For citation. Drybin Y. A., Sadau S. V., Sadau V. S. Digital model of a pseudo-random number generator based on a continuous chaotic system. *Informatics*, 2020, vol. 17, no. 4, pp. 36–47 (in Russian). https://doi.org/10.37661/1816-0301-2020-17-4-36-47

Введение. В практических задачах криптографии и стеганографии генерирование случайных данных осуществляется с помощью генераторов псевдослучайных чисел (ГПСЧ), которые на входе используют короткий ключ (семя), а на выходе предоставляют псевдослучайную последовательность чисел (ПСП), имеющую закон распределения, мало отличающийся от равномерного распределения. В настоящей статье предлагается вариант получения ПСП с использованием хаотических систем, которые во многом схожи с криптографическими алгоритмами, поскольку и в одних, и в других системах осуществляется нелинейное преобразование информации. При этом данное нелинейное преобразование, с одной стороны, является детерминированным процессом, а с другой – должно быть практически непредсказуемо для стороннего наблюдателя. Такая особенность была отмечена К. Шенноном в работах, написанных еще до обнаружения явления детерминированного хаоса, где он предлагает перемешивающие преобразования, зависящие от аргумента, и описывает базовый механизм образования детерминированного хаоса путем растяжения и складывания [1].

Методы формирования хаотических последовательностей. Схемы традиционных ГПСЧ реализуются на основе целочисленной арифметики, но в настоящее время достаточно широкое распространение получили и генераторы, использующие арифметику с плавающей запятой. Арифметика с плавающей запятой (АПЗ) дает возможность применять в качестве ГПСЧ нелинейные динамические системы с хаотическими процессами и рекуррентные отображения, поведение которых во многом схоже с нелинейными динамическими системами.

В качестве ГПСЧ чаще всего предлагается использовать дискретные отображения, такие как отображения Хенона, кусочно-линейные отображения, отображение (сдвиг) Бернулли и т. д. Программные реализации подобных ГПСЧ в настоящее время встречаются в различных пакетах прикладных программ для математического моделирования.

Основными недостатками использования дискретных отображений для получения требуемых ПСП, которые делают их неэффективными в качестве источников псевдослучайного сигнала, являются [2, 3] периодическое поведение, проявляющееся при использовании АПЗ и обусловленное невозможностью представления иррационального числа в двоичной записи, а также наличие коротких циклов, состоящих из крайне ограниченного числа возможных состояний системы, при определенных начальных условиях. Это не позволяет эффективно использовать дискретные отображения для получения ПСП, так как при формировании набора входных параметров (являющегося семенем), как правило, заранее неизвестно, какой орбите и с какой длиной периода он соответствует. Для преодоления явления возникновения коротких орбит в хаотических системах, реализованных программно с использованием АПЗ, в последнее время предлагаются две группы методов:

1) увеличение размерности хаотических систем [4] или использование более сложных хаотических систем [5, 6];

2) нарушение итерационного процесса хаотической системы с использованием другой хаотической системы с малой размерностью [7].

Отметим, что первая группа методов лишь замедляет скорость деградации хаотической системы (явление возникновения коротких орбит проявляется, но с большим числом итераций), однако не предоставляет фундаментального решения данной проблемы. Вторая группа методов с поэтапным нарушением итерационного процесса хаотической системы позволяет уменьшить погрешность вычислений с использованием АПЗ и предотвратить деградацию хаотической системы, но выходная последовательность (и длина соответствующей ей периодической орбиты) первичной хаотической системы будет определяться хаотическим отображением с малой размерностью, которая используется для нарушения итерационного процесса.

Хаотические системы с непрерывным временем. С целью преодоления ограничений дискретных хаотических отображений для формирования ПСП предлагается использовать многомерные нелинейные динамические системы с непрерывным временем, в которых возможно существование принципиально отличных структурных множеств, называемых аттракторами. Аттрактор представляет собой множество траекторий в фазовом пространстве, к которым притягиваются все траектории из некоторой окрестности аттрактора. Возникновение аттракторов возможно только в диссипативных динамических системах, а простейшими примерами аттракторов могут служить неподвижные точки или замкнутые траектории (орбиты).

В трехмерных диссипативных нелинейных системах (в общем случае в системах с размерностью больше двух) возможно существование сложного режима колебаний, называемого странным аттрактором [8]. Спектр колебаний системы в режиме странного аттрактора очень близок к спектру случайного процесса. Отметим также, что дискретные отображения, рассмотренные выше, порождают процессы, качественно схожие с процессами в нелинейных динамических системах.

При программном формировании хаотических сигналов или с использованием цифровых сигнальных процессоров неизбежно происходит дискретизация временной переменной, а для моделирования хаотических процессов применяются методы численного интегрирования систем дифференциальных уравнений. При дискретизации временного параметра непрерывных систем математические модели соответствующих генераторов сводятся к итерационной функции вида

$$x_{n+1} = f(x_n, K)\,, \tag{1}$$

где K – некоторый управляющий параметр.

Таким образом, при цифровой обработке выходной сигнал, порождаемый непрерывной хаотической системой, во многом становится эквивалентным сигналу дискретной системы. Однако в отличие от характеристик дискретного сигнала характеристики выходного сигнала могут управляться посредством изменения параметра K, который фактически является параметром временной дискретизации системы нелинейных дифференциальных уравнений.

Кроме того, цифровая реализация непрерывной хаотической системы для представления значений чисел, как правило, использует АПЗ.

Действительное число x может быть записано как бесконечная десятичная дробь в двоичном представлении $b_m b_{m-1} \dots b_1 \cdot a_1 a_2 \dots a_n$, где a_i, b_j – биты, $b_m b_{m-1} \dots b_1$ соответствует целой части числа, а $a_1 a_2 \dots a_n$ – дробной части.

При вычислениях с конечной точностью итерационную функцию $x_{n+1} = f(x_n)$ можно представить в виде

$$x_{n+1} = \mathrm{round}_k\big(f(x_n)\big)\,, \tag{2}$$

где $\mathrm{round}_k(x)$ – функция округления, которая может быть задана следующим выражением:

$$\mathrm{round}_k(x) = b_m b_{m-1} \dots b_1 \cdot a_1 a_2 \dots a_{k-1}(a_k + a_{k+1}). \tag{3}$$

Одной из существенных проблем программной реализации непрерывных динамических систем является накопление ошибки округления. Функция $\mathrm{round}_k(x)$ применяется на каждой итерации, и ошибка округления может накапливаться. Траектории движения исходной и аппроксимированной систем могут расходиться очень быстро благодаря чувствительности хаотической системы к начальным условиям. Таким образом, любая математическая модель, основанная на АПЗ, не является абсолютно достоверной реализацией непрерывной хаотической системы.

Помимо некорректного асимптотического поведения, проявляющегося по истечении относительно большого отрезка времени, аппроксимированные системы обладают рядом «опасных» свойств, которые могут проявиться уже в начале траектории. Одной из возможностей их минимизации является округление состояния системы таким образом, что траектория ее движения безвозвратно покидает странный аттрактор и переходит к периодической моде. Например, во многих нелинейных системах переменные, определяющие режим возникающих колебаний, могут иметь бесконечно малые, но не равные нулю значения. В случае «неудачного» округления такой переменной до нуля хаотическое поведение системы прекращается и она переходит в нехаотический режим. Поэтому при реализации хаотической системы с использованием АПЗ важно знать закон ее движения, что позволит ограничить используемые в модели области фазового пространства и избежать нежелательных эффектов.

Характеристики хаотических сигналов, полученных с использованием цифровой реализации непрерывной динамической системы, зависят от величины шага временной дискретизации. Выбор и оценку шага временной дискретизации Δt с целью получения требуемых характеристик выходной последовательности необходимо проводить при помощи параметра дискретизации K, определяемого следующим образом [9]:

$$K = \frac{T}{\Delta t} \ , \tag{4}$$

где T – период квазирезонансных колебаний динамической системы.

Уменьшение величины K приводит к изменению статистических характеристик сигналов в нелинейных системах с детерминированным хаосом, но за счет уменьшения количества отсчетов на период колебаний становится возможным улучшить эффективность (быстродействие) цифровых генераторов хаотических последовательностей. Поэтому при разработке цифровых генераторов хаоса необходимо оценить предельные значения параметра K и выработать рекомендации по выбору минимального значения параметра дискретизации $K_{\min}$. При значениях $K < K_{\min}$ в процессе численного интегрирования может происходить переполнение переменных координат точки в фазовом пространстве, из-за чего траектория движения системы может покинуть странный аттрактор.

Построение ГПСЧ на основе непрерывной хаотической системы. В качестве нелинейной динамической системы, которая ляжет в основу ГПСЧ, будем использовать систему Лоренца

$$\begin{aligned} \dot{X} &= -\sigma X + \sigma Y, \\ \dot{Y} &= -XZ + rX - Y, \\ \dot{Z} &= XY - bZ, \end{aligned} \tag{5}$$

где X, Y, Z – переменные системы; r, σ, b – параметры системы Лоренца.

Данный выбор основан на том, что система Лоренца обладает малым количеством параметров, проста и надежна в схемотехнической реализации и в то же время характеризуется максимальной энтропией Колмогорова ($K > 2$). Это указывает на сложность ее внутреннего устройства и протекающих в ней процессов в сравнении как с дискретными отображениями, так и непрерывными хаотическими системами Чуа и Ресслера. Динамика системы Лоренца детально исследована и описана в литературе, что позволяет легко определять диапазоны допустимых параметров и области фазового пространства, в которых система ведет себя хаотически. Кроме того, система Лоренца имеет наименьшее количество областей с регулярным поведением [10], а существование коротких орбит в хаотических режимах не описано в литературе (предполагается их возможное существование в моделях с использованием АПЗ). Знание закона движения системы позволит правильно выбрать рабочие диапазоны параметров для ее программной или аппаратной моделей.

Исследуем динамику системы Лоренца при фиксированных значениях параметров $b = 8/3$ и $\sigma = 10$ и при изменении параметра r, который обычно называют управляющим.

При значениях $r > 1$ аттрактор в системе Лоренца, представляющий собой неподвижную точку в начале координат, становится неустойчивым и появляются два новых состояния равновесия:

$$\begin{aligned} X_{01} &= \pm\sqrt{b(r-1)}, \\ Y_{01} &= \pm\sqrt{b(r-1)}, \\ Z_{01} &= r - 1 \, . \end{aligned} \tag{6}$$

Существование странного аттрактора в системе Лоренца возможно, если $r > 24{,}06$. При этом существование устойчивых точек, соответствующих стационарному режиму, сохраняется до значения

$$r = \frac{\sigma(\sigma + b + 3)}{\sigma - b - 1} = 24{,}74, \tag{7}$$

после чего странный аттрактор становится единственным притягивающим множеством в фазовом пространстве системы.

Процесс перехода системы Лоренца к странному аттрактору сопровождается квазипериодическим движением по раскручивающейся спирали увеличивающегося радиуса. При малых отклонениях от состояния равновесия период квазирезонансных колебаний в системе Лоренца можно оценить с помощью выражения

$$T \approx 4\pi[8\sigma(r-1) - (\sigma + r)^2]^{-1/2}. \tag{8}$$

Проведем аналитическое определение диапазона значений параметра временной дискретизации K для системы Лоренца, исследуя динамику решения системы дифференциальных уравнений (5), линеаризованной в окрестностях точек устойчивого и неустойчивого равновесия.

Фазовая траектория нелинейной динамической системы в хаотическом режиме может быть разбита на отдельные характерные участки для каждой из мод в этом режиме. Спектральные характеристики колебаний, порождаемых системой при движении по данному участку траектории в фазовом пространстве, позволят оценить верхнюю граничную частоту сигналов. Воспользовавшись теоремой отсчетов, можно оценить и максимальное значение времени следования отсчетов.

В фазовых траекториях системы Лоренца можно отметить характерные участки в окрестностях точки $C_0 = \big(0{,}0{,}(r-1)\big)$ и двух точек неустойчивого равновесия системы $C_{1,2}$, координаты которых определяются выражениями (6).

В окрестностях точки $C_0 = \big(0{,}0{,}(r-1)\big)$ при выполнении соотношения $XY \ll Z$ систему (5) можно привести к следующему виду:

$$\ddot{X} + \dot{X}\left(1 + \sigma + \frac{X^2}{b}\right) - X\sigma(r-1) + \frac{X^3\sigma}{b} = \frac{X\dot{Z}\sigma}{b}. \tag{9}$$

Пренебрегая малыми членами, приведем соотношение (9) к линейному дифференциальному уравнению

$$\ddot{X} + \dot{X}(1 + \sigma) - X\sigma(r - 1 - Z(t)) \approx 0, \tag{10}$$

где $Z(t) \approx Z_0 e^{-bt}$.

При условии $Z(t) > (r-1)$ выражение (10) можно привести к виду

$$T\ddot{X} + \dot{X}(1 + \sigma) + X\sigma(r-1) \approx 0, \tag{11}$$

при $Z(t) < (r-1)$ – к виду

$$\ddot{X} + \dot{X}(1 + \sigma) - X\sigma(r-1) \approx 0. \tag{12}$$

Рассмотрим решение уравнения в окрестностях точки C_0 в обоих случаях. В случае $Z(t) > (r-1)$ решение можно записать следующим образом:

$$X_0(t) = e^{a_0 t} \sin \omega_0 t,$$
$$a_0 = \frac{-(1+\sigma)}{2}, \tag{13}$$
$$\omega_0 = \frac{1}{2}[4\sigma(r-1) - (1+\sigma)^2].$$

С помощью преобразования Фурье получим выражение для спектра сигнала $X_0(t)$:

$$X_0(\omega) = \frac{(-\omega_0 \cos T\omega_0 + a_0 \sin T\omega_0 - j\omega \sin T\omega_0)}{(a_0 - j\omega)^2 + {\omega_0}^2} \cdot e^{T(a_0 - j\omega)} + \\ + \frac{\omega_0}{(a_0 - j\omega)^2 + {\omega_0}^2}, \tag{14}$$

где длительность сигнала $X_0(t)$ выбрана исходя из $T \geq 20\pi/\omega_0$.

В случае $Z(t) < (r-1)$ решение можно записать в виде

$$X_0(t) = e^{a_0 t},$$
$$a_0(t) = \frac{-(1+\sigma) - \sqrt{4\sigma(r-1) + (1+\sigma)^2}}{2}. \tag{15}$$

При этом спектр сигнала определяется равенством

$$X_0(\omega) = -\frac{1}{a_0 + j\omega} \cdot e^{T(a_0 + j\omega)} + \frac{1}{a_0 + j\omega}. \tag{16}$$

В окрестностях точек $C_{1,2}$ решение можно записать формулой

$$X_{1,2}(t) = e^{a_{1,2} t} \sin \omega_{1,2} t\,. \tag{17}$$

Спектр сигнала на данном участке с учетом $\omega_{1,2} = 2\pi/T$ примет следующий вид:

$$X_{1,2}(\omega) = \frac{\left(-\omega_{1,2} \cos T\omega_{1,2} + a_{1,2} \sin T\omega_{1,2} - j\omega \sin T\omega_{1,2}\right)}{\left(a_{1,2} - j\omega\right)^2 + {\omega_{1,2}}^2} \cdot e^{T(a_{1,2} - j\omega)} + \\ + \frac{\omega_{1,2}}{(a_{1,2} - j\omega)^2 + {\omega_{1,2}}^2}\,. \tag{18}$$

Спектры сигнала решений линеаризованной системы Лоренца в окрестностях состояний равновесия при значениях параметров r = 28, σ = 10 и b = 8/3 показаны на рис. 1.

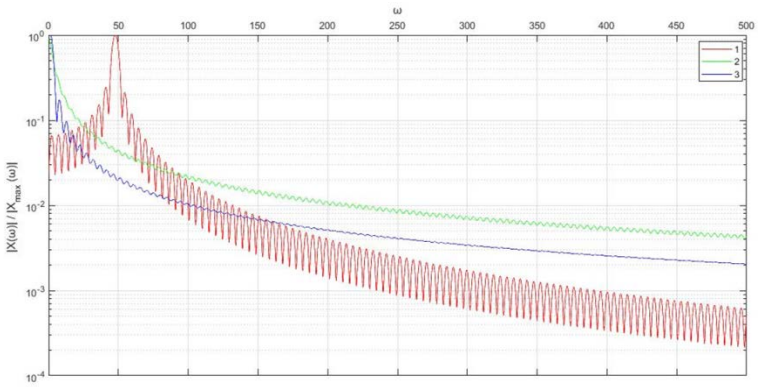


Рис. 1. Спектры сигнала решений линеаризованной системы Лоренца:
1 – рассчитанные согласно выражению (14); 2 – выражению (16); 3 – выражению (18)

Согласно зависимостям, изображенным на рис. 1, определим по уровню 0,01 верхнюю граничную частоту сигнала $\omega_{max} = 223{,}28$, что соответствует минимальному значению параметра временной дискретизации:

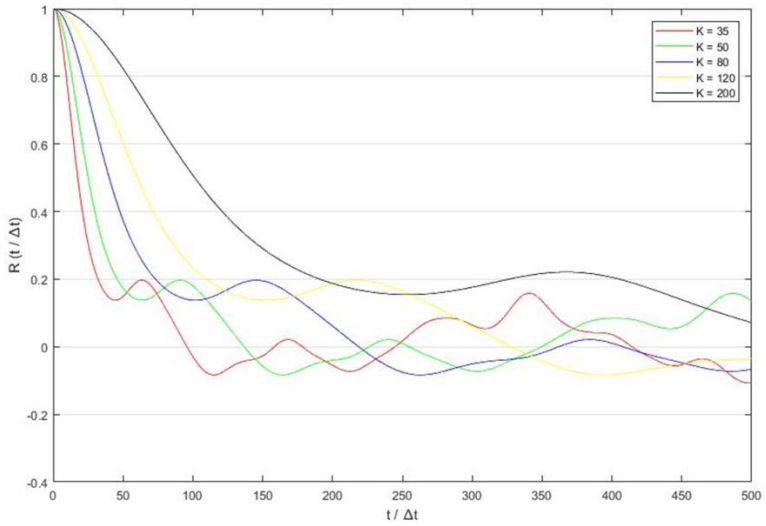
$$K_{\min} = \frac{T\omega_{\max}}{\pi} = 33{,}38, \tag{19}$$

где T – период квазирезонансных колебаний, который в системе Лоренца определяется согласно выражению (8).

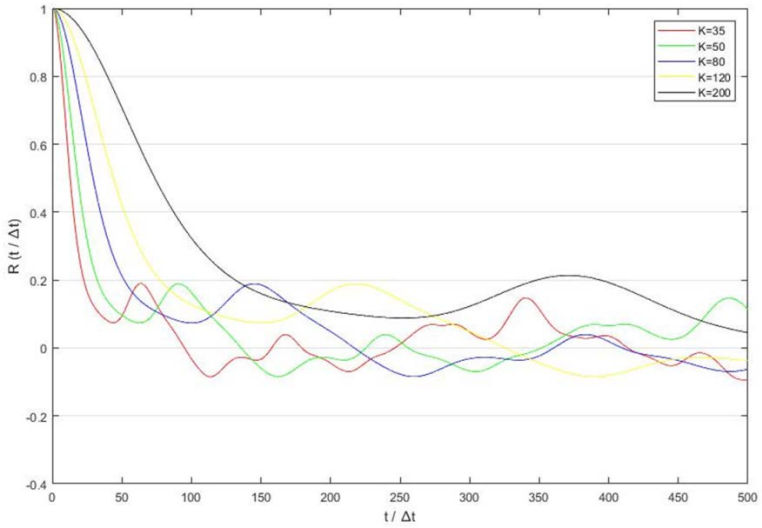
Таким образом, минимальный параметр дискретизации при численном решении системы Лоренца должен быть $K > K_{\min}$. Вместе с тем необходимо провести дополнительные экспериментальные исследования характеристик хаотического сигнала, порождаемого цифровой реализацией непрерывной нелинейной динамической системы, в зависимости от выбранного параметра K. Для этого целесообразно использовать автокорреляционную функцию. Спиральный хаос в автоколебательных системах имеет схожие свойства со свойствами зашумленных квазигармонических колебаний. При этом скорость расцепления корреляций в начале траектории зависит как от поведения мгновенной амплитуды, так и от фазы колебаний. По мере движения системы по фазовой траектории огибающая автокорреляционной функции в большей степени определяется диффузией мгновенной фазы [11].

Графики автокорреляционной функции для сигналов X, Y, Z, порождаемых смоделированной системой Лоренца при различных значениях параметра временной дискретизации K, показаны на рис. 2. Для математического моделирования и анализа хаотических процессов использовался пакет программ MATLAB. Для решения системы дифференциальных уравнений, описывающих хаотический процесс, был выбран численный метод Дорманда – Принса. Несмотря на то что данный метод относится к группе явных и, соответственно, может быть неустойчивым, он хорошо подходит для решения системы Лоренца и позволяет получить достаточно точное решение за короткое время [10]. На рис. 2 видно, что при меньших значениях параметра K автокорреляционная функция спадает быстрее и в дальнейшем держится ближе к нулевому значению. Зависимость падения автокорреляционной функции реализации Z отличается от аналогичных зависимостей для реализаций X и Y.

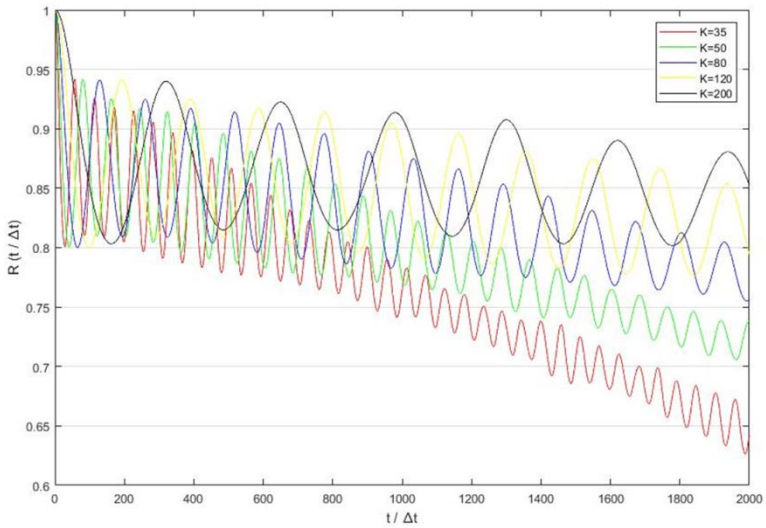
Одним из способов формирования импульсных псевдослучайных последовательностей на основе непрерывных нелинейных динамических систем является сравнение хаотического сигнала с пороговым уровнем. Оценить быстродействие генераторов такого типа можно по количеству пересечений порогового уровня хаотическим сигналом. Для системы Лоренца подобной мерой быстродействия может служить количество переходов фазовой траектории из одной области фазового пространства в другую область с отличными состояниями равновесия, которые определяются выражением (6). Зависимость количества переходов фазовой траектории между различными состояниями равновесия от параметра K в системе Лоренца при стандартных значениях параметров и неизменной продолжительности сигналов показана на рис. 3. На рисунке видно, что при уменьшении параметра временной дискретизации K (соответственно, при увеличении шага временной дискретизации и росте интенсивности шумов дискретизации) растет количество переходов фазовой траектории между различными состояниями равновесия при том же количестве временных отсчетов. Полученная зависимость также показывает, что количество переходов фазовой траектории между различными состояниями равновесия практически не изменяется при больших значениях параметра K. Кроме того, увеличение значения параметра временной дискретизации K влечет за собой и увеличение затрат на проведение численного интегрирования нелинейной системы. Следовательно, при малых значениях параметра временной дискретизации K улучшаются динамические характеристики хаотических сигналов, порождаемых системой Лоренца. Исходя из вышеизложенного, для построения программной реализации ГПСЧ на основе системы Лоренца целесообразно выбрать параметр дискретизации $K = 35$.



а)



б)



в)

Рис. 2. Автокорреляционная функция системы Лоренца
для сигнала X (*а*), сигнала Y (*б*) и сигнала Z (*в*)

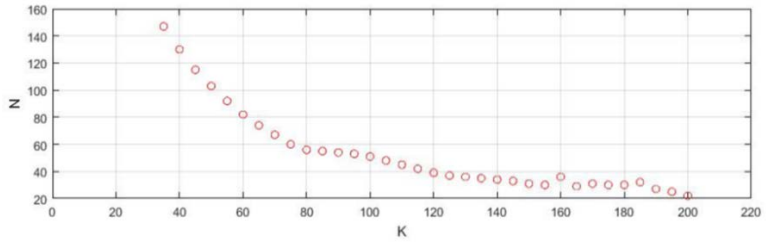


Рис. 3. Зависимость количества переходов фазовой траектории между различными состояниями равновесия от параметра K в системе Лоренца

Оценка качества выходной последовательности ГПСЧ. Для проверки статистических характеристик порождаемой двоичной последовательности используем набор статистических тестов NIST STS (NIST Statistical Test Suite), для проверки ПСП на непредсказуемость – Q-тест Льюнга – Бокса.

Для проведения тестирования построенного ГПСЧ сгенерируем $N = 1000$ двоичных последовательностей (при различных начальных условиях, заданных случайным образом так, что $X \in [1, 10]$, $Y \in [1, 10]$, $Z \in [1, 10]$) длиной $n = 1\,048\,576$ бит. Используем следующий простой и эффективный способ хеширования для отображения i-го 64-битного отсчета в i-й элемент двоичной последовательности, принадлежащий множеству $\{0,1\}$:

$$B_i = \mathrm{mod}\left(\sum_{j=1}^{64} b_{ij}, 2\right), \tag{20}$$

где $b_{ij} - j$-й бит i-го отсчета выходной последовательности сигнала X; $B_i - i$-й элемент выходной двоичной последовательности ГПСЧ.

Согласно результатам тестирования NIST STS при уровне значимости $\alpha = 0{,}01$ (таблица) построенный ГПСЧ на основе сигнала X системы Лоренца успешно прошел статистическое тестирование пакетом NIST STS, а порождаемые им ПСП обладают статистическими свойствами случайных последовательностей.

Результаты статистических тестов NIST STS

Статистический тест	Рекомендуемые NIST параметры тестирования	Фактические параметры тестирования	Значение вероятности P (выборка)
Монобитный (частотный побитовый) тест	$n \geq 100$	$n = 1\,048\,576$	0,045 675
Частотный блочный тест	$n \geq 100$; $M = 10$	$n = 1\,048\,576$; $M = 10$	0,085 587
Тест пробегов	$n \geq 100$	$n = 1\,048\,576$	0,021 999
Тест на самую длинную последовательность единиц в блоке	$n \geq 6272$; $M = 128$	$n = 1\,048\,576$; $M = 128$	0,955 835
Тест рангов бинарных матриц	$n \geq 38\,912$ или $n \geq 38MQ$; $M = Q = 32$	$n = 1\,048\,576$; $M = Q = 32$	0,816 537
Спектральный тест на основе дискретного преобразования Фурье	$n \geq 1000$	$n = 1\,048\,576$	0,262 249
Тест на совпадение неперекрывающихся шаблонов	$n = 2^{20} = 1\,048\,576$; $m = 9$	$n = 1\,048\,576$; $m = 9$	0,162 606 0,534 146 0,494 392 0,678 686 0,616 305 0,419 021 0,191 687 0,759 756 0,275 709 …

Продолжение таблицы

Статистический тест	Рекомендуемые NIST параметры тестирования	Фактические параметры тестирования	Значение вероятности P (выборка)
Тест на совпадение перекрывающихся шаблонов	$n \geq 1\,000\,000$; $m = 9$	$n = 1\,048\,576$; $m = 9$	0,162 606
Универсальный статистический тест Маурера	$n \geq 904\,960$; $L = 7$; $Q = 1280$	$n = 1\,048\,576$; $L = 7$; $Q = 1280$	0,657 933
Тест на линейную сложность	$n \geq 1\,000\,000$; $500 \leq M \leq 5000$	$n = 1\,048\,576$; $M = 1000$	0,964 295
Тест на подпоследовательности	$m < \log_2 n - 2$	$n = 1\,048\,576$; $m = 2$	0,016 717 0,017 912
Тест приблизительной энтропии	$m < \log_2 n - 2$	$n = 1\,048\,576$; $m = 2$	0,816 537
Тест кумулятивных сумм	$n \geq 100$	$n = 1\,048\,576$	0,616 305 0,719 747
Тест на произвольные отклонения	$n \geq 1\,000\,000$	$n = 1\,048\,576$	0,337 162 0,170 294 0,015 065 0,723 129 0,287 306 0,517 442 0,170 294 0,264 458
Разновидность теста на произвольные отклонения	$n \geq 1\,000\,000$	$n = 1\,048\,576$	0,585 209 0,585 209 0,170 294 0,517 442 0,105 618 0,900 104 0,242 986 0,997 147 0,551 026 …

Из таблицы видно, что построенный ГПСЧ на основе сигнала X системы Лоренца успешно прошел статистическое тестирование пакетом NIST STS, а порождаемые им ПСП обладают статистическими свойствами случайных последовательностей.

Q-тест Льюнга – Бокса (данные получены на тех же $N = 1000$ последовательностях длиной $n = 1\,048\,576$, которые использовались в предыдущем тестировании) выдает значение вероятности $P = 0{,}4485$, что свидетельствует об уровне корреляций между отсчетами порождаемых ПСП, допустимом для применения последовательностей в задачах обеспечения информационной безопасности.

Заключение. В статье рассмотрены вопросы влияния выбора параметров временной дискретизации непрерывных хаотических систем при формировании ПСП на их основе. На примере системы Лоренца показано, что, выбирая параметр временной дискретизации исходя из периода квазирезонансных колебаний динамической системы и ее динамики в окрестностях точек устойчивового и неустойчивого равновесия, можно избежать периодического поведения и наличия коротких циклов, характерных для дискретных отображений.

Проведенный анализ статистических характеристик выходных последовательностей цифровой реализации ГПСЧ на основе детерминированного хаоса позволяет говорить об их пригодности к использованию в задачах информационной безопасности.

Список использованных источников

1. Шеннон, К. Математическая теория связи / К. Шеннон // Работы по теории информации и кибернетике. – М. : ИИЛ, 1963. – С. 243–332.

2. Chaotic optimization algorithm based on Tent map / L. Shan [et al.] // Control and Decision. – 2005. – Vol. 20, no. 2. – P. 179–182.

3. Kocarev, L. Logistic map as a block encryption algorithm / L. Kocarev, G. Jakimoski // Physics Letters A. – 2001. – Vol. 289, no. 4–5. – P. 199–206.

4. Pareek, N. K. Cryptography using multiple one-dimensional chaotic maps / N. K. Pareek, V. Patidar, K. K. Sud // Physics Letters A. – 2003. – Vol. 309, no. 1–2. – P. 75–82.

5. Wong, W. K. A modified chaotic. Cryptographic method / W. K. Wong, L. P. Lee. // Computer Physics Communications. – 2001. – No. 138. – P. 234–236.

6. A unified approach to fuzzy modelling and robust synchronization of different hyperchaotic systems / H. G. Zhang [et al.] // Chinese Physics B. – 2008. – Vol. 17, no. 11. – P. 529–533.

7. Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map / Y. Wang [et al.] // Physics Letters A. – 2007. – Vol. 363, no. 4. – P. 277–281.

8. Крот, А. М. Спектральный анализ хаотических колебаний в имитационной модели схемы Чжуа, разработанной на основе матричной декомпозиции / А. М. Крот, В. А. Сычев // Информатика. – 2019. − Т. 16, № 1. – С. 7–23.

9. Капранов, М. В. Анализ фазовых траекторий в окрестностях особых точек 2-D и 3-D нелинейных систем / М. В. Капранов, А. И. Томашевский. – М. : Изд-во МЭИ, 2003. – 80 с.

10. Аливер, В. Ю. Хаотические режимы в непрерывных динамических системах / В. Ю. Аливер // Вестник МГТУ им. Н. Э. Баумана. Сер. «Приборостроение». – 2006. – № 1. – С. 65–84.

11. Корреляционный анализ режимов детерминированного и зашумленного хаоса / В. С. Анищенко [и др.] // Радиотехника и элетроника. – 2003. – Т. 48, № 7. – С. 824–835.

References

1. Shannon C. A mathematical theory of communication. *Bell System Technical Journal*, 1948, vol. 27, iss. 3, pp. 379–423.

2. Shan L., Qiang H., Li J., Wang Z. Chaotic optimization algorithm based on Tent map. *Control and Decision*, 2005, vol. 20, no. 2, pp. 179–182.

3. Kocarev L., Jakimoski G. Logistic map as a block encryption algorithm. *Physics Letters A*, 2001, vol. 289, no. 4–5, pp. 199–206.

4. Pareek N. K., Patidar V., Sud K. K. Cryptography using multiple one-dimensional chaotic maps. *Physics Letters A*, 2003, vol. 309, no. 1–2, pp. 75–82.

5. Wong W. K., Lee L. P. A modified chaotic. Cryptographic method. *Computer Physics Communications*, 2001, no. 138, pp. 234–236.

6. Zhang H. G., Zhao Y., Yu W., Yang D. S. A unified approach to fuzzy modelling and robust synchronization of different hyperchaotic systems. *Chinese Physics B*, 2008, vol. 17, no. 11, pp. 529–533.

7. Wang Y., Liao X., Xiang T., Wong K. W., Yang D. Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map. *Physics Letters A*, 2007, vol. 363, no. 4, pp. 277–281.

8. Krot A. M., Sychou U. A. A spectral analysis of chaotic oscillations in simulation model of Chua's circuit developed with use of matrix decomposition. *Informatics*, 2019, vol. 16, no. 1, pp. 7–23 (in Russian).

9. Kapranov M. V., Tomashevskiy A. I. Analiz fazovyh traektoriy v okrestnostyah osobyh tochek 2-D i 3-D nelineynyh system. *Analysis of Phase Trajectories in the Vicinity of Singular Points of 2-D and 3-D Nonlinear Systems*. Moscow, Izdatel'stvo Moskovskogo jenergeticheskogo instituta, 2003, 80 p. (in Russian).

10. Aliver V. Y. Haoticheskie rezhimy v nepreryvnyh dinamicheskih systemah [Chaotic regimes in continuous dynamical systems]. Vestnik Moskovskogo Gosudarstvennogo Tehnicheskogo Universiteta im. N. Je. Baumana. Serija «Priborostroenie» [*Herald of the Bauman Moscow State Technical University. Series Instrument Engineering*], 2006, no. 1, pp. 65–84 (in Russian).

11. Anischenko V. S., Vadivasova T. E., Okrokverchov G. A., Strelkova G. I. Korreljacionnyj analiz rezhimov determinirovannogo i zashumlennogo haosa [Correlation analysis of the modes of deterministic and noisy chaos]. Radiotehnika i elektronika [*Radio Engineering and Electronics*], 2003, vol. 48, no. 7, pp. 824–835 (in Russian).

Информация об авторах

Дрыбин Евгений Александрович, аспирант, факультет радиофизики и компьютерных технологий, Белорусский государственный университет, Минск, Беларусь.
E-mail: ydrybin@gmail.com

Садов Сергей Васильевич, аспирант, старший преподаватель кафедры интеллектуальных систем, факультет радиофизики и компьютерных технологий, Белорусский государственный университет, Минск, Беларусь.
E-mail: seregasadov@gmail.com

Садов Василий Сергеевич, кандидат технических наук, доцент, профессор кафедры интеллектуальных систем, факультет радиофизики и компьютерных технологий, Белорусский государственный университет, Минск, Беларусь.
E-mail: sadov@bsu.by

Information about the authors

Yaugen A. Drybin, Postgraduate Student, Department of Intelligent Systems, Faculty of Radiophysics and Computer Technologies, Belarusian State University, Minsk, Belarus.
E-mail: ydrybin@gmail.com
Siarhei V. Sadau, Postgraduate Student, Senior Lecturer, Department of Intelligent Systems, Faculty of Radiophysics and Computer Technologies, Belarusian State University, Minsk, Belarus.
E-mail: seregasadov@gmail.com

Vasili S. Sadau, Cand. Sci. (Eng.), Associate Professor, Professor of the Department of Intelligent Systems, Faculty of Radiophysics and Computer Technologies, Belarusian State University, Minsk, Belarus.
E-mail: sadov@bsu.by