УДК 519.688 + 621.391

О ПОСТРОЕНИИ ПРОГРАММНЫХ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ ДИНАМИЧЕСКИХ СИСТЕМ В РЕЖИМЕ ДЕТЕРМИНИРОВАННОГО ХАОСА

© 2013 Л.Ю. Герасимов[1]

В данной работе исследуется возможность программного моделирования режима динамического хаоса. Исследование проводится на примере программной модели лампового генератора Ван-дер-Поля. Для оценки криптографических свойств полученного генератора псевдослучайных чисел используется пакет статистических тестов *NIST*.

Ключевые слова: детерминированный хаос, псевдослучайные числа, криптография, *NIST*.

Введение

Явление детерминированного хаоса представляет собой возможность наличия сложного, непредсказуемого поведения даже в относительно простых и полностью детерминированных системах. С одной стороны, под непредсказуемостью здесь понимается чувствительность к начальным условиям и как следствие невозможность точного прогноза состояния системы в отдаленном будущем. С другой стороны, детерминированность означает относительную простоту математического, и в частности программного, моделирования таких систем.

Благодаря этому системы динамического хаоса обладают большим потенциалом практического использования в современной технике. Одной из областей применения является криптография, где детерминированный хаос может служить источником псевдослучайных чисел, используемых во многих криптографических приложениях.

Однако одной из главных проблем такого использования хаотических систем становится расчет динамики системы в цифровых устройствах, где можно смоделировать систему лишь с конечным фазовым пространством. Конечное фазовое пространство и детерминированность системы означают, что любая фазовая траектория неизбежно зациклится. При построении программных генераторов псевдослучайных чисел главной задачей становится обеспечение максимальной длины циклов.

При моделировании хаотических систем повышение точности вычислений не всегда приводит к увеличению длины циклов. В работе [1] приведено исследование

[1]Герасимов Леонид Юрьевич (gerasimovleo@gmail.com), кафедра безопасности информационных систем Самарского государственного университета, 443011, Российская Федерация, г. Самара, ул. Акад. Павлова, 1.

логистического отображения, задаваемого как

$$x_{n+1} = 4rx_n(1 - x_n),$$

где $x \in (0, 1)$ и $r \in (0, 1)$. Полученная зависимость длинн циклов от точности вычислений представлена на рис. 1.

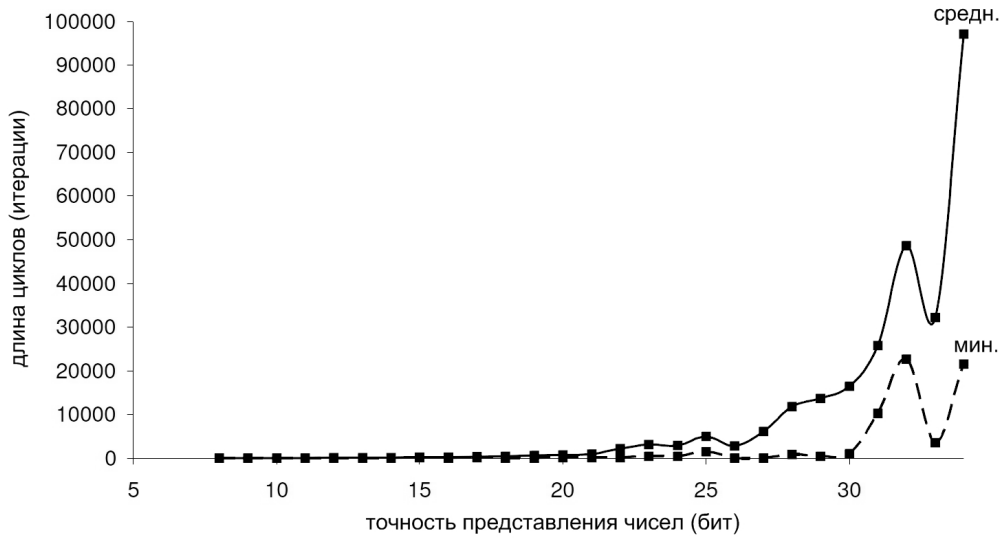


Рис. 1. Зависимость средних и минимальных длин циклов в логистическом отображении от точности вычислений с плавающей запятой

В рамках данной работы была смоделирована более сложная хаотическая система. Оценка результатов проводится с использованием набора статистических тестов. По результатам их прохождения можно также судить и о наличии циклов в получаемых фазовых траекториях.

1. Программная реализация генератора псевдослучайных чисел

В качестве моделируемой динамической системы был выбран генератор Ван-дер-Поля. Он представляет собой ламповый автогенератор, схема которого представлена на рис. 2.

Уравнение движения этой системы в безразмерном виде имеет вид:

$$\ddot{x} - (\lambda - x^2)\dot{x} + x = 0,$$

где λ — единственный управляющий параметр.

Для программного моделирования динамики системы была использована дискретно-временная модель генератора Ван-дер-Поля, предложенная в работе [2]:

$$y[n] = \lambda_1 y[n-1] + \lambda_2 y[n-2] + \gamma(1 - y^2[n-1])(y[n-1] - y[n-2]). \qquad (1.1)$$

Она представляет собой итерационное уравнение с тремя управляющими параметрами: λ_1, λ_2 и γ. Каждое новое состояние системы вычисляется из двух предыдущих. Область значений управляющих параметров, при которых система демонстрирует хаотическое поведение, была установлена в работе [3].

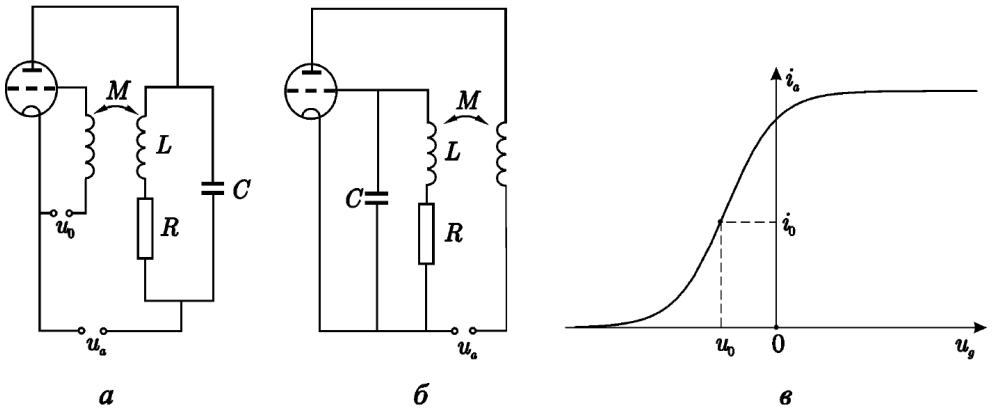


Рис. 2. Схемы лампового генератора Ван-дер-Поля с колебательным контуром в цепи анода (*а*) и в цепи сетки (*б*) и анодно-сеточная характеристика триода (*в*)

Одной из основных проблем при программном моделировании хаотических систем является представление данных. В работе данные обозначены в виде чисел с плавающей точкой двойной точности (стандарт *IEEE744*), что давало системе лишь конечное фазовое пространство. Поэтому в качестве альтернативного варианта было также реализовано представление данных в виде рациональных дробей, числитель и знаменатель которых были выражены с использованием длинной арифметики. Таким образом, достигалось плотное счетное фазовое пространство. Помимо выигрыша в точности, при использовании второго метода представления данных наблюдалось также преимущество в скорости производства информации. В то время как при использовании арифметики с плавающей запятой на каждой итерации производилось лишь 8 байт информации, при применении рациональных дробей скорость производства информации росла нелинейно за счет увеличения абсолютных величин числителя и знаменателя. Однако вместе с увеличением количества информации также росла и вычислительная сложность каждой следующей итерации, что не позволяет использовать такой способ вычислений для генерации длинных случайных последовательностей.

Для оценки хаотичности получаемых фазовых траекторий (последовательностей $y[n]$) используется функция автокорреляции:

$$\begin{aligned} C(m) &= \frac{1}{N-m}\sum_{k=1}^{N-m}\hat{y}[k]\hat{y}[k+m], \\ \hat{y}[k] &= y[k]-\bar{y}, \\ \bar{y} &= \frac{1}{N}\sum_{n=1}^{N}y[n]. \end{aligned} \tag{1.2}$$

Если исходная последовательность $y[n]$ периодическая, то и функция автокорреляции (последовательность $C(m)$) также будет периодической.

На рис. 3, *а* представлен пример фазовой траектории, произведенной дискретно-временной моделью (1.1) в режиме хаотических автоколебаний. О хаотическом характере данной траектории можно судить по быстрому убыванию соответствующей автокорреляционной функции (рис. 3, *б*).

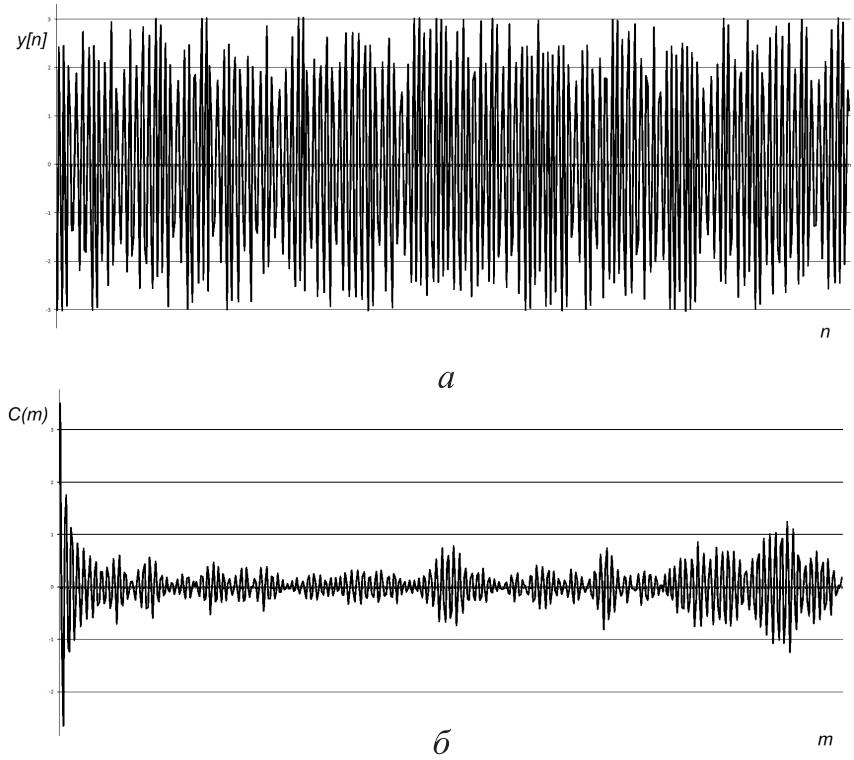
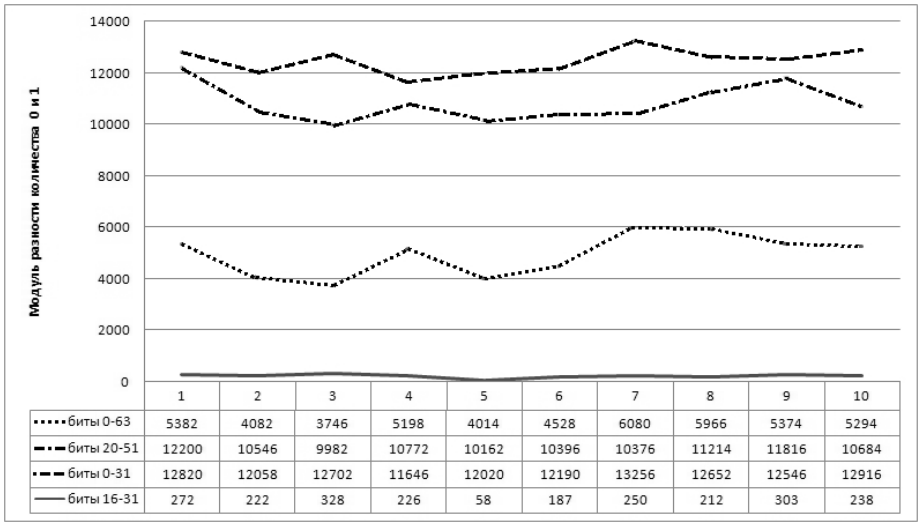


Рис. 3. Пример фазовой траектории:
$а$ — дискретно-временная модель (1.1), полученная при параметрах: $\lambda_1 = 0,605$, $\lambda_2 = -0,958$, $\gamma = 0,198$, $N = 500$ и начальных условиях $(0; 0,4)$; $б$ — функция автокорреляции (1.2) для данной траектории

2. Статистические характеристики

Главной целью создания данной программной модели было получение бинарных последовательностей с хорошими криптографическими свойствами. Для анализа бинарных последовательностей применялся набор статистических тестов *NIST (National Institute of Standards and Technologies)*. В результате исследований было установлено, что, несмотря на то что числовые последовательности были случайными, бинарные потоки, образованные их двоичными представлениями, обладали низкими статистическими показателями. В частности, число нулей в них значительно превышало число единиц. Поэтому для получения криптографически стойких бинарных последовательностей требовалось применение некоторой постобработки для коррекции частотных характеристик. При использовании для расчетов рациональных дробей на длинной арифметике длинные последовательности нулей объяснялись ростом абсолютных значений числителя и знаменателя. Проблема диспропорции количества нулей и единиц в данном случае решалась относительно просто — поиском и исключением таких длинных последовательностей нулей. В случае использования арифметики с плавающей запятой было решено

на каждой итерации включать в выходную последовательность не все 64 бита нового полученного значения, а лишь некоторое их подмножество. Для выбора этого подмножества были проведены эксперименты, результаты которых представлены на рис. 4.



	1	2	3	4	5	6	7	8	9	10
биты 0-63	5382	4082	3746	5198	4014	4528	6080	5966	5374	5294
биты 20-51	12200	10546	9982	10772	10162	10396	10376	11214	11816	10684
биты 0-31	12820	12058	12702	11646	12020	12190	13256	12652	12546	12916
биты 16-31	272	222	328	226	58	187	250	212	303	238

Рис. 4. Модуль разности количества 0 и 1 в выходной последовательности (500000 бит) при использовании разных подмножеств двоичного представления *IEEE754*

После выбора и добавления в программную модель метода постобработки числовых последовательностей было проведено исследование с использованием набора статистических тестов *NIST*.

В наборе статистических тестов *NIST* используется ряд предположений о случайных последовательностях. Идеальной случайной последовательностью считается результат многократного подбрасывания идеальной монеты с вероятностями выпадения 0 и 1 — ровно 1/2. Кроме того, все подбрасывания считаются независимыми. Поэтому в такой последовательности должно наблюдаться [0, 1]-нормальное (Гауссовское) распределение нулей и единиц [4]. Для всего набора тестов задан уровень значимости α, равный вероятности того, что случайная последовательность не пройдет тесты. Использовалось значение уровня значимости 1/100, рекомендованное в сопроводительной документации. В результате каждого теста вычисляется *P-value*, выражающее вероятность того, что идеальный генератор случайных последовательностей произведет последовательность менее случайную, чем исследуемая. Таким образом, значения *P-value*, близкие к 1, говорят о случайном характере исследуемой последовательности. Исследуемые последовательности проходят тесты, если выполнено условие $P\text{-}value \geqslant \alpha$. Выводы о случайности исследуемых данных делаются на основании доли тестируемых последовательностей, проходящих тесты [4].

На рис. 5 приведены примеры результатов работы частотного теста для 30 последовательностей по 1 500 000 бит при использовании предложенных методов постобработки двоичных последовательностей. Максимальное отклонение количества нулей и единиц в них не превышало 0,24 %.

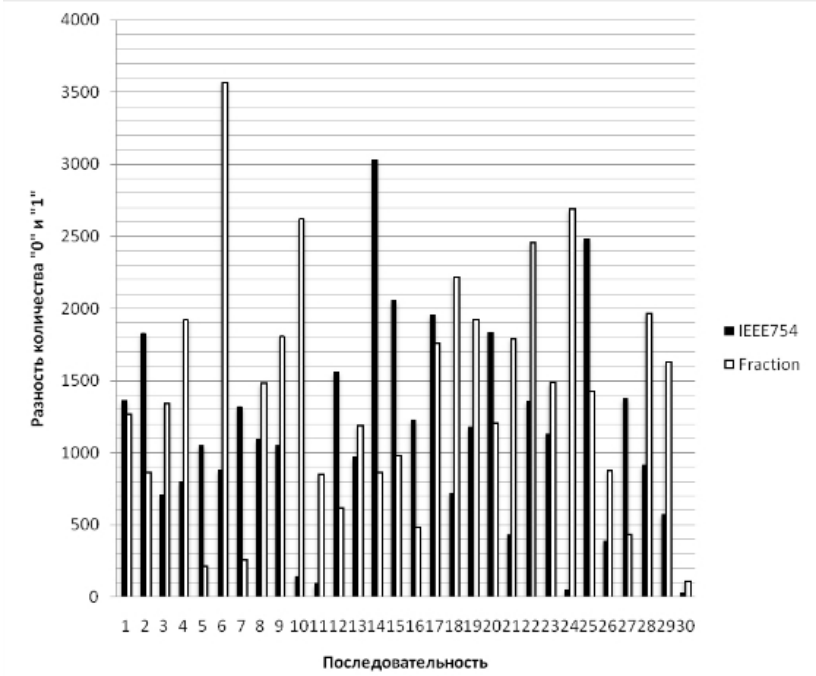


Рис. 5. Частотные характеристики последовательностей по 1 500 000 бит

Результаты прохождения тестов для данных последовательностей представлены в таблице.

Таблица

Тест	Доля прохождения		Среднее *P-value*	
	IEEE754	*Fraction*	*IEEE754*	*Fraction*
Frequency	30/30	29/30	0,431095	0,335982
Block Frequency	29/30	30/30	0,526829	0,420477
Runs	30/30	29/30	0,532709	0,545858
Longest Run	29/30	30/30	0,469816	0,599864
Rank	28/30	30/30	0,492630	0,490890
Spectral	29/30	30/30	0,480825	0,497099
Serial	30/30	29/30	0,539214	0,433550
Approximate Entropy	30/30	30/30	0,510219	0,593105
Linear Complexity	30/30	30/30	0,496125	0,531018

В наборе статистических тестов NIST рекомендована минимальная доля последовательностей, проходящих тесты, достижение которой необходимо для подтверждения гипотезы о случайности исследуемых данных. Эта величина рассчитывается на основании числа исследуемых последовательностей и уровня значимости по формуле [5]:

$$p_{min} = (1-\alpha) - 3\sqrt{\frac{\alpha(1-\alpha)}{N}},$$

где N — число исследованных последовательностей.

В результате исследований доля последовательностей, прошедших тесты, была выше рекомендованного значения, из чего можно заключить, что предложенная программная модель действительно может быть источником криптографически стойких бинарных последовательностей. Также успешное прохождение тестов свидетельствует об отсутствии циклов в полученных бинарных последовательностях, а следовательно, и в фазовых траекториях. Это означает, что средняя длина циклов для рассмотренной системы оказывается больше длин исследованных последовательностей.

Заключение

Системы детерминированного хаоса сочетают в себе уникальные свойства. С одной стороны, они способны демонстрировать сложное и непредсказуемое поведение, с другой — их детерминированность позволяет воспроизвести это поведение, зная точные начальные условия и параметры системы. Эти свойства делают их пригодными для использования в криптографии. Однако современная криптография имеет дело с цифровыми системами. Моделирование хаотических систем в конечном цифровом пространстве может негативно сказаться на их характеристиках. В данной работе исследуется программный генератор псевдослучайных бинарных последовательностей, созданный на основе дискретно временной модели автогенератора Ван-дер-Поля. Исследование проводится с использованием набора статистических тестов *NIST*, и показывает, что при определенных условиях предложенная программная модель способна производить криптографически стойкие бинарные последовательности.

Литература

[1] Blackledge Z.M., Ptitsyn N. On the Applications of Deterministic Chaos for Encrypting Data on the Cloud //Conference papers, School of Electrical Engineering Systems. Dublin: Dublin Institute of Technoligy, 2010. 11 p.

[2] Зайцев В.В., Давыденко С.В., Зайцев О.В. Динамика автоколебаний дискретного осциллятора Ван–дер–Поля // Физика волновых процессов и радиотехнические системы. 2000. Т. 3. № 2. С. 64–67.

[3] Зайцев В.В., Зайцев О.В., Яровой Г.П. Статистические оценки характеристик стохастических автоколебаний дискретного осциллятора Ван-дер-Поля // Физика волновых процессов и радиотехнические системы. 2001. Т. 4. № 1. С. 18–21.

[4] A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications // NIST Special Publication 800–22. Revision 1a: April 2010. 131 p.

[5] Игоничкина Е.В. Исследование статистических свойств кандидатов конкурса Estream // Актуальные проблемы безопасности информационных технологий: материалы II Международной научно-практической конференции (Красноярск, 9–12 сентября 2008 г.). Красноярск, 2008. С. 22–26.

Поступила в редакцию — 29/*V*/2013;
в окончательном варианте — 29/*V*/2013.

ON CONSTRUCTION OF PROGRAM PSEUDO-RANDOM NUMBERS GENERATORS ON THE BASIS OF DYNAMIC SYSTEMS IN DETERMINISTIC CHAOS MODE

© 2013 L.Yu. Gerasimov[2]

In this work possibilities of program modelling of deterministic chaos mode are investigated. The research is carried out on the example of program model of Van-der-Pol oscillator. *NIST* statistical tests suite is used for the evaluation of cryptographic properties of received generator of pseudo-random numbers.

Key words: deterministic chaos, pseudo-random numbers, cryptography, *NIST*.

Paper received 29/ *V*/2013.
Paper accepted 29/ *V*/2013.

[2]Gerasimov Leonid Yurievich (gerasimovleo@gmail.com), the Dept. of Security of Information Systems, Samara State University, Samara, 443011, Russian Federation.