УДК 004.421.5

Генератор случайных чисел на основе цепи Чуа

***О. М. Опякин*[1], *К. Д. Лишик*[1], *Д. А. Викульцев*[1]**

[1]Московский физико-технический институт (национальный исследовательский университет)

Проблема генерации случайных чисел остро стоит в различных областях науки: статистике, криптографии, машинном обучении, некоторых приложениях физики [4]. Однако получение истинно случайных чисел сопряжено с множеством проблем: высокой стоимостью аппаратных средств генерации и низкой производительностью их аналогов, использующих природные источники энтропии. Идея исследования заключается в аппаратной реализации генератора случайных чисел, отвечающего современным требованиям.

В рамках работы рассматривается способ генерации случайных чисел с помощью цепи Чуа (рис. 1)[5] - простейшей электрической схемы, способной демонстрировать режим хаотических колебаний. Она состоит из двух конденсаторов, катушки индуктивности, линейного резистора и диода Чуа - нелинейного резистора с отрицательным дифференциальным сопротивлением. В рамках реализации катушка индуктивности была заменена на соответствующий гиратор, позволяющий уйти из класса RLC – цепей в класс активных RC – цепочек. Измерялись – напряжения на емкостях C, C_1 и C_2. При определённом наборе параметров наблюдается картина трёхмерного аттрактора типа «двойной завиток».

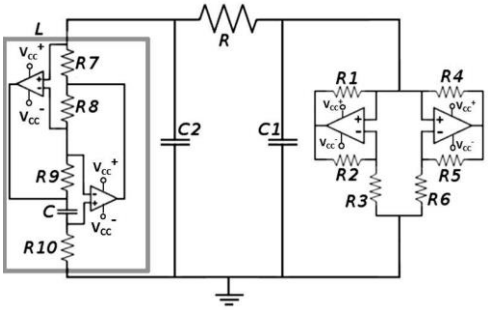

Рис. 1. Электрическая схема цепи Чуа

Цепь описывается системой уравнений, где $\mathrm{x}, \mathrm{y}, \mathrm{z}$ соответствуют напряжениям на ёмкостях и току через индуктивность соответственно, а функция $\mathrm{h}(\mathrm{x})$ описывает ВАХ диода Чуа:

$$\begin{cases} \dot{x} = \alpha\left(y - x - h(x)\right) \\ \dot{y} = x - y + z \\ \dot{z} = -\beta y \end{cases}$$

Полученная система не имеет аналитического решения, однако анализ правой части позволяет определить положения равновесия системы, а также исследовать их на устойчивость [1]. Положение равновесия $\mathrm{E}_3 = (0,0,0)^T$ находится в нуле и является неустойчивым “3D – фокусом”. Положения $\mathrm{E}_1 = \left(\frac{m_1 - m_0}{m_1 + 1}, 0, \frac{m_0 - m_1}{m_1 + 1}\right)^T$ и $\mathrm{E}_2 = \left(\frac{m_0 - m_1}{m_1 + 1}, 0, \frac{m_1 - m_0}{m_1 + 1}\right)^T$ – устойчивые “3D - фокусы” (термина "3-D фокус" не существует, однако мы будем обозначать характер фазового портрета именно так по аналогии с двумерным случаем).

Приведённая теория позволяет сделать предположение о характере поведения изучаемой системы. Ожидается, что система будет “раскручиваться” из положений E_1 и E_2.

Для проверки гипотезы реализовано численное решение системы. Метод Эйлера (рис. 2) подтверждает теоретические результаты: видно, что реальные положения равновесия системы совпадают с точками, полученными теоретически. Характеры положений равновесия также определены корректно (программное решение позволяет наблюдать динамику развития системы - она действительно "раскручивается" из E_1 и E_2).

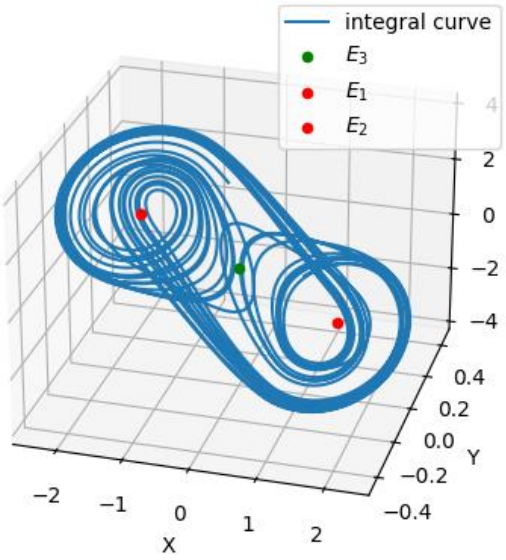

Рис. 2. Численное решение системы методом Эйлера

E_3 является положением равновесия - если выбрать её в качестве начального условия, то система сохранит своё положение. Однако при иных начальных условиях устойчивого положения в нуле не наблюдается. Возможно, это связанно с тем, что в ходе решения интегральная кривая не проходит в её достаточно малой окрестности. Точку нуля называют скрытым аттрактором системы Чуа [2].

Приведём способ получения случайной бинарной последовательности.

1) Рассмотрим вектор состояния системы $\vec{r} = (x, y, z)^T$. Назовём состояние, при котором $x > 0$ правым, а при $x < 0$ - левым. Среднее время, которое система проводит в одном из состояний, будем называть характерным временем системы τ_{ch}.

2) Пронаблюдав за системой на протяжении длительного времени заметим, что среднее время, проведённое в обоих состояниях одинаково, а интегральная кривая не образует цикл. Выдвинем гипотезу: спустя время $t \gg \tau_{ch}$ вероятности нахождения системы в левом и правом состояниях равны.

3) Будем следить за состояниями через указанные промежутки времени, сильно превышающие характерное время системы. Если система находится в правом состоянии, будем добавлять к последовательности 1, если в левом – 0. В итоге получим случайную бинарную последовательность.

Перейдем к аппаратной реализации.

Интересующие значения напряжений снимались с помощью электронного осциллографа. Полученные данные обрабатывались в соответствии с указанным выше алгоритмом.

Для оценки случайности бинарных последовательностей используется серия статистических тестов NIST [3], разработанная американским институтом стандартов и технологий (National Institute of Standards and Technology). Для исследуемой последовательности вычисляется значение P-value – вероятность того, что последовательность случайна. Если P-value для последовательности больше принятого в индустрии стандарта 0.01, то последовательность считается случайной.

На гистограмме (рис. 3) приведены результаты тестов NIST для одной из сгенерированных последовательностей.

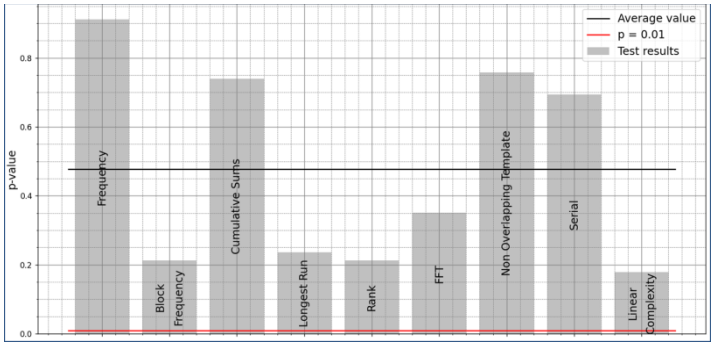

Рис. 2. Результаты тестов NIST для одной из последовательностей

Видно, что для всех тестов значения P-value значительно превышают порог, следовательно, полученная последовательность случайна. Таким образом, можно говорить о том, что предложенный способ позволяет генерировать действительно случайные числа.

Результаты данной работы могут быть полезны при создании генераторов случайных чисел, и кроме того, представляют фундаментальный интерес по исследованиям в области теории бифуркаций и детерменированного хаоса.

Литература

1. *Арнольд В. И.* Обыкновенные дифференциальные уравнения. — Ижевск: Ижевская республиканская типография, 2000.
2. *Kuznetsov N.* [et al.]. Hidden attractors in Chua circuit: mathematical theory meets physical experiments // Nonlinear Dyn (2023) 111:5859–5887.
3. Национальный институт стандартов и технологий. Генерация случайных чисел. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf (дата обращения: 20.12.2024).
4. *Marcin M. Jacak* [et al.]. Quantum generators of random numbers // Scientific Reports (2011) 11:16108.
5. Изображение электрической цепи схемы Чуа (рис. 1). URL: https://www.chuacircuits.com (дата обращения: 20.12.2024).