РЕАЛИЗАЦИЯ ГЕНЕРАТОРА ПСЕВДОХАОТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ МОДЕЛИ ЛОРЕНЦА

В. С. Садов, Р. С. Сырич
Кафедра интеллектуальных систем, Факультет радиофизики и компьютерных технологий, Белорусский государственный университет
Минск, Республика Беларусь
E-mail: romanchetto@gmail.com, vasiliy.sadov@gmail.com

В работе предлагается реализация генератора псевдохаотических последовательностей на основе модели Лоренца и исследование такой системы на криптостойкость при заданных различных начальных условиях.

Введение

Каждый криптографически стойкий генератор псевдослучайной числовой последовательности (ПСЧП) должен соответствовать трем основным требованиям:

1. Период ПСЧП должен быть достаточно большим для шифрования сообщений различной длины;
2. ПСЧП должна быть практически непредсказуемой, даже если известны тип генератора и предшествующий отрезок ПСЧП;
3. Генерирование ПСЧП не должно вызывать больших технических сложностей.

В данной работе будет проверен реализованный генератор на соответствие этим трем требованиям.

I. Модель псевдохаотического генератора на основе модели Лоренца

Модель Лоренца представляет собой хаотическую систему с трехмерным фазовым пространством. Мгновенное состояние определяется набором переменных (x,y,z), а оператор эволюции определен конкретным видом уравнений:

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(r - z) - y \\ \dot{z} = xy - bz. \end{cases}$$

Опираясь на работу [1] , были выбраны следующие параметры коэффициентов и начальные условия:

σ=10, r=28, b=8/3, x_0 = 2.345689, y_0 = 12.679135, z_0 = -5.136729.

II. Тесты NIST

Для проверки на соответствие второму требованию генератор ПСЧП должен пройти блок статистических тестов NIST. Каждый из тестов получает на вход конечную последовательность. В каждом тесте вычисляется т.н. P-значение: это вероятность того, что подопытный генератор произведет последовательность не хуже, чем гипотетический истинный. Если P-значение равно 1, то тестируемая последовательность идеально случайна, в противном случае последовательность полностью предсказуема. Затем P-значение сравнивается с порогом $\alpha = 0.01$, и если она больше α, то нулевая гипотеза принимается и последовательность признается случайной с уровнем доверия 99 процентов, в противном случае — отбраковывается [2]. Псевдослучайная числовая последовательность генератора длиной в 30 миллионов бит ($3*10^7$) с заданными выше начальными условиями была протестирована набором статистических тестов NIST. Результаты приведены в таблице.

Тест NIST	p-значение
Частотный побитовый тест	**0.578454**
Частотный блочный тест	**0.812081**
Тест на одинаковые идущие подряд биты	**0.043216**
Тест на самую длинную последовательность единиц в блоке	**0.309909**
Тест рангов бинарных матриц	**0.409172**
Спектральный тест	**0.005791**
Тест на встречающиеся пересекающиеся шаблоны	**0.428067**
Универсальный тест Мауэра	**0.471017**
Тест на линейную сложность	**0.082671**
Тест на подпоследовательности	**0.404209**
Приблизительная энтропия	**0.158597**
Тест кумулятивных сумм прямой	**0.921019**
Тест кумулятивных сумм обратный	**0.936095**

Временные затраты на генерацию ПСЧП длиной $3*10^7$ бит составили 14865,8 сек или 4,13 часа, что неудовлетворяет третье требование и большинство современных приложений.

III. Исследование поведения системы с различными заданными начальными условиями

Рассмотрим более подробно поведение генератора при заданных различных начальных условиях. Так как модель Лоренца – хаотическая система, то у реализованного генератора имеется

чувствительность к начальным условиям, что соответствует чувствительности криптосистемы к открытому тексту или семени генератора ПСЧП, то есть любое изменение начальных условий приведет к существенным изменениям во всей траектории. Для исследования расходимости траекторий были запущены два генератора с различными начальными условиями, отличающимися на 10^{-3},10^{-1}, единицы, десятки, сотни. На графиках ниже (Рис. 1-5) показаны коэффициенты корреляции между соответствующими компонентами генераторов: 1 - x-компонента, 2 - y-компонента, 3 - z-компонента.

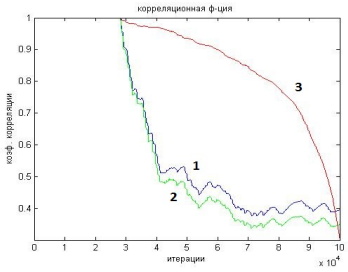

Рис. 1 – Начальные условия отличаются на 10^{-3}.

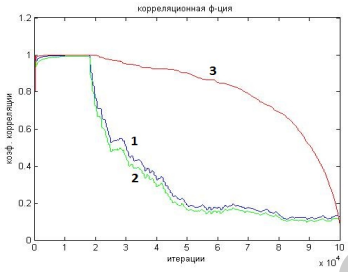

Рис. 2 – Начальные условия отличаются на 10^{-1}.

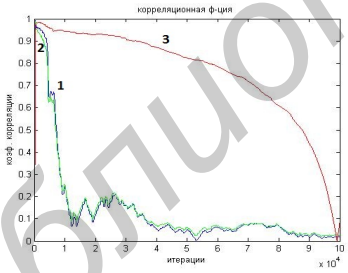

Рис. 3 – Начальные условия отличаются на единицы.

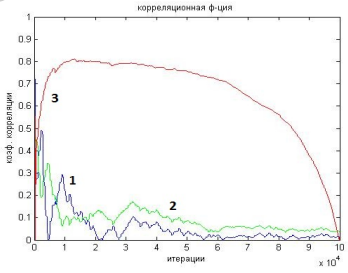

Рис. 4 – Начальные условия отличаются на десятки.

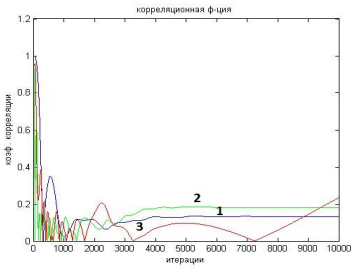

Рис. 5 – Начальные условия отличаются на сотни.

Заключение

Из полученных графиков следует:

1. Криптостойкость генератора зависит от заданных начальных условий. Результаты теста NIST будут разными для разных начальных условий.
2. Чем меньше разница в начальных условиях, тем больше итераций нужно генератору, чтобы «дойти» до точки расхождения траекторий. Следовательно, пока он не достиг этой точки, генератор имеет низкую криптографическую стойкость.
3. При большой разнице в начальных условиях траектории быстро расходятся, но потом они начинают выравниваться, следовательно, нужно будет перезапускать генератор заново, причем с новыми начальными условиями для повышения криптостойкости. Это плохо соответствует первому требованию к ГПСЧП. Однако, если требуется зашифровать короткое сообщение, этот вариант наиболее криптографически стойкий.
4. Судя по графикам, оптимальным в плане отсутствия уязвимостей на начальном и конечных этапах, является тот случай, когда разница составляет десятки. В данном варианте можно шифровать сообщения любой длины, при достаточно высокой криптографической стойкости, что хорошо соответствует первому требованию к криптостойким генераторам псевдослучайной числовой последовательности.
5. Быстродействие такого генератора оставляет желать лучшего. Оно не удовлетворяет третьему требованию к криптостойким генераторам ПСЧП. Разработка аппаратных и программных средств увеличения производительности вычислений может решить данную проблему.

1. Кузнецов С. П. Динамический хаос / С. П. Кузнецов // М.:Физматлит – 2001. – с. 56,
2. 2. National Institute of Standards and Technology. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. / NIST// Special Publication 800-22 Revision 1a. 2010.