МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра дискретной математики и информационных технологий

ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ НА КЛЕОЧНЫХ АВТОМАТАХ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

Студента 4 курса 421 группы
направление 09.03.01 - Информатика и вычислительная техника
факультета компьютерных наук и информационных технологий
Воропаева Дмитрия Николаевича

Научный руководитель
д.ф.-м.н., профессор _____ В. А. Молчанов

Заведующий кафедрой
д. ф.-м. н., доцент _____ Л. Б. Тяпаев

Саратов 2019

ВВЕДЕНИЕ

В защите информации генераторы псевдослучайных чисел играют очень важную роль Их основная задача — генерировать ключи шифрования. Главным требованием к генераторам псевдослучайных чисел является их непредсказуемость. Генераторы псевдослучайных чисел можно разделить на два основных вида. Математические генераторы легко реализуемы. Но в связи с детерминированностью, последовательности выдаваемые такими генераторами не являются истинно псевдослучайными. Каждый генератор имеет конечное количество состояний, и через некоторое время выдаваемые последовательности начинают повторятся. Именно поэтому, к такие генераторы называются генераторами псевдослучайных последовательностей. Физические генераторы измеряют различные псевдослучайные величины, например тепловые шумы, скорость распада вещества. В связи с дороговизной и сложностью в обслуживании такие генераторы применяются не везде. В отличие от математических генераторов не зацикливаются, но могут быть подвержены грубым атакам.

Кроме защиты информации, генераторы псевдослучайных чисел востребованы в разных областях науки, например моделирование псевдослучайных процессов. Качество выдаваемой последовательности прямым образом влияет на качество исследования. Но наряду с непредсказуемостью в данной области имеет большой приоритет и скорость генерации псевдослучайных чисел. Стивен Вольфрам [1] предложил идею реализовать генератор псевдослучайных чисел на основе клеточного автомата.

Целью данной работы является исследование применимости генератора псевдослучайных чисел на основе клеточного автомата. Для выполнения этой цели поставлены следующие задачи:

3. создание ГПСЧ на основе клеточного автомата,
4. статистические исследование свойств построенного ГПСЧ.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе приводится понятие генератора псевдослучайных последовательностей.

В подразделе 1.1 описываются два вида ГСПЧ: аппаратные, генерируюище псевдослучайные последовательности на основе сигналов, полученных в результате измерения величин различных физических просессов, и математические, представляющие из себя некоторый математический алгоритм.

Во всех сферах применения ГПСЧ важнейшую роль играют такие качества как случайность и непредсказуемость. Поэтому задача оценки ГПСЧ представляет большой интерес. В подразделе 1.2 приведены примеры как визуальных методов оценки ГСПЧ, так и статистических

Второй раздел посвящен описанию клеточных автоматов. Дается определение клеточного автомата, описаны основные свойства клеточных автоматов: однородность и локальность. Приведена классификация клеточных автоматов, предложенная С. Вольфрамом.

В третьем разделе приведена реализация генератора псевдослучайных чисел на основе клеточного автомата.

В подразделе 3.1 описывается алгоритм генератора. Генератор представляет собой совокупность двух двумерных клеточных автоматов и циклического двоичного счетчика. Под окрестностью клетки подразумевается сама клетка, клетки имеющие общую сторону и клетки, соприкасающиеся с данной углами. Множество возможных состояний включает в себя 0 и 1. Новое состояние каждойклетки определяется на основе значений клеток, находящихся в окрестности данной.

При генерации псевдослучайного числа каждый автомат переводится на один шаг вперед: для этого каждой ячейке задается новое состояние. После чего берется первая строка из первого автомата, первая строка из второго автомата, урезанная до размерности первой строки. Затем к этим строкам

применяется побитовое исключающее или. Новая строка является сгенерированным числом в двоичном виде.

Во подразделе 3.2 описывается реализованный в рамках данной работы прототип ГСПЧ. Прототип реализован в виде модуля для языка программирования Python3. Включает в себя два класса: класс автомат и класс генератор. В подразделе 3.3 подробно разобран пример генерации случайного числа.

Четвертый раздел полностью посвящен тестированию ГСПЧ. Тут показывается равномерное распределение, полученное с помощью ГСПЧ, подробно описывается пакет статистических тестов NIST, разработанный в Национальном институте стандартов и технологий. Целью этого набора является определение меры случайности двоичных последовательностей, порождённых ГСПЧ. В подразделе 4.3 содержатся результаты прохождения этих тестов.

В пятом разделе продемонстрирован пример применения реализованного мною ГСПЧ – выисление числа етодом Монте-Карло.

ЗАКЛЮЧЕНИЕ

В ходе данной работы мной была разработана программа для генерации псевдослучайных чисел. Были исследованы такие характеристики выдаваемой последовательности псевдослучайных чисел от 1 до 100 как дисперсия и среднее арифметическое. Было продемонстрировано применение ГПСЧ на основе клеточного автомата при решении такой задачи, как нахождение числа π. Были прведены статистические тесты NIST. По результатам исследований, можно сказать, что данный генератор можно применять в моделировании псевдослучайных процессов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Stephen Wolfram, Random Sequence Generation by Cellular Automata, Advances of applied mathematics 7, 123-169 (1986)

[2] S. Wolfram «New Kind of Science» [Электронный ресурс] сайт. URL: https://www.wolframscience.com Дата обращения 20.04.2019.

https://ru.wikipedia.org/wiki/Аппаратный_генератор_псевдослучайных_чисел

[3] Кнут, Д. Искусство программирования, том 2. Получисленные алгоритмы, 3-е изд. —М.: «Вильямс», 2007 —832 с.

[4] Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ.Электрон. журн. 2017, No 1, с.22-28.

[5]Статистическое тестирование генераторов псевдослучайных чисел с использованием набора статистических тестов NIST STS [Электронный ресурс] сайт. URL: https://cyberleninka.ru/article/n/statisticheskoe-testirovanie-generatorov-psevdosluchaynyh-chisel-s-ispolzovaniem-nabora-statisticheskih-testov-nist-sts Дата обращения 20.04.2019.

[6] Лобанов, А. И. Модели клеточных автоматов // Компьютерные исследования и моделирование No3, 2010 —21 с.

[7] Б. М. Сухинин, Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов, ПДМ, 2010, номер 2, 34–41

[8] Равномерный и нормальный законы распределения непрерывных псевдослучайных величин [Электронный ресурс] сайт. URL: http://edu.tltsu.ru/er/book_view.php?book_id=1cee&page_id=19506 Дата обращения 20.04.2019.

[9] Статистические тесты NIST [Электронный ресурс] сайт. URL: sewiki.ru/Моделирование_методом_Монте-Карло Дата обращения 25.04.2019.

[10] Слеповичев, И. И. Генераторы псевдослучайных чисел. Учебное пособие [Электронный ресурс]. URL: https://www.sgu.ru/sites/default/

/2018/07/09/slepovichev_i.i._generory_psevdosluchaynyh_chisel_2017.pdf (дата обращения: 10.09.2018).

11] Суперкомпьютерное образование [Электронный ресурс]. URL: http://hpc-education.ru/files/lectures/2011/ershov/ershov_2011_lectures02.pdf (дата обращения: 10.09.2018).

[12] Статистическая проверка псевдослучайности двоичных последовательностей методами NIST [Электронный ресурс]. URL: https://habr.com/ru/company/securitycode/blog/237695/ (датаобращения: 10.09.2018).

[13] Карпов А.В., Туктарова И. Р., Смоляков А.Д.,

Имитационная компьютерная модель криптографической системы, основанная на генераторах М-последовательности / А.В. Карпов, И.Р. Туктарова, А.Д. Смоляков – Казань: Казан. ун-т, 2015. – 30 с.

[14] Алгоритм AES (Rijndael) [Электронный ресурс] : [сайт]. URL: http://crypto.pp.ua/2010/03/algoritm-aes-rijndael (дата обращения: 08.05.2019). Загл. с экрана. Яз. рус.

[15] Коноплева, А. П. Совершенствование программно-аппаратной базы клеточных автоматов [Электронный ресурс] : [сайт]. URL: http://ea.donntu.org:8080/bitstream/123456789/3908/1/1_Коноплева.pdf (дата обращения: 08.05.2019). Загл. с экрана. Яз. рус.

[16] Технические и математические науки. Студенческий научный форум. Электронный сборник статей по материалам XI студенческой международной научно-практической конференции [Электронный ресурс] : [сайт]. URL: 12 https://nauchforum.ru/archive/SNF_tech/11%2811%29.pdf (дата обращения: 08.05.2019). Загл. с экрана. Яз. Рус

[17] Простейшие клеточные автоматы и их практическое применение [Электронный ресурс]. URL: https://itnan.ru/post.php?c=1&p=273393 (дата обращения: 08.05.2019)

[18] Методы Монте-Карло: теоретические основы и приложения [Электронный ресурс]. URL: http://www.scert.ru/conferences/cites/2009/presentation/Presentation/School/Prigarin.pdf (дата обращения: 08.05.2019)

[19] Применение клеточных автоматов для моделирования транспортных потоков [Электронный ресурс]. URL: https://icmmg.nsc.ru/sites/default/files/pubs/2.pdf (дата обращения: 08.05.2019)
[20] Клеточные автоматы в криптографии [Электронный ресурс]. URL: http://lib.itsec.ru/articles2/crypto/kletochnye-avtomaty-v-kriptografii-chast-2 (дата обращения: 08.05.2019)