Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Генератор псевдослучайных последовательностей на основе клеточных автоматов

АВТОРЕФЕРАТ

дипломной работы

студентки 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Ефремовой Анастасии Андреевны

Научный руководитель

доцент, к.ф.-м.н. _____ А.Н. Гамова

31.12.2016 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

31.12.2016 г.

Саратов 2017

ВВЕДЕНИЕ

В задачах вычислительной математики, криптографии, математического моделирования часто применяются псевдослучайные последовательности. Причем такие последовательности должны быть неотличимы от истинно случайных последовательностей по своим статистическим свойствам. Для выработки таких последовательностей используют специальные алгоритмы – генераторы псевдослучайных последовательностей (ГПСП).

Созданию хороших генераторов псевдослучайных последовательностей уделяется достаточно большое внимание в математике. Проблема в том, что все генераторы псевдослучайных последовательностей при определенных условиях дают предсказуемые результаты.

Известно, что при реализации различных криптопреобразований используются случайные значения, поэтому стойкость криптопреобразования напрямую зависит от алгоритма формирования случайных чисел, а точнее, от степени их случайности.

К настоящему времени разработано большое количество всевозможных алгоритмов генерации псевдослучайных последовательностей, основанных на использовании положений теории чисел, свойствах различных алгебраических систем, применении конечных (в том числе клеточных) автоматов и т.д.

Цель данной работы:

- рассмотреть методы генерации псевдослучайных последовательностей на основе клеточных автоматов;
- разработать программную реализацию генератора псевдослучайных чисел на основе различных клеточных автоматов;
- проверить надежность и эффективность полученных генераторов на базе известных тестов;
- оценить результаты тестирования.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе дипломной работы представлены основные сведения о генерации псевдослучайных чисел. В подразделе 1.1 приведено определение генератора псевдослучайных чисел (ГПСЧ) и его особенности. В подразделе 1.2 рассматриваются криптографически стойкие ГПСЧ и предъявляемые к ним требования.

В последнем подразделе первого раздела приведена информация о тестировании псевдослучайных последовательностей: виды тестов и известные наборы для тестирования.

Второй раздел посвящен теории клеточных автоматов. В нем приведены основные определения, виды клеточных автоматов и их свойства. Рассматриваются такие понятия как окрестности ячейки автомата разных радиусов, виды граничных условий автомата и правила переходов автомата из одного состояния в другое.

Подраздел 2.1 содержит основные свойства клеточных автоматов, такие как зависимость числа единичных заполнений ячеек от веса локальной функции связи и свойство обратимости.

В подразделе 2.2 рассматриваются проблемы классификации клеточных автоматов. Представлена классификация по типу поведения, предложенная С.Вольфрамом, а также упомянуты другие существующие классификации.

О типах клеточных автоматов, а также правил перехода рассказывается в подразделе 2.3.

Клеточные автоматы используются в симметричном шифровании, основанном на шифре Вернама. КлА применяются для генерации псевдослучайных последовательностей (ПСП), которые используются в процессе шифрования. Качество ПСП сильно зависит от набора использованных правил перехода для КлА.

В третьем разделе рассматриваются ГПСЧ на основе клеточных автоматов, реализованные разными авторами. Подраздел 3.1 посвящен

исследованиям в области клеточных автоматов как ГПСЧ. Впервые КлА были применены в качестве генератора псевдослучайных последовательностей С. Вольфрамом. Он использовал однородные одномерные КлА с радиусом окрестности $r = 1$ по правилу 30.

Далее изучались другие однородные КлА, и по тестам Diehard было выявлено, что лучшими случайными свойствами обладает автомат, использующий правило 105, следом идет 165, 90 и 150, а в конце правило 30.

В дальнейшем было обнаружено, что генераторы на основе неоднородных автоматов с применением правил 90 и 150 получаются более стойкими генераторами ПСП. И при использовании именно этих правил достигается максимальный период. Криптографические свойства неоднородных клеточных автоматов представлены в подразделе 3.2. Также в этом разделе приведены способы формирования последовательностей из ячеек автомата.

Tomassini и Perrenoud показали, что как ГПСЧ правило 30 плохо проходит тест на критерий согласия Пирсона (критерий χ^2) в сравнении с другими ГПСЧ, реализованными на основе неоднородных клеточных автоматов.

Они предложили использовать неоднородные одномерные КлА с $r = 1$ с применением четырех правил: 90, 150, 105 и 165, которые предоставляют хорошие ПСП и огромное количество секретных ключей, сложных для криптоанализа. Для получения этих правил использовалась техника клеточного программирования. Эта техника подробно описана в подразделе 3.3.

Клеточный автомат, основанный на любой комбинации этих правил создает криптостойкую ПСП.

В последние годы было обнаружено, что двумерные неоднородные КлА имеют высокую криптостойкость и проходят большинство тестов на случайность. Совсем недавние исследования показали эффективность ГПСЧ, основанного на комбинации одномерного и двумерного КлА (используются двумерный КлА с окрестностью фон Неймана и одномерный с применением

правил 90 и 150). Он показывает хорошие результаты тестирования пакетами тестов Diehard и ENT.

Существуют следующие аспекты, влияющие на качество ГПСЧ на основе КлА:

1) Граничные условия – обычно периодические граничные условия больше подходят для генерации случайных последовательностей, но иногда использование нулевых граничных условий позволяет избежать некоторых зависимостей между состояниями ячеек;

2) Количество ячеек автомата – однородный КлА, состоящий из N ячеек обычно имеет период меньше 2^N-1. С увеличением количества ячеек увеличивается максимально возможная длина периода полученной последовательности;

3) Начальное состояние автомата. Обычно влияние начального состояния на случайность мало. Чтобы проверить в работе проводились тесты на нескольких случайных начальных конфигурациях;

4) Правило перехода. Очевидно, что случайность сгенерированной последовательности сильно изменяется в зависимости от используемых правил перехода.

В подразделе 3.4 дается определение самопрограммируемого клеточного автомата и рассматриваются его особенности. Гуан и Тан в [18] предложили одномерный КлА, в котором правило перехода для каждой ячейки изменяется динамически, в зависимости от состояний ее соседних ячеек. Использование динамически изменяемых правил позволяет избежать шаблонов, возникающих, когда ячейки имеют постоянные правила.

Такой тип автомата может быть реализован как система двух связанных автоматов. Один из них (нижний) зависит от другого (верхнего) при выборе правила, которое нужно применить нижнему на следующем шаге. Окрестности этих двух автоматов не обязательно должны совпадать. В течение каждого шага одновременно происходят две следующие вещи:

- ячейка верхнего автомата применяет свое правило перехода;

- ячейка нижнего автомата применяет правило в зависимости от предыдущего состояния ячейки верхнего автомата (так как эти события одновременные, нижний автомат использует еще не изменившиеся значения).

Использование верхнего автомата для изменения правил добавляет случайности автомату.

В разделе 4 описан реализованный программный продукт, который представляет из себя реализацию ГПСЧ на основе различных клеточных автоматов, конфигурации которых можно настроить с помощью пользовательского интерфейса. Программа написана на языке C# с использованием технологии Windows Forms для создания пользовательского интерфейса.

В подразделе 4.2 приводится информация об использованном для тестирования пакете Diehard и результаты тестирования сгенерированных с помощью программы последовательностей. Для представления графических результатов тестирования написана программа с использованием технологии Windows Forms.

Работа завершается следующими приложениями:

1) Приложение А. Листинг программы представляет собой реализацию пользовательского интерфейса и ГПСЧ на основе нескольких типов КлА;

2) Приложение Б. Листинг программы представляет собой программу по переводу результатов тестирования в графический вид;

3) Приложение В. Графическое представление распределения *p*-значений включает в себя графические результаты тестирования сгенерированных последовательностей.

ЗАКЛЮЧЕНИЕ

Сфера генерации ПСП совершенствуется, появляются новые методы генерации ПСП, обладающие криптостойкостью и проходящие большое количество тестов на случайность. В том числе генерация ПСП с помощью КлА.

Исследования в области клеточных автоматов продолжаются и их применение в криптографии дало на сегодняшний момент ряд результатов. Клеточные автоматы рассматриваются в качестве эффективных генераторов псевдослучайных последовательностей.

В ходе данной работы было сделано следующее:

- Рассмотрены различные виды клеточных автоматов и методы генерации псевдослучайных чисел с помощью них;
- Разработана программная реализация ГПСЧ на основе различных клеточных автоматов;
- Проведено тестирование реализованных генераторов и оценены результаты.

Для улучшения показателей генераторов на основе клеточных автоматов можно предложить следующие методы:

- Учет значения ячейки не в каждый момент времени, а через разные отрезки;
- Для подбора используемых правил используется техника клеточного программирования;
- Применение различных комбинаций одномерных и двумерных КлА;
- Увеличение числа ячеек и радиуса.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 James, F. A review of pseudorandom number generators [Электронный ресурс] / F. James // Computer Physics Communications, 1990. P. 329-344. URL: http://lammps.sandia.gov/threads/pdfFowF57Qu9A.pdf (дата обращения: 30.11.16). Загл. с экрана. Яз. англ.

2 Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Электронный ресурс] / Б. Шнайер М.: Триумф, 2002. 816 с. URL:http://htrd.su/wiki/_media/zhurnal/2012/03/23/todo_prikladnaja_kriptografija/cryptoshn.pdf (дата обращения: 10.12.16). Загл. с экрана. Яз. рус.

3 Кнут, Д. Искусство программирования. В 3 т. Т. 2. Получисленные алгоритмы / Д. Кнут. М.: Вильямс, 2007. 788 с.

4 Иванов, М. А. Теория, применение и оценка качества генератора псевдослучайных последовательностей [Электронный ресурс] / М. А. Иванов, И. В. Чугунков М.: Кудиц - Образ, 2003. 240 с. URL: http://www.twirpx.com/file/211070/ (дата обращения: 10.11.16). Загл. с экрана. Яз. рус.

5 Salman, K. Analysis of Elementary Cellular Automata Boundary Conditions [Электронный ресурс] / K. Salman // International Journal of Computer Science & Information Technology (IJCSIT), Vol.5, №4, 2013. URL: http://airccse.org/journal/jcsit/5413ijcsit03.pdf (дата обращения: 30.11.2016). Загл. с экрана. Яз. англ.

6 Сухинин, Б. М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов [Электронный ресурс] / Б. М Сухинин // ПДМ, 2010, № 2. С. 34–41. URL: http://www.mathnet.ru/links/2a2179da3ebb2e0b2e534e173f0f4559/pdm180.pdf (дата обращения: 12.09.16). Загл. с экрана. Яз. рус.

7 Tomassini, M. Nonuniform Cellular Automata for Cryptography [Электронный ресурс] / M. Tomassini, M. Perrenoud // Complex Systems,

№12, 2000. P. 71–81. URL: http://www.complex-systems.com/pdf/12-1-3.pdf (дата обращения: 12.12.16). Загл. с экрана. Яз. англ.

8 Das, S. Analysis and synthesis of nonlinear reversible cellular automata in linear time [Электронный ресурс] / S. Das, B. Sikdar URL: https://arxiv.org/pdf/1311.6879.pdf (дата обращения: 30.11.16). Загл. с экрана. Яз. англ.

9 Тоффоли, Т. Машины клеточных автоматов [Электронный ресурс] / Т. Тоффоли, Н. Марголус М.: Мир, 1991. 280 с. URL: http://libarch.nmu.org.ua/bitstream/handle/GenofondUA/60796/9f7dbebb31db5672055237c38536f0ae.pdf?sequence=1 (дата обращения: 15.11.16). Загл. с экрана. Яз. рус.

10 Wolfram, S. A New Kind of Science [Электронный ресурс] / S. Wolfram, Wolfram Media, 2002. 1192 p. URL: http://www.wolframscience.com/nksonline/toc.html (дата обращения: 15.12.16). Загл. с экрана. Яз. англ.

11 Das, D. Programmable Cellular Automata Based Efficient Parallel AES Encryption Algorithm [Электронный ресурс] / D. Das, R. Mirsa // International Journal of Network Security & Its Applications, Vol.3, №6, 2011. URL: https://arxiv.org/ftp/arxiv/papers/1112/1112.2021.pdf (дата обращения: 14.09.2016). Загл. с экрана. Яз. англ.

12 Ganguly, N. A Survey on Cellular Automata [Электронный ресурс] / N. Ganguly, B. Sikdar, A. Deutsch, G. Canright, P. Chaudhuri URL: http://www.cs.unibo.it/bison/publications/CAsurvey.pdf (дата обращения: 10.12.16) Загл. с экрана. Яз. англ.

13 Lacharme, P. Pseudo-random sequences, boolean functions and cellular automata [Электронный ресурс] / P. Lacharme, B. Martin, P. Sole // Boolean Functions: Cryptography & Applications, Copenhague, Denmark 2008.P. 80-95. URL: https://hal.archives-ouvertes.fr/hal-00305493/document (дата обращения: 30.11.16). Загл. с экрана. Яз. англ.

14 Seredynski, F. Cellular automata computations and secret key cryptography [Электронный ресурс] / F. Seredynski, P. Bouvry, A.Y. Zomaya // Parallel Computing, Volume 30, 2004. P.753-766. URL: http://pascal.bouvry.org/ftp/parco04.pdf (дата обращения: 14.11.2016). Загл. с экрана. Яз. англ.

15 Ефремова, А. А. Генератор псевдослучайных чисел на основе клеточных автоматов / А. А. Ефремова, А. Н. Гамова // Компьютерные науки и информационные технологии Материалы Международной научной конференции, 2016. С. 131–134.

16 Nandi, S. Theory and Applications of Cellular Automata in Cryptography [Электронный ресурс] / S. Nandi, B. Kar, P. Chaudhuri, IEEE Transactions on Computers, vol. 43, №12, 1994. P. 1346-1357. URL: https://www.researchgate.net/publication/3043410_Theory_and_Applications_of_Cellular_Automata (дата обращения: 30.11.16). Загл. с экрана. Яз. англ.

17 Guan, S. Pseudorandom number generation based on controllable cellular automata [Электронный ресурс] / S. Guan, S. Zhang // Future Generation Computer Systems Vol. 20, Issue 4, 2004. P. 627-641 URL: https://pdfs.semanticscholar.org/6504/60d6a47327f8a55f0fc723748fddee6ae9dc.pdf (дата обращения: 19.11.16). Загл. с экрана. Яз. англ.

18 Guan, S.U. Pseudorandom number generation with self-programmable cellular automata [Электронный ресурс] / S. U. Guan , S. K. Tan // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,vol. 23, no. 7, 2004. P. 1095–1101 URL: https://core.ac.uk/download/pdf/333833.pdf (дата обращения: 12.11.16). Загл. с экрана. Яз. англ.

19 Hoe, D. H. K. Cellular Automata-Based Parallel Random Number Generators Using FPGAs [Электронный ресурс] / D. H. K. Hoe, J. M. Comer, J. C. Cerda, C. D. Martinez, M. V. Shirvaikar // International Journal of Reconfigurable Computing, 2012. URL:

downloads.hindawi.com/journals/ijrc/2012/219028.pdf (дата обращения: 10.09.2016). Загл. с экрана. Яз. англ.

20 Ефремова, А. А. Генератор псевдослучайных последовательностей на основе клеточных автоматов [Электронный ресурс] / А. А. Ефремова, А. Н. Гамова // Ломоносовские чтения на Алтае: фундаментальные проблемы науки и образования Сборник научных статей международной конференции. Алтайский государственный университет, 2015. С. 1073-1084. URL: http://elibrary.ru/item.asp?id=24748589 (дата обращения: 10.09.16). Загл. с экрана. Яз. рус.

21 Marsaglia, G. Diehard: A Battery of Tests of Randomness [Электронный ресурс] URL: http://stat.fsu.edu/~geo/diehard.html (дата обращения: 12.04.15). Загл. с экрана. Яз. англ.