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

Генераторы псевдослучайных двоичных последовательностей на базе обобщенных клеточных автоматов

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Шалыганова Глеба Германовича

Научный руководитель

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

31.12.2016 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

31.12.2016 г.

Саратов 2017

ВВЕДЕНИЕ

Псевдослучайные числовые последовательности давно и повсеместно используются во многих областях: при выборочных исследованиях, численном анализе, моделировании, проектировании игр, программировании, а также в криптографии (например, в шифре Вернама).

На практике, каждый из алгоритмов генерации псевдослучайных последовательностей обладает в той или иной мере различными недостатками, например, слишком коротким периодом выходной последовательности, неравномерным распределением, предсказуемостью, наличием корреляции, малой скоростью работы или сложностью реализации. По этим причинам, разработка новых генераторов, отличающихся высоким быстродействием и хорошими статистическими показателями, является актуальной научной задачей.

Идея клеточных автоматов была предложена в конце сороковых годов 20 века и нашла свое применение во многих областях науки, в том числе и в криптографии. С тех пор было написано много работ, где предлагались идеи использования клеточных автоматов в криптографических приложениях, в том числе и в качестве основы для генераторов псевдослучайных последовательностей [1].

Целью работы является исследование, разработка и анализ методов построения генераторов псевдослучайных двоичных последовательностей на базе клеточных автоматов.

Дипломная работа состоит из введения, 5 разделов, заключения, списка использованных источников и двух приложений.

КРАТКОЕ СОДЕРЖАНИЕ

1) Клеточные автоматы

Идея клеточных автоматов была задумана и сформулирована в конце сороковых годов 20 века Джоном фон Нейманом и Конрадом Цусе независимо друг от друга, как универсальная вычислительная среда для построения, анализа и сравнения характеристик алгоритмов.

Область применения клеточных автоматов достаточно обширна – начиная от простых игр, и заканчивая искусственным интеллектом. В наше время тема клеточных автоматов очень актуальна, поскольку с помощью этой теории можно смоделировать многие процессы, происходящие в окружающем мире. Так, клеточные автоматы применяются в математике, физике, биологии, экономике, социологии, а также в информатике. Но нас больше всего интересует их применение в криптографии. Именно об этом пойдет речь в данной дипломной работе.

Подраздел 1.1 «Понятие клеточного автомата» знакомит с основными используемыми в работе определениями.

Обширные исследования клеточных автоматов были проведены Стивеном Вольфрамом. В ходе своих исследований он разработал классификацию клеточных автоматов по их поведению. Об этом идет речь в подразделе 1.2 «Классификация клеточных автоматов по их поведению».

Самым известным клеточным автоматом по праву можно считать игру «Жизнь», созданную в 1970 г. Джоном Хортоном Конвеем, математиком Кембриджского университета. В подразделе 1.3 «Игра «Жизнь» Джона Конвея» приводится краткий обзор этой игры.

2) Первые генераторы псевдослучайных двоичных последовательностей на базе клеточного автомата

В подразделе 2.1 «Базовые сведения о псевдослучайных последовательностях» приводится понятие псевдослучайной последовательности.

Постановка задачи генерации псевдослучайной последовательности описывается в подразделе 2.2 «Генерация псевдослучайной двоичной последовательности».

Первый алгоритм генерации псевдослучайных последовательностей на базе клеточного автомата был предложен британским математиком Стивеном Вольфрамом. Впоследствии, этот генератор был реализован в продукте Wolfram Research – Mathematica. В подразделе 2.3 «Клеточный автомат Вольфрама и генератор псевдослучайных двоичных последовательностей» приводится обзор данного генератора. Подобный генератор показывает хорошие статистические свойства, однако он сильно зависим от начальных значений ячеек. Кроме того, доказано [1], что для автомата размером вплоть до 500 бит существует успешное вскрытие (восстановление начального состояния автомата). Поэтому, подобные генераторы не применимы для использования в криптографических приложениях и в настоящее время не представляют большого интереса.

3) Лавинный эффект в клеточных автоматах

Одними из важнейших криптографических характеристик клеточного автомата являются характеристики лавинного эффекта. Под *лавинным эффектом* понимается способность динамической системы значительно изменять выходную последовательность при небольших изменениях входных данных. Другими словами, это означает зависимость всех выходных битов от каждого входного бита. Понятие лавинного эффекта часто применяется в криптографии, в основном при построении блочных шифров и криптографических хэш-функций. Основные определения приводятся в подразделе 3.1 «Понятие лавинного эффекта».

В данном разделе описываются результаты проведенных исследований по выявлению клеточных автоматов, обладающих высоким лавинным эффектом. В подразделе 3.2 «Лавинный эффект в классических клеточных автоматах» исследуются классические клеточные автоматы, а в подразделе 3.3 «Лавинный эффект в неоднородных клеточных автоматах» - неоднородные.

Результаты проведенных исследований показали, что в неоднородных клеточных автоматах лавинный эффект проявляется намного сильнее по

сравнению с классическими автоматами, имеющими сопоставимую мощность окрестности. Характеристики лавинного эффекта быстрее (за меньшее число тактов) достигают значения, близкого к оптимальному.

4) Обобщенные клеточные автоматы

Исходя из результатов, полученных в предыдущей главе, использование неоднородных клеточных автоматов при построении генераторов псевдослучайных последовательностей является перспективным подходом. Если представить набор ячеек неоднородного клеточного автомата в виде ориентированного графа, тогда получим структуру, которую будем называть обобщенным клеточным автоматом. Более точное пояснение дается в подразделе 4.1 «Основные понятия».

Представление набора ячеек клеточного автомата в виде графа позволяет сфокусироваться на поиске подходящего графа для обобщенного клеточного автомата в целях достижения наилучших показателей лавинного эффекта.

В статье [7] Ключарева П.Г. была сформирована гипотеза о том, что обобщенные клеточные автоматы, основанные на графах Рамануджана, будут обладать хорошими характеристиками лавинного эффекта. Одной из разновидностей графов Рамануджана являются графы Любоцкого-Филипса-Сарнака (LPS – графы). Алгоритм построения таких графов приведен в подразделе 4.2 «Построение графа Любоцкого-Филипса-Сарнака».

В рамках дипломной работы была реализована программа, выполняющая построение графа Любоцкого-Филипса-Сарнака по заданным параметрам. Программа написана на языке JAVA и представляет собой библиотеку, которую можно использовать при построении обобщенных клеточных автоматов.

Для того чтобы значения ячеек клеточного автомата подчинялись равномерному закону распределения, локальная функция связи должна быть равновесной, а также обладать максимальной нелинейностью. В подразделе 4.3 «Построение обобщенных клеточных автоматов» описывается алгоритм построения таких функций, основанный на методе конкатенации бент-функций.

В подразделе 4.4 «Оценка характеристик лавинного эффекта обобщенных клеточных автоматов» проводятся результаты исследований, подтверждающих гипотезу об эффективности применения графов Рамануджана при построении обобщенных клеточных автоматов.

Таким образом, обобщенные клеточные автоматы, построенные на основе графов Рамануджана, обладают хорошими характеристиками лавинного эффекта и могут использоваться в криптографических приложениях, в том числе при построении генераторов псевдослучайных последовательностей.

5) Генератор псевдослучайной двоичной последовательности на базе обобщенных клеточных автоматов

В 2010 году в своей статье «Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов» [10] Б.М. Сухинин описал генератор, в основе которого лежит использование классических и неоднородных клеточных автоматов. В статье показано, что псевдослучайная двоичная последовательность, порождаемая этим генератором, имеет очень хорошие статистические свойства, обладает большим периодом, а сам генератор имеет несложную программную и аппаратную реализацию и при этом обладает высоким быстродействием. Таким образом, при построении генератора псевдослучайных двоичных последовательностей на базе обобщенных клеточных автоматов было решено использовать аналогичный подход.

В подразделе 5.1 «Описание генератора» приводится схема построения генератора. Характеристики обобщенных клеточных автоматов, входящих в структуру генератора описываются в подразделе 5.2 «Описание клеточных автоматов, входящих в основу генератора». Алгоритм работы генератора рассматривается в подразделе 5.3 «Алгоритм работы генератора».

Как было отмечено выше, важным свойством генераторов псевдослучайных последовательностей является длина периода выходной последовательности. В подразделе 5.4 «Оценка периода выходной последовательности генератора»

показывается, что построенный генератор производит выходную последовательность, обладающую достаточно большим периодом.

В рамках дипломной работы разработана программа на языке JAVA, реализующая алгоритм работы описанного генератора. На вход программы подается целое число – необходимая длина двоичной последовательности. Выходом программы является либо бинарный файл, либо текстовый файл, содержащий последовательность ASCII-символов. Листинг программы приведен в приложении Б.

Критерием качества псевдослучайной последовательности являются специальные статистические тесты. Одними из самых надежных тестов являются тесты, входящие в пакет NIST. В подразделе 5.5 «Результаты статистических тестов генератора» приводятся результаты испытаний генератора. По результатам тестирования были пройдены все тесты из набора NIST. Таким образом, генераторы, построенные по предложенной схеме генерируют двоичные последовательности, практически неотличимые от истинно случайных. Подробное описание результатов тестирования находится в приложении А.

ЗАКЛЮЧЕНИЕ

Клеточные автоматы являются удобным и эффективным инструментом построения генераторов псевдослучайных последовательностей. Выходные последовательности, вырабатываемые такими генераторами, обладают хорошими статистическими свойствами.

В работе были рассмотрены обобщенные клеточные автоматы, основанные на графах Любоцкого-Филипса-Сарнака (LPS-графах), и написана компьютерная программа, осуществляющая построение LPS-графа по заданным параметрам. Эксперименты показали, что такие клеточные автоматы обладают хорошими показателями лавинного эффекта.

В продолжение работы была приведена схема построения генератора на базе обобщенных клеточных автоматов и написана компьютерная программа, реализующая данный алгоритм. Результаты статистических тестов показали, что такой генератор производит двоичные последовательности практически неотличимые от истинно случайных.

Учитывая высокую скорость генерации и хорошие статистические свойства выходных последовательностей, построенный генератор можно использовать в криптографических приложениях.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. R. Diaz Len, A. Hernandez Encinas, L. Hernandez Encinas. Wolfram cellular automata and their cryptographic use as pseudorandom bit generators [Электронный ресурс]. URL: http://digital.csic.es/bitstream/10261/21267/1/WolframAC.pdf (дата обращения 18.09.2016). Загл. с экрана Яз. англ.

2. Лобанов А.И. Модели клеточных автоматов // Компьютерные исследования и моделирование № 3, 2010.

3. Астафьев Г.Б., Короновский А.А., Храмов А.Е. Клеточные автоматы: Учебно-методическое пособие – Саратов: Изд-во ГосУНЦ «Колледж», 2003.

4. Feistel H. Cryptography and Computer Privacy // Scientific American, vol. 228, no. 5, 1973.

5. Сухинин Б.М. Исследование характеристик лавинного эффекта в двоичных клеточных автоматах с равновесными функциями переходов// Наука и образование, № 8, 2010.

6. Харари Ф. Теория графов [Электронный ресурс]. URL: http://getfr.no-ip.org/pub/dc/doc/math-prog/Математические%20основы%20программирования/PDF/Graph_Theory_Harary.pdf (дата обращения 10.12.2016). Загл. с экрана Яз. рус.

7. Ключарев П.Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей// Наука и образование, № 10, 2011.

8. Lubotzky A., Phillips R., Sarnak P., Ramanujan graphs// Combinatorica 8 (3), 1988.

9. Sarnak P., Cambridge tracts in mathematics. Some applications of modular forms, Cambridge, New York, Cambridge University Press, 1990.

10. Сухинин Б.М. Разработка генераторов псевдослучайных последовательностей на основе клеточных автоматов// Наука и образование, № 9, 2010. 21 с.

11. Агафонова И.В. Криптографические свойства нелинейных булевых функций [Электронный ресурс]. URL: http://dha.spb.ru/PDF/cryptoBOOLEAN.pdf (дата обращения 25.11.2016). Загл. с экрана Яз. рус.

12. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения [Электронный ресурс]. URL: http://www.math.nsc.ru/~tokareva/mon/11-lap-book.pdf (дата обращения 26.11.2016). Загл. с экрана Яз. рус.

13. Ключарев П.Г. Обеспечение криптографических свойств обобщенных клеточных автоматов// Наука и образование, № 3, 2012.

14. Rothaus O.S. On “bent” functions. [Электронный ресурс] // ScienceDirect [Электронный ресурс]. URL: http://www.sciencedirect.com/science/article/pii/0097316576900248 (дата обращения 26.11.2016). Загл. с экрана Яз. англ.

15. A Cusick T., Stanica P. Cryptographic Boolean functions and applications. [Электронный ресурс]. URL: https://books.google.ru/books?id=OAkhkLSxxxMC&lpg=PP1&ots=g1V7bTsAuB&lr&hl=ru&pg=PP1#v=onepage&q&f=false (дата обращения 25.11.2016). Загл. с экрана Яз. англ.

16. Сухинин Б.М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика, № 2, 2010. 9 с.

17. Слеповичев И.И. Теория генераторов псевдослучайных чисел. Курс лекций. – Саратов. 2015. 55 с.

18. SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Электронный ресурс]. URL: csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22b.pdf (дата обращения 29.04.2015) // NIST, 2001. Загл. с экрана Яз. англ.