МИНОБРНАУКИ РОССИИ

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

Кафедра теоретических основ компьютерной безопасности и криптографии

Высокоскоростные генераторы псевдослучайных двоичных последовательностей на основе клеточных автоматов

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Тертеряна Арама Саркисовича

Научный руководитель

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

18.01.2019 г.

Заведующий кафедрой

д. ф.-м. н., доцент _____ М. Б. Абросимов

18.01.2019 г.

Саратов 2019

ВВЕДЕНИЕ

Псевдослучайные числовые последовательности имеют широкое применение во многих областях: численный анализ, моделирование, проектирование игр, программирование, криптография. Особую роль в криптографии играют двоичные последовательности, на которых сделан акцент в данной работе.

Каждый из алгоритмов генерации псевдослучайных последовательностей имеет те или иные недостатки: короткий период выходной последовательности, неравномерное распределение, предсказуемость, наличие корреляции, малая скорость работы, сложность реализации. Поэтому разработка и реализация новых генераторов псевдослучайных последовательностей (ГПСП) с хорошими статистическими показателями и высоким быстродействием является актуальной теоретической и прикладной научной задачей.

Целью и задачами работы является исследование генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов и бент-функций (максимально-нелинейных булевых функций), анализ методов построения таких генераторов, программная реализация одного конкретного генератора на основе клеточного автомата и бент-функций, а также изучение применимости разработанного генератора в шифраторах.

Объектами исследования данной работы являются клеточные автоматы, бент-функции, генераторы псевдослучайных двоичных последовательностей на основе клеточных автоматов и шифраторы.

Дипломная работа состоит из введения, 6 разделов, заключения, списка использованных источников и 3 приложений. Общий объем работы – 68 страниц, из них 34 страниц – основное содержание, включая 19 рисунков и 1 таблицу, список использованных источников из 31 наименования.

КРАТКОЕ СОДЕРЖАНИЕ

1) Базовые сведения о псевдослучайных двоичных последовательностях и их генерации

В данном разделе приведены понятия случайной и псевдослучайной последовательностей, кратко описаны генераторы истинно случайных последовательностей, основанные на разнообразных физических законах, имеющих случайную природу, и генераторы псевдослучайных последовательностей, которые реализуют некий детерминированный алгоритм. Также приведены 3 свойства, которым должны соответствовать генераторы псевдослучайных последовательностей, чтобы вырабатываемые ими последовательности были применимы в криптографических целях.

2) Клеточные автоматы

В наше время тема клеточных автоматов чрезвычайно 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. Особый интерес для нас представляет применение клеточных автоматов в криптографии.

В подразделе 2.1 «Понятие и математическая модель клеточного автомата» описана математическая модель клеточного автомата и рассмотрены два типа клеточных автоматов – классические (однородные) и неоднородные.

В подразделе 2.2 «Классификация клеточных автоматов по их поведению» представлена классификация клеточных автоматов из четырех классов.

Самым известным клеточным автоматом можно считать игру «Жизнь», созданную в 1970 г. математиком Кембриджского университета Джоном Хортоном Конвеем. В подразделе 2.3 «Игра «Жизнь» Джона Конвея» приводится краткий обзор этой игры.

Первый алгоритм генерации псевдослучайных последовательностей на базе клеточного автомата был предложен британским математиком Стивеном Вольфрамом [5]. Подраздел 2.4 «Клеточный автомат Вольфрама и генератор псевдослучайных двоичных последовательностей» посвящен рассмотрению данного алгоритма.

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. Рассмотрены определения интегральной и пространственной характеристики лавинного эффекта, а также понятие оптимального лавинного эффекта, при котором изменения происходят с максимально возможной скоростью.

4) Бент-функции

Задача построения булевых функций, обладающих нелинейными свойствами, естественным образом возникает во многих областях. Чаще всего наибольший интерес вызывают те функции, для которых эти свойства экстремальны. Такие булевы функции называются максимально нелинейными или бент-функциями [8].

В подразделе 2.1 «Основные понятия» даны главные определения теории бент-функций.

В подразделе 2.2 описаны основные сферы применения бент-функций – комбинаторика, алгебра, теория кодирования, теория информации, теория символьных последовательностей, криптография и криптоанализ.

5) Генератор псевдослучайных двоичных последовательностей на базе клеточных автоматов и бент-функций

В рамках данной работы была рассмотрена схема генератора псевдослучайных последовательностей на основе клеточного автомата и пары бент-функций из статьи А.В. Соколова «Быстродействующий генератор

ключевых последовательностей на основе клеточных автоматов» [11]. В приложении А представлены две бент-функции и их векторы значений, использованные в качестве функций переходов автомата.

Рассмотрение данной схемы приведено в подразделе 5.1. «Описание генератора».

Предложенный Соколовым алгоритм был доработан и модифицирован для реализации в многопоточном режиме с использованием инициализационных последовательностей в качестве ключа. Описание модифицированного алгоритма и алгоритмов создания ключа генератора и нахождения хэш-значения для двоичной последовательности приведены в подразделе 5.2 «Алгоритм работы модифицированного генератора».

Следующий подраздел 5.3. «Оценка быстродействия генератора» посвящен анализу производительности полученного ГПСП. Производительность генератора составила 1,4 МБ/с или 11,88 Мбит/с, что является достаточно высоким показателем.

В подразделе 5.4 «Лавинный эффект клеточного автомата генератора» приводится описание анализа интегральной и пространственной характеристик лавинного эффекта. Сделан вывод, что автомат обладает весьма близким к оптимальному лавинным эффектом.

Статистическое тестированных выходных последовательностей генератора с помощью программного пакета NIST STS [16] приведено в подразделе 5.5 «Результаты статистических тестов генератора». Все тесты успешно пройдены, что свидетельствует о высоком «качестве» создаваемых генератором последовательностей. Результаты тестирования представлены в приложении Б.

6) Шифратор на основе генератора псевдослучайных последовательностей на базе клеточных автоматов и бент-функций

В качестве развития работы был создан шифратор, основанный на рассмотренном выше генераторе псевдослучайных последовательностей. Принимая на вход произвольный файл F и файл ключа, данный алгоритм с

помощью операции «исключающего ИЛИ» «накладывает» на двоичное представление файла F псевдослучайные последовательности, создаваемые генератором. На выходе получается зашифрованный файл F’, в котором исходная информация полностью скрыта.

В подразделе 6.1 «Алгоритм работы шифратора» приведен алгоритм работы шифратора.

В подразделе 6.2 «Анализ свойств шифратора» иллюстрируется сокрытие информации в результате шифрования файла и анализируется производительность шифратора в сравнении с некоторыми аналогичными свободно-распространяемыми программными пакетами. Сделан вывод, что полученная производительность 0,45 МБ/с или 3,6 Мбит/с недостаточна для создания и опубликования программного продукта на основе описанного алгоритма для пользовательского шифрования файлов и папок на персональном компьютере. Слабым местом данного варианта является необходимость преобразования файла из последовательности байт в последовательность бит и обратное преобразование. Однако, если отбросить этапы предварительной и пост-обработки файла, и проанализировать непосредственно процесс шифрования, получим производительность 1,34 МБ/с или 10,7 Мбит/с. При этом данная производительность указана для программной реализации шифратора, тогда как наибольшая производительность клеточных автоматов при правильном проектировании достигается при реализации на базе программно-аппаратных комплексов [30]. Листинг программной реализации приведен в приложении В.

Таким образом, можно предположить, что реализация рассматриваемого шифратора на базе программно-аппаратного устройства, встроенного в сетевой обмен на нижних уровнях сетевой модели OSI, где информация представлена в битах, позволит добиться производительности, достаточной для современных скоростей передачи данных по сети Интернет.

ЗАКЛЮЧЕНИЕ

Клеточные автоматы являются удобным и эффективным инструментом построения генераторов псевдослучайных двоичных последовательностей. Выходные последовательности, вырабатываемые такими генераторами, могут обладать хорошими статистическими свойствами при условии применения подходящих алгоритмов и методов.

В данной работе дана общая информация о клеточных автоматах и бент-функциях, а также написаны программный генератор двоичных псевдослучайных последовательностей и шифратор на его основе. Экспериментальные исследования показали, что генератор обладает достаточно высокой производительностью, а создаваемые им последовательности являются достаточно случайными для использования в криптографических приложениях, о чем свидетельствует успешное проходящие пакета тестов NIST STS и исследование лавинного эффекта клеточного автомата, лежащего в основе генератора. Анализ быстродействия шифратора показал, что он сильно проигрывает современным свободно распространяемым аналогам при использовании в качестве пользовательского шифратора файлов и папок на персональном компьютере, однако, реализация его на программно-аппаратной основе и встраивание в сетевой обмен на нижних уровнях сетевой модели OSI, оперирующих битами, является перспективным вариантом как в плане быстродействия, так и защищенности информации от взлома из-за использования аппарата бент-функций.

Данная работа была отмечена дипломом I степени XXXII Международной научной конференции «Техноконгресс» [31], заняла 1 место в IV Международном конкурсе учебных и научных работ студентов, магистрантов, аспирантов и докторантов «Quality Education – 2018» [32], а также была представлена на XI Студенческой международной заочной научно-практической конференции «Технические и математические науки. Студенческий научной форум» [33].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Сухинин, Б. М. Разработка генераторов двоичных псевдослучайных последовательностей на основе клеточных автоматов [Электронный ресурс] : [сайт]. URL: https://cyberleninka.ru/article/v/razrabotka-generatorov-psevdosluchaynyh-dvoichnyh-posledovatelnostey-na-osnove-kletochnyh-avtomatov (дата обращения: 12.10.2018). Загл. с экрана. Яз. рус.

2 Евсютин, О. О., Шелупанов, А. А. Основные подходы к использованию математического аппарата теории клеточных автоматов для решения задач кодирования информации [Электронный ресурс] : [сайт]. URL: http://old.tusur.ru/filearchive/reports-magazine/2014-32-2/12.pdf (дата обращения: 10.09.2018). Загл. с экрана. Яз. рус.

3 Астафьев, Г. Б., Короновский, А. А. Храмов, А. Е. Клеточные автоматы [Электронный ресурс] : [сайт]. URL: http://nonlin.sgu.ru/data/papers/Train/ CellAutomat.pdf (дата обращения: 17.10.2018). Загл. с экрана. Яз. рус.

4 Лобанов, А. И. Модели клеточных автоматов // Компьютерные исследования и моделирование №3, 2010 — 21 с.

5 R. Diaz Len, A. Hernandez Encinas, L. Hernandez Encinas. Wolfram cellular automata and their cryptographic use as pseudorandom bit generators [Электронный ресурс] : [сайт]. URL: http://digital.csic.es/bitstream/10261 /21267/1/WolframAC.pdf (дата обращения: 10.06.2018). Загл. с экрана. Яз. рус.

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

7 Ключарёв, П. Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование: электронное научно-техническое издание — М.: ФГБОУ ВПО «МГТУ им. Н.Э. Баумана», 2011 — 12 с.

8 Токарева, Н. Н. Бент-функции: результаты и приложения. Обзор работ [Электронный ресурс] : [сайт]. URL: http://sun.tsu.ru/mminfo/000349342/

03/image/03-015.pdf (дата обращения: 10.09.2018). Загл. с экрана. Яз. рус.

9 Rothaus, O.S. On «bent» functions [Электронный ресурс] : [сайт]. URL: http://www.sciencedirect.com/science/article/pii/0097316576900248 (дата обращения: 10.09.2018). Загл. с экрана. Яз. рус.

10 Алгоритм CAST-256 [Электронный ресурс] : [сайт]. URL: http://crypto.pp.ua/2010/05/algoritm-cast-256/ (дата обращения: 21.11.2018). Загл. с экрана. Яз. рус.

11 Соколов, А. В. Быстродействующий генератор ключевых последовательностей на основе клеточных автоматов [Электронный ресурс] : [сайт]. URL: http://pratsi.opu.ua/app/webroot/articles/1406206756.pdf (дата обращения: 06.10.2018). Загл. с экрана. Яз. рус.

12 Мазурков, М. И., Соколов, А. В. Методы синтеза двоичных псевдослучайных последовательностей со свойством *k*-граммного распределения для задач шифрования [Электронный ресурс] : [сайт]. URL: http://pratsi.opu.ua/app/webroot/articles/1346848441.pdf (дата обращения: 16.09.2018). Загл. с экрана. Яз. рус.

13 Электронная документация класса Random языка C# [Электронный ресурс] : [сайт]. URL: https://docs.microsoft.com/en-us/dotnet/api/system.random?redirected from=MSDN&view=netframework-4.7.2 (дата обращения: 28.11.2018). Яз. рус.

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

15 DIEHARD battery of statistical tests by George Marsaglia [Электронный ресурс] : [сайт]. URL: http://www.vmpcfunction.com/c7.html (дата обращения: 01.10.2018). Загл. с экрана. Яз. рус.

16 SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Электронный ресурс] : [сайт]. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication 80022r1a.pdf (дата

обращения: 10.09.2018). Загл. с экрана. Яз. рус.

17 Миненко, А. И. Экспериментальное исследование эффективности тестов для проверки генераторов случайных чисел [Электронный ресурс] : [сайт]. URL: http://vestnik.sibsutis.ru/uploads/1298012248_6230.pdf (дата обращения: 13.11.2018). Загл. с экрана. Яз. рус.

18 Слеповичев, И. И. Генераторы псевдослучайных чисел. Учебное пособие [Электронный ресурс] : [сайт]. URL: https://www.sgu.ru/sites/default/files/textdocsfiles/2018/07/09/slepovichev_i.i._generatory_psevdosluchaynyh_chisel_2017.pdf (дата обращения: 10.09.2018). Загл. с экрана. Яз. рус.

19 Бабенко, Л. А., Ищукова Е.А. Особенности применения методов линейного и дифференциального криптоанализа к симметричным блочным шифрам [Электронный ресурс] : [сайт]. URL: https://cyberleninka.ru/article/n/osobennosti-primeneniya-metodov-lineynogo-i-differentsialnogo-kriptoanaliza-k-simmetrichnym-blochnym-shifram (дата обращения: 10.09.2018). Загл. с экрана. Яз. рус.

20 Карпов, А. В., Туктарова, И. Р., Смоляков, А. Д. Имитационная компьютерная модель криптографической системы, основанная на генераторах М-последовательности. Учебное пособие [Электронный ресурс] : [сайт]. URL: https://dspace.kpfu.ru/xmlui/bitstream/handle/net/27369/ metod-06_042_001151.pdf ?sequence=1 (дата обращения: 24.11.2018). Загл. с экрана. Яз. рус.

21 Агафонова, И. В. Криптографические свойства нелинейных булевых функций [Электронный ресурс] : [сайт]. URL: http://dha.spb.ru/PDF/cryptoBOOLEAN.pdf (дата обращения: 10.09.2018). Загл. с экрана. Яз. рус.

22 Дубровская, А. О., Бураго, Т. В., Рощин, В. М., Горшков, М. В. Информатика. Тестовые материалы. Методические указания — Владивосток: Изд-во ТГЭУ, 2009 — 72 с.

23 Crypt4Free (Free Files Encryption Utility) for Windows XP/2000/NT/9X [Электронный ресурс] : [сайт]. URL:

http://www.secureaction.com/encryption_free (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

24 Алгоритм DESX [Электронный ресурс] : [сайт]. URL: http://crypto.pp.ua/2010/12/algoritm-desx (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

25 Алгоритм Blowfish [Электронный ресурс] : [сайт]. URL: http://crypto.pp.ua/2010/04/66 (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

26 Запретный файл 1.0.2.6 [Электронный ресурс] : [сайт]. URL: https://freesoft.ru/zapretnyy_fayl_1026 (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

27 Алгоритмы IDEA, PES, IPES [Электронный ресурс] : [сайт]. URL: http://crypto.pp.ua/2011/01/algoritmy-idea-pes-ipes (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

28 Using AES Crypt on Windows. Graphical User Interface (GUI) Option [Электронный ресурс] : [сайт]. URL: https://www.aescrypt.com/windows_aes_crypt.html (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

29 Алгоритм AES (Rijndael) [Электронный ресурс] : [сайт]. URL: http://crypto.pp.ua/2010/03/algoritm-aes-rijndael (дата обращения: 08.11.2018). Загл. с экрана. Яз. рус.

30 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: 08.11.2018). Загл. с экрана. Яз. рус.

31 Технические и математические науки. Студенческий научный форум. Электронный сборник статей по материалам XI студенческой международной научно-практической конференции [Электронный ресурс] : [сайт]. URL:

https://nauchforum.ru/archive/SNF_tech/11%2811%29.pdf (дата обращения: 16.11.2018). Загл. с экрана. Яз. рус.

32 IV Международный конкурс учебных и научных работ студентов, магистрантов, аспирантов и докторантов «Quality Education – 2018». Итоги конкурса [Электронный ресурс] : [сайт]. URL: https://eee-science.ru/wp-content/uploads/2018/11/QE-2018-02-22.10.2018.pdf (дата обращения: 16.11.2018). Загл. с экрана. Яз. рус.

33 Точная наука [Текст]: естественнонаучный журнал. – Кемерово: Издательский дом «Плутон», 2018. N 11. ISSN 2500-1132.