Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной физики
и метаматериалов на базе
Саратовского филиала
Института радиотехники и электроники
им. В.А. Котельникова РАН

ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ НА БАЗЕ КУСОЧНО-НЕЛИНЕЙНЫХ ОТОБРАЖЕНИЙ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса, 431 группы
направления подготовки 03.03.02 «Физика»
физического факультета СГУ имени Н.Г. Чернышевского
Пешкова Сергея Сергеевича

Научный руководитель
заведующий кафедрой
компьютерной физики и метаматериалов,
д.ф.-м.н. профессор _____В.М. Аникин
(подпись, дата)

Саратов
2016 год

Актуализация работы. Традиционные генераторы псевдослучайных чисел (с равномерным распределением) строятся на базе кусочно-линейных отображений. В работе доказывается возможность построения датчиков псевдослучайных чисел на базе **кусочно-нелинейных** отображений. Предложен алгоритм нахождения подобных отображений – посредством поиска базового (с равномерным инвариантным распределением) отображения (эндоморфизма) для отображения с инвариантным распределением, отличающимся от равномерного.

В качестве примеров рассмотрены переходы к датчикам псевдослучайных чисел от отображения Гаусса, отображения Реньи и отображения специального вида.

Предмет исследования – нелинейные разностные уравнения, решения которых демонстрируют хаотическое поведение.

Цель ВКР – построение хаотических генераторов псевдослучайных чисел (с равномерным распределением) как сопряженных кусочно-нелинейных отображений или кусочно-линйеных отображений с неполными ветвями.

Задачи работы:

1. Изучение методики построения сопряженных хаотических отображений.

2.. Выявление отображений, обладающих точным представлением для инвариантной плотности, отличной от равномерной, и допускающих возможность построения сопряженного отображения с равномерным инвариантным распределением.

3. Аналитическое построение сопряженных отображения, обладаю-щих равномерным распределением, на базе:

А) отображения Гаусса,

Б) отображения Реньи,

В) отображения с итеративной функцией в форме полинома с дробной степенью.

Научная новизна. Впервые поставлена и решена задача синтеза генераторов псевдослучайных чисел на основе кусочно-нелинейных хаотических отображений.

Содержание работы.

Глава 1. Сопряженные хаотические отображения

1.1. Математические определения

1.2. Алгоритм построения сопряженных отображений

Глава 2. Эндоморфизм, сопряженный отображению Гаусса.

2.1. История задачи Гаусса.

2.2. Отображение Гаусса.

2.3. Отображение с инвариантной плотностью, сопряженное отображению Гаусса

Глава 3. Эндоморфизм, сопряженный отображению Реньи

Глава 4. Нелинейное отображение, генерирующее равномерное распределение

ЗАКЛЮЧЕНИЕ

С применением методики построения сопряженных хаотических отображений в выпускной квалификационной работе найдены новые отображения, с которыми соотносится инвариантное распределение в форме равномерного закона, т.е. получены новые генераторы псевдослучайных чисел.

Отображения, построенные в главах 2-4 выпускной квалификационной работы на базе отображений Гаусса, Реньи, специального распределения расширяют класс кусочно-нелинейных отображений, обладающих равномерным инвариантным распределением. Это более редкий класс

отображений (по сравнению с кусочно-линейными отображениями с полными ветвями), генерирующими равномерное распределение.

На базе новых хаотических отображений с равномерной инвариантной мерой, можно построить отображения, вероятностные свойства которых описываются законами, не связанными с инвариантными плотностями исходных отображений, т.е. новые инвариантные отображения могут рассматривать самостоятельными базовыми отображениями для отображений с новыми итеративными функциями.

Разнообразие хаотических отображений обеспечивает возможность проведения математического моделирования задач методом статистических испытаний, также расширяет возможности хаотического кодирования информации, передаваемой по информационным сетям. Дело в том, что дополнительная степень защиты кодовой системы обеспечивается за счет применения сопряженных отображений, зависящих от параметра (параметров), который (ые) входят в состав ключа криптографической системы.