Отчет о проделанной работе с использованием оборудования ИВЦ НГУ

Тема работы: Разработка и тестирование генератора случайных чисел с доказанными свойствами

Состав коллектива: Журавлев Вячеслав Александрович, НГУ, студент 2го курса магистратуры ММФ. Email: slawajur@mail.ru.

Научное содержание работы:

1. Постановка задачи: Предложен алгоритм генерации псевдослучайных чисел на основе двуликих Марковских процессов. Теоретически доказана асимптотическая статистическая эффективность этого алгоритма. Цель работы - найти такие параметры, при которых данный алгоритм работает на практике, при этом минимизировав количество входных данных. Для проверки качества работы используются статистические тесты Alphabit, Rabbit, SmallCrush, Crush, BigCrush из библиотеки на языке C TestU01 и программы pRand - самые сильные статистические тесты на данный момент.
2. Современное состояние проблемы: теоретически доказана эффективность алгоритма, были проведены эксперименты с алгоритмом с одной ступенью и тестами NIST.
3. Подробное описание работы, включая используемые алгоритмы:

Описание алгоритма генерации псевдослучайных чисел. Для генерации с помощью данного алгоритма нужна входная последовательность бит. Допустим ее длина равна k > 0. Выходная последовательность генератора формируется следующим образом:

$$output_i = input_{i+k}, \text{ если } i \in [-k; -1]$$

$$output_i = \bigoplus_{j=i-k}^{i-1} output_j, \text{ если } i \geq 0 \text{ и } i \bmod k \neq 0$$

(1)

$$output_i = random, \text{ если } i \geq 0 \text{ и } i \bmod k = 0$$

, где *random* - случайное число, сгенерированное с помощью более слабого генератора, взявшего данные для инициализации из входной последовательности.

Это был описан алгоритм генерации с помощью одной ступени алгоритма. Также можно получить выходную последовательность генератора с помощью нескольких ступеней алгоритма. Допустим, есть x > 1 генераторов с конструкцией (1), причем:

$$input_i^0 = random$$

$$input_i^j = output_i^{j-1}, \text{ если } j > 0$$

$$k^0 < \ldots < k^{i-1} < k^i < k^{i+1} < \ldots < k^{x-1}$$

, где *random* - случайное число, переданное в алгоритм, k - длина входной последовательности. Тогда выходная последовательность такого генератора генерируется следующим образом:

$$output_i = \bigoplus_{j=0}^{x-1} output_i^j$$

4. Полученные результаты:

Были проведены эксперименты с помощью наборов статистических тестов Alphabit, Rabbit, SmallCrush, Crush и BigCrush из библиотеки TestU01, а также набором тестов pRand. Тестировались генераторы, с количеством ступеней от 2 до 4. Цель

была максимально сократить количество входных данных для генератора, чтобы он прошел все наборы тестов, в связи с чем были выбраны генераторы с двумя ступенями, где первая ступень заполняется маленьким количеством бит (сид), а вторая генерируется с помощью первой ступени. В качестве размера первой ступени в итоговом варианте было выбрано 127 бит. По результатам точно известно, что для прохождения всех наборов тестов для 127 бит достаточно размера второй ступени 16381 бит. Для тестирования наборами тестов Alphabit и Rabbit были использованы последовательности длиной 1 гигабайт.

5. Иллюстрации, визуализация результатов.

m_1	m_2	bookstack	NIST	DIEHARD	Alphabit	Rabbit	SmallCrush	Crush	BigCrush	pRand
127	257									
127	509									
127	1021									
127	2053									
127	16381									
127	32749									
127	65531									

m_1	m_2	m_3	m_4	bookstack	NIST	DIEHARD	BigCrush	pRand
127	257	509	-					
127	257	509	1021					
127	8191	524287	33554393					

Эффект от использования кластера в достижении целей работы: кластер очень сильно помог для выполнения данной работы, поскольку наборы тестов Crush и BigCrush занимают очень много времени и ресурсов компьютера. На кластере прохождение набора тестов Crush занимает от 12 часов до 20 часов, а прохождение набора тестов BigCrush занимает от 90 часов до 243 часов. Набор тестов pRand работал в течении 480 часов на кластере за 1 эксперимент. Используя предоставленную многозадачность данного кластера, можно ускорить тестирование генераторов в несколько раз.

Перечень публикаций, содержащих результаты работы: конференции CTCrypt 2020 и МНСК 2021.

Ваши впечатления от работы вычислительной системы и деятельности ИВЦ НГУ, а также предложения по их совершенствованию: положительные, данный кластер очень сильно помогает в данной работе, ускоряя процесс тестирования генераторов.