

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет радиофизики и компьютерных технологий
Кафедра интеллектуальных систем

Аннотация к дипломной работе

**«Генератор псевдохаотической числовой последовательности с
использованием технологии CUDA»**

Сырич Роман Сергеевич

Научный руководитель: кандидат технических наук,
профессор кафедры интеллектуальных систем, доцент В.С. Садов

2017

РЕФЕРАТ

Дипломная работа: 74 страницы, 48 рисунков, 3 таблицы, 18 использованных источников, 2 приложения.

ГЕНЕРАТОР ПСЕВДОХАОТИЧЕСКОЙ ЧИСЛОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ CUDA

Объект исследования - генератор числовой последовательности.

Цель работы - разработка генератора псевдохаотической числовой последовательности на основе модели Лоренца с использованием технологии CUDA, а также исследование характеристик разработанного генератора:

- Характер генерируемой последовательности;
- Чувствительности к начальным условиям;
- Быстродействие;

Методы исследования - компьютерное моделирование.

В работе произведена разработка и исследование псевдохаотического генератора числовой последовательности. В ходе исследований было установлено, что период генератора составляет от -2147483648.0 до 2147483647.0. Это связано с тем, что для генерации чисел используется тип данных с плавающей запятой и одинарной точностью, что обеспечивает максимальную производительность технологии CUDA.

Результаты статистических тестов показали, что генерируемая последовательность является псевдослучайной.

Множество генераторов, запущенных с разными начальными условиями, эффективно покрывают пространство состояний.

Проведенные эксперименты показали, что генератор чувствителен к начальным условиям, что является одним из требований хаотичности системы. В то же время, было показано, что у реализованного псевдохаотического генератора отсутствуют недостатки хаотического.

С помощью технологии CUDA удалось достичь десятикратного выигрыша в производительности при шифровании файлов большого объема.

Таким образом было доказано соответствие генератором требований, которые предъявляются к потоковым генераторам псевдослучайно числовой последовательности.

РЭФЕРАТ

Дыпломная праца: 74 старонкі, 48 малюнкаў, 3 табліцы, 18 выкарастанных крыніц, 2 дадатка.

ГЕНЕРАТАР ПСЕЎДАХААТЫЧНАЯ ЛІКАВАЙ ПАСЛЯДОЎНАСЦІ З ВЫКАРЫСТАННЕМ ТЭХНАЛОГІІ CUDA

Аб'ект даследавання - генератар ліквай паслядоўнасці.

Мэта - распрацоўка генератар псеўдахаатычнай лікавай паслядоўнасці на аснове мадэлі Лорэнца з выкарыстаннем тэхналогіі CUDA, а таксама даследванне характарыстык распрацаванага генератара:

1. Характар генераванай паслядоўнасці;
2. Адчувальнасць да пачатковых умоў;
3. Хуткадзейнасць;

Метады даследавання - кампутарнае мадэляванне.

У працы праведзена распрацоўка і псеўдахаатычнага генератара лікавай паслядоўнасці. Пад час даследванняў было, што перыяд генератара складаецца ў прамежку ад $-2\ 147\ 483\ 648.0$ да $2\ 147\ 483\ 647.0$. Гэта тлумачыцца тым, што для генерацыі лікаў выкарыстоўваецца нецэлаалікавы тып дадзеных з адзінарнай дакладнасцю, што забяспечвае максімальную прадукцыйнасць тэхналогіі CUDA.

Вынікі статыстычных тэстаў паказалі, што генераваная паслядоўнасць з'яўляецца псеўдавыпадковай.

Мноства генератраў, запушчаных з рознымі пачатковымі ўмовамі, эфектыўна пакрываюць прастору станаў.

Праведзеныя эксперыменты паказлі, што генератар адчувальны да пачатковым умовам, што з'яўляецца адным з патрабаванняў хаатычнасці сістэмы. У той жа час, было паказана, што ў рэалізаванага псеўдахаатычнага генератара адсутнічаюць недахопы хаатычнага.

З дапамогай тэхналогіі CUDA ўдалося дасягнуць дзесяцікратнага выйгрышу ў прадукцыйнасці пры шыфраванні файлаў вялікага аб'ёму.

Такім чынам была даказана адпаведнасць генератарам патрабаванняў, якія прад'яўляюцца да патокавых генератраў псеўдавыпадковай лікавай паслядоўнасці.

ABSTRACT

Thesis: 74 pages, 48 figures, 3 tables, 18 sources, 2 applications.

GENERATOR OF PSEUDOCHOTIC NUMERICAL SEQUENCE USING CUDA TECHNOLOGY

The object of research - numerical sequence generator.

Objective - Development of a pseudochaotic number sequence generator based on the Lorenz model using CUDA technology, and the study of the developed generator characteristics:

1. Nature of the generated sequence;
2. Sensitivity to initial conditions;
3. Performance;

The methods - Computer simulation.

In the work, a pseudo-chaotic generator of the numerical sequence was developed and studied. During the research it was found that the period of the generator is from -2 147 483 648.0 to 2 147 483 647.0. This is due to the fact that a floating point with single precision data type is used to generate numbers, which ensures the maximum performance of CUDA technology.

The results of statistical tests show that the generated sequence is pseudorandom.

A number of generators started with different initial conditions effectively cover the state space.

The conducted experiments have showed that the generator is sensitive to the initial conditions, which is one of the requirements of the chaotic system. At the same time, it was shown that the realized pseudochaotic generator does not have such disadvantages, that chaotic one has.

It is possible to achieve a tenfold gain in performance when encrypting large files using CUDA technology.

Thus, it was proved that the generator meets the requirements that are imposed on the stream pseudorandom number sequence generators.