БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

Построение датчиков базовой случайной величины по «уникальным» последовательностям

Ковалёв Матвей Сергеевич

Научный руководитель – доктор физико-математических наук, профессор кафедры математического моделирования и анализа данных ФПМИ Жук Е. Е.

Минск, 2024

РЕФЕРАТ

Дипломная работа, 31с., 10 рис., 1 табл., 1 приложения, 16 источников.

Ключевые слова: ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ, БАЗОВАЯ СЛУЧАЙНАЯ ВЕЛИЧИНА, МЕТОД ОБРАТНОЙ ФУНКЦИИ, ИСТОЧНИКИ ИСТИННО СЛУЧАЙНЫХ ЧИСЕЛ, ЭКСТРАКТОРЫ ЭНТРОПИИ

Объект исследования: датчики истинно случайных чисел, способы повышения энтропии результата датчика, построение базовой случайной величины на основе «уникальных» источников энтропии.

Цели работы: привести возможные способы получения истинно случайных чисел, реализовать метод прямой и обратной функции на основе истинно случайных источников, привести способы тестирования датчиков.

Методы исследования: а) теоретические: изучение доступной литературы и научных работ, посвященной построению истинно случайных генераторов чисел, б) практические: реализация программного датчика базовой случайной величины с использование «уникальных» источников чисел, тестирование результатов работы датчика доступными пакетами статистических тестов.

Результат: рассмотрены источники истинно случайных чисел, основывающиеся на тепловых шумах электронных систем; предложены методы получения БСВ из «уникальных» источников и методы получения случайных величин с произвольным законом распределения; написана программа реализующая метод прямой и обратной функции генерации базовой случайной величины; предложены алгоритмы экстракторов энтропии и тесты, проверяющие корректную работоспособность датчика случайных чисел.

РЭФЕРАТ

Дыпломная праца, 31с., 10 рыс., 1 табл., 1 дадаткі, 16 крыніца.

Ключавыя словы: ГЕНЕРАТАР ВЫПАДКОВЫХ ЛІКАЎ, БАЗАВАЯ ВЫПАДКОВАЯ ВЕЛІЧЫНЯ, МЕТАД ЗВАРОТНАЙ ФУНКЦЫІ, КРЫНІЦЫ ПРАЎДЗІВА ВЫПАДКОВЫХ ЛІКАЎ, ЭКСТРАКТАРЫ ЭНТРАПІІ

Аб'ект даследвання: датчыкі праўдзіва выпадковых лікаў, спосабы павышэння энтрапіі выніку датчыка, пабудова базавай выпадковай велічыні на аснове «унікальных» крыніц.

Мэты працы: прывесці магчымыя спосабы атрымання праўдзіва выпадковых лікаў, рэалізаваць метад прамой і зваротнай функцыі на аснове праўдзіва выпадковых крыніц.

Метады даследвання: а) тэарэтычныя: вывучэнне даступнай літаратуры і навуковых прац, прысвечанай пабудове праўдзіва выпадковых генератараў лікаў, б) практычныя: рэалізацыя праграмнага датчыка базавай выпадковай велічыні з выкарыстанне «унікальных» крыніц лікаў, тэставанне вынікаў працы датчыка даступнымі пакетамі статыстычных тэстаў.

Вынік: разгледжаны крыніцы праўдзіва выпадковых лікаў, якія грунтуюцца на цеплавых шумах электронных сістэм; прапанаваны метады атрымання БСВ з "унікальных" крыніц і метады атрымання выпадковых велічынь з адвольным законам размеркавання; напісана праграма рэалізуе метад прамой і зваротнай функцыі генерацыі базавай выпадковай велічыні; прапанаваны алгарытмы экстрактараў энтрапіі і тэсты, правяраючыя карэктную працаздольнасць датчыка выпадковых лікаў.

ABSTRACT

Thesis, 31p., 10 pic., 1 tables., 1 application, 16 sources.

Keywords: RANDOM NUMBER GENERATOR, BASIC RANDOM VARIABLE, INVERSE FUNCTION METHOD, SOURCES OF TRULY RANDOM NUMBERS, ENTROPY EXTRCTORS

Object of study: sensors of truly random numbers, ways to increase the entropy of the sensor result, the construction of a basic random variable based on "unique" sources.

Objectives: to give possible ways to obtain truly random numbers, to implement the method of direct and inverse functions based on truly random sources.

Methods: a) theoretical: the study of available literature and scientific papers devoted to the construction of truly random number generators, b) practical: the implementation of a software sensor of a basic random variable using "unique" sources of numbers, testing the results of the sensor with available statistical test packages.

Result: the sources of truly random numbers based on thermal noise of electronic systems are considered; methods for obtaining basic random variables from "unique" sources and methods for obtaining random variables with an arbitrary distribution law are proposed; a program is written that implements the method of direct and inverse functions of generating a basic random variable; algorithms for entropy extractors and tests that verify the correct operation of the random number sensor are proposed.