БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к магистерской диссертации

«Разработка критериев на основе статистического расстояния и закона повторного логарифма для статистического тестирования и оценки качества генераторов»

Грудинский Павел Васильевич

Научный руководитель – кандидат физ.-мат. наук, доцент
В.Ю. Палуха

Минск, 2022

РЕФЕРАТ

Магистерская диссертация: 43 с., 22 рис., 3 таб., 13 источников, 3 приложения.

Ключевые слова: КРИПТОГРАФИЧЕСКИЙ ГЕНЕРАТОР; ЗАКОН ПОВТОРНОГО ЛОГАРИФМА; СТАТИСТИЧЕСКОЕ ТЕСТИРОВАНИЕ; ПРОВЕРКА ГИПОТЕЗ; JAVA; STATISTICA; C++; R.

Объект исследования – криптографические генераторы случайных и псевдослучайных последовательностей.

Предмет исследования – вероятностные характеристики выходных последовательностей криптографических генераторов.

Цели работы – разработать критерии для статистического тестирования последовательностей криптографических генераторов, разработать программную реализацию алгоритма на основе этих критериев.

Задачи:

1. Разработать алгоритмы на основе статистического расстояния и закона повторного логарифма для статистического тестирования выходных последовательностей криптографических генераторов.
2. Написать эффективную программную реализацию этих алгоритмов.
3. Протестировать последовательности различных криптографических генераторов.
4. Оценить полученные результаты и сделать соответствующие выводы о точности реализованного алгоритма.

Полученные результаты:

1. Рассмотрены двухэтапные процедуры проверки гипотез для тестов Монобит и серий. Описаны алгоритмы этих процедур.
2. На языках Java и C++ написаны две программы, проводящие вычисления по разработанным алгоритмам.
3. При помощи разработанных программ протестированы последовательности криптографических генераторов разной степени стойкости.
4. При помощи программы «Statistica» и скрипта на R визуализированы гистограммы итоговых результатов.
5. Проведена оценка точности и эффективности используемых алгоритмов на основе полученных результатов.

Область применения – организации, которые используют генераторы случайных и псевдослучайных последовательностей разной степени стойкости.

ABSTRACT

Master thesis: 43 pages, 22 figures, 3 tables, 13 sources, 3 attachments.

Keywords: CRYPTOGRAPHIC GENERATOR; LAW OF THE ITERATED LOGARITHM; STATISTICAL TESTING; TESTING OF HYPOTHESIS; JAVA; STATISTICA; C++; R.

Object of research – cryptographic generators of random and pseudorandom sequences.

Subject of research – probabilistic characteristics of output sequences of cryptographic generators.

Work purpose – to develop criteria for statistical testing of sequences of cryptographic generators, to develop a software implementation of the algorithm based on these criteria.

Tasks:

1. Develop algorithms based on statistical distance and the law of the iterated logarithm for statistical testing of output sequences of cryptographic generators.
2. Create an efficient software implementation of these algorithms.
3. Test sequences of various cryptographic generators.
4. Evaluate obtained results and draw appropriate conclusions about the accuracy of the implemented algorithm.

Results:

1. Two-stage procedures for testing hypotheses for the Monobit and series tests are considered. The algorithms of these procedures are described.
2. Two programs are written in Java and C++ that perform calculations according to the developed algorithms.
3. Using the developed programs, the sequences of cryptographic generators of varying degrees of strength were tested.
4. Histograms of the final results are visualized using «Statistica» program and the R script.
5. The accuracy and efficiency of the algorithms used are estimated based on the obtained results.

Application area – organizations that use generators of random and pseudorandom sequences of varying degrees of strength.