БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

«Программный комплекс для оценки качества криптографических генераторов на основе информационной энтропии»

Грудинский Павел Васильевич

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

Минск, 2020

РЕФЕРАТ

Дипломная работа: 42 с., 11 рис., 2 таб., 13 источников, 3 приложения.

Ключевые слова: КРИПТОГРАФИЧЕСКИЙ ГЕНЕРАТОР; ФУНКЦИОНАЛЫ ЭНТРОПИИ ШЕННОНА, ТСАЛЛИСА И РЕНЬИ; ЧАСТОТНЫЕ ОЦЕНКИ ВЕРОЯТНОСТИ; ПРОВЕРКА ГИПОТЕЗ; C++.

Объект исследования – криптографические генераторы случайных и псевдослучайных последовательностей.

Предмет исследования – вероятностные характеристики выходных последовательностей криптографических генераторов.

Цель работы – разработать алгоритм и его программную реализацию для статистического тестирования выходной последовательности криптографического генератора.

Задачи:

1. Разработать алгоритмы нахождения функционала энтропии и, соответствующих ему математического ожидания и дисперсии.
2. Написать наиболее эффективную программную реализацию этих алгоритмов.
3. Протестировать последовательности различных криптографических генераторов.
4. Оценить полученные результаты и сделать соответствующие выводы о точности реализованного алгоритма.

Методы исследования – а) теоретическое: изучение литературных источников по направлению исследования, анализ полученной информации б) практическое: реализация алгоритма на основе изученной информации, оценка итоговых результатов.

Полученные результаты:

1. Были разработаны алгоритмы нахождения оценки энтропии от математического ожидания, и проанализированы возможности применения этих алгоритмов для различных входных данных.
2. На языке C++ написана программа, проводящая вычисления по разработанным алгоритмам.
3. Программа протестирована на последовательностях двух криптографических генераторов разной степени стойкости. Итоговые значения отображены на графиках.

4. Проведена оценка точности и эффективности используемого алгоритма на основе полученных результатов.

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

ABSTRACT

Diploma thesis: 42 pages, 11 figures, 2 tables, 13 sources, 3 attachments.

Keywords: CRYPTOGRAPHIC GENERATOR; SHENNON, TSALLIS AND RENYI ENTROPY; FREQUENCY ESTIMATORS OF PROBABILITY; TESTING OF HYPOTHESIS; C ++.

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 an algorithm and its software implementation for statistical testing of output sequence of cryptographic generator.

Tasks:

1. Develop algorithms for finding the entropy functional and the corresponding mathematical expectation and variance.
2. Create the most effective 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.

Research methods – a) theoretical: study of literary sources in direction of the research, analysis of received information b) practical: implementation of the algorithm based on the information studied, evaluation of the final results.

Results:

1. Algorithms were developed for finding the estimate of entropy from mathematical expectation, and the possibilities of using these algorithms for various input data were analyzed.
2. In C++ programming language, a program is written that performs calculations according to the developed algorithms.
3. The program was tested on the sequences of two cryptographic generators. The total values are displayed on the graphs.
4. The accuracy and efficiency of the algorithm used are estimated based on the results.

Application area – organizations that use generators of random and pseudorandom sequences of different levels of security.