ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

REVIEWER'S OPINION OF FINAL THESIS

I. IDENTIFICATION DATA

Thesis name:	**Random number generator based on multiplicative convolution transform**
Author's name:	**Nikolai Antonov**
Type of thesis:	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Department of Computer Science
Thesis reviewer:	Enikeev Arslan Ilyasovich, associate professor, Ph.D.
Reviewer's department:	Kazan Federal University, Institute of Computational Mathematics and Informational Technologies, Department of Software Technologies

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **extraordinarily challenging**

Evaluation of thesis difficulty of assignment.

The objective of this work is to create a fundamentally new algorithmic random number generator. This is an extraordinarily difficult task, since a modern generator of this type must satisfy several very strong requirements at once. At first, the output sequences must meet statistical criteria for a sample from a uniform distribution. Secondly, the software implementation of the generator must achieve high performance so that the generator can compete with its hardware counterparts. Finally, an important advantage of the algorithmic generator is the possibility of using it for the purposes of modern cryptography and encryption; therefore, it is required to ensure the non-trivial cracking of the initial state of the generator. The specifics of this task requires the student to have significant knowledge in the field of software engineering: to construct an effective algorithm for generating pseudorandom sequences, to analyze its complexity, create a highly effective software implementation, test it by choosing a modern testing methodology. An additional difficulty of the assignment is the proof or demonstration of the suitability of the generator for the purposes of modern cryptography.

Satisfaction of assignment **fulfilled**

Assess that handed thesis meets assignment. Present points of assignment that fell short or were extended. Try to assess importance, impact or cause of each shortcoming.

The handed thesis fully satisfies the assignment. The constructed conceptual model has a formal mathematical definition and contains a clear algorithm for obtaining pseudo-random output sequences. A precise theoretical estimate of the complexity of the algorithm is given. The software implementation of the algorithm corresponds to the specified generator concept and is characterized by high performance. In the final part of the work, it is demonstrated that the generator is resistant to attempts of cracking the initial state through statistical analysis and the basic methods of linear algebra.

The handed thesis has no significant shortcomings, however a small drawback is contained in the section of the thesis devoted to the demonstration of the statistical and cryptographic properties of the generator. It should be pointed out more explicitly and distinguished which of the studies carried out affect only the statistical properties of the output sequences and which affect the cryptographic strength of the generator itself.

The handed thesis is significantly expanded in the part of assignment connected with the quality of sequences produced by the generator: the conducted studies not only prove the generator's compliance with the NIST standard, but also demonstrate an outstanding quality of pseudorandom sequences by being passed a lot of tests from the DIEHARDER package.

Method of conception **correct**

Assess that student has chosen correct approach or solution methods.

The proposed concept of a multiplicative convolution operator has correct mathematical definition. The algorithm for obtaining pseudo-random bits presented in the work can be completed in a finite time, and the resulting bit sequence satisfies the properties of a sample from a uniform distribution. The study of algorithmic complexity is correct and very detailed. The software implementation of the generator is effective both in runtime and in memory used. Studies and experiments related to the statistical and cryptographic properties of the generator contain all the necessary data for their reproduction and are completely correct.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

REVIEWER'S OPINION OF FINAL THESIS

Technical level **A - excellent.**

Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by experience.

The handed thesis demonstrates the student's knowledge in several areas of mathematics and software technologies at once: knowledge of programming languages and software engineering methodology, possession of information from the theory of numbers, mathematical statistics, coding theory and cryptography. The information contained in the introduction of the thesis, as well as in the section affecting software implementation, demonstrates the student's ability to work with expert literature.

Formal and language level, scope of thesis **B - very good.**

Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.

The work is absolutely correct from a mathematical formal point of view. The work is correctly arranged, there are small number of language inaccuracies that make it difficult to perceive the work

Selection of sources, citation correctness **B -very good.**

Present your opinion to student's activity when obtaining and using study materials for thesis creation. Characterize selection of sources. Assess that student used all relevant sources. Verify that all used elements are correctly distinguished from own results and thoughts. Assess that citation ethics has not been breached and that all bibliographic citations are complete and in accordance with citation convention and standards.

Citation ethics is respected; the links to sources are placed correctly. The used sources are relevant. A small drawback is that most sources have a certain limitation period.

Additional commentary and evaluation

Present your opinion to achieved primary goals of thesis, e.g. level of theoretical results, level and functionality of technical or software conception, publication performance, experimental dexterity etc.

Creating a high-quality random number generator is quite worthy of becoming the goal of research for a Ph.D. thesis, but Nikolai chose this topic for his master's thesis. The task is extraordinary and very ambitious. It is my opinion that Nikolai did an excellent job. Firstly, to solve the problem, he introduced the concept of a fundamentally new algebraic operator, the multiplicative convolution. The idea of using the order numbers of register cells to enhance its cryptographic strength is incredibly interesting and seems promising. Secondly, it is important to note the high efficiency of the created software implementation: the speed of the program with the proper settings of the compiler allows to encrypt the information signal at maximum communication speeds of 4G technology. Finally, the material presented in the thesis as a whole makes a very positive impression and indicates a large amount of work done.

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

1. Is it possible to implement the concept of the generator on super-long registers, using parallel programming technologies?

2. The length of the generator's register is limited to a prime number of a special form. How many of such primes are among the first hundred, first thousand, first million of natural numbers?

I evaluate handed thesis with classification grade **A - excellent.**

Date: **4.6.2020** Signature: