ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

REVIEWER'S OPINION OF FINAL THESIS

I. IDENTIFICATION DATA

Thesis name:	**Implementation of Goldwasser-Kilian primality test on elliptic curves**
Author's name:	**Marat Gimadiev**
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Department of Computer Science
Thesis reviewer:	Roustam Latypov
Reviewer's department:	Kazan Federal University, Institute of Computational Mathematics and Information Technologies, Department of Data Analysis and Operations Research

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment — **challenging**

Evaluation of thesis difficulty of assignment.

Modern systems with a public key are based on elliptical cryptography and on practical impracticability of solving the factorization problem in the modern state of algorithmics (without a quantum computer, which is not clear when will be built). In this case, the problem arises of generating large prime numbers. An attempt was made to improve perfomance of primality test based on modern cryptographic tools in the master's thesis "Implementation of Goldwasser-Kilian primality test on elliptic curves" submitted by Marat Gimadiev. The idea of using the Shanks-Mestre algorithm in Goldwasser-Kilian primality test, as I understand, is quite original.

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 randomness of the final test reduces the significance of the obtained result. However, obtaining deterministic test for primality with complexity (ln n)^k for k close to three is an open problem and it would be unreasonable to require this from student.

Method of conception — **correct**

Assess that student has chosen correct approach or solution methods.

The material presented in the paper testifies to the author's understanding of the topic under consideration.

Technical level — **C - good.**

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

The paper does not show the result of testing for large integers. For the experimental substantiation of the proposed test, it is required to research not only average behavior of the algorithm, but also more complete statistics on the probability distribution of the behavior of the algorithm.

Formal and language level, scope of thesis — **C - good.**

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

Historically, the Solovay-Strassen test was developed earlier than Miller-Rabin test, so the relevant subsections could be rearranged. In addition, Legendre symbol is used in the first test and it would be better to give its definition earlier, and not later, when it was needed while implementation of the algorithms by the author. The text is well written, however algorithms, which were described, are not aligned well.

Selection of sources, citation correctness — **C - 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.
List of sources is not well formed. Author could have cited recently published works.

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.
In general, the content of the master's thesis is consistent with the assignment.
The remarks, which were made, do not affect to the main points of the work and do not reduce its value. I think that the work deserves mark "good", and Marat Gimadiev deserves to award master's degree.

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

Summarize thesis aspects that swayed your final evaluation. Please present apt questions which student should answer during defense.

- *Why haven't you included results of experiments for large numbers?*

I evaluate handed thesis with classification grade **C - good.**

Date: **4.6.2018** Signature: