OPINION

by Prof. Dr. Stoyan Nedkov Kapralov

Technical University - Gabrovo,

regarding

the dissertation of Miroslav Tsvetkov Markov

"Efficient Algorithms with Application to Cryptography

with public key and coding theory"

presented for the acquisition of the educational and scientific degree "doctor"

in the field of higher education 4. Natural sciences, mathematics and informatics

professional direction 4.6. Informatics and Computer Science

doctoral program Informatics

This opinion is written on the basis of Order No. 208/18.07.2024 of the Director of IMI BAS and on the decision of the first meeting of the scientific jury on the procedure.

1. Data on the doctoral studies

Miroslav Markov was enrolled in full-time doctoral studies at the IMI of the BAS in 2019. In 2022, he was dismissed with the right of defense.

On 26.06.2024 a preliminary discussion of the presented dissertation work was held.

2. Structure of the dissertation

The dissertation consists of 12 preliminary pages and 75 pages of main text.

Preliminary pages contain a statement of originality, acknowledgments, table of contents, list of tables, list of abbreviations.

The main text consists of a Summary, an Introduction, three chapters, a Bibliography, two appendices, lists of dissertation reports and publications.

3. Relevance of the researched problem

The use of elliptic curves in cryptography was proposed about 60 years ago, and in the last 20 years, research and practice in this field has seen an extraordinary flourishing.

The main advantage of elliptic curve cryptography, compared to traditional public key cryptography, is to provide a similar level of protection, but with shorter keys.

The number of points on an elliptic curve over a finite field is an important parameter on which the security, key size, and performance of a cryptographic system depend.

Reed-Mahler codes are an important class of codes in coding theory used to correct errors when transmitting information over a noisy channel. These codes are widely used in a variety of applications, including communication systems and space missions, where reliability of transmitted information is critical.

The dissertation is dedicated to research in two topical areas: 1) determination of the number of points on elliptic curves of two families; 2) calculate the weight distribution of the binary Reed-Muller code R(4,9).

4. Content and contributions of the dissertation

At the beginning of the dissertation, the purpose of the research is formulated, as well as the specific tasks to be solved.

Chapter 1 – "Method for counting points on elliptic curves of the type $y^2 = x^3 + a \ (mod\ p),\ a \neq 0$" consists of five sections. Sections 1.3 and 1.4 are the main ones.

A description of the method is presented in Section 1.3, and examples are given in Section 1.4.

Chapter 2 is devoted to the study of elliptic curves of the type $y^2 = x^3 + ax \ (mod\ p),\ a \neq 0,$ and the structure of Chapter 2 is similar to that of Chapter 1.

The exposition in these two chapters demonstrates the author's high mathematical erudition as well as his expertise in algorithm construction and analysis.

I accept the scientific contributions, regarding Chapter 1 and Chapter 2, formulated by the author in the Author's Reference for the contributions in the dissertation work, namely, explicit formulas for the order of curves from two families have been obtained. As scientific-applied contributions in these chapters, the development of efficient algorithms for simultaneous calculation of the possible series associated with curves from the studied families can be indicated.

In Chapter 3, with the application of a multi-step strategy, a new result was obtained – the weight distribution of the R(4,9) binary Ried-Mahler code was calculated. Only the description of the approach and the implementation of the individual steps takes up more than 20 pages.

It is worth noting that the study is based on the latest results of other authors published in 2023.

The result is the impressive Table A3.

5. Publications on the dissertation work

A total of 4 publications are presented on the dissertation. The publications are in English. One of the publications is an article in an international scientific journal, and the other three are reports at international conferences. All publications are co-authored with the supervisor.

In terms of volume and quality, the publications meet the minimum requirements for obtaining the educational and scientific degree "doctor".

Some of the results in the publications have previously been reported at national and international workshops.

Data on observed citations of the dissertation publications are not presented.

6. The PhD-Thesis-Summary correctly reflects the content of the dissertation.

7. Notes on the dissertation work

I have no critical notes.

8. Conclusion

Having familiarized myself with the dissertation work presented in the procedure and the accompanying scientific works and based on the analysis of their significance and the scientific and scientific-applied contributions contained in them, I give my positive assessment and confirm that the presented dissertation work and scientific publications to it, as well as the quality and originality of the results and achievements presented in them, meet the requirements of ZRAS in the Republic of Bulgaria, the Regulations for its application and the relevant regulations of IMI and BAS for the candidate's acquisition of the educational and scientific degree "doctor" in field of higher education 4. Natural sciences, mathematics and informatics, professional direction 4.6 Informatics and computer sciences.

The candidate satisfies the minimum national requirements in the professional direction and no plagiarism has been found in the scientific papers submitted under the procedure.

Based on the above, I strongly recommend the scientific jury to award Miroslav Tsvetkov Markov the educational and scientific degree "Doctor" in the field of higher education 4. Natural sciences, mathematics and informatics, professional direction 4.6 Informatics.

11.08.2024 **Signature:**

/Prof. DSc Stoyan Kapralov/