OPINION

on the procedure for receiving educational and scientific degree "Doctor" (PhD) in field of higher education: 4. Natural Sciences, Mathematics and Informatics, professional field: 4.6 Informatics and computer sciences.

Author: Miroslav Tsvetkov Markov, PhD student in department Mathematical Foundation of Informatics, IMI – BAS.

Dissertation: Efficient Algorithms with Application to Public Key Cryptography and Coding Theory.

The opinion was prepared by Assoc. Prof. PhD, Zlatko Georgiev Varbanov, Faculty of Mathematics and Informatics, University of Veliko Tarnovo, field of higher education 4. Natural Sciences, Mathematics and Informatics, in my capacity as a member of the Scientific Jury according to Order No. 208/18.07.2024 of the Director of IMI-BAS and decision of the Scientific Jury (Protocol 1/24.07.2024).

1. General characteristics of the dissertation and the presented materials

In the dissertation, efficient algorithms are developed and presented for determining the number of points on elliptic curves over a prime field (two specific families of elliptic curves are considered) and for calculating the weight distribution of the binary Reed-Muller code $R(4,9)$. For each of the algorithms presented in Chapters 1 and 2, a performance comparison is made, showing that these algorithms significantly improve the performance of the known algorithms. In Chapter 3, the calculation of the weight distribution of the binary R(4,9) Reed-Muller code is performed, first demonstrating an experiment using Gleason's theorem and showing that there are quite a few problems and difficulties in doing so, so in the next section the Sarwate method has been used, by which the result is already obtained. Appendix A contains tables describing the weight distribution.

The presented dissertation consists of 74 pages in general. It contains an introduction, three chapters, conclusion, list of author's contributions, bibliography, list of publications and two applications A and B.

2. Data of the candidate

Miroslav Markov graduated with a master's degree in "Communication and security technology and systems" in 1996 at TU-Sofia and an additional bachelor's degree in "Mathematics and Informatics" in 2006 at Sofia University. From April 1992 to March 2008, he worked in various structures of the Ministry of the Interior. He started working at SANS in the spring of 2008. From August 2022, he works at IMI-BAN.

3. Content analysis of the candidate's scientific and scientific-applied achievements, contained in the presented dissertation and the publications to it, included in the procedure

The introduction contains a presentation of the problems that are solved in the dissertation, as well as a description of the content of the following chapters. At the beginning of each chapter, the theoretical foundations of the development and preliminary results are presented. Chapter 1 is devoted to the development of an efficient deterministic algorithm for calculating the order (number of points) of the family of elliptic curves:

$$E_p = \{E_a: y^2 = x^3 + a \ (mod\ p), a \neq 0\}$$

After an initial presentation (Section 1.2) of the prior knowledge, Section 1.3 sets out the approach to the problem, including improved estimations of the computational complexity for large values of *p*. Section 1.4 contains examples with modulus primes (in one example, *p* is the modulus of the elliptic curve *secp256k1* and in the other the number *p* is specially constructed) and also discusses the results of a program experiment to compare the performance of the proposed algorithmic technique against that of the SEA algorithm in the considered scenario.

Chapter 2 presents a method for counting points on elliptic curves of the type:

$$D_p = \{D_a: y^2 = x^3 + ax \ (mod\ p), a \neq 0\}$$

After the introduction and introductory remarks, Section 2.3 describes the approach used in the development. First, an explicit formula for the order of the elliptic curve D_a is given. Then the possible series of curves in the essential case p ≡ 1 (mod 4) are characterized more precisely. The third part of this section considers the computational aspects of counting the points in D_p when *p* is a large prime number. Section 2.4 provides an example of a prime used for modulus in *secp224r1* (NIST specification for 224-bit elliptic curve) elliptic curve parameters. The chapter ends with a summary of the results.

Chapter 3 is entirely oriented to coding theory and in particular to computing the weight distribution of the *R*(4,9) binary Reed-Muller code. Section 3.1 presents the

basic concepts. Section 3.2 presents an attempt to find the weight distribution by Gleason's theorem and the related problems and difficulties. In Section 3.3, the calculation of the weight distribution is performed using Sarwate's method, the computational costs are estimated, and the computer resources used are presented. The conclusion of this chapter summarizes the results.

4. Approbation of the results

The dissertation is written on 4 papers. They are published as follows:

- 1 in proceedings of international conference with SJR and IF;
- 3 in proceedings of international conference referenced in Scopus;

The publication with IF and a quartil Q2 is fully sufficient to fulfill the minimum national requirements (this one give the candidate 75 points, and the publications in the refereed proceedings carries another 3x18 = 54 points). In general, the presented scientific works definitely cover and exceed the minimum national requirements and, accordingly, the additional requirements of the IMI - BAS for the acquisition of an educational and scientific degree "doctor" in the scientific field and professional direction of the procedure.

5. Citations of the candidate's papers

A list with a total of 5 citations of 3 of the candidate's works is presented. Three of the citations are to the publication "Weight Distribution of the Binary Reed-Muller Code $R(4, 9)$". The other two publications cited are "An Approach for Computing the Number of Points on Elliptic Curve $y^2 = x^3+a \pmod p$ via Explicit Formula for That Number Modulo p" and "An Efficient Approach to Point-Counting on Elliptic Curves from a Prominent Family over the Prime Field F_p" .

6. Evaluation of the candidate's contribution to joint publications

The presented publications are co-authored with the PhD student's supervisor. It is clear from the attached documents that the applicant's contribution to the joint publications is indisputable and can be considered to be equal to that of the other co-authors.

7. Quality of the abstract

The abstract give a clear and adequate idea of the content and main results of the dissertation.

8. Conclusion

Having become acquainted with the dissertation thesis presented in the procedure and the accompanying scientific papers and based on the analysis of their significance and the scientific and scientific-applied contributions contained in them, I confirm that the presented dissertation and the scientific publications to it, as well as the quality and originality of the results and achievements presented in them meet the requirements of the Low for the Development of the Academic Staff in the Republic of Bulgaria, the Rules for its Implementation and the corresponding Rules at the IMI - BAS for the acquisition by the candidate of the educational and scientific degree “Doctor” in field of higher education 4. Natural Sciences, Mathematics and Informatics, professional field 4.6 Informatics and computer sciences. In particular, the candidate satisfies the minimum national requirements in the professional field and no plagiarism has been found in the presented dissertation and scientific papers. Based on the above, I recommend the scientific jury to award Miroslav Tsvetkov Markov an educational and scientific degree "doctor" in the field of higher education 4. Natural sciences, mathematics and informatics, professional field 4.6. Informatics and Computer Science.

29.08.2024 г. Signature:

/Assoc. Prof. PhD Z. Varbanov/