# REVIEW

**under the procedure for acquisition of the educational and scientific degree "Doctor" by** candidate **Miroslav Tsvetkov Markov,**
**of the PhD Thesis entitled: "efficient algorithms with application to public key cryptography and encoding theory ",**
In the Scientific field: **4. Natural Sciences, Mathematics and Informatics**
Professional field: **4.6. Informatics and Computer Sciences**

Doctoral program "Data processing and protection methods",
Department "Mathematical foundations of Informatics",
**Institute of Mathematics and Informatics (IMI)**, **Bulgarian Academy of Sciences (BAS).**

The review has been prepared by: **prof. dr. Vladimir Todorov Dimitrov – Faculty of Mathematics and Informatics, Sofia University "St. Kliment Ohridski"**,
as a member of the scientific jury for the defense of this PhD thesis according to Order № 208 / 18.07.2024 of the Director of the Institute of Mathematics and Informatics.

1. **General characteristics of the dissertation thesis and the presented materials**

The following materials are presented for the defense:

1. Application (request) to the Director of IMI-BAA for admission to defense, entry No. 468 / 11.07.2024.
2. Professional CV - European format, 2 pages.
3. Order for enrollment in doctoral studies, No. 239 / 01.07.2019.
4. Passed exam reports, according to the doctoral plan, five passed exam reports in Excel, English, Blockchain technologies, Cryptology, Security of Elliptical Cryptography. All exams were taken with excellent grades.
5. Order for deduction from the doctoral studies, No. 217 / 18.07.2022, with right of defense.
6. Order of the Director of IMI for discussion of the dissertation work from the extended scientific unit of the Mathematical Foundations of Informatics section, No. 172 / 10.06.2024.
7. Minutes of the discussion of the dissertation work by the extended scientific unit of the Mathematical Foundations of Informatics section from 26.06.2024. With a decision on admission to defense.
8. NACID information card – sample 1 and sample 3. Registration of the doctoral student with the topic of the dissertation and publications:

- Borissov, Y. & Markov, M. An Approach for Computing the Number of Points on Elliptic Curve y2 = x^3+a (mod p) via Explicit Formula for That Number Modulo p. In Proceedings of the 2019 Ninth International Workshop on Signal Design and its Applications in Communications, Dongguan, China, 20–24 October 2019, pp. 1–5, Date Added to IEEE Xplore: 23 January 2020, ISSN: 2150-3699 (electronic). https://doi.org/10.1109/IWSDA46143.2019.8966127 - 18 точки.
- Borissov, Y. & Markov, M. An Efficient Approach to Point-Counting on Elliptic Curves from a Prominent Family over the Prime Field Fp, Mathematics 2021, 9(12), 1431, ISSN: 2227-7390, https://doi.org/10.3390/math9121431 - 75 точки от IF (Q1).

9. List of dissertation publications:
    1. Borissov, Y. & Markov, M. An Approach for Computing the Number of Points on Elliptic Curve $y^2 = x^3+a$ (mod p) via Explicit Formula for That Number Modulo p. In Proceedings of the 2019 Ninth International Workshop on Signal Design and its Applications in Communications (IWSDA), Dongguan, China, 20–24 October 2019, pp. 1–5, Date Added to IEEE Xplore: 23 January 2020, ISSN: 2150-3680 (print on demand), 2150-3699 (electronic). https://doi.org/10.1109/IWSDA46143.2019.8966127
    2. Markov, M. & Borissov, Y. Point-Counting on Elliptic Curves Belonging to One Prominent Family: Revisited. In Proceedings of the 2020 Algebraic and Combinatorial Coding Theory (ACCT), Bulgaria, 11–17 October 2020, pp. 106–109, Date Added to IEEE Xplore: 25 March 2021, ISBN: 978-1-6654-0288-0 (print on demand), 978-1-6654-0287-3 (electronic). https://doi.org/10.1109/ACCT51235.2020.9383390
    3. Borissov, Y. & Markov, M. An Efficient Approach to Point-Counting on Elliptic Curves from a Prominent Family over the Prime Field Fp, Mathematics 2021, 9(12), 1431, ISSN: 2227-7390, IF: 2.3 Q1 (2023), SJR: 0.475 Q2 (2023). https://doi.org/10.3390/math9121431
    4. Markov, M. & Borissov, Y. Weight Distribution of the Binary Reed-Muller Code R(4, 9)(4,9). In Proceedings of 2024 The Thirteenth International Workshop on Coding and Cryptography (WCC), Perugia, Italy, 17-21 June 2024, pp. 288–298. https://wcc2024.sites.dmi.unipg.it/WCC_proceedings.pdf
10. List of citations of the dissertation publications. Publication 1 – 1 citation; publication 3 – 1 citation; post 4 – 3 citations.
11. Copies of the dissertation publications - 4 copies according to the presented list.

12. Dissertation work of 87 pages. Content:
    - Title page, 2 pages;
    - Declaration of originality, 2 pages;
    - Acknowledgments, 2 pages;
    - Contents, 2 pages;
    - List of tables, 2 pages;
    - List of abbreviations and acronyms, 2 pages;
    - Summary, 2 pages;
    - Introduction, 6 pages;
    - Chapter 1 Method for counting points on elliptic curves of the form $y^2 = x^3 + a \pmod p$, $a \neq 0$, 20 pages;
    - Chapter 2 Method for counting points on elliptic curves of the form $y^2 = x^3 + ax \pmod p$, $a \neq 0$, 8 pages;
    - Chapter 3 R(4, 9) R(4, 9) binary code weight distribution, 24 pages;
    - Bibliography, 6 pages, 59 publications in the period 1896 – 2024;
    - Appendix A: R(4,9) tables, 4 pages;
    - Appendix B, 2 pages, terminology;
    - Delivered reports on the topic of the dissertation, 2 pages, 6 reports, including 4 publications on the dissertation;
    - Dissertation topic publications, 1 page, 4 publications.
13. Reference for dissertation contributions and dissertation publications.
14. Abstract, 50 pages, in Bulgarian.

## 2. Short CV and personal impressions of the candidate

**Education**: The candidate completed his secondary education in 1987 at 95 EUPU "Vladimir Mayakovsky", Sofia. In 1996, he received a master's degree at the Technical University, engineer in electronics and informatics, majoring in communication and security technology and systems. In 2006, he received a bachelor's degree at the "St. Kliment Ohridski", Mathematics and Informatics.

**Professional career**: From 1992 to 2002, he worked as a team commander in the Special Counter-Terrorism Squad of the Ministry of Internal Affairs. From 2002 to 2008, he was the head of a group at the Directorate for the Protection of Means of Communication at the Ministry of the Interior. From 2008 to 2014, he was the chief expert at the National Security State Agency. From 2022 until now, he is a mathematician at IMI, BAS.

I do not know the candidate personally, nor was I familiar with his work before the pre-defense of this dissertation.

**3. Content analysis of the scientific and applied achievements of the candidate, contained in the presented PhD thesis and the publications to it, included in the procedure**

The dissertation begins with a summary in which the aim and objectives of the research are presented. The goal is the development of efficient algorithmic methods for solving two specific tasks: "Counting the points on elliptic curves" and "Calculating the weight distribution of binary Reed-Muller codes". The problems are in three groups: for the elliptic curves of the family $y^2 = x^3 + a \pmod p$, $a \neq 0$, for the elliptic curves of the family $y^2 = x^3 + ax \pmod p$, $a \neq 0$ and for the binary code of Reed-Muller R(4, 9). In the case of elliptic curves, the derivation of an explicit formula for the order of the curve, the development of an efficient algorithm and a comparative analysis of the efficiency with that of SEA are sought. The task for the binary R(4, 9) Reed-Muller code is to find an efficient algorithm for computing its weight distribution. The summary ends with a brief description of the content of the dissertation.

The Summary is followed by an Introduction in which the main concepts related to the subject of the study are presented - on the counting of points on an elliptic curve and on the weight distribution of Reed-Muller binary codes. Given the specific field of study, this is a good approach. In the individual chapters, the focus is narrowed on the obtained results. This is where the value of elliptic curve based encryption is justified. It should be noted that for quantum computing, this kind of public key encryption is highly relied upon given the proven breakthrough in the traditional approach.

Chapter 1 presents the solution of problems for elliptic curves from the family $y^2 = x^3 + a \pmod p$, $a \neq 0$. A formally explicit formula for the order of the curve is derived. The computational complexity of the resulting formula at fixed $p \equiv 1 \pmod 6$ is evaluated and shown to be almost two orders of magnitude better than that of SEA and one order of magnitude better than Munuera, C. & Tena, J. G. An algorithm to compute the number of points on elliptic curves of j-invariant 0 or 1728 over a finite field. Rendiconti del Circolo Matematico di Palermo 42, pp. 106-116 (1993). The experimental results confirm the theoretical conclusions about rapid action. This is certainly confirmed for SEA, but not for [Munuera, C. & Tena].

Then follows in Chapter 1 an exposition of the algorithms based on the developed formula. The code of the algorithms themselves is published and available on GitHub. Finally, the chapter presents some concrete examples with calculations based on the presented algorithms.

Chapter 2 is dedicated to elliptic curves from the family $y^2 = x^3 + ax \pmod p$, $a \neq 0$. The tasks set on the topic in the study were solved: an explicit formula for the order of the elliptic curve was derived, the complexity of calculation was estimated at $p \equiv 1 \pmod 4$ and an example of the application of the algorithm is given. In fact, the performance comparison is with SEA.

Chapter 3 is about the weight distribution of the R(4, 9) binary code of length 512 of order 4. A theoretical justification of the approach is made. Two calculation algorithms are presented. Two powerful computing platforms were used for the calculation.

The candidate divides the obtained results into two main categories: scientific and scientific-applied contributions.

Scientific contributions:

1. An explicit formula for the order of a curve from the family is derived
   $Ep = \{Ea : y^2 = x^3 + a \pmod p, a \neq 0\}$,
   reduced modulo p.
2. An explicit formula for the order of a curve from the family is derived
   $Dp = \{Da : y^2 = x^3 + ax \pmod p, a \neq 0\}$,
   reduced modulo p.

Scientific and applied contributions:

1. An efficient method has been developed for the simultaneous calculation of the six possible orders associated with the family Ep, for a fixed $p \equiv 1 \pmod 6$. The complexity of this method is $\tilde{O}(\log_2 p)$, which improves the best known algorithmic solution [3] by almost an order of magnitude.
2. An efficient method has been developed for the simultaneous computation of the four possible orders associated with the family Dp, for a fixed $p \equiv 1 \pmod 4$. The complexity of this method is $\tilde{O}(\log_2 p)$.
3. An efficient algorithm for computing the weight distribution of the R(4, 9) binary Reed-Mahler code is developed by combining the approach described in D. V. Sarwate's 1973 PhD thesis [4] with results for Boolean classification functions according to their affine equivalence, published in 2008 in [2] and 2023. in [1].
4. The weight distribution of the binary Reed-Mahler code R(4, 9) is calculated.

References:


1. Gillot, V. & Langevin, P. Classification of some cosets of the Reed-Muller code. Cryptography and Communications 15, 1129–1137. doi:10 . 1007 / s12095 - 023 - 00652-4 (2023).
2. Langevin, P. & Leander, G. Classification of Boolean Quartic Forms in eight Variables in Boolean Functions in Cryptology and Information Security (eds Preneel, B. & Logachev, O. A.) 18 (IOS Press, 2008), 139–147.
3. Munuera, C. & Tena, J. G. An algorithm to compute the number of points on elliptic curves of j-invariant 0 or 1728 over a finite field. Rendiconti del Circolo Matematico di Palermo 42, 106–116 (1993).
4. Sarwate, D. V. Weight enumeration of Reed-Muller codes and cosets Advisors: E. R. Berlekamp and J. D. Ullman. PhD thesis (Princeton University, Princeton, NJ, Aug. 1973).

I accept the presented scientific and scientific-applied contributions, which are supported by relevant references.

**4. Approbation of the results**

The dissertation is formed on the basis of the presented four publications. The results have been published in two other forums in addition to those of the dissertation publications.

Publications [1] and [2] are in IEEE Explore. Publication [3] is in the journal Mathematics with IF and SJR. Publication [4] is among the accepted abstracts of the conference, but has not yet been published.

I checked the reference for available citations of the dissertation publications. Citations to [3] should be reported as indicated in the reference by the name of the identical article in ArXiv, albeit with a different name: M. Markov, Y. Borissov. Computing the Weight Distribution of the Binary Reed-Muller Code R(4, 9), ArXiv, 2023.

In the four submitted publications, the candidate is co-authored with his supervisor, and in two of them he is the first co-author. Equality of contributions can be assumed.

A total of 100 points are required to meet the minimum national requirements for ONS "doctor", and their distribution by groups of indicators is as follows: Group of indicators A - 50 points and group of indicators D - 30 points. From Indicator Group A there are 50 points (dissertation work is presented), and from Indicator Group D according to indicator 7 with publication [3] there are 75 points (25 x 3 from a publication in a publication indexed in WoS from Q1). There are more points on the presented materials and even on the NACID reference, but the minimum national requirements are met.

The scientific works meet the minimum national requirements (according to Article 2b, paras. 2 and 3 of the ADASRB) and, respectively, the additional requirements of BAS and IMI, BAS for the acquisition of an educational and scientific degree "doctor" in the scientific field and professional direction of the procedure .

The results presented by the candidate in the dissertation work and related scientific works do not repeat those from previous procedures for acquiring a scientific title and academic position.

There is no proven plagiarism in the submitted dissertation and scientific works under this procedure.

**5. Qualities of the abstract**

The submitted abstract is 52 pages long with a 35 page abridged content of the dissertation. It presents the results of the research.

The abstract meets the requirements for its preparation, as well as correctly presents the results and content of the dissertation work.

## 6. Critical notes and recommendations

In Chapter 2, examples of calculation based on the obtained theoretical results are given, but nothing is said about the algorithmization and the method of their calculation. Missing post of code used. In fact, the algorithm and code are almost identical to that of Chapter 1.

In Chapter 3, computation algorithms are presented, but a code publication is missing. The reasons for this are not clear.

Publishing the code allows interested readers to check the results obtained.

## 7. Conclusion

Having become acquainted with the PhD thesis presented in the procedure and the accompanying scientific papers and on the basis of the analysis of their importance and the scientific and applied contributions contained therein, **I confirm** that the presented PhD thesis 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 ADAS in the Republic of Bulgaria, the Rules for its Implementation, the corresponding Rules at the Bulgarian Academy of Sciences and the corresponding Rules at the Institute of Mathematics and Informatics in BAS for acquisition by the candidate of educational and scientific degree "Doctor" in the Scientific field 4. Natural Sciences, Mathematics and Informatics, Professional field: 4.6. Informatics and Computer Sciences. In particular, the candidate meets the minimal national requirements in the professional field and no plagiarism has been detected in the scientific papers submitted for the competition.

Based on the above, **I strongly recommend** the scientific jury to award Miroslav Tsvetkov Markov, the educational and scientific degree "Doctor" in the Scientific field 4. Natural Sciences, Mathematics and Informatics, Professional field: 4.6. Informatics and Computer Sciences

Date: 2024, 02 September

Reviewer: .....
/Vladimir Dimitrov, prof. dr./

**ADASRB - Act on Development of the Academic Staff in the Republic of Bulgaria*