STATEMENT REPORT

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 Marinov Dimitrov, part-time PhD student in department Mathematical Foundation of Informatics, IMI – BAS.

Dissertation: Designing Boolean Functions and Digital Sequences for Cryptology and Communications.

The opinion was prepared by **Prof. Dr. Sci. Tsonka Stefanova Baicheva**, Institute of Mathematics and Informatics, BAS, field of higher education 4. Natural Sciences, Mathematics and Informatics, in my capacity as a member of the Scientific Jury according to Order No. 521/2.12.2022 of the Director of IMI-BAS and decision of the Scientific Jury (Protocol 1/06.12.2022).

1. General characteristics of the dissertation and the presented materials

In the dissertation methods for constructing vector Boolean functions and digital sequences with best-to-date values for some of their key parameters are developed. The computer implementations of the developed methods have very good characteristics in terms of used memory and time complexity, and some of them effectively use the possibilities of parallel execution or modern video accelerators. With the developed software, a rich collection of vector Boolean functions used in various applications was analyzed, 8x8 vector Boolean functions composed only of coordinates with nonlinearity 116, binary sequences with small peak sidelobe levels (PSL) and with large merit factor (MF) were constructed. Different strategies have been proposed for spectral analysis of vector Boolean functions for anomaly detection.

The dissertation is written in English, contains 212 pages, 56 of which are an appendix with tables of obtained results. The cited bibliography includes 152 titles.

Miroslav Marinov Dimitrov has presented all the required documents, according to the Low for the Development of the Academic Staff (LDAS) in the Republic of Bulgaria, the Regulations for its implementation and the relevant Regulations for the acquisition of scientific degrees and the occupation of academic positions at IMI, BAS. The submitted documents show that the candidate meets the minimum national requirements of the LDAS in the Republic of Bulgaria.

2. Data and personal impressions of the candidate

Miroslav Marinov Dimitrov graduated with a master's degree in FMI of SU "St. Kliment Ohridski" in 2016. Since 2017 he has been working as an expert in DANS and is a part-time doctoral student at IMI-BAN. He was dismissed with the right of defense by Order No. 619/30.06.2021.

Miroslav Dimitrov had very serious preliminary training on the topic of the doctoral studies, which he significantly enriched and developed during his doctoral studies. He is very motivated, responsible, and because of his good fundamental education in mathematics and informatics, he quickly progress in new research tasks. During his PhD, he participated in 4 prestigious international cybersecurity competitions and took first places, as well as co-authored two chapters of e-textbook CryptoTool Book. He also showed skills to work independently.

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 dissertation consists of an introduction presenting the scientific contributions of the doctoral student, the publications on the dissertation and their citations, five chapters, references and an appendix.

Chapter one is an introduction presenting the various applications of the combinatorial objects studied in the dissertation and their main characteristics, which are relevant for their application in cryptology and communications. The results known so far for these characteristics are summarized and the methods used to obtain them are commented. It is made a brief overview of the content of the next four chapters of the dissertation.

In the second chapter, vector Boolean functions are discussed from the point of view of their application in cryptography. The definitions and notations used in the following sections and chapters are given. The cryptographic properties of a wide range of popular S-boxes are analyzed in detail. Known strategies for constructing S-boxes with good cryptographic properties are summarized and classified into four categories. A special place is devoted to vector Boolean functions constructed using chaos theory and an efficient algorithm is proposed that improves all the results obtained so far. The very important clarification is made that other authors proposing similar constructions only optimize the nonlinearity of the S-box coordinates, ignoring their linear combinations. Thus, the overall nonlinearity of these S-boxes is significantly lower and they are highly vulnerable to linear cryptanalysis. New concepts and characteristics of the S-boxes that allow the formulation of the optimization problem of their nonlinearity as a satisfiability problem that can be solved using SAT solvers are introduced. The proposed algorithm achieves increasing the nonlinearity of the S-box by minimal changes

to its structure, thus the optimization focuses on its weak elements without reducing the good characteristics of the remaining elements. Thus, an 8x8 balanced S-box is built with the average coordinate nonlinearity 116 and total nonlinearity 92.

A third chapter examines a strategy for finding anomalies in S-box structures through the use of spectral analysis. The presence of anomalies may allow S-box creators to implement attacks known only to them, use them for their efficient hardware implementation, or even embed malicious structures in them. A spectral analysis of a large collection of popular S-boxes has been performed and the results are graphically illustrated. It is shown that the spectral analysis process can be automated and applied not only to the linear approximation (LAT) table, but also to other tables such as DDT, ACT, XOR.

In the fourth chapter, the problem for determination the maximum peak sidelobe level (PSL) of a binary sequence with low autocorrelation is considered. Because of their diverse practical applications, these sequences have been widely studied and various methods for their generation have been developed. The optimal PSL values for binary sequences with lengths up to 84 have been determined. In the thesis, a fast and easy-to-implement heuristic algorithm for constructing binary sequences with low PSL values has been proposed. Using the algorithm binary sequences with lengths between 106 and 300 have been investigated. For 95 of them, those with better values than those known so far were found. The algorithm can also be used to construct sequences with lengths greater than 300. A method for constructing sequences with large lengths and small PSL values that has linear time and memory complexities has been developed. The implementation of the method is compared with a collection of algorithms known in the literature, and for all tested lengths, sequences with better PSL values are obtained, in some cases in less than a second. Comparisons are also made for lengths above 2^{12} using m-sequences that have lengths 2^n-1 and for which there are known results. For all tested lengths, for n between 13 and 17, better PSL values were obtained. The problem for finding the lowest PSL value among a given sequence B and all its possible rotations is also considered. It is shown that if some mathematical properties of these sequences are used, the problem can be solved by a perfectly balanced parallel algorithm. By complete search, the optimal PSL values of the m-sequences of lengths 2^n-1 for n=18,19 and 20, as well as for all Legendre sequences, with and without rotation, of lengths up to 432100 were calculated.

The fifth chapter deals with the problem for constructing numerical sequences whose aperiodic autocorrelation is collectively small with respect to some suitable measure. One such measure is the merit factor (MF), and determining the largest MF value for long binary sequences is a task that has been addressed for decades in complex analysis and combinatorial optimization. In this chapter, some properties of skew-symmetric binary sequences are derived and used to reduce from quadratic to linear the memory complexity of known algorithms for constructing such sequences without changing their time complexity. An algorithm that optimizes randomly generated skew-symmetric binary sequences of lengths up to 10^5+1 to those with MF > 5 is proposed. This way, Bernasconi's conjecture that no

stochastic procedure will be created to find binary sequences of length greater than 200 and MF > 5 is disproved. For even lengths, where there can be no skew-symmetric binary sequences, pseudo skew-symmetric binary sequences are introduced with MF values close to those of the skew-symmetric series found by Golay. Sequences generated by using the partition number problem that improve the known MF values for many of the sequences with lengths up to 255 and for all with lengths greater than 255 have also been proposed. The algorithm for constructing such sequences is extremely efficient and in a few hours leads to construction of sequences that would take tens to billions of years with other known algorithms. In the last section of the chapter, a strategy to discover hidden internal connections between the coordinates of an S-box by visualizing the sidelobe levels of all possible linear combinations of the pairs of coordinates composing the S-box is proposed.

4. Approbation of the results

The dissertation is written on 9 papers. They are published or placed on arXiv as follows:

- 6 in international journals with impact factor,
- 1 in a proceedings of international conference referenced in Scopus and IEEE Xplore ,
- 2 in arXiv.

Three of the publications were co-authored with the PhD student's supervisor, and one of them was co-authored with three other co-authors. In the remaining five publications the doctoral student is the only author. Three of them are published in impact factor journals and two in arXiv. In my capacity as the PhD student's supervisor, I consider his contribution to joint publications equal to that of his co-authors. The number and quality of the works on which the dissertation is written are in accordance with the minimum national requirements for obtaining the educational and scientific degree "doctor".

By 20.11.2022, 45 citations of the publications on which the dissertation was written were noticed, with 35 of the citations in journals with impact factor, 5 in international conferences, 4 in dissertations abroad and 1 in a preprint.

5. Quality of the abstract

The author's abstract in Bulgarian is 58 pages long and gives a clear and adequate idea of the content and main results of the dissertation. The abstract in English is 59 pages long and accurately presents the results of the dissertation work and its content.

6. 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 Marinov Dimitrov 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.

10.01.2023 r. Signature:

/Prof. Dr. Sci. T. Baicheva /