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 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 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. 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 Boolean functions, S-boxes and various types of digital sequences applicable in cryptology and modern communications are developed. S-boxes generated using functions from chaotic functions (CF) are analyzed in detail to measure their resistance to linear cryptanalysis. Most of the published papers related to CF consider only the average value of the nonlinearity of the coordinates of the given S-box, ignoring the other components. The proposed two heuristic methods, which started from pseudo-random S-boxes, repeatedly reached S-boxes, which significantly outperform all previously published CF-based S-boxes. Also, there is proposed an efficient algorithm for constructing binary sequences. By this algorithm in the dissertation record-breaking PSL values for binary sequences of lengths between 106 and 300 are reached. By another proposed algorithm MF (Merit Factor) values greater than 5 for binary sequences of lengths up to $10^5 + 1$ are reached.

The presented dissertation consists of 190 pages in general. It contains an introduction, four chapters, conclusion, list of author's contributions, bibliography, list of publications and two Appendices A and B (55 pages).

2. Data of the candidate

Miroslav Marinov Dimitrov graduated with a bachelor's degree of Computer Science in 2009 and master's degree in 2016, both in FMI of SU "St. Kliment Ohridski". Since 2017 he has been working as an expert in DANS and is a part-time doctoral student 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 (noted as Chapter 1) consists of a representation of the problems solved in the dissertation as well as a description of the content of the following chapters. Chapter 2 first contains theoretical foundations and some preliminary results. Here the definitions and notations used further on are included. Section 2.3 consists of an analyze of some well known S-boxes and the next section shows how they can be divided into 4 different types. In the last section of this chapter the S-box nonlinearity optimization problem is presents as a satisfiability problem.

Chapter 3 is devoted to the S-box reverse-engineering. In this chapter a strategy of analyzing various spectra channels to detect hidden patterns and anomalies in popular S-boxes is discussed. It could serve as a more fine-grained extension to the methods discussed by Perrin in his PhD Thesis „Cryptanalysis, reverse-engineering and design of symmetric cryptographic algorithms", 2017 г.

Chapter 4 addresses the PSL optimization problem. PSL is a criteria for finding binary sequences with collectively small aperiodic autocorrelation characteristics. In Section 4.1, a simple and efficient algorithm based on a heuristic search by shotgun hill climbing to construct binary sequences with small peak sidelobe levels is suggested. The algorithm is applied for the generation of binary sequences of lengths between 106 and 300. Then, in Section 4.2, another method (with linear complexity) to generate long binary sequences with low PSL value is proposed. In Section 4.3 different parameters of the evaluation function of the above presented algorithms are considered. Finally, in Section 4.3.3, a well-known computational problem is finding the lowest possible PSL among the set of a binary sequence B, and all binary sequences generated by rotations of B is discussed.

Last chapter deals with the Merit Factor (MF) problem. MF is another criteria for finding binary sequences with collectively small aperiodic autocorrelation characteristics. There are considered some useful mathematical properties that describe the connection between a given skew-symmetric binary sequence and the binary sequence obtained by changing of exactly two elements of the initial sequence. These properties allow to reduce the memory complexity from $O(n^2)$ to $O(n)$. The proposed algorithm reaches MF values over 5 for binary sequences of lengths up to $10^5 + 1$.

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.org.

These six publications with impact factor and quartile Q2 are definitely enough to fulfil the minimum national requirements for obtaining the educational and scientific degree "doctor". Generally, the presented papers cover (and significantly overcome) the minimum national requirements in the professional field 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.

5. Citations of the candidate’s papers

There is presented a list that contains 45 citations of 8 papers of the candidate. Almost half of them (22) are for the publication „On the design of chaos-based S-boxes“. Another publication „Efficient generation of low autocorrelation binary sequences”, is cited 11 times.

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

In five publications the doctoral student is the only author. 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. I consider his contribution to joint publications equal to that of his co-authors.

7. Quality of the abstract

The abstracts (in Bulgarian and English) 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 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.

12.01.2023 г. Signature:
/Assoc.Prof. PhD Z. Varbanov/