STATEMENT REPORT

under the procedure for public defence of the Ph.D. Thesis entitled:
”Designing Boolean Functions and Digital Sequences
for Cryptology and Communications”
under the procedure for acquisition of the educational and scientific degree ”Doctor”
by Miroslav Marinov Dimitrov

In the Scientific field: 4. Natural Sciences, Mathematics and Informatics,
Professional field: 4.6. Informatics and Computer Science,
Doctoral program: ”Informatics”,
Department: ”Mathematical Foundations of Informatics”,
Institute of Mathematics and Informatics (IMI),
Bulgarian Academy of Sciences (BAS).

The statement report has been prepared by Prof. Maya Miteva Stoyanova, Ph.D., Deputy Dean of the Faculty of Mathematics and Informatics, Sofia University ”St. Kliment Ohridski”, Department of ”Algebra”, 4.5. Mathematics (RAS), in my capacity as a member of the Scientific jury, according to Order 521/02.12.2022 of the Director of the IMI, BAS, and decision of the Scientific jury (Protocol 1/06.12.2022).

1 General characteristics of the dissertation thesis and the presented materials

The presented Ph.D. thesis is in English and has 212 pages long. It consists of an introduction, four chapters, 2 parts - appendices and a bibliography of 152 titles. The (extended) abstract in Bulgarian, within 59 pages, summarizes the content of the dissertation, clearly and accurately reflecting both the main contributions of the Ph.D. student and where the results are tested. The dissertation is based on results published in seven publications and two submitted for publication and available in the arXiv preprints. The materials and documents presented by Ph.D. student Miroslav Dimitrov certify that all the requirements of the Act on Development of the Academic Staff in the Republic of Bulgaria (ADAS in the Republic of Bulgaria) and its regulations have been met. It is evident from the publications of Miroslav Marinov Dimitrov that he fulfills and repeatedly exceeds the minimum national requirements under Art. 2b. para. 2 and para. 3 of the ADAS in the Republic of Bulgaria for the acquisition of an educational and scientific degree ”Doctor”.

2 Short CV and personal impressions of the candidate

I have known Miroslav Dimitrov and his scientific work from the National Seminar on Coding Theory ”Prof. Stefan Dodunekov”. I have known from personal conversations with his supervisor Prof. D.Sc. Tsonka Baicheva that they have an excellent professional working relationship as supervisor and Ph.D. student, which is also evident from the joint scientific results presented by them (in the Ph.D. thesis of M. Dimitrov).

Miroslav Dimitrov obtained the Bachelor’s degree at the Faculty of Mathematics and Informatics of Sofia University ”St. Kliment Ohridski”, majoring in Mathematics in 2009. In 2016, he acquired the Master’s degree at the FMI of Sofia University, master’s program ”Protection of information in computer systems and networks”. Since 07.05.2017 he has been enrolled as a part-time Ph.D. student in the doctoral program ”Informatics”, Department MOI, IMI, BAS. By Order 619/30.06.2021, he was assigned the right of defence. From 2017 to the present, Miroslav Dimitrov is an expert at the DANS in the Republic of Bulgaria.

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

The present Ph.D. thesis examines various strategies for construction and analysis of Boolean functions, S-boxes and digital sequences are proposed.

In the second chapter, the necessary definitions and notations are included, and some popular S-boxes generated by using chaotic functions (CF) are analyzed to measure their actual resistance to linear cryptanalysis. In Chapter 3, a strategy of analyzing various spectra channels to detect hidden patterns and anomalies in popular S-boxes is discussed. Chapter 4 addresses the PSL optimization problem. Chapter 5 deals with the Merit Factor (MF) problem.

The main scientific contributions of Ph.D. student Miroslav Dimitrov in the presented Ph.D. thesis are:

1. A rich collection of popular S-boxes is analyzed in great detail. It is shown that the majority of chaos-based S-boxes are vulnerable to linear cryptanalysis. A simple and lightweight algorithm is proposed, which significantly outperforms all previously published chaos-based S-boxes, in those cryptographic terms, which they utilize for comparison.

2. By introducing some new definitions like couplings, coordinate decomposition, degree of descendibility, and CELAT, the S-box nonlinearity optimization problem is projected to a satisfiability problem, which could be attacked by using SAT solvers. By applying the SAT solver it is shown that 8×8 bijective S-boxes with all eight coordinates having the nonlinearity value of 116 do exist.

3. A strategy of analyzing various spectra channels to detect hidden patterns and anomalies in S-boxes is proposed. A simple and efficient algorithm based on a heuristic search by shotgun hill climbing to construct binary sequences with small peak sidelobe levels (PSL) is proposed. The algorithm successfully revealed binary sequences of lengths between 106 and 300 with record-breaking PSL values. An improvement of the aforementioned algorithm is proposed to reduce the time complexity and required memory to linear values. The modifications made allow record PSL values to be reached in less than a second, even with lines of greater length.

4. A detailed comparison and fine-grain analysis of the proposed algorithms is performed. By using the insights of this analysis, a heuristic algorithm is proposed, which successfully reached all the optimal PSL values known in the literature, which was previously discovered by an exhaustive search.

5. A GPU efficient algorithm addressing the well-known computational problem of finding the lowest possible PSL among the set of a binary sequence B and all binary sequences generated by rotations of B is proposed. The problem is projected to a perfectly balanced parallelizable algorithm. By using the algorithm, the search space of all m-sequences with lengths $2^n - 1$, for $n = 18, 19, 20$ is successfully exhausted. Furthermore, a complete list of all PSL-optimal Legendre sequences for lengths up to 432100 is revealed. A conjecture is made, that all PSL-optimal Legendre sequences, with or without rotations, and with lengths N greater than 235723, are strictly greater than $\sqrt{N}$.

6. Some useful mathematical properties related to the flip operation of the skew-symmetric binary sequences are discovered, which could be exploited to significantly reduce the memory complexity of state-of-the-art stochastic Merit Factor (MF) optimization algorithms from $O(n^2)$ to $O(n)$ without affecting the timing their complexity. As a proof of concept, a lightweight algorithm was constructed, which could optimize pseudo-randomly generated skew-symmetric binary sequences with long lengths (up to $10^5 + 1$) to skew-symmetric binary sequences with a MF greater than 5. This contradicts the Bernasconi's conjecture, that a stochastic search procedure will not yield MF higher than 5 for long binary sequences (sequences with lengths greater than 200).

7. A new class of finite binary sequences with even lengths with alternate autocorrelation absolute values equal to 1, called pseudo skew-symmetric class, is found. It is

shown that the MF values of the new class are closely related to the MF values of adjacent classes of Golay's skew-symmetric sequences. Sub-classes of sequences based on the partition number problem, as well as the notion of potentials, measured by helper ternary sequences, are proposed. Binary sequences with MF records for binary sequences with many lengths less than 225, and all lengths greater than 225, are revealed. Two extremely hard search spaces of lengths 573 and 1009 are also attacked. It was estimated that a state-of-the-art stochastic solver requires respectively 32 and 46774481153 years to reach MF values of 6.34, while the required time from the proposed algorithm to reach such MF values is just several hours. Using aperiodic autocorrelation functions for the S-box reverse engineering problem is proposed.

The results presented above give me reason to claim that the candidate Miroslav Marinov Dimitrov has in-depth knowledge of the Ph.D. thesis, and that his original contributions are more than sufficient to acquire the educational and scientific degree "Doctor".

4 Approbation of the results

From the presented documents it is evident that Ph.D. student Miroslav Dimitrov has designed his PhD thesis on the basis of results published in seven publications and two submitted for publication and available in the arXiv preprint. Three of the publications are standalone, as are the two preprints. Of the remaining four publications, three are co-authored by his scientific supervisor Prof. D.Sc. Tsonka Baicheva and Nikolay Nikolov, Ph.D., and the last publication is co-authored by M. Iliev, N. Nikolov and B. Bedjev. Two of the papers published in 2020 are in IEEE Signal Processing Letters, IF : 3.109 (2020) and second quartile Q_2 (2020) in Web of Science, which (according to the Regulations for the Application of ADAS in the Republic of Bulgaria in Professional field 4.6 Informatics and Computer Science) bring the candidate 60 points each; three of the papers, published as follows: one in 2020 and two in 2021, are in IEEE Access, IF : 3.367 (2020) and second quartile Q_2 (2020) in Web of Science and IF : 3.476 (2021) and second quartile Q_2 (2021) in Web of Science, respectively earning the candidate 60 points each; the sixth publication of 2020 is in IEEE Communications Letters, IF : 3.436 (2020) and second quartile Q_2 (2020) in Web of Science and earns the applicant 60 points; the seventh publication is in the proceeding of the 2020 International Conference on Information Technologies (InfoTech) volume, which is referenced in Scopus and IEEE Xplore and carries 18 points. As a result, with a total of 378 points (if 30 points are needed), the candidate Miroslav Dimitrov covers and repeatedly exceeds the minimum national requirements under Art. 2b, para. 2 and 3 of the ADAS in the Republic of Bulgaria, required for the acquisition of the educational and scientific degree ”Doctor” in Professional field 4.6. Informatics and Computer Science. I have no information and no suspicions of plagiarism in the presented Ph.D. thesis and scientific papers on this procedure. There are 45 citations to the publications so far.

5 Qualities of the abstract

The presented abstracts, respectively in Bulgarian and in English, are 59 pages long, both of which are prepared according to all requirements and correctly reflect the content of the Ph.D thesis and the scientific contributions of the Ph.D. student.

6 Critical notes and recommendations

I have no critical notes.

7 Conclusion

Having become acquainted with the Ph.D. 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 give my positive rating and confirm** that the presented Ph.D. thesis and the scientific publications to it, as well as the quality and originality of the results and achievements presented in them, fulfils the requirements of the ADAS in the Republic of Bulgaria, the Rules for its Implementation and the corresponding Rules at IMI and 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 Science. 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 to Miroslav Marinov Dimitrov, the educational and scientific degree ”Doctor” in the Scientific field: 4. Natural Sciences, Mathematics and Informatics, Professional field: 4.6. Informatics and Computer Science, Doctoral program: ”Informatics”, Department MOI, IMI, BAS.

January 10, 2023
Sofia

Signature:
Prof. Maya Stoyanova, Ph.D.