Dr. Smile Markovski, Full Professor
Faculty of Computer Science and Engineering,
Ss Cyril and Methodius University, Skopje, Macedonia

O P I N I O N

for the dissertation

New Heuristic Methods for Generation of Bijective S-boxes with Good Cryptographic Properties

submitted by **Georgi Velkov Ivanov**,

employed at "Орган по криптографска сигурност" in Sofia, Bulgaria, for obtaining degree

Doctor of informatics at the Institute of Mathematics and Informatics of BAS

The dissertation has 129 pages and it is written in very well English, with quite readable text. Its structure consists of Keywords, Abstract, List of 16 included Tables, Published Papers and 7 chapters. The first three chapters are introductory and survey chapters. The main contributions of the dissertation are presented in the fourth and the fifth chapter. The conclusion is given in the sixth chapter and in the seventh chapter 21 different types of (8×8) bijective S-boxes are presented.

The motivations, objectives, outcomes and the structure of the thesis are given in Chapter 1 – Introduction.

Chapter 2 reviews Boolean functions theory and S-box theory. It is given a survey of several properties of the Boolean functions and the S-boxes that will be used further on in the text: representations, characteristics and the cryptographic properties of Boolean functions (balanceness, nonlinearity, avalanche effects and correlation immunity), affine transformations, invariance analysis, bent and plateaued Boolean functions, and others; S-box representations and types, S-box characteristics, linear and differential cryptanalyses on S-boxes, correlation attacks, S-box regularity, S-box nonlinearity, S-box algebraic degree, resiliency, almost bent S-boxes, and others.

S-box generation methods are presented in Chapter 3. Here are given generations of S-boxes by using pseudo-random number generators, algebraically based constructions and those based on heuristic techniques: Hill Climbing Method, Simulated Annealing Method, Genetic Algorithms and Immune Algorithms. By a comparative analysis the good and weak points of each method are considered.

The main results of the dissertation are given in Chapter 4. Here five new heuristic methods for generation of bijective S-boxes are presented: three reverse genetic algorithms (RGA 1, RGA 2 and RGA 3) and two special immune algorithms (SIA 1 and SIA 2). Descriptions and pseudo-codes of all of the algorithms are provided. They are based either on

a genetic algorithm working in a reverse way or on a special immune algorithm, both aiming at rapidly producing large sets of cryptographically strong bijective S-boxes of each possible dimensions between (6×6) and (16×16).

A lot of experiments are made in order to evaluate the performances of the proposed heuristic algorithms. The obtained experimental results are given in Chapter 5 for the S-boxes of dimensions (n×n), n = 8, 10, 12, 14 and 16. A comparison is performed between the results, obtained by both of the methods as well as between all variants within each specific method.

In Chapter 6 conclusions, separated in three parts, are given: thesis summary, thesis contribution and future directions. The objectives that have been set are considered and their respective level of fulfillment in accordance to the obtained results is discussed. Five modifications of the algorithms, promising for obtaining better results, are proposed.

The results of the dissertation "New Heuristic Methods for Generation of Bijective S-boxes with Good Cryptographic Properties" of G. V. Ivanov are presented to scientific community in four published papers and with talks given at several conferences. The fact that already there are 9 citations of the obtained results proves that they are wider accepted and verified.

The author provided a summary on 30 pages where all of the achievements of the thesis are completely presented.

Conclusion: The topic of the dissertation are the so called S-boxes, which are one of the main crypto primitives for building suitable strong cryptographic products. An S-box is a vector valued Boolean mapping with a role to produce confusion during the encryption process. For that aim an S-box have to have several properties that will provide the needed protection against cryptanalyses. Consequently, finding new methods for generation such S-boxes is important of both theoretical and practical aspects.

The presented five new heuristic algorithms in the thesis allow to be generated several thousands of S-boxes of dimensions between (6×6) and (16×16). Many of them are with suitable cryptographic properties for building secure ciphers. The obtained S-boxes of dimension (16×16) open new research problems, and it is a challenge for further investigations how they can be effectively applied.

The dissertation "New Heuristic Methods for Generation of Bijective S-boxes with Good Cryptographic Properties" submitted by G.V. Ivanov gives worthy contribution in the part of the cryptography where S-boxes as crypto primitives are considered. It should be emphasizes that in both part of the dissertation, the introductory and survey part (Chapters 1, 2 and 3) and the part with achievements (Chapters 4, 5 and 7), the presentations are complete, clear and readable.

Having in mind the above considerations, it is a pleasure of mine to support Georgi Velkov Ivanov for obtaining the degree Doctor of informatics and computer science.

In Skopje,
23. 12. 2016.

Smile Markovski