OPINION

by Professor Eng. Rossen St. Iliev, PhD,
"Prof. Tsvetan Lazarov" Defence Institute,
1592 Sofia, 2 "Prof. Tsvetan Lazarov" Blvd, tel.: 02 92 21821,

member of the scientific jury of the dissertation work of

Eng. Andrey Georgiev Ivanov

on the topic

"Analysis of the stability of cryptographic systems with public key"

for the acquisition of an educational and scientific degree "doctor" in the doctoral program "Automated systems for information processing and management", professional direction 5.2 "Electrical engineering, electronics and automation", field of higher education 5. "Technical sciences"

Supervisor: **Col. Assoc. Prof. Dr. Nikolai Todorov Stoianov**

1. Relevance and significance of the developed scientific problem

The dissertation examines an actual problem related to the algorithms and approaches of public cryptography applied in practice, evaluation of the degree of their resistance to attacks and the degree of vulnerabilities. It is clear from the goal formulated in the dissertation that it proposes decision models for checking the stability of operation of cryptographic systems based on the RSA encryption algorithm.

The dissertation is structured with an introduction, three chapters, a conclusion, references, a list of publications related to the dissertation, a list of used terms, mathematical notations and basic functions, a list of figures, in a total volume of 144 pages, with the appendices. The indicated bibliography is from 114 sources, mostly in English from the field of the dissertation work. The list of publications related to the dissertation includes three joint publications with its supervisor, one of which is in the Springer edition.

The content of the dissertation fully corresponds to the topic of the dissertation. It is a useful study of mathematical and algorithmic foundations of public cryptography with the proposal of two models for achieving greater efficiency and reliability of the result in determining the divisibility of a number using the probabilistic Miller-Rabin algorithm, as well as for more an efficient implementation of the Silver-Pohlig-Hellman algorithm, which implements attacks on the most widely used cryptographic algorithm in public cryptography. The presented decision model for determining the divisibility of numbers enables to improve the evaluation of the generated keys for cryptographic systems based on RSA.

2. Evaluation of the scientific results and the contributions of the dissertation work

The dissertation work of Engineer Andrey Ivanov has been developed in the necessary volume and completeness, and from its content it is clear that the author is very well acquainted with the problem area and with the possibilities for solving the research tasks. The formulated results in the dissertation are a logical consequence of the carried out scientific and applied research, including the necessary models and mathematical apparatus for their description. Of interest is the presented approach for creating a kleptographic algorithm with a description of its practical implementation, generation of public key domains and the presented verification of the achieved results through a comparative analysis with other existing kleptographic algorithms. A mathematical apparatus and a practical solution for the creation of a kleptographic algorithm for attacking RSA-based cryptographic systems are also proposed.

I accept the results defined by the author as the development and enrichment of existing knowledge and the application of scientific achievements to solve important practical tasks related to increasing the protection of information and the stability of cryptographic systems with public keys. I believe that the dissertation work and the results obtained in it are the personal work of Engineer Andrey Ivanov and are a consequence of his high theoretical training, as well as his active activity in conducting relevant scientific research and practical implementations.

I have not noticed any plagiarism in the author's work. The style of presentation and the logical sequence of his speech give me confidence about the indisputable personal participation of Engineer Andrey Ivanov in the contribution part of the dissertation.

The abstract corresponds to the dissertation work and adequately reflects the results achieved by the author.

3. Critical notes

I have no significant critical comments on the dissertation work and the abstract. I am familiar with the initial version of the dissertation presented at the preliminary defence and I am happy to note that a large part of my recommendations and those of my colleagues have been taken into account. Although the achieved results could have been more clearly formulated, this in no way reduces the quality of the presented dissertation work.

I recommend the author to continue his further work on the ideas that arose during the writing of the dissertation and to direct his future research into more concrete practical implementations, publishing their results in prestigious scientific publications.

4. Conclusion

I know Engineer Andrey Ivanov as a doctoral student at the Defence Institute. My personal impressions are that he is a very good and consistent researcher, with extensive professional experience in the field of cryptography and information security, showing great diligence and establishing his own style in conducting research studies in the field of his scientific interests.

The developed dissertation work of Eng. Andrey Ivanov is a completed scientific study on a current and important problem and in terms of content, volume and structure it fully meets the requirements provided for in the Law on the Development of the Academic Staff of the Republic of Bulgaria (ZRASRB) for the awarding of the educational and scientific degree "doctor".

5. Evaluation of the dissertation work

From the content of the dissertation, the author's abstract, the fulfillment of the procedural requirements for compliance with the ЗРАСРБ, as well as my personal impressions, gives me the reason to give a POSITIVE ASSESSMENT of the dissertation work "Analysis of the stability of cryptographic systems with public key" and I offer to the author, Andrey Georgiev Ivanov, to award the educational and scientific degree "doctor", in the field of higher education 5 "Technical sciences", professional direction 5.2 "Electrical engineering, electronics and automation".

Jury member: ..../S/.............

08.02.2022 (Professor Eng. Rosen Iliev, PhD)