MINISTRY OF DEFENSE

DEFENSE INSTITUTE „PROFESSOR TSVETAN LAZAROV”

Sofia 1592, bul. „Prof. Tsvetan Lazarov” № 2, fax: 02/92 21 808, http://di.mod.bg

OPINION

by Professor. STOYAN GEORGIEV DENCHEV, D.Sc.

STATE UNIVERSITY FOR LIBRARY STUDIES AND INFORMATION TECHNOLOGIES

of dissertation for awarding educational and scientific degree “Doctor of Philosophy”

on the topic:

“The Resilience Analysis of Public Key Cryptographic Systems”

PhD candidate:

eng. Andrey Georgiev Ivanov

in Doctoral program

Automated systems for processing information and management

professional field

5.2 Electrical engineering, electronics and automation

Thesis supervisor: **col. assoc. prof. PhD Nikolai Todorov Stoianov**

Sofia

January 22, 2023

1. **General description of the submitted materials.**

The materials presented for evaluation (Dissertation and Abstract) meet the requirements of the Law on the Development of the Academic Staff, its Regulations, and the Regulations of the "Professor Tsvetan Lazarov" Defense Institute for its application, in order to obtain the scientific and educational degree of "Doctor".

The dissertation is structured in the following traditional and comprehensive manner: Introduction, three (3) Chapters, Conclusion, Used Literature, List of Publications related to the dissertation, List of Used Terms, Mathematical Notations and Basic Functions, and List of Figures, with a total of 144 pages.

The dissertation includes 10 figures and 25 described algorithms. The list of used literature contains 114 sources.

2. **Relevance and significance of the research.**

The materials presented for discussion by eng. Andrey Georgiev Ivanov, Doctoral thesis, and Abstract on the topic **“THE RESILIENCE ANALYSIS OF PUBLIC KEY CRYPTOGRAPHIC SYSTEMS”** demonstrate the author's desire to present to the scientific community in Bulgaria and specifically to the Professor Tsvetan Lazarov Defense Institute the results of their scientific research, which is in the final realization stage.

I definitely consider that the dissertation is relevant and timely.

The goal of this research, as formulated by the author, is to demonstrate that public key cryptography continues to develop and be applied extensively, but in order to be maximally useful for current social practice, it is necessary to

minimize the possibilities for compromise through the use of methods for full attack against public key generation processes.

In this regard, I would like to emphasize that Eng. Andrey Ivanov has successfully achieved the goal he has defined himself, by fully addressing the following questions:

- Is it possible to investigate and apply in practice the technologies and mechanisms for creating models that can serve as a basis for the implementation and application of an algorithmic framework for working in the upcoming post-quantum era?
- How to increase the resilience and reliability of generating keys used in public key cryptography?
- How to implement a fast and high-quality assessment for the presence of implemented kleptography in systems using public key cryptography?

The author has successfully solved several other tasks, which at the moment have found similar solutions in a number of scientifically advanced countries around the world, but the emphasis on their specificity gives him the right to claim some scientific and practical innovations.

3. **Main scientific and applied contributions. Evaluation of the candidate's results and contributions.**

I accept not only in principle, but also in substance the scientific and applied contributions obtained in the dissertation, but I do not agree with the way in which they have been formulated by eng. Andrey Ivanov.

Regardless of the latter statement, the described contributory

characteristics of the research prove that the dissertation fulfills its purpose and can be considered a successful attempt to respond to an actual and significant need.

4. **Evaluation of the author's contribution.**

I did not identify any plagiarism and I would like to emphasize that the authorship of the PhD candidate is indisputable. The stated results and contributions were obtained after a prolonged accumulation of personal observations, gathering of empirical data, and persistent research work.

5. **Critical remarks and recommendations.**

During the evaluation of the presented scientific and applied research, some terminological inaccuracies were noticed. There is also a disproportion in the substantiation of various author's theses. Too much attention is paid to the constative part of the dissertation. The contributions could be visually divided into scientific and applied.

After discussions and in-depth discussions with the PhD candidate Andrey Ivanov and his esteemed thesis supervisor, Associate Professor PhD Nikolay Todorov Stoyanov, some of the identified shortcomings were overcome before the final editing of the dissertation.

The critical comments and recommendations made do not diminish the significance of the contributions achieved. They do not in any way limit their scientific, methodological, and applied value.

6. **Conclusion.**

Based on the above, I have grounds to vote positively for awarding the educational and scientific degree of "Doctor" to **eng. Andrey Georgiev Ivanov** in the doctoral program "**Automated Information Processing and**

Management Systems" in professional field **5.2 "Electrical Engineering, Electronics, and Automation"**.

January 22, 2023 Jury member: _____

Sofia Professor. Stoyan Georgiev Denchev, D.Sc.