МИНИСТЕРСТВО НА ОТБРАНАТА
ИНСТИТУТ ПО ОТБРАНА „ПРОФЕСОР ЦВЕТАН ЛАЗАРОВ
София 1592, бул. „Проф. Цветан Лазаров" № 2, факс: 02/92 21 808, http://di.mod.bg

OPINION

from Full Prof. Eng. Zhaneta Nikolova Savova, DSc.
department "Computer Systems and Technology", Faculty "Artillery, Air Defense and Communication and Information Systems" of National Military University "Vasil Levski", Bulgaria
the member of the scientific jury

of PhD thesis by Eng. Andrey Georgiev Ivanov
the author of the PhD thesis

on topic „**The Resilience Analysis of Public Key Cryptographic Systems**"

presented for acquiring educational and scientific degree
"**Doctor of Philosophy**"

in PhD program
„**Automated systems for processing information and management**"
field of higher education **5. "Technical sciences"**
professional field **5.2 "Electrical engineering, electronics and automation"**

1. Actuality and importance of the researched scientific problem

The relevance of the problem of researching the resistance of the currently most used asymmetric RSA cryptosystem is undeniable, due to the fact that over 90% of the protection of modern Internet communications use this method. The fact that in 2017 a critical vulnerability CVE-2017-7526 was discovered in the GPG (Gnu Privacy Guard) library, which allows breaking RSA-1024 and obtaining the key with which to decrypt the message, confirms the relevance of research in the PhD thesis' problem. The significance of the problem is even more indisputable today, at the beginning of the era of real quantum computing and communications, when a group of Chinese researchers proposed a practical algorithm and calculated that it was possible to scale it to attack 2048-bit RSA keys using a quantum computer with only 372 qubits. Such a quantum computer actually exists, it is the IBM Osprey, which is a 443-qubit processor.

2. Evaluation of the scientific results and contributions of the PhD thesis

I classify the main contributions of the dissertation as scientific-applied and applied:

1. A model which determines whether a given number is likely to be prime is proposed, based on the Miller-Rabin algorithm, which allows achieving a deterministic result without reducing the speed of the Miller-Rabin algorithm.
2. A model to solve congruence system is proposed, in which there are no limitations for the modulo numbers to be a prime. This model is implemented in conjunction with Pohlig-Hellman algorithm to attack the RSA system, which the author claims increases the speed of the attack.
3. A kleptographic algorithm for attacking RSA-based cryptographic systems is synthesized and mathematically grounded. A comparative

analysis and assessment of the resistance of the system was made depending on the choice of the generated pair of RSA keys.

I believe that the contributions have relevance, usefulness and practical application in the cryptanalysis of RSA-based cryptosystems, and they can be defined as enrichment and further development of already existing, models and algorithms, obtaining confirmation of scientific knowledge and its application in practice.

I am convinced that the research in the dissertation and its publications are author's personal work of the Eng. Andrey Georgiev Ivanov and confirms the significance of the contributions made to the practical application of the RSA cryptanalysis.

3. Critical remarks

A huge amount of research with high practical applicability has been done, but in reviewer's opinion, some lapses, remarks and recommendations can be noted:

1. The results of the proposed models and algorithms are not sufficiently well described and statistically investigated. Phrases such as "a number of tests were performed" (p. 91), "an analysis involving a number of tests was performed" (p. 93) were used. I recommend the author to continue his statistical analysis on the proposed models and algorithms.
2. I recommend the author to familiarize himself with the algorithm of the German mathematician Schnorr, who in 2021 proposed a fast factorization algorithm by using SVP (Shortest Vector Problem) algorithms, as well as with the publications of Chinese scientists which proposed a combined implementation of the algorithm of Schnorr with the QAOA (Quantum Approximate Optimization Algorithm) to crack RSA-2048.

4. Conclusion

I believe, that the dissertation on topic "The Resilience Analysis of Public Key Cryptographic Systems", developed by Eng. Andrey Georgiev Ivanov, has all the qualities of a complete scientific-applied research on topical problems, related to the study of resistance of modern asymmetric cryptographic systems. It contains significant for practice scientific-applied results which are author's personal work and confirm his ability to formulate and research independently significant for practice problems in professional field "Electrical engineering, electronics and automation" and scientific specialty "Automated systems for processing information and management".

The submitted dissertation and extended abstract completely meet the requirements of the Law for development of academic staff in the Republic of Bulgaria and the Regulations for its application for acquiring educational and scientific PhD degree.

5. Assessment of the dissertation

Based on the above, I give a **positive assessment** of the submitted dissertation and extended abstract. I suggest the honorable members of the scientific jury to award Eng. Andrey Georgiev Ivanov the educational and scientific **PhD degree** in scientific specialty "**Automated systems for processing information and management**", science field of higher education **5 "Technical sciences"**, professional field **5.2 "Electrical engineering, electronics and automation"**.

11.02.2023 г.

The member of the scientific jury:

Full Prof. Eng. Zhaneta Savova, DSc.