MINISTRY OF DEFENSE

DEFENSE INSTITUTE „PROFESSOR TSVETAN LAZAROV”

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

REVIEW

by Professor. VESELIN TSELKOV, 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***

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

I. ACTUALITY AND SIGNIFICANCE OF THE SCIENTIFIC DEVELOPED PROBLEM

Actuality

The actuality of the presented dissertation is determined by the widespread use of the Internet, the perception of information as a critical resource, and the increasing threats to information security. In the process of the Internet's total dissemination, issues of protecting information resources and using cryptography algorithms, mechanisms, and services become extremely relevant.

The relevance of the research performed is determined by several problems related to the implementation and security of public key cryptography algorithms, such as:

- Finding large prime number pairs;
- Factoring a large number into prime factors;
- How, knowing the public key, can a reasonable assumption with high reliability be made about the value of the private key or that private key be fully derived;
- Possibilities to attack the security of the algorithm, under certain conditions.

Significance

The significance of the research is undoubtedly determined by the place and role of the proposed solutions in the dissertation work to part of these tasks. Solving these tasks is an important part of the solution to the problem of ensuring information security, the use of asymmetric cryptography algorithms, and overcoming this problem has substantial significance for specialists working in this field. Part of the posed problems are presented in the dissertation research.

I note:

1. The foundation of the most commonly used public key algorithms is prime numbers and the decomposition of a number into prime factors. In practice,

there are numerous algorithms for evaluating the divisibility (decomposition) of a number into prime factors. The algorithm with the widest application is the Miller-Rabin algorithm, which has high speed, but in practice, it is used as a probabilistic algorithm for evaluating divisibility. ***The author synthesized an original algorithm based on a new solution model, a modification (expansion) of the Miller-Rabin algorithm. The solution allows for an increase in the likelihood of accurate results and creates the opportunity to achieve a deterministic outcome without sacrificing the speed of performance that the Miller-Rabin algorithm possesses in its implementation as a probabilistic one.***

2. The analysis and comparison of the most effective algorithms for decomposing large numbers into prime factors, which are used to attack RSA-based cryptographic systems, has been performed. One of the algorithms used in practice is the Silver-Pohlig-Hellman proposal. Part of the implementation of this algorithm involves solving a system of congruent equations through the use of one of the most fundamental algorithms in number theory, the Chinese Remainder Theorem. Solving a system of congruent equations using the Chinese Remainder Theorem requires the numbers to be calculated modulo to be mutually prime. ***Andrey Ivanov has developed and presented a new solution model that includes an algorithm for solving systems of congruential equations that can be performed without any restrictions and can function and achieve solutions without requiring the numbers used in the modular calculation to be mutually prime.***

3. A mathematical model and practical solution of a Kleptographic algorithm that when used in practice seriously affects the stability and secure functioning of RSA-based cryptographic systems has been presented.

II. A GENERAL CHARACTERIZATION AND STRUCTURE OF THE DISSERTATION WORK.

For review, the following are proposed:

- Dissertation research – 144 pages;
- Dissertation review – 40 pages;
- Publications - 3.

The content of the presented dissertation work is presented on 144 pages, including a list of abbreviations and 10 figures. It is structured as an introduction, three chapters, conclusion, results obtained, and appendices (4 pieces). A list of used and cited information sources is given (114 titles, of which 2 are in Bulgarian, 77 in English, and 35 Internet addresses). A list of the author's publications on the topic is attached, including 3 titles.

Each chapter is a separate part of the work and ends with conclusions that treat the results obtained. The connection between the chapters is ensured by the logic of the presentation and allows a comprehensive understanding of the scientific research.

The analysis of information from the used literature and the results of the author's own scientific research have allowed the author to clearly and concisely formulate the purpose and tasks of the research. The consistent solution of the tasks set in the dissertation work implies the successful achievement of the set goal. The reliability of the results obtained is confirmed by the results and their application in practice. The detailed study of the dissertation allows for tracing the logic and causal connections of synthesis and analysis, eliminating any doubts about the originality and reliability of the presented scientific material.

The research methods used in the dissertation, including the planning of the experiment, the verification of the adequacy of the developed mathematical models, and the processing of the data, are well selected and properly presented. All of this ensures a high degree of reliability of the obtained results and their

correct interpretation.

The abstract fully reflects the results obtained in the research.

The doctoral thesis and abstract presented by candidate engineer Andrey Ivanov are following the requirements of the law and regulations and fully meet the criteria for obtaining a doctoral degree.

III. CHARACTERISTICS OF SCIENTIFIC AND SCIENTIFIC-APPLIED CONTRIBUTIONS

The contributions of the candidate can be attributed to the scientific specialty of **Automated Information Processing and Management Systems** and in the aforementioned directions and can be summarized (according to the reviewer) in the following areas:

- Methods, approaches, models, and studies for improving the reliability of the evaluation result of a number divisibility as a complement to the most widely used algorithms in practice, that of Miller-Rabin;
- New models for solving systems of congruential equations without any restrictive conditions for the model to be executable. The lack of restrictive conditions distinguishes it from previously known algorithms in practice, such as the "Chinese Theorem" algorithm, and allows solutions to be achieved without the numbers used in the calculation by modulo having to be relatively prime;
- Development of a mathematical apparatus and practical solution that allows the creation of a Kleptographic algorithm for attacking RSA-based cryptographic systems.

The reviewer fully accepts the contributions as formulated by the candidate in the conclusion and achieved results.

IV. EVALUATION OF SCIENTIFIC RESULTS AND CONTRIBUTIONS

Published results can generally be divided into scientific, scientific-applied and applied.

Scientific contributions

The candidate's scientific contributions can be reviewed and evaluated in the following directions:

- Enhancement of existing knowledge;
- Discovering and proving essential new aspects of an existing scientific field;
- Application of scientific achievements in practice and realized economic effect.

Scientific-applicable contributions

The scientific-applicable contributions are in the field of information security, cryptographic algorithms, mechanisms, services and applications.

Applicable contributions

The practical contributions are in the area of designing, developing, and implementing mathematical models and algorithms in specific applications.

The significance of the contributions can be evaluated based on their applicability in different implemented projects. It is worth noting the scientific research developments that have been incorporated into practice (projects, tasks, complexes, and systems).

V. ASSESSMENT OF THE ABSTRACT, DISSERTATION PUBLICATIONS, AND AUTHORSHIP

Abstract

The abstract of the dissertation work is properly formatted according to the requirements of the law and regulations. In its substantive part, it accurately reflects the dissertation work, namely: the title, objective, tasks, contributions, author's claims, factual data obtained, conclusions, recommendations, implementation and use of results, report on contributions, and list of publications based on it.

Publications

Three publications are presented on the subject of the dissertation:

- [1] Stoianov, Nikolai, and Andrey Ivanov. "Public Key Generation Principles Impact Cybersecurity." Information & Security: An International Journal 47, no. 2 (2020): 249-260, https://doi.org/10.11610/isij.4717
- [2] Ivanov A., Stoyanov N., “Analysis of Approaches for Evaluating the Robustness of Public Key Cryptographic Algorithms”, Tenth International Scientific Conference "Scientific Research and Investments in Technological Innovations - a Decisive Factor for Defense and Security", HEMUS 2020, Plovdiv.
- [3] Ivanov A.G., Stoianov N.T. (2020) New Approach of Solving Congruence Equation System. In: Dziech A., Mees W., Czyzewski A. (eds) Multimedia Communications, Services and Security. MCSS 2020. Communications in Computer and Information Science, vol 1284. Springer, Cham, https://doi.org/10.1007/978-3-030-59000-0_2

These publications allow for a comprehensive understanding of the results obtained and ensure the necessary public visibility of the scientific contributions and author's claims. The reviewer considers that the main results of the

dissertation work are reflected in the publications.

Authorship

The candidate's personal contribution to obtaining the results in the presented works is undeniable. His authorship is without doubt. A careful analysis of the candidate's overall scientific output allows the conclusion to be drawn that the above-mentioned scientific contributions are entirely his own personal work. No plagiarism has been detected, and it is assumed that the works and contributions therein are the personal work of the candidate.

VI. LITERARY AWARENESS AND COMPETENCE OF THE DOCTORAL STUDENT

The list of sources used and cited in the text (114 titles, including 2 in Bulgarian, 77 in English and 35 internet addresses) demonstrate the literary knowledge and competence of the doctoral candidate, confirmed by the presented scientific and applied results.

VII. CRITICAL NOTES AND RECOMMENDATIONS

The reviewer does not find significant scientific errors in the presented research and publications. The critical comments made to Eng. Andrei Ivanov during the preliminary defense have been fully addressed and **the reviewer allows themselves to note the precise formatting of the dissertation and abstract.**

VIII. PERSONAL IMPRESSIONS AND APPROVAL OF THE RESULTS

I have known Andrey Ivanov since 2004. We have worked together on several projects related to the development of cryptographic systems for information security. I am familiar with and have observed his scientific and professional development almost continuously. He has a broad general culture,

deep and persistent scientific interests in the field of programming, research and development of cryptographic systems. Some of the results presented have been implemented in international projects related to research and development of solutions in the subject area. Another part has been implemented in systems (encrypting devices) that have been approved for use in protecting information in computer systems and networks. The scientific results have been published in prestigious scientific journals.

IX. CONCLUSION AND EVALUATION OF THE DISSERTATION

I express my absolute conviction that eng. Andrey Ivanov is an erudite, educated, and correct academic employee and researcher. His overall assessment, as well as the specific assessment of his scientific and practical results and contributions, provide a basis for expressing **my positive stance and my firm belief** that the presented dissertation, abstract, and publications on the research topic meet the requirements for obtaining the educational and scientific degree of "Doctor" and I propose to the esteemed jury members to vote **POSITIVELY** for the granting of **the educational and scientific degree of "Doctor"** in the field of higher education **5. Technical Sciences**, professional direction **5.2 Electronics, electronics and automation,** scientific specialization **Automated systems for processing information and control** of candidate Andrey Ivanov.

13.02.2023 г. **Member of the jury:**

Sofia **/Professor. VESELIN TSELKOV, D.Sc./**