ANNOTATION

of dissertation for the Philosophy Doctor (PhD) degree in according to the educational program "8D06201 – Radioengineering, electronics and telecommunications" by Skabylov Alisher on the topic **"Hardware and software of FPGA-based data encryption"**

The doctoral dissertation discussed in this study is aimed at implementing hardware and software encryption of data in telecommunications networks, including the Internet of Things and secure communication systems. The research suggests an approach based on the use of programmable logic integrated circuits (FPGA) to achieve high-speed and reliable encryption through parallel and pipelined data processing. A key aspect of the work is the use of chaos generators to generate pseudorandom numbers used as keys, which significantly increases the security of encrypted information. The encryption algorithm presented in the dissertation is based on the non-positional polynomial number system (NPN) and offers new solutions for data protection that differ from traditional encryption methods. By introducing this algorithm into the FPGA, the research is aimed at creating a domestic hardware encryption device that meets modern information security standards, ensuring technological independence and security. This research significantly advances the development of technologies for data encryption and the creation of reliable methods to enhance security based on information and communication technologies (ICT). Such progress is important for the field of information security and protection of technological confidentiality, affecting the fundamental elements of data protection in modern communication systems.

Relevance of the dissertation theme.

The relevance of this study is due to the increased requirements for ensuring the protection of electronic information resources, information systems and communication infrastructure, as well as specialized systems such as confidential communications and video communications. In the context of an ever-growing volume of digital information and its strategic importance, the issues of effective data encryption are of paramount importance.

FPGA offers unique opportunities to solve these problems due to its flexibility, scalability and ability to process parallel data with high performance. FPGA information security systems can significantly increase the speed of data encryption, while ensuring a high degree of confidentiality and integrity. This makes FPGAs the preferred solution where security and performance requirements are higher.

One of the key aspects of this research is the use of chaos generators as a source of pseudorandom numbers to generate encryption keys. This approach significantly increases data security, since chaotic sequences are difficult to predict and analyze, which makes the decryption process without an appropriate key very difficult.

The NPN–based encryption algorithm developed as part of this study is a solution that differs significantly from traditional encryption methods. This not only increases the level of encryption security, but also increases its efficiency by optimizing data processing processes.

This encryption method allows you to create a domestic encryption device that meets modern information security requirements. In the modern world, when technological sovereignty is becoming more and more relevant for ensuring national security, the ability to create their own algorithms and encryption technologies for each country is a strategic advantage. The development and implementation of proprietary data encryption solutions not only ensures reliable information protection, but also contributes to the development of national technological and scientific competencies, strengthening the technological independence and security of the country.

Thus, the relevance of this study is due to not only the technical aspects of developing effective and reliable data encryption methods, but also to the strategic need to ensure technological sovereignty in the field of information security. Investigation of electrical, optical, morphological characteristics of nanostructured porous silicon and surface-modified porous silicon, on the surface of which a metal-oxide semiconductor and a metal layer are deposited, as well as the development of a highly sensitive and selective electronic gas sensor based on them for polar and non-polar types of gases.

The purpose of the dissertation is the realization and implementation of integrated information software for data encryption based on FPGA.

The subject of research includes telecommunication systems and specialized communication systems, including Field-Programmable Gate Arrays (FPGA), non-positional polynomial number systems, and pseudo-random number generators.

Research Objectives:

1. Study of data encryption algorithms: research and comparison of traditional and modern encryption methods used for data encryption;
2. Assessing the potential use of FPGA as the foundation for data encryption systems. Creation of hardware architecture based on FPGA, optimization of encryption algorithms, and integration of software and hardware components;
3. Development of an encryption algorithm: creation of an efficient data encryption algorithm based on non-positional polynomial number systems and adapted for implementation in FPGA;
4. Use of chaos generators: development of a methodology for using chaos generators to generate pseudo-random numbers that serve as reliable encryption keys;
5. Security and efficiency evaluation: analysis of the performance, power, and efficiency of the developed tools compared to other data encryption methods in ICT;
6. Implementation and testing of the encryption algorithm implemented in FPGA to assess its practical application and performance.

The novelty and specificity of the dissertation, for the first time:

An FPGA-based encryption algorithm using non-positional polynomial number systems has been implemented and tested;

For the first time, the use of chaos generators directly in FPGA for generating pseudo-random numbers, which serve as encryption keys, has been realized, significantly enhancing the security level of the system;

A comprehensive solution combining FPGA hardware and specialized software, capable of providing high-performance and secure data encryption in simple telecommunication systems, was proposed for the first time;

A database of irreducible polynomials for use in encryption algorithms was created and systematized in FPGA for the first time, which is a fundamental process in selecting polynomials for generating encryption keys. Hardware verification of the irreducibility of polynomials was introduced directly in FPGA for the first time, allowing for the automation and acceleration of the polynomial verification process, including ensuring high reliability and promptness in selecting keys for data encryption.

The main provisions for the defense.

1. The generator of irreducible polynomials developed for the purpose of hardware protection can reach up to a key length of 16 bits of the physical resources of the FPGA Artyx-7.

2. The generators of chaotic signals and pseudo-random numbers implemented on FPGAs contribute to increasing the security of encrypted information by randomly distributing the length of data blocks in transmitting and receiving devices.

3. Thanks to parallel, pipeline computing methods, the speed of hardware implementation of public key encryption algorithms based on FPGA can be increased up to 6.239 ns per clock cycle.

Practical and theoretical importance of the dissertation.

The theoretical significance of this research lies in the development of theoretical foundations and understanding of ICT and their applications in the field of data encryption and decryption, as well as information security. The study will allow a deeper exploration of the principles of ICT operation, the specifics of data encryption and decryption, and the development of new methods and algorithms for ensuring information security.

The practical significance of the research lies in the creation of hardware and software based on FPGA for implementing effective and reliable systems of data encryption and decryption. This ensures the protection of information from unauthorized access and maintains the confidentiality of transmitted and stored data.

The results of this scientific research, hardware and software solutions based on FPGA, can be integrated into various devices and ICT systems to ensure data security and information protection in various fields, including telecommunications, electronics, information systems, and more. This opens new possibilities for the development of modern communication and data transmission systems, ensuring their reliability, confidentiality, and integrity.

The results and the methods and algorithms for data encryption and decryption developed on the basis of FPGA can be used in information and communication technologies, cloud storage, e-commerce systems, and other experimental applications requiring information protection. This contributes to the development of information security and the creation of more reliable and efficient data protection systems.

The practical significance of the obtained results is confirmed by publications in international peer-reviewed journals and participation in regular international conferences, as well as by the author's certificate RK № 22917.

The reliability and validity of the results.

The reliability of the results achieved in the dissertation work is confirmed by the presence of publications in local journals recommended by the Committee for Quality

Assurance in Science and Higher Education of the Ministry of Science and Higher Education of the Republic of Kazakhstan, in foreign journals included in the Web of Science (Clarivate Analytics, USA) and Scopus (Elsevier, Netherlands) databases, and in the proceedings of international conferences, as well as consistency with the results of other authors.

The personal contribution of the author consists in independently carrying out the entire research process, from selecting the research method to developing regulatory and technical documentation. The author also worked collaboratively with supervisors on setting objectives and discussing results.

Approbation of the dissertation.

Based on the materials of the dissertation, 10 printed works have been published:

Articles with a high impact factor in the Thomson Reuters database or in publications included in the international scientific database Scopus:

1. Ibraimov M.K., Tynymbayev S.T., **Skabylov A.A.,** Kozhagulov Y., Zhexebay D.M. Development and design of an FPGA-based encoder for NPN //Cogent Engineering. – 2022. – Vol. 9, № 1. – 2008847 **[Q2, 67%]**
2. Aitkhozhayeva Y.Zh., Tynymbayev S., Adilbekkyzy S., **Skabylov A.,** Ibraimov, M. Design and research of the behavioral model for the modular reduction device // Eurasian Physical Technical Journal 7. – 2020. – Vol. 17, № 1. – C. 151–156. **[Q3, 25%]**

Scientific publications recommended by the Committee for Quality Assurance in the Field of Science and Higher Education of the Ministry of Science and Higher Education of the Republic of Kazakhstan for the publication of main results of scientific activity:

1. Kalimoldayev M., Tynymbayev S., Almen D., **Skabylov A.** Implementation of the nonconductivity check algorithm for a given binary polynomial on the FPGA // Bulletin of KazNITU. – 2020. – Vol. 141, No. 5. – Pp. 629-635.
2. **Skabylov A.A.,** Ibraimov M.K., Zheksebay D.M., Kozhagulov E.T. Software-hardware implementation of QPSK based on Zynq and MATLAB // Bulletin of Abai KazNPU, series "Physical and Mathematical Sciences", No. 1(77), 2022.
3. **Skabylov A.A.,** Zheksebay D.M., Ibraimov M.K., Nalibayev E.D. Application of chaotic generators for the secret key in electronic transmitting-receiving devices // Bulletin of KazNPU. – 2023. – Vol. 82, No. 2. – Pp. 194-201.

Publications in the proceedings of international conferences:

1. Almen D.B., **Skabylov A.A.** Creation of a database of irreducible polynomials in the finite field GF(2) based on FPGA // International Scientific Conference of Students and Young Scientists, "FARABI WORLD", 2020. – P. 269.
2. **Skabylov A.A.,** Almen D.B., Zheksebay D.M., Azamat R.M. Design and research of the operational model of a modulo division device // International Scientific Conference of Students and Young Scientists, "FARABI WORLD", 2021. – P. 217.
3. **Skabylov A.A.,** Almen D.B., Zheksebay D.M., Azamat R.M. Hardware implementation of encryption and decryption algorithms based on FPGA // International Scientific Conference of Students and Young Scientists, "FARABI WORLD", 2021. – P. 218.

4. **Skabylov A.A.,** Zheksebay D.M., Almen D.B., Ikhsan G.B. FPGA-based software-information complex for QPSK // International Scientific Conference of Students and Young Scientists, "FARABI WORLD", 2022. – P. 215.
5. **Skabylov A.A.,** Nalibaev E.D., Ibraimov M.K., Danabekov B., Azamat R.M. "Chaos and Structures in Nonlinear Systems. Theory and Practice" XII International Scientific Conference, 2022. – P. 155.

Certificate of copyright:

1. **Skabylov A.A.,** Ibraimov M.K., Sakhybai T., Zheksebay D.M., Kozhagulov E.T. Hardware complex for data encryption based on FPGA // Author's certificate, 2022. No. 22917.

Act of implementation of the completed research work into the educational process:

1. Protocol No. 1 dated August 31, 2023

The scope and structure of the thesis.

The dissertation consists of an introduction, three chapters, a conclusion, and a list of used literature. The work includes 54 figures, 20 formulas, 6 tables, 117 literature references and 114 pages.