ВЕСТНИК АСТА

ТУРИНСКОГО ПОЛИТЕХНИЧЕСКОГО УНИВЕРСИТЕТА В ГОРОДЕ ТАШКЕНТЕ

OF TURIN POLYTECHNIC UNIVERSITY IN TASHKENT

ВЫПУСК EDITION 3/2023

TOSHKENT SHAHRIDAGI TURIN
POLITEXNIKA UNIVERSITETI
AXBOROTNOMASI
3/2023 SONI

ВЕСТНИК
ТУРИНСКОГО ПОЛИТЕХНИЧЕСКОГО
УНИВЕРСИТЕТА В ГОРОДЕ ТАШКЕНТЕ
ВЫПУСК 3/2023

ACTA
OF TURIN POLYTECHNIC UNIVERSITY
IN TASHKENT
EDITION 3/2023

TASHKENT – 2023

Журнал Ўзбекистон Ахборот ва оммавий коммуникациялар агентлиги томонидан 0890-сонли гувоҳнома билан рўйҳатга олинган.
ISSN 2181-8886
E-ISSN 2181-1512

Журнал зарегистрирован в Узбекском Агентстве информации и массовых коммуникаций. Свидетельство о регистрации № 0890.
ISSN 2181-8886
E-ISSN 2181-1512

The journal was registered at the Agency of Information and Mass Communications of Uzbekistan. Certificate of Registration № 0890.
ISSN 2181-8886
E-ISSN 2181-1512

Тошкент шаҳридаги Турин Политехника Университети 100095, Тошкент ш., Кичик Халқа Йўли 17 уй.

Тел.: (+99871) 246-70-82
E-mail: actattpu@polito.uz
www.actattpu.polito.uz

Туринский Политехнический Университет в городе Ташкенте 100095, г. Ташкент, ул. Кичик Халка Йули 17.

Тел.: (+99871) 246-70-82
E-mail: actattpu@polito.uz
www.actattpu.polito.uz

Turin Polytechnic University in Tashkent 100095, Tashkent city, Kichik Halqa Yo'li str. 17.

Tel.: (+99871) 246-70-82
E-mail: actattpu@polito.uz
www.actattpu.polito.uz

CONTENTS

ACTA TTPU

Preface

Dear readers! I am pleased to announce the publication of a new edition of ACTA TTPU, the journal of Turin Polytechnic University. It is an № 3 issue to be published in 2023 year which includes selected articles submitted to the editorial board. Since the beginning of the year, we have seen an increase in the number of articles submitted to our journal, and I believe that the growing popularity of the journal is partly due to the excellent work of the editorial board. We will continue our efforts to improve the quality as well as the submission requirements and simplify the selection procedures in order to raise the quality to a higher level.

I am very grateful to our editorial board for their contribution to the quality of our journal and to all authors for their submissions. We are always open to any criticism and suggestions to improve the readability and content of the articles published in our journal.

Editor-in-chief
DSc., Professor J.Sh.Inoyatkhodjaev

Acta of Turin Polytechnic University in Tashkent, 2023, 30, 7-11
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

PERSPECTIVES AND CHALLENGES OF ASSEMBLY 4.0 TECHNOLOGIES FOR FINAL AUTOMOTIVE ASSEMBLY OPERATIONS IN UZBEKISTAN

[1]I. Kambarov, [2]J. Inoyatkhodjaev
Turin Polytechnic University in Tashkent
Email: [1]ikrom.kambarov@polito.uz, [2]j.inoyatkhodjaev@polito.uz

Abstract– Nowadays, manufacturing is moving to the next phase of digitalization through the "Assembly 4.0" concept. This new paradigm is supported by innovative technologies such as the Internet of Things, assembly control systems, augmented reality, system simulation, system integration, and other advanced digitalization technologies. These advanced technologies allow optimizing final automotive assembly systems to achieve greater flexibility and efficiency in production processes, generate a value-added proposition for their customers, and provide a timely response to their market needs. However, despite the potential benefits of Assembly 4.0, organizations face common obstacles and challenges in adopting new technologies and successfully implementing them in their assembly operations. Therefore, this article identifies and analyzes the problems that may hinder the implementation of Assembly 4.0 technologies in final automotive assembly organizations and gives practical recommendations for their elimination.

Key words– Assembly 4.0, digitalization, manufacturing, developing country

I INTRODUCTION

The automobile sector in the Republic of Uzbekistan is currently expanding rapidly, increasing exports, luring foreign investment, and modernizing manufacturing procedures dramatically in terms of technology. The automobile industry includes dozens of large and medium-sized enterprises, including companies with foreign participation in the automotive industry and manufacturers of consumer goods. Figure 1 shows passenger car production volume in Uzbekistan between 1999 and 2020. It shows that passenger car production has increased over the years, but some have decreased due to the economic crisis in the world. Nevertheless, it can be seen that it started to increase in recent years, and according to Presential Degree No. PQ-4397 of July 18, 2019, the passenger car production volume must reach 350 000 units per year until the end of 2023. To cope with these requirements, the final automotive assembly systems must be integrated with advanced technologies to increase the production volume and flexibility of the manufacturing systems.

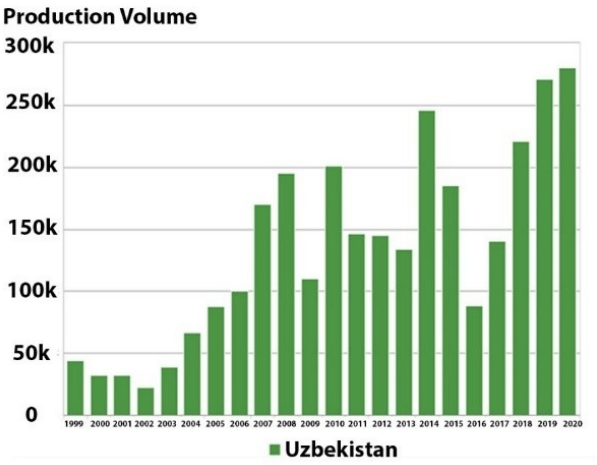

Fig. 1: The passenger car production volume in Uzbekistan

However, today's final automotive assembly systems in Uzbekistan have to manage hundreds of different product mixes, distinguished by different assembly cycles, as well as thousands of different parts, hundreds of tools and, equipment, and several workers [1]. Besides, final automotive assembly processes struggle with several challenges, such as the growing complexity of their operations and value chain, cost requirements, increasing customer demands for product quality, time to market, and personal customization [2, 3]. The literature analyses indicate the importance of assem-

bly and the potential savings that can be achieved by the efficient deployment of advanced Assembly 4.0 technologies and system changes. The optimal design and management of these system features are crucial to achieving final automotive assembly operation efficiency, product quality, and customer satisfaction. In response to these requirements, assembly systems are being managed with several Lean Principles, like just-in-time (JIT) to deal with market demand [4, 5]. Moreover, to respond to frequent market changes and reduce time to market, - flexible, adaptable, changeable and reconfigurable assembly system concepts must be developed. Therefore, in this article, the authors identify and analyze the problems that may hinder the implementation of Assembly 4.0 technologies in final automotive assembly organizations and give practical recommendations for their elimination.

To deal with this problem, this paper is organized as follows: Section 2 presents the research approach and its underlying rationale in detail; Section 3 gives a brief review of the of Assembly 4.0" technologies and vision; and Section 4 outlines the challenges and perspectives of the "Assembly 4.0" technologies for final automotive assembly systems. Finally, Section 5 concludes the study with insightful perspectives on the results and findings.

II THE METHODOLOGY

The approach followed in this study includes a System Development Methodology, to get a systematic background on the Assembly 4.0 technologies as shown in Figure 2.

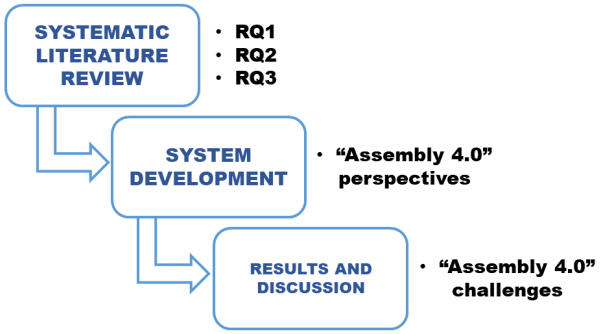

Fig. 2: System Development Methodology

To fulfill the scope of the research, the following three-point methodology was implemented: A systematic literature review (SLR) study of "Assembly 4.0", to understand its practical aspects and requirements in final automotive assembly. Based on the outcomes of SLR, the conceptual framework of "Assembly 4.0 was highlighted for final automotive assembly operations.

Then we defined the perspectives of the Assembly 4.0 technologies. In the results and discussion phase, it depicts the existing challenges of Assembly 4.0 technologies on final automotive assembly systems and gives practical recommendations for their elimination. In this paper, the authors answer the following research questions:

RQ1: What are the key "Assembly 4.0" enabling technologies and features proposed to be integrated into final automotive assembly systems?

RQ2: What are the perspectives of Assembly 4.0 technologies when integrated into final automotive assembly systems?

RQ3: What are the adoption challenges of Assembly 4.0 technologies in the final automotive assembly systems organization?

III STATE OF ART

As part of a high-tech strategy plan for 2020, the German government initially announced the "Industry 4.0" paradigm in 2011. It refers to the fourth industrial revolution. [8]. This industrial revolutions are depicted in Figure 3 below, together with the related cutting-edge technology.

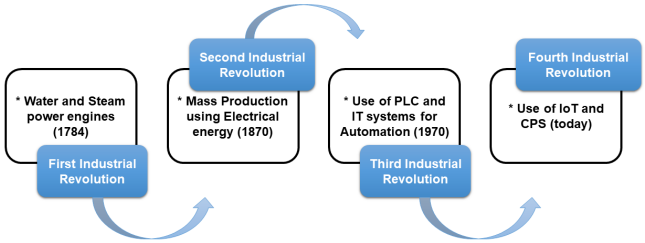

Fig. 3: Development four industrial revolutions

As "Assembly 4.0" is a rapidly expanding field of study in system engineering, it makes sense to analyze the idea of assembly under the "Industry 4.0" period with this investigation's primary focus being the design and administration of assembly systems. [13, 14].

Despite, that the terms "Assembly System 4.0" and "Smart Assembly Stations" are novel and evolving concepts, which remain abstract phenomenon, [6] highlighted the advanced assembly technologies. In addition, they also concluded that integrated IT systems are a key element of design smart and digital manufacturing systems. Alternatively, [14] on their keynote paper, divided the main design principles of the efficient "Assembly System 4.0" into four layers, namely into connectivity, information, knowledge, and smart layers. In addition, they proposed a future framework of the assembly paradigms as an effect of the integration with the "Industry 4.0" technologies. However, case uses are needed to quantify the different impacting variables for validating the proposed framework. The later one [13] developed a general framework of assembly system design in the "Industry 4.0" era

using Assembly System (AS) design method, which is illustrated in the corresponding Figure 4. This illustrates the vision of future assembly systems as assisted technologies for human operator to increase the product quality, production volume and decrease production time.

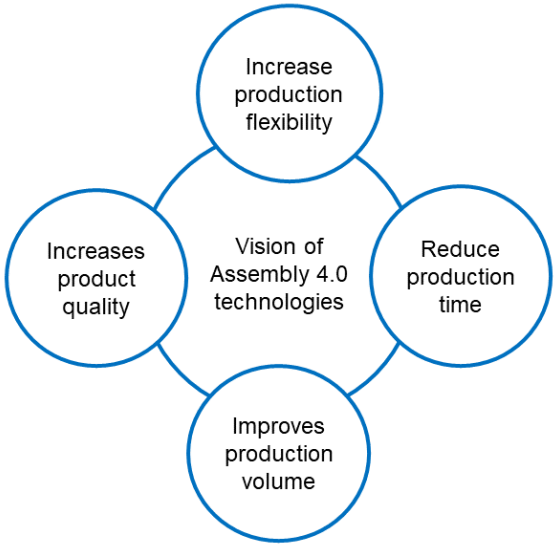

Fig. 4: Main characteristics of assembly system 4.0

Improves ergonomics: According to systematic literature review [13], technologies of the aided assembly boost the handling and joining tasks by different technologies decreasing their continuity and securing safe and ergonomic work condition. For instance, when a product arrives at an assembly station, assisted handling equipment, such as a tightening system, automatically directs the components to handle from the storage positions for the operator while taking the finished product's assembly and the best picking sequence that reduces worker execution time into consideration. Alternately, augmented reality technologies, which direct the sequencing of the jobs to finish an assembly task while taking into account the client personalisation, could assist the operator during assembly processes. Light robots are another example of how Assembly 4.0 advanced technology helps the operators during assembly operations. They adjust their layout automatically and in real-time to best suit the anthropometric characteristics of the assembly task and the worker. Additionally, collaborative robots offer operators a synthetic force to perform risky and uncomfortable activities, lowering the risk of damage.

Increase flexibility: An intelligent storage management system is another Assembly 4.0 technology that has been approved. These systems have an integrated storage system for the assembly station that tracks the inventory level and automatically notifies the supply chain department when it needs to be refilled [13]. Because of the system's adaptability, unexpected usage rates do not result in stock-outs. Additionally, this system might be linked to the supply chain division in order to transfer the out-of-date raw materials used in the assembly process, eliminating needless orders, and maintaining the just-in-time principles of the system. The inventory level at the assembly station eventually stays as low as it can give the manufacturing cost regulations.

Reduce assembly time: A self-configured workstation is the next emerging technology that Assembly 4.0 is proposing. With the assembly product and the designated operator for the assembly process taken into consideration, this technology independently modifies the layout dimensions of the workstation. The assembly station construction has integrated sensors and actuators that allow the shelves and workstation dimensions to be adjusted automatically. By reducing handling and joining times, this technology hopes to provide an ergonomic working environment.

Increase operation efficiency: In order to assure total product and process detectability, the resources have smart sensors implanted into the assembly system. Each work is decentralized and detects potential errors or disobedience in real-time [13]. This results in an improvement in product quality by replacing statistical fault analysis with unique item. Additionally, operator tasks are observed as they are carried out to course the built pieces and keep an eye on task completion.

IV RESULTS AND DISCUSSION

In order to meet the expectations of the contemporary market, vehicle manufacturers in Uzbekistan must digitize and intellectualize their assembly operations as they go from mass manufacturing to personal production. With the use of cyber-physical products and human-machine interfaces, assembly 4.0 technologies integrate the digital and physical worlds, increasing the efficiency of assembly processes. Through smart machines, smart sensors, and other computer-based technologies, Assembly 4.0 will offer individualized and effective production at a fair price. The vehicle manufacturing companies in our nation will need to create clearly defined strategies for transforming their assembly processes from analogue to digital and human-centered. Despite the many benefits of Assembly 4.0 technologies, adoption of these new cutting-edge technologies and their influence on current assembly procedures are hampered by a number of issues. It is crucial to identify the obstacles to the adoption of Assembly 4.0 technologies and to keep track of how they interact in order to solve these challenges. The auto industry in our nation needs to be aware of potential issues with the digital transformation process and be equipped to deal with them. We can benefit from the practical research of sev-

eral scientists who have performed research in this area as well as the experiences of international businesses for this purpose. We can identify a number of obstacles that may exist in assembly systems for the adoption of Assembly 4.0 after studying and analyzing them, including cyber security, an unskilled work force, and excessive implementation costs. Below are the identified challenges and their description.

Table 1 represents the existing challenges of Assembly 4.0 technologies for adoption in automotive assembly operations in Uzbekistan.

Challenges	Description
Complexity of value chain integration	IoT (internet of things) integration is a big problem in the assembly 4.0 environment as creating infrastructure between cyber - physical technologies and systems is difficult task.
Lack of relevant skills in the workforce	The lack of digital skills is a major challenge in the successful implementation of Assembly 4.0.
High investment necessity	Difficulties in introducing new technologies in their production environment due to the lack of resources.
Unemployment level	Ongoing technological progress and automation are changing the structure of existing jobs, creating challenges for labor markets.
Abstraction of economic efficiency	The economic benefits of capital investments in the introduction of Assembly 4.0 technologies have not been clearly assessed.

TABLE 1: CHALLENGES OF ASSEMBLY 4.0 TECHNOLOGIES FOR AUTOMOTIVE ASSEMBLY IN UZBEKISTAN

The table shows that "Lack of Value chain integration" is the most important root or major barrier to the adoption of Assembly 4.0 technologies in final automotive assembly operation. The uncertainty about economic benefits and lack of necessary skills in the workforce can be caused by a lack of infrastructure to implement Assembly 4.0. Inadequate skills of employees and lack of clarity about economic benefits can lead to difficulties in value chain integration between assembly stations units and other organizational department of the company. It can be seen from the that “high investment necessity” is third barrier of adoption Assembly 4.0 technologies. In addition, "unemployment level" is the fourth level. Finally, abstraction efficiency of Assembly 4.0 technologies can be considered as last challenges. In order to successfully implement Assembly 4.0 technologies, automotive manufacturing organizations in Uzbekistan must have sufficient and capable technological infrastructure in their production facilities, such as reliable high-speed connectivity, uninterrupted power supply, and IoT architecture for cyber-physical systems. This is the most important factor that plays an important role in the successful implementation of Assembly 4.0 technologies into assembly stations. Unless this barrier is alleviated, it may not be effective to focus on alleviating other barriers. Next, it is necessary to improve the technical skills of employees in these emerging technologies, as well as to improve the entire value chain network of suppliers and partners through networking and rapid connectivity. Organizations should evaluate the economic benefits of using these technologies in assembly stations. A poor value chain can lead to high investments, cybersecurity issues, and challenges in data quality and management. Therefore, automotive manufacturers must take necessary measures to overcome these obstacles, as they can lead to ineffective implementation of Assembly 4.0 technologies.

V CONCLUSION

In this paper, the authors identified and analyzed the problems that may hinder the implementation of Assembly 4.0 technologies in final automotive assembly organizations in Uzbekistan and gives practical recommendations for their elimination.

The findings indicate that in order for Assembly 4.0 technologies to be properly adopted by the industry, the companies must give it access to the required digital infrastructure. The financial advantages of Assembly 4.0 to industry must be shown by academic institutions and research groups. To increase trust in the automobile sector, it is desirable to create pilot initiatives. Another significant and essential barrier that requires immediate eradication is a lack of the necessary workforce skills. Therefore, universities should develop training programs in various aspects such as sensor technology, cyber security, machine-machine-human integration, data analytics, business intelligence, collaborative robotics, CPS, IoT, etc

VI REFERENCES

[1] T. AlGeddawy and H. ElMaraghy, "Design of single assembly line for the delayed differentiation of product variants," Flexible Services and Manufacturing Journal, vol. 22, pp. 163-182, 2010.

[2] K. Efthymioua, A. Pagoropoulos, N. Papakostas, D. Mourtzis and G. Chryssolouris, "Manufacturing Systems Complexity Review: Challenges and Outlook," Procedia CIRP, vol. 3, pp. 644-649, 2012.

[3] V. Modrak, D. Marton and S. Bednar, "Modeling and Determining Product Variety for Mass-customized Manufacturing," Procedia CIRP, pp. 258-263, 2014.

[4] M. Faccio, "The impact of production mix variations and models varieties on the parts-feeding policy selection in a JIT assembly system.," International Journal of Advanced Manufacturing Technology, vol. 72, no. 1-4, pp. 543-560, 2014.

[5] C. Antonio, M. Pacifico and P. Salini, "Selection of assembly lines feeding policies based on parts features," IFAC-International Federation of Automatic Control, pp. 185-190, 2016.

[6] K. Zhou, T. Liu and . L. Zhou , "Industry 4.0: Towards Future Industrial Opportunities and Challenges," 2015.

[7] M. Bortolini, E. Ferrari, M. Gamberi, F. Pilati and M. Faccio, "Assembly system design in the Industry 4.0 era: a general framework," IFAC, pp. 5700-5705, 2017.

[8] Y. Cohen, M. Faccio, F. Galizia, C. Mora and F. Pilati, "Assembly system configuration through Industry 4.0 principles: the expected change in the actual paradigms," IFAC, pp. 14958-14963, 2017.

[9] H. ElMaraghy, "Smart Adaptable Assembly Systems," Procedia CIRP, no. 44, pp. 4-13, 2016.

[10] M. Hermann, T. Pentek and B. Otto, "Design Principles for Industrie 4.0 Scenarios: A Literature Review," Hawaii International Conference on System Sciences (HICSS), 2016.

[11] R. Davies, "Industry 4.0. Digitalisation for productivity and growth," European Parliamentary Research Service, 2015.

[12] A. C. Pereira and F. Romero, "A review of the meanings and impications of the Industry 4.0 concept," Precedia Manufacturing, vol. 13, pp. 1206-1214, 2017.

[13] S. Vaidya, P. Ambad and S. Bhosle, "Industry 4.0 - A Glimpse," Procedia Manufacturing, no. 20, pp. 233-238, 2018.

Acta of Turin Polytechnic University in Tashkent, 2023, 30, 12-19
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

DEVELOPMENT OF ENCRYPTION AND ARCHIVING ALGORITHMS IN ACCORDANCE WITH GOST 28147-89 IN OPEN SOURCE OPERATING SYSTEMS

N.N. Ochilov
State Testing Center under the Cabinet of Ministers Republic of Uzbekistan
Email: nizom.ochilov91@gmail.com

Abstract– Operating systems belonging to the Linux family are somewhat more secure due to the limited access to system files. However, due to the fact that unlimited access is created when logged in using the system administrator (root), it requires special encryption methods to keep some data confidential. According to the level of data confidentiality, only the GOST 28147-89 standard is a highly durable encryption algorithm.

Key words– lossless compression, cryptanalysis, concatenation of cypher text blocks, initialization vector.

I INTRODUCTION

This article is dedicated to the development of encryption algorithms. The encryption algorithm requires at least an 80386 processor, 32 MB of RAM, at least 2 GB of hard disk space, and a C compiler to compile special modules. The software requirements are set according to the requirements of the 7zip archiving software. Downloading the system archiving module is done by downloading the 7zip program. This module cannot be accessed from outside. This module has the ability to encrypt and archive system files with a password. For this reason, 7zip was chosen as a convenient archiver for encryption based on the GOST 28147-89 standard.

The article describes the principles and methods underlying the creation of an application in secure operating systems, which provides reliable data encryption. The aim of the research is to analyze and indicate the specifics of encryption methods and algorithms based on domestic standards in open-source operating systems. Cryptanalysis was used in the article, as this avoids vulnerabilities identified in previously created implementations. In the article, the authors draw attention to the fact that 7-Zip uses CBC encryption (concatenation of encrypted text blocks), but the Counter Mode is supported. The same support was provided in the encrypt implementation. Since the key expansion function initially fills the special array created by p7zip with round keys using a unique property of the domestic standard, only one round encryption function was created (performed both during encryption and decryption). This method is also used in various modes. In many cases, initialization time deviations depending on the selected mode are insignificant. The created cryptographic module was tested to meet the domestic standard, which contains several test cases. It was confirmed during the tests that the created module really implements the algorithm of the domestic standard. The article shows a way to implement a fairly convenient graphical interface for accessing the cryptographic module, which enables the user not to call the command line and remember the sequence and types of parameters passed to p7zip. This implementation also takes into account the verification of the correctness of decryption and the reading of other error codes.

The open-source operating system ensures the protection of processed and stored data through Security Policies, kernel settings, additional software. One of the requirements is to support encryption in accordance with the law. It was required to create an application that performs encryption in accordance with the domestic standard, the only encryption algorithm allowed for use when working with information containing state secrets.

However, the lack of open-source software available in the public domain that performed the assigned tasks, while having sufficient performance, with open source, necessitated the development of a cryptographic module.

The main problem in creating a cryptographic application is to provide all verification procedures — splitting the data stream into blocks, padding to the desired length, creating a pseudo-random sequence initializing vector (IV). As a result,

it was decided to use ready-made software, in which these procedures were successfully implemented, [3,7].

For block ciphers, the use of IV is described by modes of operation. Randomization is also required for other primitives such as generic hash functions and derived message authentication codes. An initialization vector (IV) is introduced in CBC, CFB, and OFB encryption. Moreover, both the sender and the receiver must have the same IV at the beginning of the communication session. The IV does not have to be secret at all and can be transmitted along with the first ciphertext block. What's really important is that this value should be unpredictable in CBC and CFB modes and unique in OFB mode. Unpredictability in CBC and CFB modes can be achieved in several ways. For example, the value of a counter (say a message counter) can be converted using the same function. GPC can also be used to generate a pseudo-random sequence of the desired length.

As encryption in everyday work is more often applied to text information, especially to documents in DOC, DOCX format, the presence of standard expected sections in them creates a serious danger in the reliability of the password used for encryption. To eliminate this effect, it is recommended to pre-compress the information, thus reducing data redundancy. For this reason, the archiver was chosen as the main application, [8, 9].

The encryption algorithm in WinZIP versions earlier than 9 is not strong enough with the current computing power, but it also has a 64-bit key size. In this case, it is necessary to correct not only the encryption module, but also key extensions, check it for statistical properties, and so on. Moreover, the encryption block is one byte, [10, 11].

The most popular archiver WinRAR is proprietary, which means that it does not have open source, thereby automatically excluding this software from consideration.

7-Zip is a free, highly compressed file archiver. It supports multiple compression algorithms and multiple data formats, including proprietary 7z format with the highly efficient LZMA (Lossless Compression Algorithm) compression algorithm, [8]. The encryption algorithm used is AES with a block size of 128 bits, a key size of 256 bits.

II METHODS AND RESULTS OF EXPERIMENTAL RESEARCH

Based on the presence of an encryption mechanism in archiving programs and the feature of working in open-source operating systems, they are divided into the following classifications:

- WinRAR archiver is a version of RAR archiver developed for Windows operating systems. This program is designed to create archives in RAR and ZIP formats. In addition, this archiver provides the ability to archive and open 7Z, ACE, ARJ, BZIP2, CAB, GZ, ISO, JAR, LZH, TAR, UUE, Z formats;

- Unlike WinRAR archiver, 7zip archiver is absolutely free. 7zip is open-source software and most of its source code is licensed under the GNU LGPL. One of the main advantages of this archiving program is that it supports working with the command line. 7zip archiver can compress files 2% better than WinRAR. The compression efficiency of the 7zip archiver can be increased up to 10% using the LZW (Lempel-Ziv-Welch) algorithm. The LZW algorithm uses the idea of expanding the information alphabet. Instead of the traditional 8-bit representation of 256 characters in the ASCII table, 12 bits are used to define a table of 4096 entries.

The main purpose of the LZW algorithm is to replace a string of characters with codes using 4096 entries without analyzing the sequence of incoming characters. Each time a new character string is added, the character table is revised. A compression algorithm works when a string of characters is replaced by a code.

During encoding, the characters of the input stream are read sequentially and checked for the presence of such a line in the generated string table (Fig. 1).

A special feature of the LZW algorithm is that there is no need to save the string table to a file for decoding. The algorithm is designed in such a way that it is possible to reconstruct the table of strings using only the code flow.

As a result of using the LZMA version of the LZW algorithm in the 7zip archiver, it is possible to optimize the compression efficiency up to 10% by properly choosing the size of the dictionary, the word length and the number of streams. In open-source operating systems, it is possible to develop an encryption archiving program based on the GOST 28147-89 standard using this algorithm [4].

To organize encryption and archiving in the 7zip archiving program based on the GOST 28147-89 standard [10-11], the following modules should be developed and implemented:

- Gostvars() method does not perform any function. Used to maintain 7zip's compatibility with other archiving methods, it initializes the values of three global variables;

- GOST_SetKey_Enc method is designed to create round keys used in encryption according to GOST 28147-89 standard;

- the GOST method performs the round function of the Feistel network according to GOST 28147-89;

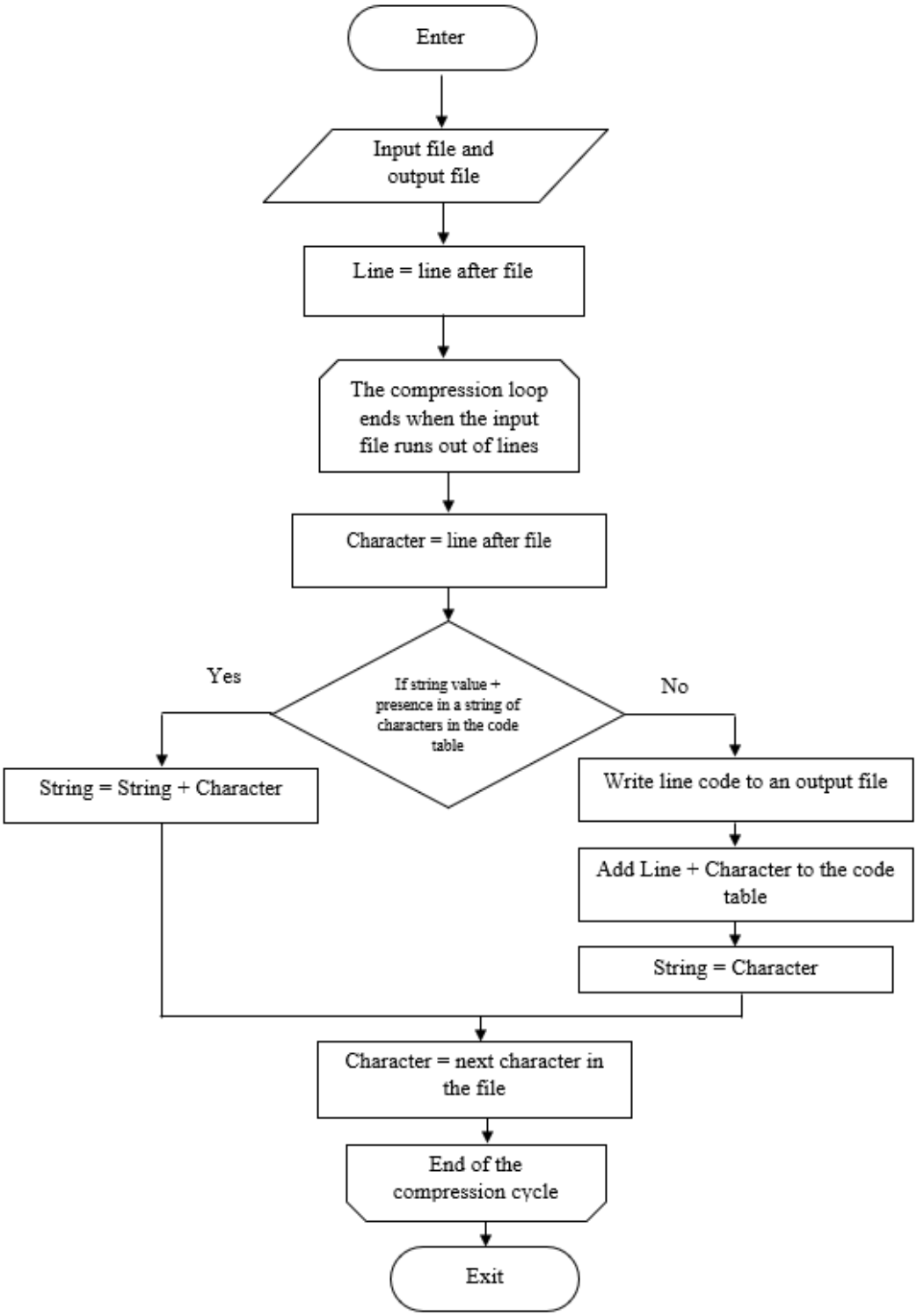

Fig. 1: Block diagram. The LZW algorithm is an information alphabet expansion algorithm.

- GOST_Code method encrypts/decrypts one message block (8 bytes) according to GOST 28147-89 standard;
- GOSTCbc_Init method is designed to write the initialization vector required for CBC mode in array form;
- GOSTCbc_Encode method is designed to encrypt a message whose length is a multiple of 16 bytes in CBC mode according to the GOST 28147-89 standard;
- GOSTCbc_Decode method is designed to decode a message whose length is a multiple of 16 bytes in CBC mode according to GOST 28147-89;
- the GOSTCtr_Code method is designed to encrypt/decrypt a message with a length of 16 bytes in STR mode according to GOST 28147-89;
- the get method is designed to convert a 4-byte unsigned byte into a single 4-byte unsigned number;
- the set method is designed to convert a 4-byte unsigned number to a 4-byte one.

The module is considered part of the 7zip archiver. Used to encrypt archive files with a password. The password is converted to an encryption key using the SHA-2 hash algorithm built into 7zip. Input data to the encryption module is prepared by 7zip according to the standard defined by the SVS encryption mode.

The characteristics of the data included in the module are as follows:

- the initialization vector iv must be a pseudo-random sequence. 64 bits are enough for GOST 28147-89, which are obtained by shifting 64 bits to the right to 128 bits. Only the 7zip archiver performs this check;
- the encryption key (byte array key) is obtained from the password entered by the user using hashing with the SHA-2 algorithm. The use of this algorithm depends only on its statistical, not cryptographic, properties. The length of the encryption key is 256 bits. Only the 7zip archiver performs this check;
- round keys (an array of unsigned 4-byte integers w) are generated from the encryption key by the module based on the key generation procedure established by the GOST 28147-89 standard. The result is a 1024-bit sequence;
- a message (byte array src) is created for encryption/decryption of files being archived. Only the 7zip archiving program is involved in creating the message and filling it with a length of 128 bits;
- the number of 128-bit blocks in the message (an unsigned 4-byte number). To use GOST 28147-89, this number in the module is multiplied by 2 to get the number of 64-bit blocks in the message [2].

When using these methods, the size of files for archiving (with encryption) should not exceed 32 GB, otherwise, it will cause an overflow of the used variables. The characteristic of the main working array is an unsigned 32-bit number for incoming and outgoing data (Fig. 2).

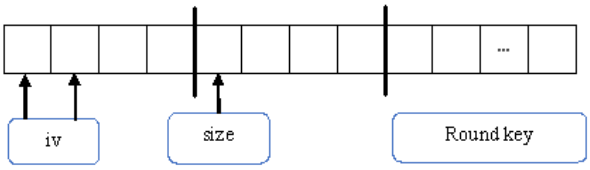

Fig. 2: Characteristics of the main working array.

Since the 7zip archiver uses the AES algorithm for encryption, there are some inconveniences in applying the GOST 28147-89 standard. Since the number of elements required for storing round keys in AES exceeds the number of elements required for GOST 28147-89 round keys, the number in the "size" field is kept the same as in AES. All unused elements of the array have no data (all data in this array is entered and used only by this module, other 7zip modules do not make any changes to it) [4].

To ensure the confidentiality of encrypted files, it is recommended to create a copy by calling the command 7za a –p <archive_name> <list_of_files_to_archive> from the command line. After this command, the archiving program will ask you to enter a password. In this case, the entered password is not saved in the history of the commands called in the system. To increase work efficiency, it is recommended to encrypt files before the end of the work session (turn off the computer) and decrypt them before working with these files. No special programs and actions are required during the operation of this module.

III ANALYSIS OF THE RESULTS

Depending on the specific archiving methods of open-source operating systems, different data formats may produce different results. For example, in many types of formats, the 7zip archiver shows the best result due to the very large size of the dictionary (32 MB). One of the important features below is that 7zip archives have 5% more archiving capacity than WinZIP archives, but are much slower to archive (Fig. 3). On average, it can be observed that the volume of archives is 30% larger than that of other types of archives (Fig. 4). A pilot test for high archiving speed

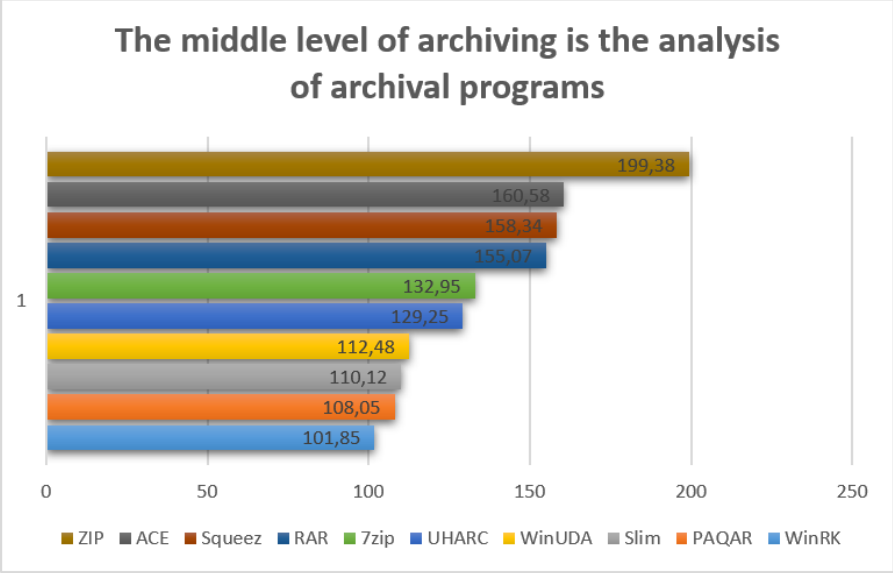

Fig. 3: The middle level of archiving is the analysis of archival programs.

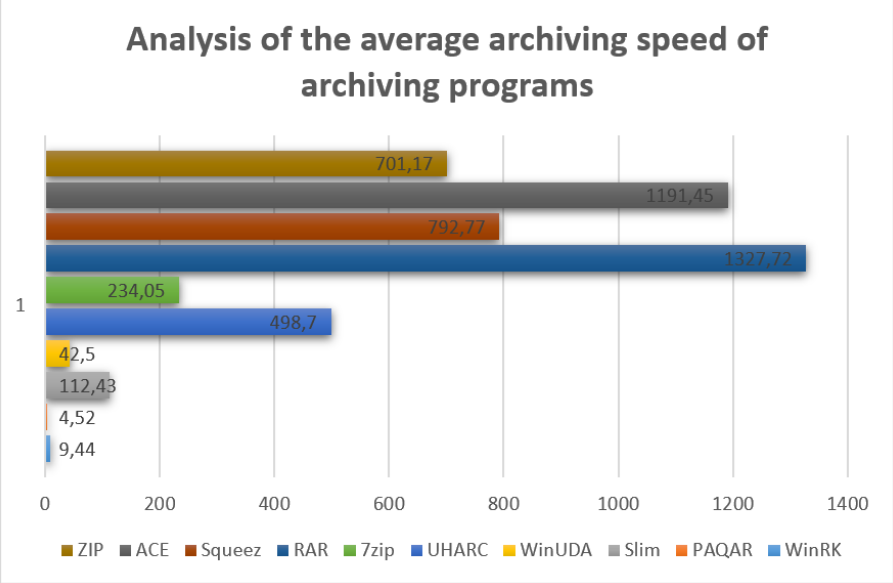

Fig. 4: Analysis of the average archiving speed of archiving programs.

was carried out. In this test, archiving software with the best archiving ratio was found to have a faster archiving speed. A 5 Mbps hard drive was chosen as the high archiving speed in the test system. This speed seems close to optimal.

Later, as speed increases, file storage may become the limiting factor of the subsystem. At the same time, for archiving 1 GB of data can be collected in 3-4 minutes. In addition, a limit on the use of RAM for archiving is set at 32 MB. According to the results of the experiment, such archiver programs can be used in systems with limited resources. The maximum archiving speed differs for different archiving programs. Since the difference between different archiving programs is relatively small at high archiving speeds, there is no need to test different datasets. The results of experimental tests can be expressed as follows (Table 1).

For many archiving programs, including 7zip, on computers with limited resources, a compression rate of 5 Mb/s was taken as the limiting speed in the test (Fig. 5).

	7zip	ACE	WinZIP	RAR	Win RAR	Squees	UHARC
Output directories	+	+	+	+	+	+	+
Creation of self-extracting (SFX) archives	+	+	+	+	+	+	-
Change the contents of the archive	+	+	+	+	+	+	+
Encryption mode	+	+	+	+	+	+	+
Restore archive	-/+	+	+	+	+	+	+
Split the archive into parts	+	+	+	+	+	+	-
Console version	+	+	+	+	+	+	+
Graphic version (GUI)	+	+	+	+	+	+	+
Asymmetry	+	+	+	+	+	+	-
RAM requirements, MB	5	14	8	8	21	8	21

TABLE 1: PROGRAM ARCHIVE "COMPARISON TABLE"

Highly compressed archive applications have some difficulty reaching the required 5 Mbps speed. The most common ZIP archiving program was chosen as a reference. Only archiving programs that provide the ability to archive directories have been tested.

The ACE, RAR and Squeeze archivers show good results but lag far behind the leading archivers in terms of maximum compression. The difference ranges from 25% to 105%, averaging 55% (Fig. 6).

7zip and UHARC can be recommended as universal archivers with a good compression ratio (30% worse than the best archivers). An important advantage of these archiving programs is that they are free and open-source. UHARC almost always archives with the best compression level, but it is a bit less functional. In the maximum mode, the UHARC archiver requires 54 MB of RAM, which allows you to use this program on computers with a limited amount of RAM. UHARC is the leader in high-speed archiving. 7zip is the best asymmetric archiver in terms of archive quality. Archives created with it can be used on almost any computer, but keep in mind that the size of the dictionary does not exceed 256 MB. In the maximum mode, the archiving speed can be increased by 2-3 times by decreasing the value of the Word size parameter. The archiving speed will decrease by more than a few percent. The 7zip archiver has a special PPMd method for archiving text. This method is similar to the RAR text compression method. 7zip uses special methods to archive media data.

WinUDA and Slim are among the programs with a high degree of archiving. Despite the low performance and relatively small functionality, the WinUDA archiving program leaves a good impression on the user. All necessary functions are available, including the ability to create self-extracting (SFX) archive files. Also, the unpacker module takes 18 KB. There is Mode-0 compression, requiring 24 MB of RAM. At the same time, the speed increases to 127 Kbps, and the compression ratio is somewhat worse. Slim has a slightly higher level of archiving (taking into account the specifics of testing processes) and speed but lacks such important features as creating offline decompressed (SFX) archives, a graphical (GUI) version and continuous archiving mode.

PAQAR, one of the best conventional archiving software, has a speed of 5 Kbps. Work is currently underway to develop special methods designed only for certain file formats.

IV CONCLUSION

In conclusion, it should be noted that several archiving programs that support data encryption have been reviewed and tested. The WinRAR archiver uses its own encryption algorithm, which works in blocks of 1 byte. The 7zip archiver program performs AES encryption and performs

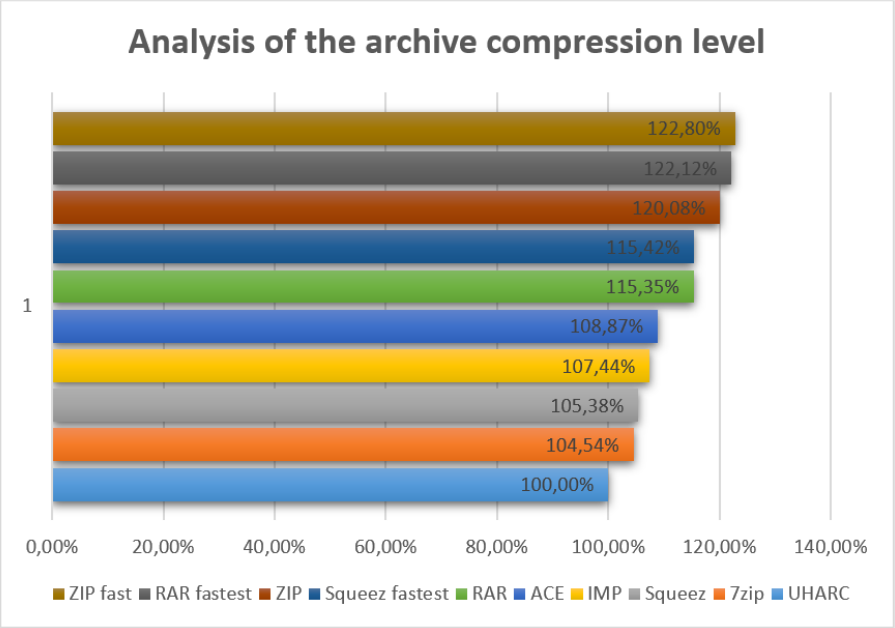

Fig. 5: Analysis of the archive compression level

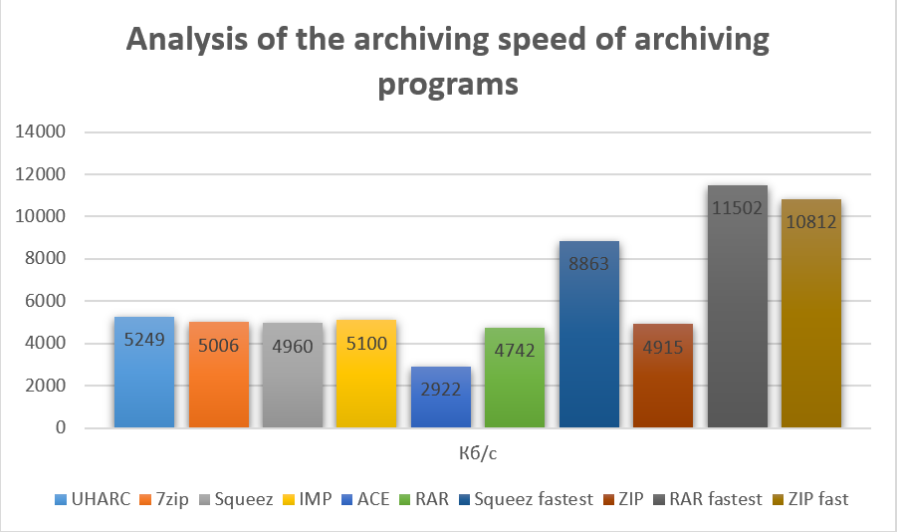

Fig. 6: Analysis of the archiving speed of archiving programs

all the necessary data preparation before encryption (creating a key from a password, adding a multiple-message to the block length by checking the decryption using an extended sequence, creating an initialization vector, etc.). Using GOST 28147-89 also slightly improves the encryption speed since the AES block size is twice the GOST 28147-89 block size. In the course of the analysis, 7zip was adopted as an archiver in which the maximum archiving speed mode can be increased up to 2-3 times by reducing the file parameters, and with the help of these tests, a specially created archiving and encryption program according to the local standard can be used on almost any computer, with that the size of the dictionary does not exceed 256 MB.

V REFERENCES

[1] Qi Luo, Advancing Computing, Communication, Control and Management, Springer Science & Business Media, 2009, p.290.

[2] Algorithm of cryptographic transformation GOST 28147-89, IPK Publishing House of Standards, Moscow, (Russian), 1996.

[3] Qi Luo, Advancing Computing, Communication, Control and Management, Springer Science & Business Media, 2009., p.290.

[4] Algorithm for cryptographic transformation GOST 28147-89, IPK Standards Publishing House, Moscow, 1996.

[5] Mao, V. Modern cryptography: theory and practice: trans. from English / B. Mao. - M .: Publishing House "Williams", 2005.

[6] Stallings, V. Cryptography and protection of networks: principles and practice: trans. from English / V. Stallings. - M .: Publishing House "Williams", 2001.

[7] Ferguson, N. Practical cryptography: trans. from English / N. Ferguson, B. Schneier. - M .: Publishing House "Williams", 2005.

[8] Shannon, K. Communication theory in secret systems // Works on information theory and cybernetics: trans. from English / K. Shannon. - M .: Publishing house of foreign literature, 1963. p. 333-369.

[9] Schneier, B. Applied cryptography: protocols, algorithms, source texts in C: per. from English / B. Schneier. - M .: Triumph, 2012.

[10] GOST 28147—89 “Information processing systems. Cryptographic protection. Algorithm for cryptographic transformation ".

[11] GOST R 34.13—2015 “Information technology. Cryptographic information protection. Modes of Operation of Block Ciphers ".ISO/IEC 18033-2:2006 Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers.

[12] FIPS PUB 197. Federal Information Processing Standards Publication. Advanced Encryption Standard (AES). November 26, 2001.

Acta of Turin Polytechnic University in Tashkent, 2023, 30, 20-24
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

EFFICIENT IMPLEMENTATION OF A BUCK CONVERTER CONTROL USING A LOW PERFORMANCE MICROCONTROLLER

Francesco Gregoretti* **and Maksudjon Usmonov**
Turin Polytechnic University in Tashkent, Uzbekistan
*Email: francesco.gregoretti@polito.uz

Abstract– The implementation of power switching converters by low-cost embedded systems is in general limited by the low operating frequency as well as the resolution of the variable duty cycle waveform which controls the power converter. The paper analyzes how the use of dedicated hardware units may partially overcome these limits and whether a microcontroller in an embedded system may both operate as a power supply controller and at the same time perform other application tasks which do require a limited amount of processing power.

Key words– component, formatting, style, styling, insert (key words)

I INTRODUCTION

A number of simple applications mapped to embedded systems require both to control a subsystem to control and the same time to generate a voltage source different from the main supply and in battery operated devices the conversion task must be efficient. Often the processing power required for the control task is limited and for a large part of the time the processor is idle even with a simple architecture. If the application where the processor is embedded requires power conversion from/to different sources the control and the power generation tasks may be performed in parallel.

In order to evaluate the feasibility of such an approach we decided to implement a test system and to perform a number of measurements to identify the limits of power regulation by a microcontroller and the processing power required.

The organization of the paper is the following one. Section II describes the experimental testbench used. Section III briefly reviews the main parameters of a switching converter and the description of the design choices taken in the experiment.

Section IV describes the results of the measurements and finally section V will derive some conclusions and suggest possible further investigations

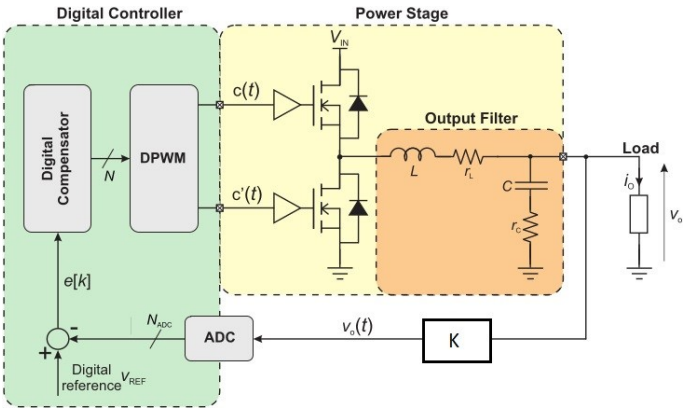

Fig. 1: The experimental testbench.

II THE EXPERIMENTAL TESTBENCH

The structure of the experimental testbench is shown in fig.1. The two main blocks are the Digital Controller and a Power Stage which is controlled by means of a Digital Pulse Width Modulator (DPWM).

A. The Digital controller

In order to demonstrate the feasibility of the approach we decided to start from a well-known but performance limited microcontroller system. In the frame of the development of teaching modules for power electronics, we chose a simple Arduino Uno board [1] which includes a 10bit Analog to Digital Converter (ADC) with a reference voltage VREF equal to 5 V. The core is an ATmega328P processor with a 16 MHz clock, corresponding to an average instruction time of 0.1 us and a number of peripherals among which a timer unit that may be configured as DPWM as better described in the next section.

B. The power stage The power stage is a synchronous buck

power converter developed in a previous project composed of two power switches, driven by the two non-overlapping outputs of the DPWM, an inductor and an output filter capacitor.

The value L is 100 mH and the value of C is 220 mF giving a characteristic resonant frequency of the filter of approximately 1 kHz. The parasitic series resistance rC of the capacitor is 90 mW. The system is designed to operate with an input voltage varying from 10 to 18 V and the digital reference may be set for an output voltage from 2V to 10V and the maximum output current is 2 A. The load resistance used in the experiments has been 100 W.

The output voltage is scaled down by a factor **K** in order to make the input voltage to the ADC always lower than the reference voltage of the ADC itself even in the worst condition when $V_o = V_{in}$ which may happen if the upper switch is always closed.

III DESIGN AND PARAMETERS

The operation of a switching buck converter is quite straightforward. The DPWM sets the duty cycle D of a square wave which opens and closes the power switches in such a way that a fraction of the input voltage V_{in} is filtered by the LC output filter and becomes the output voltage V_o. If the frequency of the square wave is far higher than the cutoff frequency of the filter, then V_o is almost constant and equal to:

$$V_o = D \cdot V_{in} \tag{1}$$

The period of the square wave with variable duty cycle is referred to as *switching cycle.*

The compensator in the digital controller has the task to compare the input value of the ADC to a digital reference setting the value of the output voltage and to set the value of the duty cycle D on the basis of the error signal derived from this comparison. The operation of the compensator is periodical with a period referred to as *control cycle*. In integrated controllers the two cycles are coincident, that is the new value of D is computed by the compensator during the switching cycle and applied to the following one. However, depending on the implementation of the control cycle the control frequency may be lower than the switching frequency, that is

$$f_{control} = f_{sw} \tag{2}$$

Let us now first consider the main parameters of a switching power converter, which are basically the output regulation and the output noise. Then we will analyze the implementation choices which have been taken in the design of the experiment.

A. Output Regulation

The output regulation (OR) is the maximum variation of the D.C. output voltage from its nominal value and is the sum of two components, namely the line regulation considering the variations of the input load and the load regulation considering the variations of the load. The main factor affecting this parameter is the precision of the ADC (N_{ADC}), that the minimum variation of the output voltage which may be detected.

$$OR = V_{ADC} \cdot K \cdot 2^{-N_{ADC}} \tag{3}$$

The output regulation decreases by increasing the number N_{ADC} of bits of the ADC converter and for a precise output value a large value of N_{ADC} is required.

B. Output Noise

Although the output voltage is ideally constant there are A.C. noise components due both to parasitic parameters of components and to the digital operation of the controller which implies a quantization of the output to the DPWM and of the output of the ADC. The two main components are the Ripple noise (δV) and the Limit Cycle (LC) noise.

1) Ripple noise

The ripple noise is due to the A.C. component of the inductor current which flows in the output capacitor of the power stage and, due to the non-zero value of the Equivalent Series Resistance (shown as rC in fig. 1) of the capacitor, generates a variable voltage at the switching frequency f_sw. It is known in the literature that the peak value is equal to:

$$\triangle V = \triangle I \cdot ESR = \frac{V_{in} D(1-D)}{L \cdot f_{sw}} ESR \tag{4}$$

It may be easily verified that it has a maximum for $D = 0.5$ and the key point is that for a given value of inductance the noise decreases when the switching frequency is increased.

2) Limit Cycle noise The Limit Cycle (LC) noise derives from the fact that the output of the DPWM is quantized, that is the number of values of possible values of the duty cycle D is limited to $2^{N_{PWM}}$ where N_{PWM} is the number of bits controlling the modulator. The voltage difference between two output signals corresponding to duty cycles D_i and D_{i+1} is

$$\triangle V_i = V_{in} 2^{N_{PWM}} \tag{5}$$

If the target voltage is not equal to one of the quantized output levels the output voltage will oscillate between levels V_{oi} and V_{oi+1} because the controller tries to keep the output voltage equal to the target.

This oscillation takes place at a frequency equal to the control frequency or one subharmonic because the output averaging depends on many parameters such the filter cutoff

frequency, the controller setting, the load and also the amplitude of the ripple voltage. If the control frequency is far higher than the cutoff frequency of the filter, then the higher components of the LC noise will be filtered. A large research activity has been devoted to the reduction of the lower frequency components of this noise, mostly by dithering techniques [2,3,4] which aim to move these components to higher frequencies where they may be filtered. Unfortunately, these techniques may not be applied if the fundamental control frequency is of the same order of magnitude of the filter cutoff frequency.

The only other solution to cancel this noise is to avoid the oscillation between two different output levels. To obtain this the ADC quantization bin must be larger than the LSB of the Pulse Width Modulator (PWM) so at least one of the quantized DC output levels at a fixed duty cycle falls in the zero-error bin of the converter, i.e:

$$q_{ADC} = q_{PWM} \tag{6}$$

If the number of bits of the ADC is N_{ADC}, its reference voltage is V_R, the number of bits controlling the PWM modulator is N_{PWM} and the maximum input voltage V_{inMAX} the previous equation becomes:

$$\frac{V_{REF}}{2^{N_{ADC}}} > \frac{V_{inMAX}}{2^{N_{PWM}}} \tag{7}$$

If we assume that $V_R = V_{inMAX}$ then the condition for avoiding the limit cycle becomes:

$$N_{PWM} > N_{ADC} \tag{8}$$

This may be obtained by reducing the number of bits of the ADC, but it is clear from equation 3 that also the output regulation will be reduced.

C. Implementation choices

The design of a converter using a simple microcontroller must start from the consideration that a full realization in software is not feasible. The critical unit is the DPWM modulator whose straightforward implementation would be a nested loop of two counters, one for the duty cycle and one for the switching period. With $N_{PWM} = 8$ it would require a few thousands of instructions per switching cycle, leading to switching frequencies of the order of 4 kHz. According to equation (4) this would lead to a ripple noise of the order of 1V which is clearly unacceptable. Moreover, such a solution would use all the available CPU time voiding the possibility of performing other tasks in parallel.

For this reason, we took advantage of dedicated timer/counter unit of the ATmega328P processor which may directly implement a DPWM without software intervention. It is a counter which has two programmable thresholds. When the first one is reached an output pin is toggled from the high to the low level and when the second one is reached the counter is reset. The first threshold set the duty cycle and the second the switching frequency. The counter may be directly fed by the input clock at 16 MHz and the value of the second threshold it is possible to make a tradeoff between the number of bits N_{PWM} and the switching frequency f_{sw}. We chose for most of the experiments the combination with $N_{PWM} = 8$ and $f_{sw} = 64kHz$ with an expected ripple noise of 70mV in the worst case conditions.

The control loop has been implemented in software with a Proportional-Integrative (PI) compensator which performs a control cycle in approximately every 200 ms, out of which 100 ms are required to perform the analog to digital conversion. A maximum control frequency of 5 kHz may be expected and for any value under that we cannot expect the limit cycle noise to be filtered by the output filter at 1 kHz. We therefore chose to set the control frequency at 1 kHz using a timer interrupt. In such a way the control task takes 200 ms/1 ms = 20% of the total CPU time leaving 80% for other tasks.

IV MEASUREMENTS AND ANALYSIS

Two main set of measurements have been performed, the first one without limiting the effect of the limit cycle and the second one setting the condition indicated by equation 6.

In each measurement, the output voltage was set to a given value (ranging from 2 to 9) by setting the internal reference and then the input voltage varied, in steps of 1V from 10 to 18V.

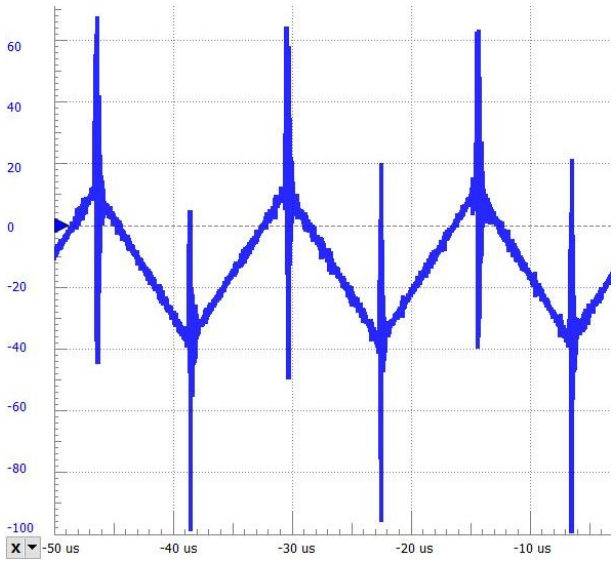

Fig. 2: Maximum ripple at switching

The first result is that the ripple voltage appears to be limited. Fig. 2 shows the ripple waveform for the maximum peak to peak case ($V_{in} = 18V, V_{out} = 9V$). In the picture, the voltage spikes are artifacts due to the coupling of the probe to the drivers of the gate switches. The value of the ripple is slightly lower than the predicted one, probably due to the lower value of the parasitic resistance of the capacitor.

The second result is that the LC noise is clearly present on the output as shown in the example of Fig.3 which was recorded in one of the measurements performed.

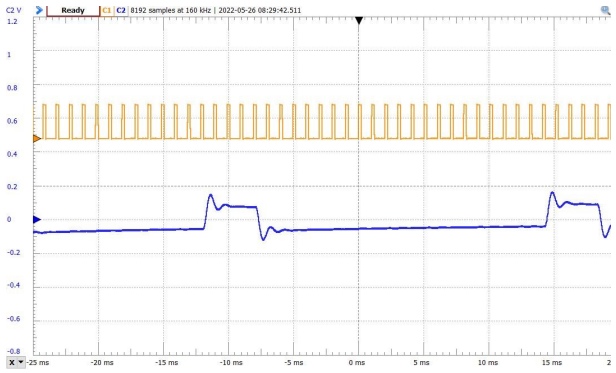

Fig. 3: Limit cycle noise

The top timing diagram of the figure is a signal synchronized to the control cycle. In this case the output is for 4 cycles at the upper value of the duty cycle and for 24 at the lower one. The table in fig. 4 shows the occurrence, and the peak value in mV of the LC noise, for all the combinations of the input and output voltages for which the measurements were taken.

V_{in} / V_{out}	10	11	12	13	14	15	16	17	18
2	0	0	0	0	0	0	0	0	120
3	0	0	0	0	80	0	0	0	130
4	0	0	0	70	0	0	0	0	150
5	0	60	0	70	0	0	0	0	150
6	0	0	0	0	0	0	0	100	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	90	100	0
9	0	0	0	0	70	0	90	0	0

Fig. 4: LC noise (in mV) for all V_{in} and V_{out} combinations

As clearly visible the noise is not present in all cases but only when the input and output values make a variation of one value of D change the output value of the ADC. It should be pointed out that since the noise is dependent on many parameters another measurement run could produce a very different picture.

Figure 5 shows the variation of the output voltage as a function of V_{in} for different output nominal values and the table of fig. 6 contains the maximum error e in mV with respect to the nominal value.

The output error and the line regulation appear to be satisfactory for most applications.

Another set of measurements was performed with a controller modified in order to cancel the LC noise according to equation 8. This has been obtained by masking the lower bits of the data acquired from the ADC, reducing in practice its precision. Fig. 7 shows the variation of the output voltage as a function of V_{in} and in the case of Fig. 8 the error with respect to the nominal value. As expected, the error is significantly larger, from 4 to 5 times, than in the previous case.

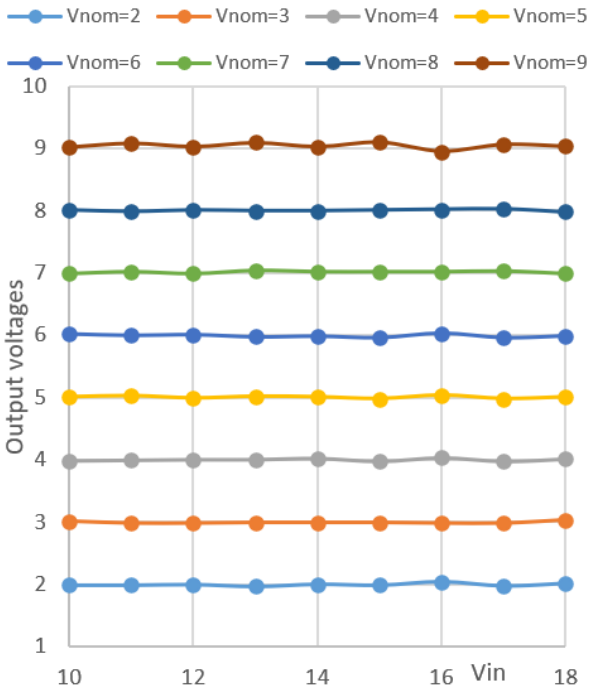

Fig. 5: V_{out} as a function of V_{in} for a non LC free setting

Vout	2	3	4	5	6	7	8	9
e	45	30	30	40	30	40	25	90

Fig. 6: Output error (mV) for a non LC free setting

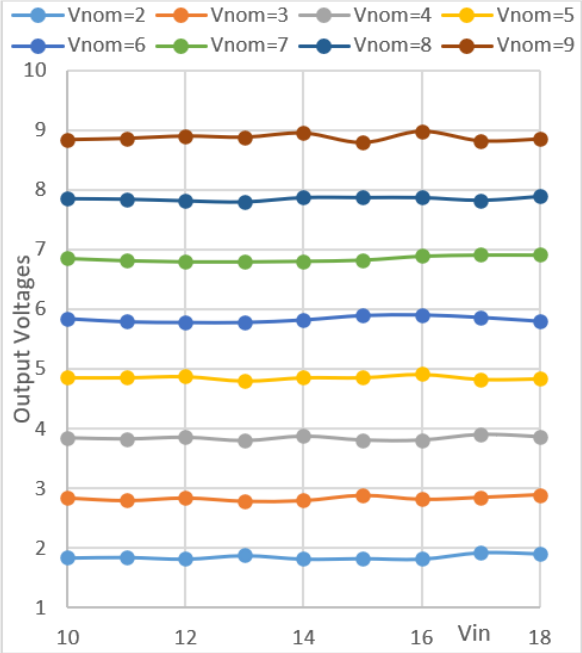

Fig. 7: V_u as a function of V_{in} for a LC free setting

Vout	2	3	4	5	6	7	8	9
e	180	200	200	200	210	200	200	200

Fig. 8: Output error e in mV for a LC free setting

V CONCLUSIONS AND DEVELOPMENTS

The paper has shown the design of the controller for a buck converter implemented using a popular and limited performance microcontroller and has the demonstrated that, taking advantage of the hardware characteristic of the processor it is possible to efficiently implement a power converter. The performance limits of the processor make it impossible to fully optimize the output characteristics of the converter.

In a real application, depending on the characteristics of the system to be implemented it is necessary to make a choice between a higher precision of the output D.C. value associated to a higher noise due to the limit cycle phenomenon and a lower output precision associated to a lower level noise.

The work described here requires to be extended to consider also the dynamic parameters of the converter such as the response to input voltage and load transients which have not fully investigated due to the requirements for more sophisticated measurement equipment.

VI REFERENCES

[1] L. Louis, "Working principle of Arduino and using it as a tool for study and research," International Journal of Control, Automation, Communication and Systems, vol. 1, no. 2, pp. 21-29, 2016.

[2] H. Peng, A. Prodic, E. Alarcon, and D. Maksimovic, "Modeling of quantization effects in digitally controlled DC–DC converters," IEEE Trans. Power Electron., vol.22, no. 1, pp. 208–215, Jan. 2007.

[3] J. Fang, X. Yang, L. Zhang, and Y. Tang, "An optimal digital pulse width modulated dither technique to enhance the resolution of high frequency power converters," IEEE Trans. Power Electron., vol. 32, no. 9, pp. 7222–7232, Sep. 2017.

[4] M. Usmonov, P. S. Crovetti, F. Gregoretti, and F. Musolino, "Suppression of quantization-induced limit cycles in digitally controlled DC-DC converters by dyadic digital pulse width modulation," in Proc. IEEE Energy Convers. Congr. Expo., Baltimore, MD, USA, 2019, pp. 2224–2231.

Acta of Turin Polytechnic University in Tashkent, 2023, 30, 25-29
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

STUDYING FACTORS DETERMINING THE SERVICE LIFE OF ELECTRIC MACHINES

Jamilov Sh.
Tashkent State Transport University, Tashkent Uzbekistan.
Email: shuhratjamilov@mail.ru

Abstract– In this article, the process that occurs during the use of electric machines, that is, what reactions occur in the insulating part of electric machines as a result of temperature rise, when the temperature of electric machines exceeds the external ambient temperature specified in the regulatory documents, i.e. 40^oC, the temperature of electric machines increases. The composition of the insulation materials, which should be used for the thermal class permitted in the insulation materials, is also analyzed.

Key words– electric machine, temperature, insulation, coil, durability, material, collector, ring, temperature, heat resistance, reliability.

I INTRODUCTION

Electric machines heat up during operation. Temperature changes can vary, meaning that some electric machines will heat up less, while others will heat up more. The stable value of the temperature of electric machines depends on the load on its shaft. With a large load, a large amount of heat is released per unit of time, that is, the temperature in the steady state of the electric motor is higher. The permissible temperature of electric machines depends on the insulation class of the coils [1].

Since temperature is an important factor in the deterioration of electrical insulation materials and insulated systems for electric machines, heat resistance classes are adopted to evaluate the temperature resistance of electrical insulation.

The heat resistance class of insulation of electric machines reflects the maximum operating temperature characteristic of these electric machines under nominal load and other conditions.

II EFFECTS ON THE SERVICE LIFE OF ELECTRIC MACHINES

In electrical machines with all information, the insulation class is indicated. Heat resistance is one of the most important qualities of electrical insulation materials, because it determines the permissible loads of electrical machines and devices. The ability of electrical insulating materials to withstand high temperature effects, as well as sudden changes in temperature, without damaging them, is called heat resistance. You should know that when the temperature of the windings of electric machines exceeds the permissible values, the service life of the insulation decreases sharply. Therefore, the heat resistance of the insulation is the main requirement that determines the reliability and service life of electric machines, which should usually be 15-20 years [2].

Electric machines with class A insulation are almost never produced, and class E is used in limited areas in low-power machines. They are mainly used for insulation of B and F classes and H class in special machines working in difficult conditions (metallurgy, mining equipment, transport). In the last 60-70 years, the mass of electric machines has been reduced by 2.5-3 times as a result of increased use of heat-resistant materials, improvement of the properties of electrical engineering steels and improvement of constructions [3].

With a constant load on the shaft, in electric machines, a certain amount of heat is released per unit of time. The maximum allowable temperature increase of active parts of electric machines is shown in Table 1.

In Table 2, as an example, when measuring the temperature of coils using the resistance method, the maximum permissible temperature rises for individual parts of electric machines for general use (U) and traction (T) for continuous operation.

The temperatures of the collector and slip rings are determined by matching (i.e., by measuring the coil resistance) and thermometers as a result of the temperature rise. These data are assumed for an ambient temperature of $+40^oC$ for U machines and $+25^oC$ for T machines [4].

The temperature of the ambient air at which electrical machines used in general industry can work at rated power is considered to be 40^oC.

For electric machines used in general industry, if the ambient temperature is more or less than +40, then the standard allows certain changes in the permissible temperature rise.

Heat resistance class	**Temperature, characterizing the heat resistance of this class ^{o}C**	**Electrical insulation materials corresponding to this heat resistance class**
Y	90	Textile and paper materials made of organic fillers from cotton, natural silk, cellulose and polyamides (ribbons, paper, cardboard, fibers), wood and plastics
A	105	Fibrous materials made of cellulose or silk impregnated or impregnated with a liquid electrical insulating material and other materials and combinations of materials of this class. In fact, class Y materials impregnated with insulating material or immersed in liquid dielectrics (natural resins, oil, asphalt, cellulose ether varnishes, transformer oil, thermoplastic compounds); varnished fabrics, insulating tapes, varnished papers, electrical cardboard, getinax, textolite, impregnated wood, wood laminates, some synthetic films, wire insulation made of cotton, silk and lavsan (PBB, PEVLO, PELSHO, etc.), enamel wire insulation (PEL PEM PELR and LDPE, etc.);
E	120	Some synthetic organic films, as well as other materials and combinations of materials corresponding to this class, synthetic varnishes, some lacquered based on thermosetting synthetic resins and mixtures (epoxy, polyester, polyurethane, PLD wire insulation, PEPLO from lavash, enamel wire insulation) fabrics. PEVTL, PETV, etc., based on polyurethane and polyamide resins);
B	130	Mica-based materials (including organic substrates), asbestos and glass fibers used with organic binders and impregnations, as well as other materials and combinations of materials suitable for this class. Materials based on paper, cloth or organic substances, mica (micanites, mica tapes, mica, mica-plastics), fiberglass (glass cloth, glass fiber), asbestos fibers (thread, paper, fabrics); film glass plastic "Isoflex"; plastics with inorganic filler; laminated plastics based on fiberglass and asbestos materials; thermosetting synthetic compounds; enamel insulation of PETV, PETVP, etc. wires based on polyester varnishes and thermoplastic resins. Absorbent compositions are bitumen oil-resin varnishes based on natural and synthetic resins;
F	155	Mica-based materials (including organic substances), asbestos and glass fibers used with organic binders and absorbents, as well as other materials and combinations of materials suitable for this class. In fact, mica, fiberglass, asbestos are listed in class B, but unsupported or inorganic supported materials; fiberglass "Imidoflex", PSD, PSDT type wires with fiberglass and asbestos insulation, as well as capron-based PET-155, PETP 155 type enamel insulation. Absorbent compositions are heat mresistant synthetic varnishes and resins.
H	180	Materials based on mica, asbestos and glass fibers used in combination with synthetic binders and absorbents, as well as other materials and combinations of materials suitable for this class. In fact, the materials listed in class B are mica, fiberglass and asbestos without substrate or with inorganic substrate, organosilicon elastomers, fiberglass and asbestos insulation of PSDK wires, PSDKT types, enamel insulation of PET-200 wires, types based on PETP-200 Organosilicon varnishes, etc.; impregnating compositions are organosilicon varnishes and resins.
C	above 180	Mica, ceramic materials, glass, quartz, unbindered or with inorganic binders, as well as other materials and combinations of materials suitable for this class.

TABLE 1: THE MAXIMUM ALLOWABLE TEMPERATURE INCREASE OF ACTIVE PARTS OF ELECTRIC MACHINES.

Electric machine parts	**Maximum permissible temperature rise, with insulation class ^{o}C**									
	A	E	B	F	H	A	E	B	F	H
	U in general use					traction T				
Armature windings of DC machines and windings of synchronous machines	60	75	80	100	125	85	105	120	140	160
Multi-layer excitation coils of DC and AC machines, compensation coils	60	75	80	100	125	85	115	130	155	180
Single-line excitation coil on non-insulated surfaces	65	80	90	110	135	85	115	130	155	180
In the collector part and connecting rings	60	70	80	90	100	95	95	95	95	105

TABLE 2: MEASURING THE TEMPERATURE OF COILS USING THE RESISTANCE METHOD.

When the ambient temperature exceeds 40^{o}C, the load on electric machines should be reduced so that the temperature of its individual parts does not exceed the permissible values. When using the car in mountainous areas, where the heat transfer decreases due to the decrease in atmospheric pressure, the standard allows for a slight decrease in temperature rise [5].

Despite the decrease in ambient temperature, it is not allowed to increase the current load by more than 10% of the nominal current. Asynchronous electric machines can be affected by changes in the supply voltage, which, along with the decrease in voltage, reduces the power on the machine shaft by the square, and in addition, when the voltage is below 95% of the nominal, there is a significant increase in the current of the machine and the causes ams to heat up. An increase in voltage above 110% of the nominal also leads to an increase in the current in the machine windings, and the heating of the stator increases due to inrush currents [6].

When the temperature rises, many materials begin to burn and become conductors. As a result of prolonged exposure to elevated temperatures, all materials become brittle long before burning, are easily destroyed, and lose their insulating properties. This process is called thermal aging. Experience shows that an increase in insulation temperature by 10^{o}C reduces its service life by about half. Thus, for Class A insulation, an increase in temperature from 95 to 105^{o}C reduces its service life from 15 to 8 years, and an increase in temperature to 120^{o}C reduces it to two years. This phenomenon is based on the general law of the dependence of the rate of chemical reactions on temperature, described by the Van't Goff-Arrhenius equation.

The rate of many reactions increases with temperature.

According to Van't Goff's rule: for every 10^{o}C increase in temperature, the rate of most reactions increases 2-4 times.

$$\frac{vt_2}{vt_1} = \gamma^{\frac{t_2-t_1}{10}} \tag{1}$$

where γ is the temperature coefficient, which shows how many times the reaction rate increases with an increase in temperature by 10^{o}C.

An increase in the reaction rate with an increase in temperature is not only due to an increase in kinetic energy and the number of collisions of reactant particles. If all the colliding particles were to react with each other, the reaction would be like an explosion. But some collisions do not lead to the formation of new substances (a, Figure 1).

The reaction occurs only as a result of effective collision (b, Figure 1) of particles with excess energy - activation energy.

This energy is sufficient to break or weaken bonds, which can cause atoms to rearrange into new molecules.

As the temperature increases, the percentage of active molecules increases; the number of effective collisions increases. Thus, the rate of chemical reaction increases.

Van't Goff's rule is very inconvenient and can be used only in a very limited temperature range.

The Arrhenius equation describing the temperature dependence of the rate constant is more accurate.

$$k(T) = Aexp\left[-\frac{E_A}{RT}\right] \tag{2}$$

Here, R is the universal gas constant; A is a pre-exponential multiplier that does not depend on temperature and is determined only by the type of reaction; E_A is the activation en-

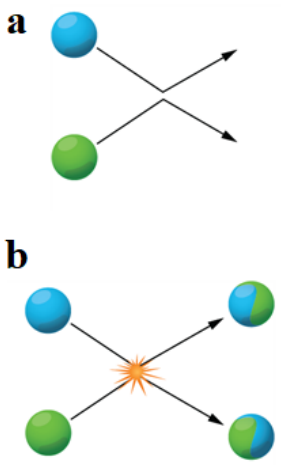

Fig. 1: Collision of inactive and active particles.

ergy, which can be described as a kind of threshold energy: if the energy of the colliding particles is less than E_A, then no reaction will occur in the collision, if the energy exceeds E_A, the reaction will occur ladi The activation energy does not depend on the temperature. E_A

Graphically, the relationship k(T) looks like this:

Chemical reactions almost do not occur at low temperatures: $k(T) \to 0$. At very high temperatures, the rate constant tends to a limiting value: $k(T) \to A$. This means that all molecules are chemically active and each collision causes a reaction.

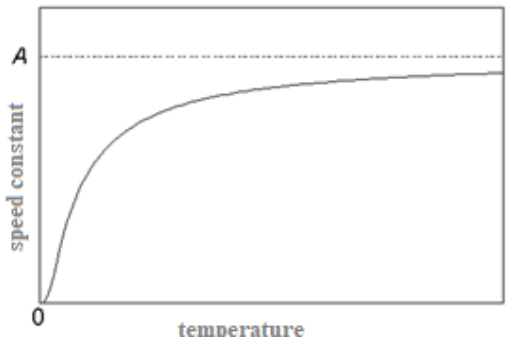

Fig. 2: Graphical dependence of k(T)

The activation energy can be determined by measuring the rate constant at two temperatures. Equation (3) implies the following:

$$E_A = \frac{R \cdot T_1 \cdot T_2}{T_2 - T_1} \cdot ln\frac{k_2}{k_1} \tag{3}$$

More specifically, the activation energy is determined from the rate constant values at several temperatures. For this, the Arrhenius equation (3) can be written in logarithmic form.

$$lnk = lnA - \frac{E_A}{RT}$$

we record experimental data in $lnk - \frac{1}{T}$ coordinates. The tangent of the slope of the obtained straight line is equal to $-\frac{E_A}{R}$. For some reactions, the pre-exponential factor is slightly dependent on temperature. In this case, the so-called experimental activation energy is determined:

$$E_{taj} = RT^2 \frac{dlnk}{dT} \tag{4}$$

If the exponent factor is constant, then the experimental activation energy is equal to the Arrhenius activation energy: $E_{taj} = E_A$.

For example, using the Arrhenius equation, we estimate at what temperature and activation energy the Van't-Hoff law holds [8].

We express Van't-Hoff law (1) as a power-law dependence of the rate constant:

$$k(T) = B \cdot \gamma^{\left(\frac{T}{10}\right)}$$

Here B is constant. We compare this expression with the Arrhenius equation (2), taking the value $\sim e = 2.718$ for the temperature rate coefficient:

$$Bexp\left(\frac{T}{10}\right) \approx Aexp\left[-\frac{E_A}{RT}\right]$$

We get the natural logarithm of both parts of this approximate equation:

$$lnB + \left(\frac{T}{10}\right) \approx lnA - \frac{E_A}{RT}$$

That is, technological overloading of working machines or changes in the voltage in the supply network lead to an increase in the current in the machine coils and the temperature of the coil is higher than allowed for this class, as a result of which the service life of the machine decreases rapidly [7]. By differentiating the obtained relationship depending on the temperature, we find the desired relationship between the activation energy and the temperature:

$$E_A \approx \frac{RT^2}{10}$$

If activation energy and temperature roughly satisfy this relationship, Van't-Hoff's rule can be used to determine the effect of temperature on reaction rates.

III CONCLUSION

The basis for establishing rational temperature limits for insulation is made only on the basis of experience or appropriate tests (see: GOST 8865-93). The above-mentioned limited heating temperature for individual classes of insulation is not fully applicable in practice, since it is impossible to establish exact control over the temperature of the insulation of the hottest parts in the use of electrical machines and devices. Therefore, the current standards for electric machines set lower limits for the permissible temperatures of individual machine parts, depending on the appearance and location of these parts in the machine.Taking into account the above, it should be noted that insulation is a factor that determines the long-term operation of electric machines.

IV REFERENCES

[1] V. Madonna, P. Giangrande and M. Galea, "Introducing physics of failure considerations in the electrical machines design," in 2019 IEEE International Electric Machines & Drives Conference (IEMDC). IEEE, 2019, pp. 2233–2238.

[2] Khamidov O., Yusufov A., Kudratov S., & Yusupov A. (2023). Evaluation of the technical condition of locomotives using modern methods and tools. In E3S Web of Conferences (Vol. 365, p. 05004). EDP Sciences.

[3] ANSI/NEMA MG 1-2016. Motors and generators. Virginia, Rosslyn: National Electrical Manufacturers Association, 2016.

[4] Rustamovich K.O., (2022). Development of a System for Cold Installation of a Leading Gear Transmission on the Electric Electric Electric Electric Electric Locomotive of Uzbekistan ELR Asynchronous Traction. Nexus: Journal of Advances Studies of Engineering Science, 1(4), 72-75.

[5] Jamilov S., Abdurasulov S. & Azimov S. (2022). The effect of moisture on electrical insulating parts of electric machines of locomotives. Vol. 6, No. 6, (2022): Journal of new century innovations. Volume-6, Issue-6, www.wsrjournal.com.

[6] Djanikulov A.T., Jamilov Sh.F., Miravazov A.R., Examination of the effect of moisture on the insulation of the electric machines of the locomotive., Oriental renaissance: Innovative, educational, natural and social sciences. 2022. Volume-2, No. 3., 953-956.

[7] Djanikulov A.T., Jamilov Sh.F., Miravazov A.R., Checking the insulation parameters of electric machines with a switching scheme. Academic research in educational sciences, 2021.2(11), 877-882.

[8] Restoration of dielectrical properties of insulation of electrical vehicles in the context of "Uztemiryolmashtamir" enterprise. "Scientific progress" Scientific journal. Volume-6 , Issue-6, 2021. 140-144.

Acta of Turin Polytechnic University in Tashkent, 2023, 30, 30-33
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

METHOD AND SOFTWARE TO FIND SPELLING MISTAKES IN TEXT WRITTEN IN UZBEK LANGUAGE BASED ON THE LATIN ALPHABET

[1]Alloyorov O.M., [2]Allaberganov S.M.
[1]Urgench branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
[2]Data Training Center
Email: [1]alloyorovoybek1997@gmail.com, [2]alsimur@mail.ru

Abstract– This article is devoted to software development for Uzbek texts, which detects spelling errors and corrects them in some places. Due to the constant use of the Uzbek language based on the Latin script and some misunderstandings in the transition from Cyrillic to Latin, it is especially important to find and correct spelling errors. The article describes the importance and advantages of the software developed for finding spelling errors in texts written in Uzbek.

Key words– correction of spelling mistakes, roots, prefixes and suffixes, spelling of letters “o‘”, “g‘”, spelling of letters “x” and “h”.

I INTRODUCTION

The relevance of spelling correction software is that it helps to eliminate spelling errors and omissions that may occur in various documents, texts, and articles. This, in turn, is important to prevent situations such as violations of language norms, an increase in the misuse of lexemes in languages, and the gradual normalization of these errors.

To date, the Uzbek Spelling Dictionary has identified more than 85,000 correct spelling words and word forms [1]. One of the most common mistakes is the inverted use of the upper right side of the letter “o‘” in our alphabet, which represents the sound and the letter “o‘”, and the same confusion is used with the letter “g‘”, which represents “g‘”. There are also errors in the use of the letters “x” and “h”. For this reason, it is important to check and correct the Uzbek text for spelling errors.

Analysis of the most common spelling mistakes in the Uzbek language.

Many spelling mistakes are made in the process of writing in Uzbek. If spelling mistakes are not corrected regularly, these words will be misspelled and the words will change altogether. There are different ways to detect errors [3]. They can be used in Uzbek spelling dictionary, annotated dictionary or in programs that help to find and edit mistakes [2].

One of the most common mistakes in the Uzbek language is given in the following table:

	wrong	**wrong**	**wrong**	**right**
The symbol used in the letters “o‘” and “g‘”	o‘, g‘	o’, g’	o’, g’	o‘, g‘
The modifier letter apostrophe	‘	’	‘	’

Another common mistake is to misuse the letters “x" and “h”. Because these two letters represent different sounds, it is important to use each one correctly. For example, the words “xush” and “hush” are semantically different. For example: “Xush kelibsiz”, “Hushidan ketmoq” [1].

It follows that it is important to know the norms of literary language when writing and using texts in Uzbek. Knowledge of literary language norms is also required in the process of software development. This, in turn, will greatly help to understand how mistakes are made and how to fix them.

Roots and suffixes

In Uzbek, as in other languages, words consist of root and suffixes. That is, a word may contain a root and one or more suffixes. The root word is the part of speech that can come into its own and is independent and meaningful. Adding prefixes and suffixes to word stems creates completely new words. There are many such suffixes in Uzbek language. For example, conjunctions: “-ning”, “-ni”, “-ga”, “-dan”, “-da” help to connect words by joining the root, and they are also

called word-changing suffixes.

The genitive case can be answered by questions “kimning?”, “nimaning?”, “qayerning?”. The suffix of the genitive case is “-ning”. “-ning” suffix connects a noun to another noun. The nouns of the genitive case are in the main role. Examples: “o‘quvchining kitobi”, “ko‘ylakning yoqasi”, “daraxtning kurtagi”, “buloqning ko‘zi”.

Accusative case can be answered by questions “kimni?”, “nimani?”, “qayerni?”. The suffix of accusative case is “-ni”. Accusative case suffix connects a noun to verb in the sentence. The nouns of accusative case are main parts of sentence. Examples: “She’rni o‘qidi”, “Multfilmni tomosha qildi”.

Dative case can be answered by questions “kimga?”, “nimaga?”, “qayerga?”. The suffix of dative case is “-ga”, (“-ka”, “-qa”). Accusative case suffix connects a noun to verb in the sentence. The nouns of accusative case are main parts of sentence. The “-ka” suffix is added to the nouns which end with the sound “k”, the “-qa” suffix is added to the nouns with the last sound “-q” and in other cases “-ga” suffix is added to the nouns.

Ablative case can be answered by questions “kimda?”, “nimada?”, “qayerda?”. The suffix of ablative case is “-da”. Ablative case suffix connects a noun to verb in the sentence. The nouns of ablative case are main parts of sentence. Examples: “Saroyda ishladi”, “Tog‘da yashaydi”.

In addition, there are word-forming, noun-forming, adjective-forming and verb-forming suffixes.

For instance:

- word-changing suffixes are “-ning”, “-ni”, “-ga”, “-da”, “-dan”;
- word-forming suffixes are “-chi”, “-la”, “-li”, “-kor”, “-dosh”;
- noun-forming suffixes are “-chi”, “-zor”, “-dosh”, “-kor”, “-k”, “-q”;
- adjective-forming suffixes are “-ser”, “-be”, “-siz”, “-li”, “-chan”, “-dor”, “-q”;
- verb-forming suffixes are “-la”, “-lan”, “-sira”, “-illa”, “-(ulla)”, “-lash”.

Noun-forming suffixes are added to words and made nouns. Examples: “chi”, “hasharchi”; “-zor”, “g‘allazor”; “-dosh”, “sinfdosh”; “-kor”, “paxtakor”; “-k”, “elak”; “-q”, “-taroq”.

Verb-forming suffixes are added to words and made words which is in the category of verbs. Examples: “-la”, “bog‘la”; “-lan”, “tayyorlan”; “-sira”, “suvsira”; “-illa”, “-(-ulla)”, “vizilla”, “shivilla”; “-lash”, “tiklash”.

The present continuous tense verb (“hozirgi zamon fe’li”) refers to an action that is performed (or not performed) while speaking. “-yap”, “-moqda” are present continuous tense (“hozirgi zamon”) suffixes. For example: “O‘rik bechora oppoq, nozik gullarini qayoqqa yashirishni bilmayapti”.

The future tense verb (“kelasi zamon fe’li”) refers to an action that can be performed (or will not be performed) after the speech. “-moqchi” is a future tense (“hozirgi zamon”) suffix. Example: “Sevara o‘zi yozgan she’rini o‘qib bermoqchi”.

The past tense verb (“o‘tgan zamon fe’li”) refers to an action performed (or not performed) before the present tense. “-di”, “-gan” are past tense (“hozirgi zamon”) suffixes. For example: “Dilnozaning uyiga Sarvi xola chiqdi”.

The past tense suffix “-kan” for verbs ending in “k”; for verbs ending in “-q”, “-qan”; added to other verbs in the form “-gan”. Examples: “qirq” – “qirqqan”, “qo‘rq” – “qo‘rqqan”, “cho‘k” – “cho‘kkan”, “chop” – “chopgan”.

Software development process

In the process of developing the program, an attempt was made to find a solution by studying the norms of the Uzbek language. From the above information, it follows that words in the Uzbek language are formed from suffixes added to the roots, and by adding many suffixes to one root, completely different words are formed. So, it can be a bit tricky to check every word in the text to see if it’s incorrect. For example, the word “kitoblarimizning” consists of parts such as “kitob”, “-lar”, “-imiz”, and “-ning”.

The solution is to examine the roots and suffixes separately. This makes the software less cluttered and easier to find errors.

How the program works

With the help of the Uzbek dictionary based on the Latin script, a separate database for stems and suffixes was created. Suffixes are also divided into prefixes and suffixes. The program is installed in Microsoft Word in macro mode, the desired text is selected, and macro is run to detect spelling errors in the text. When the macro starts, it first checks to see if the selected word has prefixes. All prefixes are compared, and if there is a prefix, it is removed and re-checked. The process continues until there are no prefixes left. The next step is to check for the presence of suffixes by comparing them through a database of suffixes. This process continues until there are no more suffixes in the word. The word without suffixes is checked from the base database. If the word does not exist in the database, it is considered an error. Even if there is an error in the suffixes, it will not be found when comparing through the databases of suffixes and the database of roots, and will be automatically recognized as an error. Words found to be incorrect are highlighted in red. All words in the text are checked in the same way.

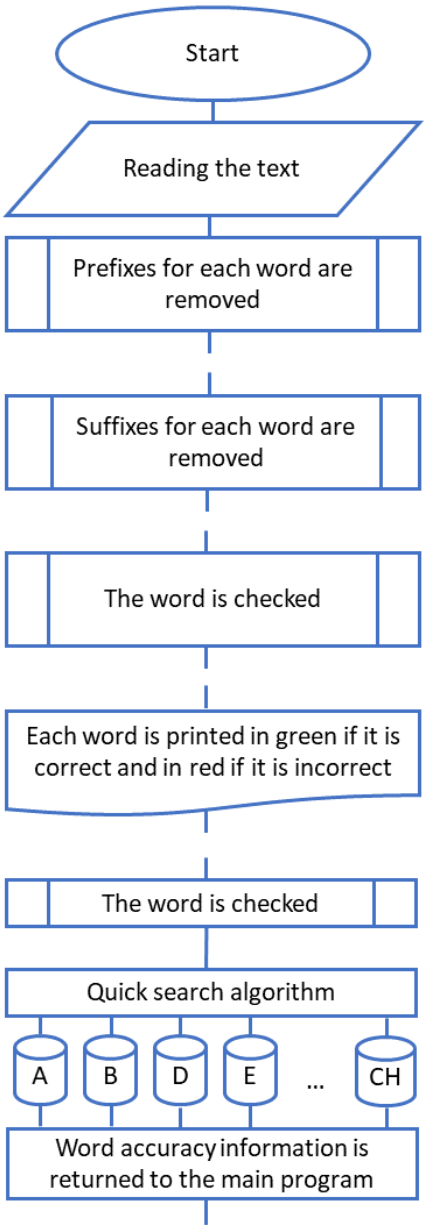

Fig. 1: Block scheme of program

The program also includes the function of correcting the special character of the letters “o‘” and “g‘”. The function searches for the symbols “o” and “g”, if one of the symbols “ ’ ”, “ ‘ ”, “ ’ ” is used after them, it replaces the characters with the symbol “ ‘ ”. If the special character “ ‘ ” of the letters “o‘” and “g‘” is dropped, the program will recognize the word as an error. In the same way, if one of the “ ’ ”, “ ‘ ” or “ ‘ ” characters is used instead of the modifier letter apostrophe “ ’ ” in a word, the program will replace it with the modifier letter apostrophe “ ’ ”.

The following is a view of the text before the scan and after the scan is completed:

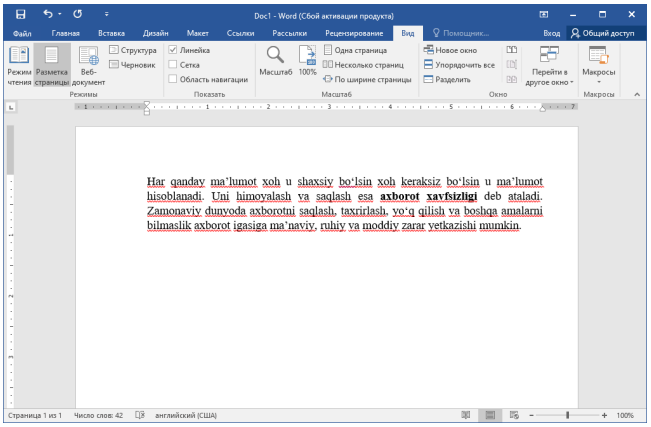

Fig. 2: View of the text before the program starts

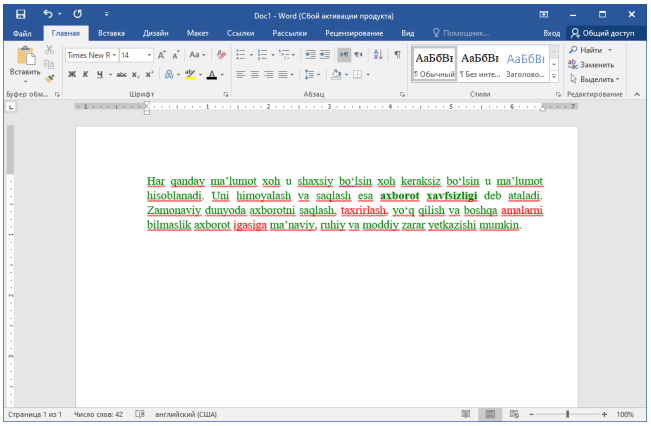

Fig. 3: The appearance of the text after the start of the program

There are three misspelled words in the given text, and as shown in Figure b, the program marked the correct words in green and the incorrect words in red.

II CONCLUSION

This software, which detects errors in Uzbek texts based on Latin script, can detect word errors relatively quickly using the above methods. This is due to the fact that the bases and suffixes in the words are placed in separate databases, the front and back suffixes of the word, and the base is checked separately. Dividing the base database into sections by letter, determining which letter the word starts with, and checking the word base that only starts with that letter can significantly increase performance. This is because there is no need to check for incorrect databases in this case, which saves time.

This software detects text errors, highlights correct words in green and incorrect words in red.

III REFERENCES

[1] "Explanatory dictionary of the Uzbek language". - Tashkent: National Encyclopedia of Uzbekistan, 2006. 1-2-3 years.

[2] A software tool designed to popularize Uzbek spelling rules and improve literacy. Makes it possible to detect spelling errors in the text and improve the quality of your content. https://savodxon.uz/

[3] Google Docs Editor Google's browser-based word processor for creating, editing, and sharing documents online. Can be accessed from any computer with an Internet connection. https://support.google.com/docs#topic=1382883

[4] Grammarly is an artificial intelligence-based online platform to help you communicate in English. To effectively create text in English, it provides recommendations on the correctness, clarity, engagingness and tone of the message. https://www.grammarly.com/grammar-check

[5] Prüfer, D & Kawchuk, Lawrence & Rohde, W. (2006). Polerovirus ORFO genes induce a host-specific response resembling viral infection. Canadian Journal of Plant Pathology - Revue Canadienne de Phytopathologie, v.28, 302-309 (2006). 28. 10.1080/07060660609507299.

[6] Alessandro Agostini, Timur Usmanov, Ulugbek Khamdamov, Nilufar Abdurakhmonova, and Mukhammadsaid Mamasaidov. 2021. UZWORDNET: A Lexical-Semantic Database for the Uzbek Language. In Proceedings of the 11th Global Wordnet Conference, pages 8–19, University of South Africa (UNISA). Global Wordnet Association.

[7] "Explanatory dictionary of the Uzbek language". - Moscow: Russian, 1981.

[8] Mirxanova Gulandom Rustamovna. (2020). Presenting synonyms in the explanatory dictionaries of the Uzbek language. Middle European Scientific Bulletin, 6, 117-120.

Acta of Turin Polytechnic University in Tashkent, 2023, 30, 34-37
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

DATA STRUCTURE SPARSE TABLE

Iskandarov I.Z.
Urgench branch of Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi
Email: islom.iskandarov@ubtuit.uz

Abstract– This article discusses the sparse table data structure: description, capabilities, and scope of application. The results of comparison with such data structures as a segment tree and a sqrt decomposition for two problems are shown. The listing codes are presented in the C++ programming language.

Key words– data structures, algorithms, sparse table.

I INTRODUCTION

Data structure is a way to store and organize data in order to facilitate access and modifications [1]. Each data structure has its own scope, that is, the types of tasks that it can solve. In this article, we will consider a sparse table data structure that stores data in a special (sparse) form and allows you to quickly respond to queries in a segment without modifying elements.

II THE METHODOLOGY

This data structure was introduced in the article The LCA Problem Revisited [2] as part of an optimized solution for the problem. The LCA problem is as follows: Let a tree G be given. Requests of the form (V1, V2) are received as input, and for each request it is required to find their least common ancestor, i.e., vertex V, which lies on the path from the root to V1, on the path from the root to V2, and from all such vertices, the lowest one should be chosen.

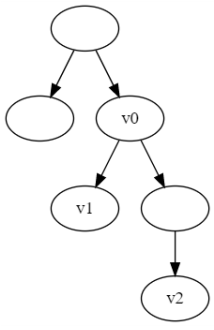

Fig. 1: Graph example for LCA

In the example shown in Figure 1 node v0 is LCA for nodes v1 and v2. The solution to the problem presented in this article is related to the RMQ (Range Minimum Query) problem of finding the minimum on a segment, and the sparse table data structure allows you to effectively solve this problem.

In the book Competitive Programmer's Handbook [3] in *Static array queries* section also shows a solution for querying the minimums with an example with a static array. This algorithm is also presented in Internet resources dedicated to data structures and algorithms. For example, in [4] this algorithm is presented with an implementation in the C++ language, the topic is considered in more detail in [5], including its application for commutative operations.

Formulation of the problem. Suppose we have an array of numbers A consisting of N elements and we need to find a certain value for some segment of the array A. Values can be, for example: the minimum element on the segment, the maximum element on the segment, the sum, etc. A sparse table allows for time and memory overhead $O(NlogN)$ for idempotent operations (minimum, maximum, GCD, etc.) respond to the request in time $O(1)$. Next, consider, as an example, the use of a sparse table to find the minimum element on a segment in queries.

Structure Description. The idea behind the sparse table data structure is the use of a table T for storing answers for segments. But we cannot store values for all segments, since the memory consumption will be $O(N^2)$, and we will store values for segments of length 2^k where $0 \leq k \leq [log_2 n]$. Formally in $T[l][j]$ the value for the segment with the left border l of length 2^j, that is, the value for the segment with indices $[l; l+2^j-1]$. For example, for an array with elements [3, 2, 4, 5, 1, 1, 5, 3] of length 8 the table would look like this:

rmq[3]:	1						
rmq[2]:	2	1	1	1	1		
rmq[1]:	2	2	4	1	1	1	3
rmq[0]:	3	2	4	5	1	1	5	3

Fig. 2: Table structure for 8 elements

Building. Consider the construction for storing the value

of the minimum element on the segment. First of all, we need to calculate the values of binary logarithms; we will calculate them as integers rounded down. Let's do a pre-calculation and store the values in an array:

```
1. int lg[N+1];
2. lg[1]=0;
3. for (int i=2; i<=N; ++i){
4.     lg[i]=lg[i/2]+1;
5. }
```

Listing 1. Calculation of values of binary logarithms of numbers.

The next step is to build the table itself:

```
1. for (int i=1; (1<<i) <=N; ++i) {
2.     int len = (1<<i);
3.     for (int j=1; j+len-1 <=N; j++) {
4.         int tail = j+len-1;
5.         T[j][i]=min(T[j][i-1], T[tail-len/2+1][i-1]);
6.     }
7. }
```

Listing 2. Building a sparse table for the minimum

Getting answers. To obtain a value for the segment $[l;r]$ we "combine" the answers for the two segments $[l;l+2^j-1]$ and $[r-2^j+1;r]$, where j the largest integer for which $2^j \leq r-l+1$, i.e. $j=[log_2(r-l+1)]$.

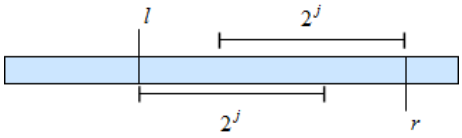

Fig. 3: Combining segments to answer a query

```
1. int get (int l, int r) {
2.     int len = r-l+1;
3.     int p=lg[len];
4.
5.     return min(T[l][p], T[r-(1<<p) + 1][p]);
6. }
```

Listing 3. Receiving a response to a request for a minimum in a segment

Further in requests we can use this function:

```
1. int Q;
2. cin >> Q;
3. for (int i=1; i<=Q; i++) {
4.     int l;
5.     int r;
6.     cin >> l >> r;
7.     cout << get(l, r) << "\n";
8. }
```

Listing 4. Getting an answer to a query

The above example can be used for other idempotent operations, for example, for finding the maximum, GCD, etc. by changing the calculation function for building a table and receiving an answer.

III RESULTS AND DISCUSSION

Here is a comparative analysis of a sparse table and other data structures for various tasks (queries) and data size. As a comparison metric, we take the execution time of programs using these data structures in the C++ language. The calculation includes the total time spent (in milliseconds) on the following operations: building a structure, reading requests from a file, calculating and outputting results to a file[1]. The size of the array is denoted by N, the number of requests is equal to Q.

Structure / Data size	$N=10^4$ $Q=10^4$	$N=10^5$ $Q=10^5$	$N=10^5$ $Q=10^6$	$N=10^6$ $Q=5*10^6$
Segment tree	56 ms	619 ms	5754 ms	34178 ms
SQRT-decomposition	63 ms	806 ms	7235 ms	58415 ms
Sparse table	67 ms	802 ms	5594 ms	30761 ms

TABLE 1: COMPARISON OF STRUCTURES FOR THE PROBLEM RMQ

[1]Standard input operator cin and standard output operator cout were used to read and write data.

Structure / Data size	$N = 10^4$ $Q = 10^4$	$N = 10^5$ $Q = 10^5$	$N = 10^5$ $Q = 10^6$	$N = 10^6$ $Q = 5 * 10^6$
Segment tree	57 ms	613 ms	6387 ms	32323 ms
SQRT-decomposition	56 ms	762 ms	7058 ms	58890 ms
Sparse table	63 ms	722 ms	5586 ms	31661 ms

TABLE 2: COMPARISON OF STRUCTURES FOR THE PROBLEM OF FINDING GCD ON A SEGMENT

Structure / Data size	$N = 10^4$ $Q = 10^4$	$N = 10^5$ $Q = 10^5$	$N = 10^5$ $Q = 10^6$	$N = 10^6$ $Q = 5 * 10^6$
Segment tree	58 ms	634 ms	6863 ms	40786 ms
SQRT-decomposition	56 ms	890 ms	8863 ms	86058 ms
Sparse table	123 ms	722 ms	5922 ms	33616 ms

TABLE 3: COMPARISON OF STRUCTURES FOR THE PROBLEM OF FINDING SUM ON THE SEGMENT

Below are data histograms for problems RMQ and sum (Fig.4, Fig.5). Data sizes are divided into 4 groups: $A(N = 10^4, Q = 10^4), B(N = 10^5, Q = 10^5), C(N = 10^6, Q = 10^6), D(N = 10^6, Q = 5 * 10^6)$. Time values are calculated using the natural logarithm for a smoother presentation. More formally, the time value is replaced by the following expression:

$$Time = lnTime$$

Based on the data above, we can see that a sparse table gives a gain with a larger number of queries relative to the size of the input data. The first two tables refer to problems for which this algorithm calculates the answer in constant time. Additionally, an associative operation (sum) is given in the third table. For such operations, the structure calculates the response in logarithmic time. It is noteworthy that in this case the sparse table gives good results with large data sizes, especially in the latter case it gives a significant advantage.

Fig. 4: Comparison of structures for the problem RMQ

Fig. 5: Comparison of structures for the problem of finding sum on the segment

IV CONCLUSION

The sparse table data structure is appropriate to use in the following cases:

1. There is no element modification, that is, the values of the array elements do not change;
2. The number of queries is large;
3. It is necessary to find the value of an idempotent function for a segment such as minimum, maximum, etc. For such operations, a sparse table gives answers in time $O(1)$, in other cases for $O(logN)$ which no longer gives advantages over other data structures.

V REFERENCES

[1] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, “Introduction to Algorithms”, 3rd ed, pp. 9.

[2] Antti Laaksonen, Competitive Programmer’s Handbook, Draft August 19, 2019. http://www2.compute.dtu.dk/courses/02282/2021/nca/CPbook.pdf

[3] M.A. Bender, M.Farach-Colton. The LCA problem revisited. In Latin American Symposium on Theoretical Informatics, 88–94, 2000.

Acta of Turin Polytechnic University in Tashkent, 2023, 30, 38-42
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

SOLVING THE PROBLEMS OF NORMALIZATION OF NON-STANDARD WORDS IN THE TEXT OF THE UZBEK LANGUAGE

[1]Ibragimova S.N., [2]Turayev B.Sh., [2]Abdullayeva M.I.
[1]Research Institute for the Development of Digital Technologies and Artificial Intelligence
[2]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Email: snibragimova@mail.ru

Abstract– Text normalization is an important component of the text-to-speech (TTS) system, and the difficulty of text normalization lies in distinguishing between non-standard words (non-standard words). In this paper, a taxonomy of non-standard words based on Uzbek speech has been developed, and a two-stage strategy for determining non-standard words has been proposed. The proposed two-stage strategy for identifying non-standard words provides an accuracy of 98.53% in the open test. Experiments show that non-standard taxonomy of words provides high initial performance.

Key words– non-standard words, taxonomy, text normalization, state machine, classification, maximum entropy classifiers.

I INTRODUCTION

In life, when working with real text for machine translation, automatic speech recognition or speech synthesis and analysis, the text always contains numbers, abbreviations, dates, currencies, etc. The text may consist of words whose pronunciation is usually not found in dictionaries or lexicons, such as “BMT”, “UzKhDP”, “TATU”, etc. Such words are called non-standard words. In principle, any system that works with unrestricted text should be able to work with non-standard words. In this case, each text document goes through a series of processing steps to standardize it. The text of the Uzbek language, in addition to ordinary words and names, contains non-standard words, including numbers, abbreviations, dates and amounts of money. As a rule, non-standard words cannot be found in the dictionary, and it is also impossible to interpret their pronunciation using the standard rules for converting the “letter-sound” transition [1-2, 13].

Non-standard words have several categories:

- numbers whose pronunciation changes depending on whether they refer to currency, time, telephone numbers, postal codes;
- abbreviations, abbreviations, acronyms;
- punctuation;
- dates, times, units and URLs.

Many non-standard words are also homographs, i.e. words with the same written form but different pronunciation:

- IV, which can sound differently: four (to‘rt), fourth (to‘rtinchi);
- three- or four-digit numbers, which can be dates and regular numbers (e.g. 2040-yil, 2040 tonna).

Non-standard words need to be normalized to their corresponding standard words, a process called text normalization. In English, numeric expressions and abbreviations are non-standard words. Even sentence segmentation is part of text normalization. For the Uzbek language, numbers, symbols and alphabets that are not Uzbek words must be normalized to the forms of the Uzbek language. Non-standard words may be replaced by other standard words depending on the local context and the genre of the text. Hence, the problem is reduced to finding complex homographs [3]. In Nuance Vocalizer, more than 20% of the main application code (code metric line) is devoted to text normalization, and new input formats continue to be added [4]. Conventional text normalization methods are based on simple rules. However such simple custom rules are difficult to write, maintain, and adapt to new domains. On the other hand, when detecting homographs, many machine learning methods are used

that have shown their advantages. Decision trees and decision lists are used to normalize text in English and Hindi, as well as for Uzbek [5]. Text data is classified and used according to the support vector machine (SVM) classification algorithm [6].

However, most Uzbek text normalization modules are rule-based and run before the word segmentation process. Because in the Uzbek text spaces between words are used in different cases. In literature, he adopts the method of normalizing the Uzbek text based on an external rule. It uses over 15 external rules and verbal and speech data. Still, others put word segmentation, named object recognition, and custom word processing into a single framework.

This article proposes a two-stage strategy for identifying non-standard words in the Uzbek text. The proposed text normalization algorithm does not require a word segmentation process. This algorithm includes finite automata that identify non-standard words from the text and perform an initial classification, then classifiers with maximum entropy are used for further classification.

II THE METHODOLOGY

1. CLASSIFICATION OF NON-STANDARD WORDS

A non-standard taxonomy of words was developed following a systematic review of the extensive TTS corpus. Based on this taxonomy, a three-level normalization process was developed. Finite automata are used for non-standard word detection and initial classification. Maximum entropy classifiers are used to further classify non-standard words, and numeric state converters are used to generate standard words [7-9]. Non-standard taxonomy of words underlies text normalization. It defines categories of non-standard words, according to which non-standard words are identified, classified and modified. Arabic, Roman numerals and some symbols are the main normalized objects in the text in Uzbek [10-11].

Table 1 provides a brief description of the taxonomy of non-standard words. Non-standard words are first classified according to their format. 95% of the 276 non-standard words in the algorithm are numeric strings and various combinations of characters (period, hyphen, slash, colon, etc.). Symbols is another category to change and some symbols have multiple pronunciations. The normalization of URLs and email addresses is obvious. Strings of the English alphabet have corresponding Uzbek translations. All other unique non-standard words are also added to the "Other" category. In total, the taxonomy includes 48 types of non-standard words in different formats. Some of these species have excellent pronunciation, while others do not.

Non-standard words whose pronunciation is determined by formats are called basic non-standard words (BNSW), and ambiguous non-standard words are called ambiguous non-standard words (ANSW). Tables 2 and 3 below show some examples of BNSW and ANSW, respectively. Table 2 shows the proportional distribution of non-standard words in the Uzbek text. From the table, you can see that the probability of occurrence of BNSW among all non-standard words is 55%, and their number is 84% of all possible non-standard words. It follows that 84% of non-standard words are written according to the established format (for example, 30%, 10 kg, 6 yil) and only 16% are ambiguous (for example, b2b, 115, 1998-2000).

Numbers	numbers	1,2,3, ... etc....
	with a dot	1.29, 2000.9.10, 162.105.81.14, ...
	with a hyphen	1998-2002, 2000-9-10, 4-3-2-1, ...
	with a slash	1/3, 2000/9/10, ...
	indicators	10:15, 10:15:20, ...
	additions	%, (ten thousand), adjectives, ...
	range	100-200 Ď (from 100 to 200), ...
	other	'99, ...
Symbols	-, /, :, ., ×, >, =,	
Other	URL, Email, Alphabets, ...	

TABLE 1: TAXONOMY OF NON-STANDARD WORDS BASED ON INPUT FORMATS

Class of non-standard words	Example	Percentage
Indicative numbers	35 P inchi,nchi	55%
Integer	100 $	8%
Percent	10%, 12.5%	6%
Date	27 oktabr	4%
Numbers and words	15 ming	3%
Number basis	5 kg, 10 sm	2%
Year	5 yil	2%
Other	Win32	4%

TABLE 2: BNSW EXAMPLES

Table 3 shows some categories of responses and possible ways to record them. It is clear that some non-standard words have a high level of ambiguity and their meaning requires internal and contextual information.

2 TEXT NORMALIZATION METHOD

To normalize the Uzbek text, an algorithm has been developed that consists of three main stages.

1. Highlighting non-standard words and preliminary

Class of non-standard words	Words	Example
Numbers	Decimal numbers	2 ga 11 (2.11 metr)
	Integer numbers	110
	Vote	110
	English alphabet	p2p
a-giper	year-year	1998-1999
	Phone number	+99893 385 34 34
	number-number	737-200 (Boying 737-200)
	Subtraction	100-1=99
Slesh	Fraction	1/3
	Date	2001/01
Dominant	Time	10:15 (10:15 soat)
	Steps	10:15

TABLE 3: ANSW EXAMPLES

classification. In the first stage, a machine learning algorithm is used to extract non-standard words from the real text and carry out a preliminary classification. At this point, the BNSW classification is completed.

2. Definition of subclasses to display the answer. To derive the answer, the result of the initial classification is used to determine the subclass. To perform this step, maximum entropy classifiers are used.

3. Generation of the Standard word. If a non-standard word is tagged with a class tag, the restricted state switch converts it to a standard word. The text normalization scheme is shown in Figure 1.

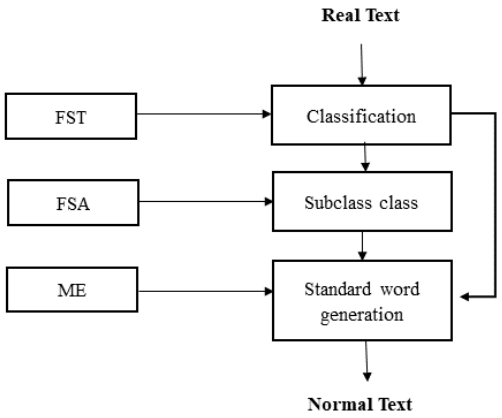

Fig. 1: Text normalization scheme

The full cycle of normalization of non-standard words is shown in Figure 2.

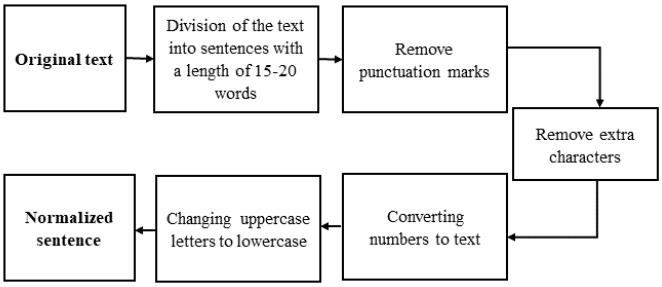

Fig. 2: Text normalization process.

III RESULTS AND DISCUSSION

An experimental study of the performance of the proposed algorithm was carried out on the example of solving a practical problem. The system interface consists of two fields, as shown in Table 4. In the left field of the system, the source text in Uzbek is entered, and the normalized text in Uzbek is displayed in the right field. The text contained words from the BNSW and ANSW classes.

Denormalized text	Normalized text
Bugun sana 27-mart 2023-yil. Meni bugu 1-param bor.	bugun sana yigirma yettiinchi mart ikki ming yigirma uchinchi yil. meni bugu birinchi param bor.
1 kg da 1000 gr bor	bir kilogramm da bir ming gramm bor
1998-1999 yillari men maktabga borgan edim	bir ming to'qqiz yuz to'qson sakkizinchi bir ming to'qqiz yuz to'qson to'qqiz yillari men maktabga borgan edim

Figure 3-4 shows the system interface and the results of Uzbek text normalization.

IV CONCLUSION

This article provides a comprehensive study of the normalization of the Uzbek text. On the basis of a large corpus, a non-standard taxonomy of Uzbek words was developed. A two-stage non-standard strategy for word classification is proposed, which is carried out using an automaton with a

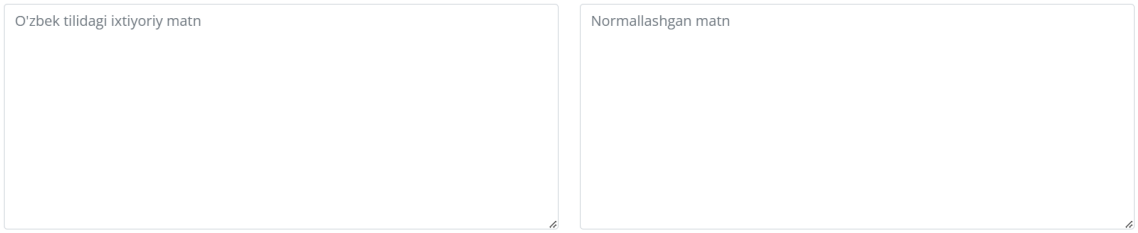

Fig. 3: System interface.

Fig. 4: Result of text normalization.

finite number of states for the initial classification and classifiers with maximum entropy. Experimental results show that this approach provides good performance and generalizes well to new areas. In addition, this algorithm is based on working with symbols and does not require a word segmentation process.

V REFERENCES

[1] Jurafsky D. Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition (University of Colorado, Boulder) Upper Saddle River, NJ: Prentice Hall (Prentice), D. Jurafsky, J.H. Martin, Computational Linguistics, 2000, T. 26, N 4.

[2] Richard Sproat, Alan Black, Stanley Chen, Shankar Kumar, Marsi Ostendorf, and Christopher Richards, «Normalization of Non-Standard Words», Computer Speech and Language, 2001, 15(3): pp. 287-333.

[3] Allen, Jonathan, M. Sharon Hunnicutt, and Dennis Klatt, «From Text to Speech: the MITalk System», Cambridge University Press, Cambridge, 2001.

[4] Abdurakhmonova N. Z. "Modeling Analytic Forms of Verb in Uzbek as Stage of Morphological Analysis in Machine Translation" Journal of Social Sciences and Humanities Research. 2017, 5(03):89-100.

[5] Abduraxmonova, N. Z. "Linguistic support of the program for translating English texts into Uzbek (on the example of simple sentences): Doctor of Philosophy (PhD) il dis. aftoref.", 2018.

[6] Musaev M. M., "Modern methods of digital processing of speech signals" Bulletin of TUIT, 2017, Vol. 2, N 42, pp. 2-13 [In Russian].

[7] Musaev M.M., Xujayarov I.Sh., Ochilov M.M., "Recognition of phonemes of the Uzbek language based on machine learning algorithms" Informatics and energy problems, 2019, Vol. 6, [In Uzbek].

[8] Alimuradov A.K., Churakov P.P., "Review and classification of methods for processing speech signals in

speech recognition systems" Measurement. Monitoring. Control. Control, 2015, Vol. 2, N 12, pp. 27-35 [In Russian].

[9] Musaev M., Khujayorov I. and Ochilov M., "The Use of Neural Networks to Improve the Recognition Accuracy of Explosive and Unvoiced Phonemes in Uzbek Language", Information Communication Technologies Conference (ICTC), Nanjing, China, 2020.

[10] Musaev M. M., Rakhimov M. F. "Algorithms for parallel processing of speech signals" Bulletin of TUIT, 2018, Vol. 2, N 46, pp. 2-13 [In Russian].

[11] M.M. Musaev, U.A. Berdanov, K.E. Shukurov, «Hardware and software solution signal compression algorithms based on the Chebyshev polynomial» International Journal of Information and Electronics Engineering, 2014, t. Vol. 4, N 5, pp. 380-383.

[12] Jalil, Masita, Ismailov, Alisher and others The Development of the Uzbek Stemming Algorithm. Advanced Science Letters. 2017, pp. 4171-4174.

[13] Sproat, Richard, editor, "A Computational Theory of Writing System", Cambridge University Press, Stanford, 2000

Acta of Turin Polytechnic University in Tashkent, 2023, 30, 43-46
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

ANALYSIS OF THE RECOVERY SYSTEM BRAKING ELECTRIC VEHICLES.

Umerov F.Sh.
Turin Polytechnic University in Tashkent
«Research Laboratory of Electric Vehicles and their infrastructure»
Email: fikret.umerov@polito.uz.

Abstract– Electrically powered vehicles are a relatively new industry in the automotive world today. The first electric cars, which were created in the early stages of development in the automotive industry, had much-improved characteristics in relation to cars running on internal combustion engines. Over the years, the development of technologies for producing fuel for internal combustion engines has become significantly more affordable and much cheaper, as a result of which the need for electric vehicles has significantly decreased. At the beginning of the 21st century, environmental degradation due to exhaust emissions from internal combustion engines of cars gave a new impetus to the development of electric vehicles [1]. This article is devoted to the analysis and evaluation of the use, as well as the effectiveness of the regenerative braking system of electric vehicles.

Key words– Electric car, regenerative system, brake system, ecology, transport.

I INTRODUCTION

Using the conventional braking system of classic cars on electric vehicles is not very effective for the braking system of an electric vehicle. When braking with classic brake pads, mechanical energy is converted into thermal energy. The use of a regenerative system in electric vehicles makes it possible to save part of the energy during braking, which can be stored in batteries and later used for electric drive. Thereby the range of the electric vehicle on one charge increases. Such braking can also save wear on the friction linings in the brake system, which increases their service life. Based on the above, this study is relevant. [2].

This issue was dealt with by such scientists as Dembitsky V.M., Kashuba A.M., Le V.N., Dam P.H., Nguyen C.H., Kharitonchik S.V., Kusyak V.A. [3, 4, 5]. Having examined the works [3, 4, 5], one can see the effectiveness of using recuperation systems on electric vehicles, which save the electrical energy of the traction battery.

The purpose of the article is to identify the types of braking systems that can be used in electric and hybrid vehicles, as well as to analyze them.

II MAIN PART

Electric vehicles and hybrid electric vehicles have two braking systems: a conventional one with friction brakes and a regenerative braking system.

In a conventional brake system, the pads or friction brakes are driven by a hydraulic drive, in which hydraulic fluid is supplied under pressure to the brake cylinders, which operate the brake mechanisms.

Regenerative braking is the process of returning part of the energy for reuse in the same technological process. Brake energy regeneration, or energy regeneration during deceleration, significantly increases the range of any electric vehicle. In new models of electric vehicles from BYD, Volkswagen, Tesla, Toyota and many other companies, this concept is aimed at ensuring maximum energy efficiency [6].

A description of the main components of the regenerative braking system of a modern passenger electric vehicle driven by the front axle is shown in Fig. 1.

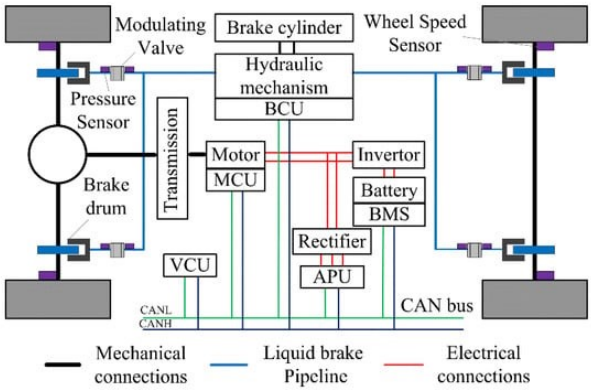

Fig. 1: Diagram of an electric vehicle's regenerative braking system. [7]

As shown in Fig. 1, the braking system of an electric vehicle consists of two systems: a hydraulic braking system and an electric braking system. In a hydraulic brake system, the pressure in the master wheel cylinder can be adjusted using modulating valves. Each wheel is equipped with modulating valves. Each wheel can be controlled independently by a hydraulic brake controller [7].

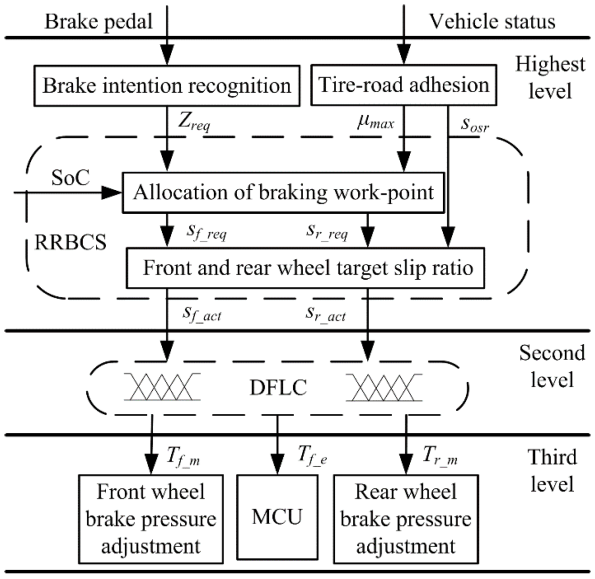

Fig. 2: Control level of the revised regenerative braking control strategy (RRBCS). [7]

The revised regenerative braking control strategy (RRBCS) studied in this paper was divided into three levels: the highest level (regenerative braking controller), the second level (fuzzy controller), and the third level (actuator), as shown in Figure 2.

At the top level are the hydraulic braking controller and the electrical controller in the regenerative braking system (RBS), whose main task is to coordinate the regenerative braking torque and the hydraulic braking torque. The second level contains a double fuzzy logic controller (DFLC), which differs from the fuzzy controller in [8,9,10,11]. In addition, it can adjust the braking torque in real-time to control the slip ratio of the front and rear wheels to ensure that the target slip ratio is well maintained. The third level includes a regenerative-hydraulic braking system without a controller, the task of which is to implement the braking process under the control of the controller.

When the brake pedal is activated, the regenerative system initially comes into play, which replaces the friction braking system by creating artificial resistance to wheel rotation through an electric drive which works in the generator mode. The effective maximum braking torque of a traction motor in generator mode depends not only on the strength of the excitation current but also on the armature speed, which in turn depends on the speed of the electric vehicle. Thus, braking efficiency varies depending on the driving speed. If the traction motor does not provide sufficient braking efficiency, the difference between the level of efficiency set by the driver and the one created by the electric motor is compensated by the friction braking mechanism.

The higher the high-voltage battery charging current produced by the electric motor in generator mode, the greater the braking force. Regenerative braking control is achieved through joint control of the braking system and transmission. In this control, the regenerative braking system and the hydraulic braking system combine their efforts, taking into account fluctuations in the parameters of the regenerative system caused by the battery charge or vehicle speed. As a result, it is possible to minimize the loss of kinetic energy.

The extraction of electricity during braking of electric vehicles represents a significant source of reducing energy consumption in an electric traction system. The modern technological base also allows you to smoothly adjust the braking force until the vehicle comes to a complete stop. This reduces emissions of harmful substances into the environment resulting from mechanical braking and increases driving comfort and safety.

A vehicle design using electric braking with energy recovery requires virtually no additional braking system. However, the vehicle is actually still equipped with a hydraulic braking system. Thus, the braking process of a vehicle with an electric motor, in addition to the conventional system with friction braking mechanisms, is complemented by another component - electric braking, which increases the active safety of the vehicle.

Today, there are two types or categories of regenerative braking systems, the definition of which is given in European regulations [11].

1. Category A – electrical regenerative braking system, which is not part of the service braking system;

2. Category B – electric regenerative braking system, which is part of the service braking system.

These two categories of braking systems differ mainly in the way they are activated. A Category A regenerative braking system is activated when the accelerator pedal is released, while a Category B regenerative braking system is activated when the accelerator pedal is moved to the zero position and the service brake is applied. In the case of category B regenerative braking system, the electric motor typically generates electrical energy while coasting.

The main problem is that over long distances the efficiency of using the regenerative system is practically negligible,

since the car is mainly in acceleration mode, and braking is only a small part of the time. This reduces the efficiency of braking energy recovery, making battery charging less efficient and making the electrical system more complex. Therefore, regenerative braking is widely used in hybrid vehicles, where it has achieved approximately 30% savings in the total energy required to drive the vehicle.

III CONCLUSION

As a result of the study, the author came to the following conclusion: Thus, the use of a regenerative system in electric vehicles increases their economic and environmental performance, and also increases the service life of the high-voltage battery by optimizing the processes of regenerative braking, starting the traction motor and charging the battery.

IV REFERENCES

[1] Umerov F., Inoyatkhodjaev J., Asanov S. Prospects for the development of electric vehicles in Uzbekistan. Acta of Turin Polytechnic University in Tashkent, 2022, 30, No2 – pp. 65-68.

[2] Inoyatkhodjaev J., Umerov F., Asanov S. Method for sizing an electric drive of small class electric vehicles. Universum: Technical Sciences Russian Federation, 2022, LLC "ICNO" issue 4(109).

[3] Sitovsky O.F., Dembitsky V.M. Electrodynamic braking of a hybrid vehicle on roads with low coefficient of adhesion. Automobile transport. - 2013. - No33. - pp.13-18. (Russian)

[4] Kashuba A. M. Recuperation of kinetic energy in automobiles with hybrid propulsion system. Naukov notatki. - 2011. - Issue. 35. - pp. 93-95. (Russian)

[5] Le V.N., Dam P.H., Nguyen Ch.H., Kharitonchik S.V., Kusyak V.A. Investigation of regenerative braking strategy for electric vehicles. Energetika. Izvestiya vysshee obrazovaniya vysshee obrazovaniya i energeticheskikh obshchestva CIS. 2023, 66 (2):105-123. (Russian)

[6] Yudina A.E., Kisneeva L.N. Regime of Recuperation in Electric Vehicles. World tendencies of science and technology development: ways of improvement Moscow, - 2022. - No33. - pp.275-276. (Russian)

[7] Liu H., Lei Y., Fu Y., Li X. Multi-Objective Optimization Study of Regenerative Braking Control Strategy for Range-Extended Electric Vehicle. School of Automotive Engineering, Jilin University, Changchun 130022, China – Appl. Sci. 2020, 10 (5).

[8] Roumila Z., Rekioua D., Rekioua T. Energy management based fuzzy logic controller of hybrid system wind/photovoltaic/diesel with storage battery. Int. J. Hydrog. Energy 2017, 42, 19525–19535.

[9] Aksjonov A., Vodovozov V., Augsburg K., Petlenkov E., Design of regenerative anti-lock braking system controller for 4 in-wheel-motor drive electric vehicle with road surface estimation. Int. J. Automot. Technol. 2018, 19, 727–742.

[10] Maia R., Silva M., Araújo R., Nunes U. Electrical vehicle modeling: A fuzzy logic model for regenerative braking. Expert Syst. Appl. 2015, 42, 8504–8519.

[11] Topalov A.V., Oniz Y., Kayacan E., Kaynak O. Neurofuzzy control of antilock braking system using sliding mode incremental learning algorithm. Neurocomputing 2011, 74, 1883–1893.

[12] UNECE Regulation No. 13 "Uniform provisions concerning the approval of vehicles of categories M, N and O with regard to braking".

[13] Umerov F.Sh., Juraboev A.Z. Analysis of the block diagram of the traction drive and the stages of calculation of a mechatronically controlled hybrid vehicle. Scientific journal of the Tashkent State Technical University (TSTU) named after Islam Karimov, "Yulduzlari Technique", Tashkent 2022. No. 1 - P. 29-33.

[14] Du J., Ouyang D. Progress of Chinese electric vehicles industrialization in 2015: A review. Appl. Energy 2016, 188, 529–546.

[15] Chen B., Wu Y., Tsai H. Design and analysis of power management strategy for range extended electric vehicle using dynamic programming. Appl. Energy 2014, 113, 1764–1774.

[16] Ma H., Balthasar F., Tait N., Riera-Palou X., Harrison A. A new comparison between the life cycle greenhouse gas emissions of battery electric vehicles and internal combustion vehicles. Energy Policy. 2012, 44, 160–173.

[17] Qiu C., Wang G. New evaluation methodology of regenerative braking contribution to energy efficiency improvement of electric vehicles. Energy Convers. Manag. 2016, 119, 389–398.

[18] Lv C., Zhang J., Li Y., Yuan Y. Novel control algorithm of braking energy regeneration system for an electric vehicle during safety–critical driving maneuvers. Energy Convers. Manag. 2015, 106, 520–529.

[19] Guo J., Jian, X., Lin G. Performance evaluation of an anti-lock braking system for electric vehicle with a fuzzy sliding mode controller. Energies 2014, 7, 6459–6476.

[20] Kumar C.N., Subramanian S.C. Cooperative control of regenerative braking and friction braking for a hybrid electric vehicle. Proc. Inst. Mech. Eng. J. Automob. Eng. 2015, 230, 103–116.

Acta of Turin Polytechnic University in Tashkent, 2023, 30, 47-50
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

THE INTERNATIONAL CONSEQUENCES OF CYBER WARFARE: A STUDY OF THE "STUXNET" CASE

Musakhanov D.
Turin Polytechnic University in Tashkent
Email: diyor.musakhanovv@gmail.com

Abstract– This article attempts to analyse the international consequences of cyber warfare. As an example, the author considered an episode of joint operation of the U.S. and Israel against a nuclear facility located in Natanz, Iran with the aim to destabilise it using the "Stuxnet" computer worm. The study aims to define the concept of cyber warfare and its characteristics, briefly analyse the principle of the virus, understand the impact and consequences of the virus on the international community, and determine further prospects and threats that await us with the development of cyberwars.

Key words– Stuxnet, cyber warfare, cybersecurity.

I INTRODUCTION

Cyber warfare is one of the most pressing challenges for international relations at present. With the development of technology and the increase in the number of people who use the Internet and digital technologies, cybercriminals, and government hackers can use cyberattacks to carry out large-scale operations against other states, corporations, or individual users [2].

Cyber warfare can have serious implications for international security, economics, and politics. Cyber attacks can damage critical information infrastructure, and disrupt the functioning of the banking system, energy supply, water supply, transport, and other important sectors of the economy [5]. Cyber warfare can also be used to interfere in the elections and political processes of other states. In this regard, the study of the impact of cyber war on international relations is a relevant and important topic that can help understand how cyber war affects the political map of the world and the role of cyber security in ensuring international security.

The purpose of the study is to create a general picture of the impact of cyber warfare on international relations and an understanding of what global threats are possible due to the high potential of the use of cyber weapons. The results of the study can be used by politicians, cybersecurity specialists, and the scientific community to gain an understanding of the consequences of cyber warfare.

II THEORETICAL BACKGROUND

1. Cyberspace - the complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form [1;9;10].

2. Cyber warfare is the use of cyber-attacks against an enemy state, causing damage comparable to real war and/or disrupting vital computer systems. Some intended outcomes could be espionage, sabotage, propaganda, manipulation, or economic warfare [1;9;10].

3. Cybersecurity - measures and practices aimed at protecting computer systems, networks, and data from threats such as cyber-attacks, viruses, hacker attacks, and cyber espionage [1;9;10].

4. Cyber-attack - malicious activity in cyberspace aimed at violating the confidentiality, integrity, or availability of information systems, networks, or data [1;9;10].

5. Information warfare is a form of conflict in which the parties use information technology, communication tools, and media to achieve their political, military, or informational goals by manipulating information, spreading disinformation, conducting cyber-attacks, and other similar actions [10]. The purpose of the information war is to influence public opinion, weaken the enemy, create chaos, and strengthen one's position. It is necessary to take into account that one of the features of cyber warfare is the possibility of anonymity and elusiveness of attackers, which makes it even more dangerous. Cyber warfare has both short-

term and long-term consequences, including confidential information, critical loss business interruption, disruption of public order, and others. Cyber warfare can be waged by both state and non-state actors such as cybercriminals, terrorists, and hackers.

III LITERATURE REVIEW

Relatively recently, the world is faced with a completely new principle of warfare, which is completely different from any of the others. Over the years, cyberspace has become one of the key places for the use of military weapons, becoming one of the most important phenomena arising from the development of information and computing technologies. In this literature review, the author attempts to provide brief data regarding existing literature on the theme of cybersecurity and cyber warfare.

To begin with, the book Fundamentals of Cybersecurity. Standards, search, methods, and media (Belous A.I. & Solodukha V.A., 2021) [10] introduces us to the basic concepts of cyberspace, cyber attack, cyberterrorism, cybersecurity, cyber and information warfare. This book is the starting point for understanding the basic principles and terminology in the field of cybersecurity.

In the article (Singer P. & Friedman A., 2014) [9] Cybersecurity and Cyberwar: What everyone needs to know, the authors offer an overview of the general concepts of cyber warfare and cyber security, and discuss possible trends that may affect the field of cybersecurity in the future. In addition, in the article, Cyber Attacks as a Means of Political (Volkova E. 2020) [5], specific cases of cyberattacks and their use as a tool of political influence are considered. The author analyses these cases in detail and provides insight to better strengthen cybersecurity.

Moreover, there is interesting research regarding Stuxnet, particularly by Marie; Robin, Patrice (2017): Hotspot Analysis: Stuxnet. In this study many aspects have been considered, however, some of them were considered quite briefly. For instance, there is not enough information to find out a real international effect. There is a book by (F. Kaplan, 2016) Dark Territory: The Secret History of Cyber War [11], that sheds light on the main events of cyber warfare, such as sabotage, espionage, and attacks on critical infrastructure. Furthermore, this book provides an overview of the challenges which governments and military organisations face in the process of repelling cyber attacks.

Overall, the presented literature review provides us with information on a general overview of the field of cyber warfare and cybersecurity. However, the lack of information in the literature regarding possible consequences is noticed. Probably, it is because of the rapid development of technology and cyberspace in general. In order to raise awareness, expand horizons and provide adequate security in this area, it is important to constantly update the knowledge base, conduct new research in the field of cybersecurity and set international standards in this field.

IV ANALYSIS OF THE IMPACT OF CYBER WARFARE ON INTERNATIONAL RELATIONS

Let us consider the example of the use of cyber warfare tools, in particular the computer worm "Stuxnet" designed by U.S. and Israeli intelligence against the Iranian nuclear facility in Natanz. It is a well-known fact that the most pressing problem of the world community is the unresolved issue of Iran's nuclear program. This problem was actively discussed at the meetings of the International Atomic Energy Agency (IAEA) in the period from 2006 to 2008 [12]. Several resolutions demanding that Iran stop further development of its own nuclear program did not lead to significant shifts in the resolution of the Iranian crisis [8]. The government of the country announced its intention to continue to develop its own nuclear program for meeting the internal needs of the state and in the interests of the Iranian people. Iran's refusal to comply with IAEA requirements to stop the uranium enrichment process, set out in the resolutions of the period 2006-2008, led to the dissatisfaction of the world community, primarily the United States and Israel. Statements on the peaceful nature of Iran's nuclear program were also questioned. As a result, the United States and Israel, in secrecy, began preparing military options to prevent further development of nuclear capabilities. The use of the latest weapons of cyber warfare has become part of this operation. Stuxnet is malware used jointly by the United States and Israel against Iran in order to undermine the further development of the latter's nuclear program [3;6].

The structure and functionality of "Stuxnet". Stuxnet uses a variety of distribution methods, including infected USB sticks and network vulnerabilities. It likewise contains several zero-day exploits to gain access to vulnerabilities in "Windows" operating systems. After getting into the computer, Stuxnet tries to spread over the local network by finding vulnerable systems. One of the main tasks of Stuxnet is to damage the centrifuges used in nuclear installations so that they can quickly fail [7].

On the domestic political level, the cyberattack discredited the Iranian government, as the Iranian authorities were not able to protect their nuclear facilities against a foreign cyberattack. Moreover, Iranian authorities did not retaliate against cyberattacks because the identity of the perpetrators was unknown or unclear, and because there was no precedent for how a state should respond to such an attack. Iran acknowledged a cyberattack on its nuclear program, but did not specifically mention "Stuxnet" [3]. This prompted Iran

to step up measures to protect its critical systems and infrastructure, as well as to develop its cyber capabilities in response to such a threat. It is believed that Iran is responsible for the course of the retaliatory counter-attack called Ababil [4]. Iran tried to portray itself as a victim of foreign aggression and deflect attention from its own actions. Iran called on international organisations such as the UN and The International Atomic Energy Agency to increase their controls. IAEA began investigating and analysing the attack in order to determine its source and implications for nuclear safety. Also, in a joint statement, the IAEA and Iran have agreed to allow inspectors to conduct closer joint inspections, though the specific terms of what that would mean are unknown [4].

In general, the “Stuxnet” increased tensions between Iran, the US, and Israel, provoked counterattacks, and escalated conflict in cyberspace. The response from the UN has been rather mixed. In 2010, Martin Schulz, then head of the UN General Secretariat, raised concerns about the use of cyber weapons against states. However, there are still no clearly defined international norms in the field of cybersecurity.

In a 2012 episode of 60 Minutes, retired US Air Force General Michael Hayden admitted that despite not being specific about Stuxnet’s creators, he considered the attack a "good idea" [6]. However, he noted that the use of sophisticated cyberweapons designed to affect the psyche has a revealed side. Such technologies are used by other countries in order to achieve their interests. He also took advantage of the fact that Stuxnet’s source code is now available on the Internet, which opens up the possibility of modifying it and targeting it against new targets. Thus, the creation of Stuxnet demonstrated a new reality in cybersecurity, where cyberweapons can take physical damage seriously and have consequences [1]. The openness and accessibility of using the Stuxnet source code highlight the irreversibility of the possibility of artificial change and cyberweapons. An article in Wired that Stuxnet developers "opened the box" demonstrated the capabilities of such a weapon that cannot be returned back [6;10]. Stuxnet has set an important precedent for cyberattacks and has raised questions about international security and the legality of such actions and showed that cyber weapons could sweep the environment with industrial systems, opening up new possibilities for countries and hackers. This is the identification of potentially dangerous vulnerabilities and the possibility of a critical security situation. Stuxnet takes advantage of possible cooperation between states in the development and assembly of cyber weapons. Israel and the US are investigated as the main contender for the creation of this worm, although the exact details have been found unknown [6].

Overall, Stuxnet has been a notable discovery of how cyberattacks can involve multiple sources and have serious consequences. This case demonstrated a new cybersecurity environment where the development and use of sophisticated cyberweapons require close attention, international cooperation, and the development of security measures.

Finally, the manifestation of the Stuxnet virus showed that there are not only amateurs who write viruses of different directions for the purpose of earning money but that technological progress has given rise to "professionals" who perceive information systems solely as a "battlefield" [1;2;10]. Such attacks can cause heightened tensions and mistrust between states, as seen in the case of the United States, Israel, and Iran.

V CONCLUSION

Nowadays, cyber warfare is an integral part of modern international relations, posing a serious threat to critical infrastructure and national security. In addition, the use of cyber weapons for the purpose of physical harm raises complex ethical and legal issues. The origin of Stuxnet remains unclear, but possible collaboration between Israel and the United States points to the need for international cybersecurity norms and agreements in the field of cybersecurity.

Based on the foregoing, it becomes clear that cyber warfare has the potential to change the geopolitical balance of power, as a successful cyber attack can seriously affect the economy, defence, national security, critical infrastructure, and political situation of the victim country. This is a matter of concern and requires continuous strengthening of the readiness and protection of the national cyberinfrastructure.

At the same time, cyber war increases the risks of nuclear war, as the use of cyber weapons becomes an alternative to traditional warfare in the doctrines of some states. For instance, penetration and control of nuclear systems through cyberattacks can have catastrophic consequences, involving unauthorised activation or destruction of nuclear facilities. This creates a potentially dangerous situation where a conflict in cyberspace could escalate into the nuclear realm, putting international stability and security at risk.

VI REFERENCES

[1] Even Sh., Siman-Tov D. Cyber Warfare: Concepts and Strategic Trends, URL: https://www.files.ethz.ch/isn/152953/inss%20memorandum_may2012_nr117.pdf

[2] Roscini M. 2014. Cyber operations and the use of force in international law. Oxford Oxford University Press.

[3] Marie; Robin, Patrice (2017) : Hotspot Analysis: Stuxnet, October 2017, Center for Security Studies (CSS), ETH Zürich, URL :

https://www.researchgate.net/publication/323199431_Stuxnet

[4] Anderson C., Sadjadpour K., 2018. Iran's Cyber Threat, URL: https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

[5] Volkova E. 2020. Cyber Attacks as a Means of Political Influence, URL:https://cyberleninka.ru/article/n/kiberataki-kak-sredstvo-politicheskogo-vliyaniya

[6] Wikipedia, Stuxnet, URL : https://en.wikipedia.org/wiki/Stuxnet#

[7] Falliere N., Murchu L.O., Chien E., Symantec Security Response, W32.Stuxnet Dossier, URL : https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en

[8] Broad W. Markoff J., 2011. and Sanger D. E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay, URL : https://www.nytimes.com/2011/01/16/world/-middleeast/16stuxnet.html

[9] Singer P., Friedman A. Cybersecurity and cyberwar: What everyone needs to know.Oxford: Oxford univ. press, 2014. - 320 p., URL: https://cyberleninka.ru/article/n/zinger-p-fridman-a-kiberbezopasnost-i-kibervoyna-chto-kazhdyy-dolzhen-znat/viewer

[10] Belous A.I. and Solodukha V.A., 2021. Fundamentals of cybersecurity. Standards, search, methods and medium, Moscow: "Tekhnosfera", ISBN 978-5-94836-612-8

[11] Kaplan F., 2016. Dark Territory: The Secret History of Cyber War, Simon and Schuster Paperbacks, ISBN 978-1476763262

[12] IAEA, IAEA and Iran: Chronology of Key Events, URL: https://www.iaea.org/newscenter/focus/iran/chronology-of-key-events

Acta of Turin Polytechnic University in Tashkent, 2023, 30, 51-55
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

DYNAMIC MULTICRITERIA ANALYSIS DEVELOPMENT OF THE ELECTRIC VEHICLE MARKET AND THEIR INFRASTRUCTURE IN UZBEKISTAN

[1]Umerov F.Sh. [2]Asanov S.E.
[1]Research laboratory of electric vehicles and their infrastructure
[2]Department of Mechanical and Aerospace Engineering
Turin Polytechnic University in Tashkent
Email: [1]fikret.umerov@polito.uz, [2]seyran.asanov@polito.uz

Abstract– The development of the electric vehicle industry in the world, as well as in Uzbekistan, is one of the promising directions in the field of transport aimed at improving the environment. The development of this industry requires solving a number of problems, including the development of regulatory documents, the formation of solution methods and infrastructure development. The formation of infrastructure for electric vehicles requires the creation of new markets for innovative products and therefore needs active support in various industrial and social sectors of the state. It is also necessary to constantly analyze the state and dynamics of the development of the electric vehicle market in the world and in Uzbekistan. This article is devoted to the analysis of the dynamics of the development of the market of electric vehicles and their infrastructure for 2018-2023. Due to the steady growth in the number of electric vehicles and charging stations in Uzbekistan, the analysis is based on a multifactorial assessment of the technical characteristics of the vehicle, including the type of electric motor, drive topology (front/rear/full), range on a single charge, etc.

Key words– Electric car, development prospects, statistics, ecology, transport.

I INTRODUCTION

The development of the electric vehicle industry in the world, as well as in Uzbekistan, is one of the promising directions in the field of transport aimed at improving the environment. The development of this industry requires the solution to several problems, as well as the development and formation of solutions and infrastructure improvement. The formation of infrastructure for electric vehicles requires the creation of new markets for innovative products and therefore needs active support in various productive and social sectors of the State [4]. Constant analysis of the state and dynamics of the market for electric vehicles in the world and in Uzbekistan is also necessary. A study of individual companies and analysts on the prospects for electric vehicles and their components is needed [8;10]. Conducting research and studies in this area will contribute to the solution of tasks outlined in the Decree of the President of the Republic of Uzbekistan № PP-4477 of 04.10.2019. "On approval of the Strategy for the transition of the Republic of Uzbekistan to a "green" economy for the period 2019 - 2030", as well as the Decree of the Cabinet of Ministers № 812 of 2020. "On additional measures to support the rental and leasing of motor vehicles, as well as the expansion of the use of electric cars, motor vehicles and bicycles to move around the country [1;8].

II MAIN PART

Figure 1 shows a diagram of statistics of imported cars in Uzbekistan. [7].

Figure 2 shows the statistics of imported cars for the period 2019-2020-2021-2022-2023 Jan-Mar

In 2019 and 2020, sales of electric vehicles in China grew, and while total passenger car sales recovered only 4.6% compared to the crisis year 2020, the growth of electric vehicles by 108% means a doubling of their market share. However, the differences between market regions are strong: in Europe, the share of electric vehicles increased from 10% to 17%, peaking at 26% in December, with a consistently weak overall market. In North America, the share of electric vehicles was 4.4% (2.3% in 2020), in China their share increased from 5.5% to 13.3%. For the remaining 70 markets we track, the combined share of electric vehicles was 1.5% [5].

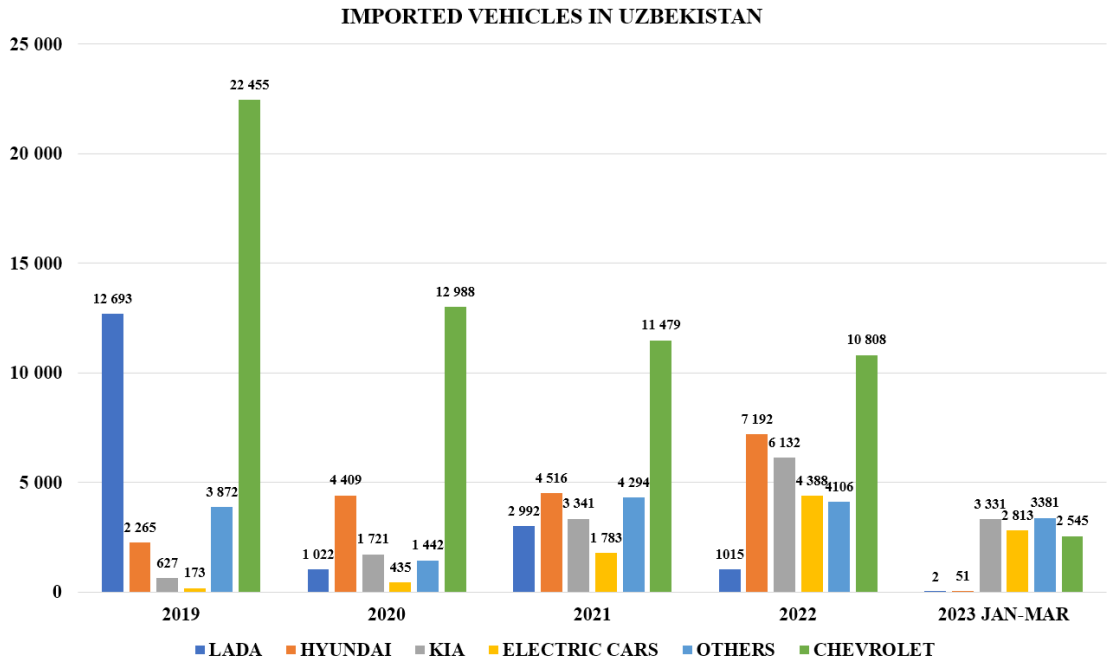

Fig. 1: Chart statistics of imported cars in Uzbekistan [7]

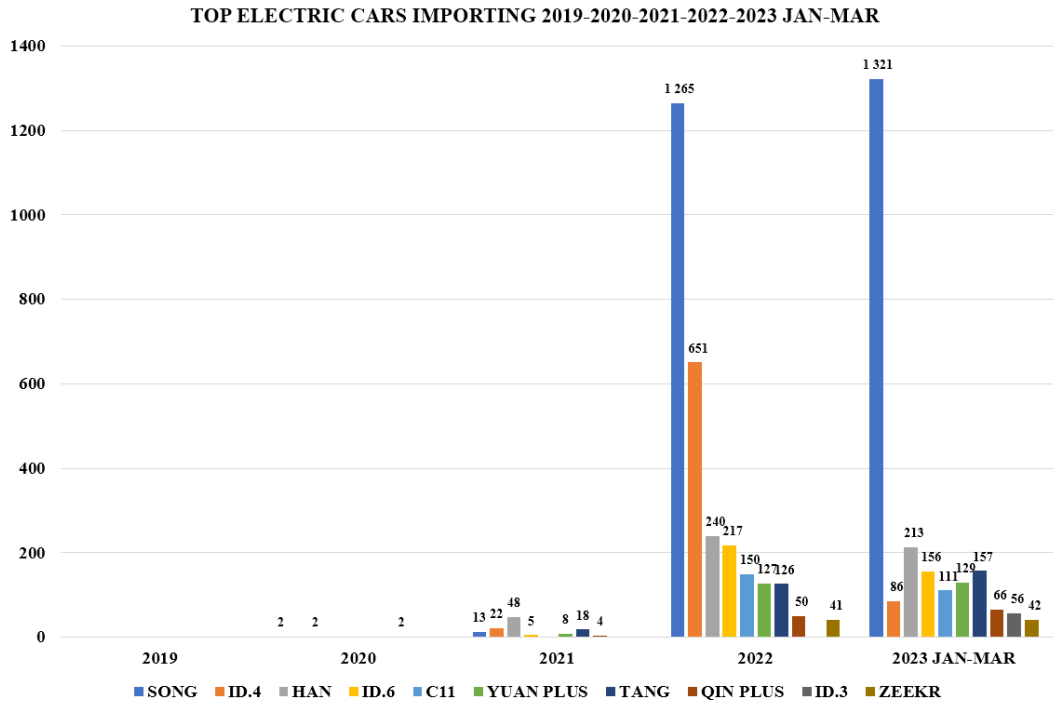

Fig. 2: Statistics of most popular cars by model for the period 2019-2023 [7]

Figure 3 shows the diagram with the most popular electric cars by quarter.

Figure 4 shows the statistics of the most popular cars presented on the domestic market.

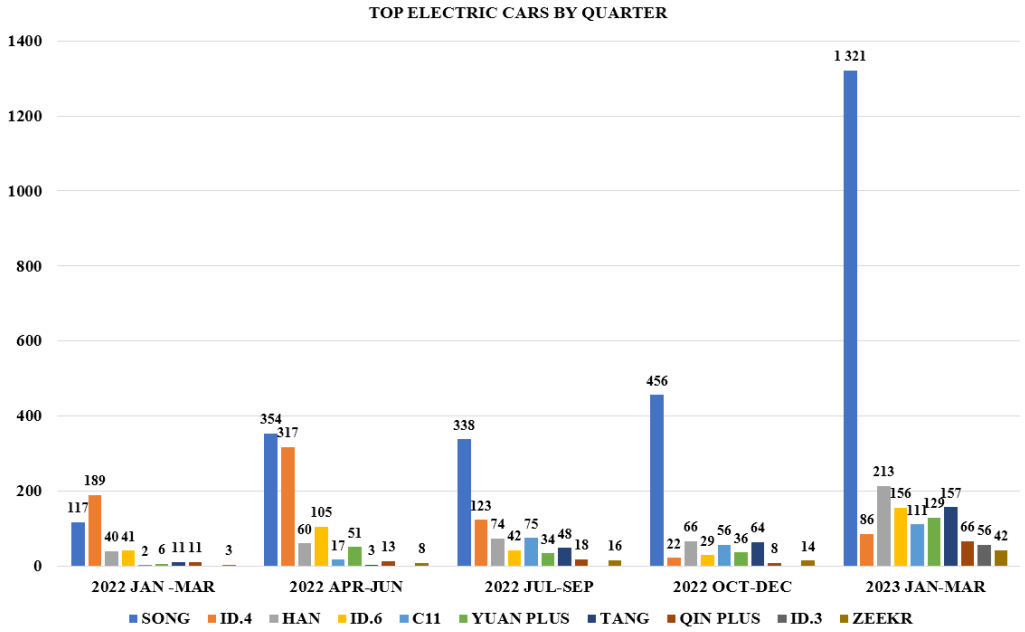

Fig. 3: Statistics of most popular cars by model by quarter 2019-2023 [6]

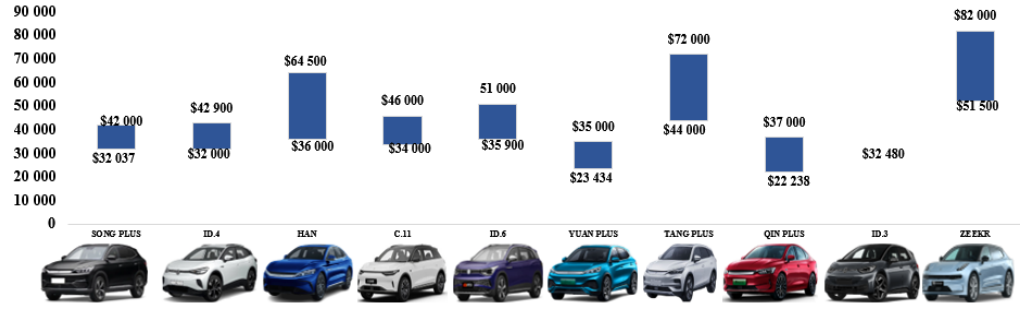

Fig. 4: Statistics of the most popular cars presented on the domestic market.[7]

Manufacturer	The volume of planned investments, bln. dollars	Model number
FORD	11	24 PHEV & 16 BEV
GM	8	20 BEV & FCEV
Toyota	13,3	10 BEV
Volkswagen	40	BEV
Daimler	11,7	
Changan Automobile Co	15	12 PHEV & 21 BEV
SAIC Motor	3	
Great Wall Motor	10	
BMW	10	13 PHEV & 21 BEV

TABLE 1: DISTRIBUTION OF ELECTRIC VEHICLE MODELS BY MANUFACTURERS.

By 2030, by some estimates, all new cars sold will be electric. Table 1 shows the plans of automakers.

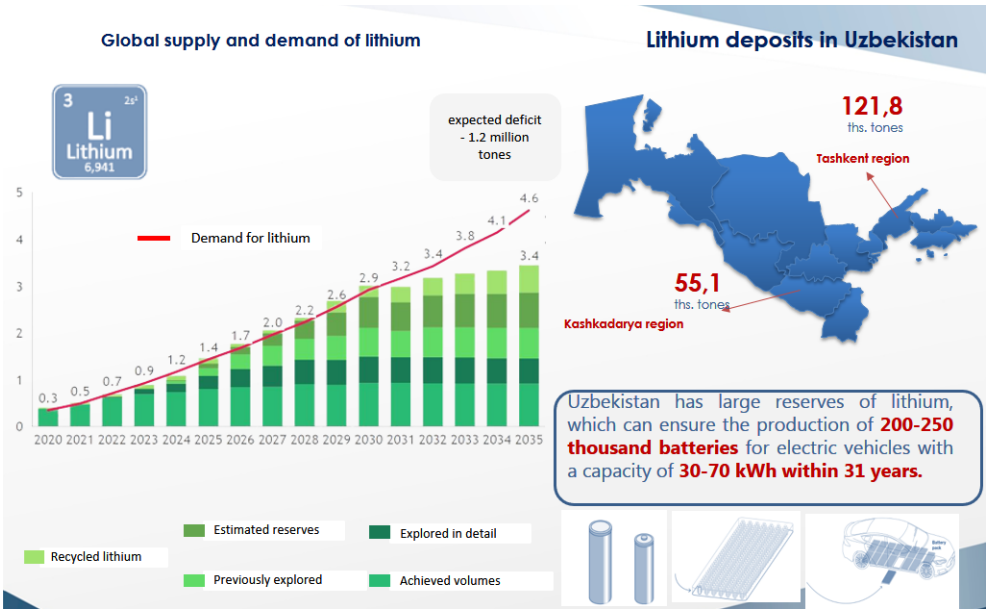

Fig. 5: Share of lithium reserves in Uzbekistan [5]

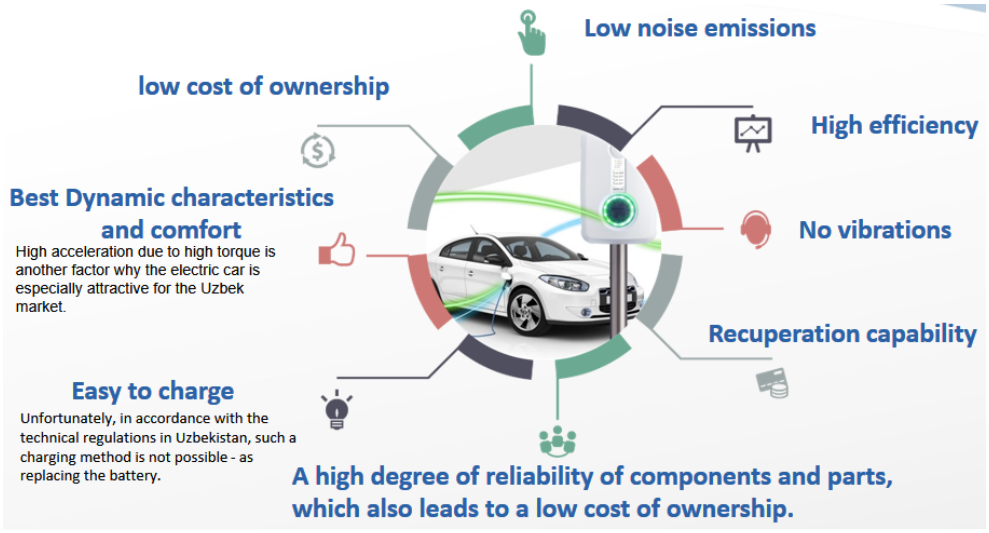

Fig. 6: Advantages of electric vehicles [1]

The share of lithium reserves in Uzbekistan is shown in Figure 5. Lithium is the main element in the production of batteries for electric vehicles [6].

The main advantages of electric vehicles are shown in Figure 6.

The electric motor generator is very reliable and does not require expensive maintenance. The transmission device is simpler, because such components and parts as the gearbox, clutch, muffler, particulate filter, fuel tank, starter, alternator, and spark plugs, missing. With the exception of the gearbox on the electric motor generator, the electric vehicle does not require oil for lubrication.

Zero CO_2 emissions. If the high-voltage battery is recharged from renewable energy sources, then the electric vehicle can be operated without CO_2 emissions.

Barriers preventing the expansion of the use of electric vehicles:

- high cost of an electric car. Not everyone can afford such a luxury;
- operation is possible only within the city limits;
- such a serious load as an electric car will most likely

require changes in the requirements for electrical wiring inside houses and structures;

- lack of infrastructure. For mass recharging of electric vehicles, it is necessary to create appropriate refuelling stations;
- the probability of overload of the power system. Mass recharging can lead to an overstrain of the power grid during peak load hours.

III CONCLUSION

As a result of the research, the authors formed the following conclusion:

1. topical problems of electric transport development in Uzbekistan were considered;
2. the basic concepts, as well as the functions and possibilities of infrastructure development were studied;
3. using an electric car as a generator/consumer of electricity allows you to achieve a positive effect both for an individual motorist and for the entire energy system of the country as a whole.

Based on the forecasts of the analysis carried out in the automotive industry, the approximate intensive development of the infrastructure of electric vehicles in Uzbekistan will be possible in 4-5 years, taking into account the interest of the population in the transition to electric vehicles, infrastructure development and the creation of relevant regulations for the successful implementation of their individual areas.

IV REFERENCES

[1] Umerov, F., Inoyatkhodjaev J., Asanov S., The prospects for the development of electric vehicles in Uzbekistan. Acta of Turin Polytechnic University in Tashkent, 12(2).

[2] Decree of the President of the Republic of Uzbekistan dated 04.10.2019, No. PP-4477 "On the application of the strategy for the transition of the Republic of Uzbekistan to a "green" meeting for the period 2019-2030".

[3] Umerov F.Sh., Juraboev A.Z. Analysis of the block diagram of the traction drive and the stages of calculation of a mechatronically controlled hybrid vehicle. Scientific journal of the Tashkent State Technical University (TSTU) named after Islam Karimov, "Yulduzlari Technique", Tashkent 2022. No. 1 - P. 29-33.

[4] Spot.uz. Electric vehicles in Uzbekistan: how this market is changing and what to expect in the future, https://www.spot.uz/ru/2022/07/18/megawatt-motors/

[5] Gazeta.uz. Import of electric vehicles, https://www.gazeta.uz/ru/

[6] Ben Kilbey, Rocco Canonica. Electric vehicles to make up 50% of new autos by 2040: Platts analytics // S&P Global Platts - https://www.spglobal.com/platts/en/market-insights/latest-news/electric-power/120419-electric-vehicles-to-make-up-50-of-new-autos-by-2040-platts-analytics, 04.12.2019.

[7] Electric Vehicle Market: Battery Electric Vehicle, Hybrid Electric Vehicle, and Plug-in Hybrid Electric Vehicle – Global Industry Size, Share, Trends and Forecast 2019-2026 // Acumen Research and Consulting website – https://www.acumenresearchandconsulting.com/electric-vehicle-market

[8] UZA.UZ. Strategy for the transition to a "green" economy: goals and objectives // Website of the National News Agency of Uzbekistan – http://uza.uz/ru/society/strategiya-po-perekhodu-na-zelenuyu-ekonomiku-tseli-i-zadach-08-11-2019, 08.11.2019.

[9] Annex No. 1 to the Decree of the President of the Republic of Uzbekistan dated October 4, 2019, No. PP-4477.

[10] Press service of the President of the Republic of Uzbekistan. The issues of the development of the machine-building industry were considered // Official website of the President of the Republic of Uzbekistan – https://president.uz/ru/lists/view/4077, 13.01.2021.

Acta of Turin Polytechnic University in Tashkent, 2023, 30, 56-61
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

ADVANCING BLOCKCHAIN SECURITY: POST-QUANTUM CRYPTOGRAPHY IN THE QUANTUM ERA

Bakhtiyor Yokubov
Turin Polytechnic University in Tashkent
Email: b.yokubov@polito.uz

Abstract– The emergence of quantum computing presents significant challenges for the security of blockchain technology, traditionally reliant on cryptographic methods now vulnerable to quantum capabilities. This article examines how current blockchain cryptography is at risk due to advancements in quantum computing and emphasizes the urgent need to shift towards more secure, quantum-resistant cryptographic methods. It explores various advanced cryptographic approaches, including lattice-based, code-based, multivariate polynomial, hash-based, and isogeny-based cryptography, highlighting their potential to enhance blockchain security against quantum threats. The focus then shifts to strategies for incorporating these advanced methods into existing blockchain systems, detailing a step-by-step transition process, the importance of comprehensive testing, ensuring compatibility across different systems, and adhering to new global standards. The discussion also covers the potential difficulties and opportunities in this integration, such as performance considerations, maintaining the ability to handle an increasing number of transactions, and the importance of ongoing innovation and research. Finally, the article emphasizes the need for collaborative efforts in research and development to successfully adapt blockchain technology to this new era of quantum computing, ensuring the future security of digital transactions.

Key words– blockchain, quantum computing, post-quantum cryptography, quantum-resistant algorithms

I Introduction

The advent of Bitcoin heralded a pivotal moment in the digital era, thrusting blockchain technology into prominence within digital currencies. This association between blockchain and digital currency is justified, considering that a blockchain serves as a continually updated transaction database across an extensive network of computers [1]. The allure of digital currencies and their valuation underpins the endurance of this network.

Blockchain technology's evolution has seen Ethereum (ETH) attain a level of computational universality known as Turing completeness [2]. This advancement signifies that computational capabilities on ETH are as extensive as those on any contemporary computer, effectively transforming the blockchain into a vast, globally connected computational entity [1].

Money, as a universal medium of exchange, embodies value. The macroeconomic circulation of money reflects the collective intentions of society. Extending this analogy to blockchain, a Turing-complete system like ETH may be viewed as an immense, networked computer utilising digital currency to manifest computational desires.

This understanding naturally posits an open currency system as the foremost and most intuitive application of blockchain when envisaged as a networked computer. Nevertheless, alternative blockchain forms exist, such as permissioned and private blockchains, which operate independently of digital currency generation and consumption for their operational security and reliability. However, when integrated with the internet, these blockchains still face the paramount challenge of authentication.

Authentication remains critical across all types of blockchains—public, permissioned, or private. A verifiable identity for each node within the network is imperative. While many blockchain solutions endeavour to fully virtualize currency and transactions, and despite the deployment of smart contracts like ERC725 to address digital identity fraud, challenges persist [3]. Presently, digital signatures, based on cutting-edge cryptography, are the primary authentication method.

The stability of blockchain technology is deeply rooted in its cryptographic foundation. A compromise in this area could lead to severe disruptions, enabling malicious actors to rapidly access numerous user credentials and jeopardising the blockchain's very essence. Such a breach's consequences could be far-reaching, potentially causing divisions

within the blockchain community, as previously observed in the DAO attack [4].

Quantum computing poses a significant risk with its potential to disrupt conventional cryptographic principles. Particularly, Shor's algorithm poses a formidable threat by enabling the factorization of large integers, a fundamental aspect of many cryptographic protocols. This would directly undermine the integrity of digital signatures [5].

Furthermore, quantum algorithms like Grover's could expedite hash computations, quicken block generation, and facilitate potential modifications to the blockchain, thus compromising its integrity. While Grover's algorithm's limitations suggest that increasing hash lengths could mitigate these risks, incorporating quantum-resistant algorithms into the blockchain's security framework is essential for safeguarding against such quantum computational advancements.

II BACKGROUND

Blockchain technology aims to digitise all transactional processes, with the digital signature as the sole authentication mechanism. In a decentralised architecture, this signature essentially represents the user's identity. A compromise of the digital signature by an unauthorised entity poses significant challenges for the legitimate user in rectifying the situation.

Digital signatures, integral to asymmetric cryptography, employ a dual-key system: the public key, which is openly available for identification, and the private key, which is kept confidential. These keys are created so that deriving the private key from the public key is unfeasible. The user utilises the private key to sign messages. A message encrypted with the private key can only be decrypted with its corresponding public key, confirming the message's origin from the private key holder and validating its identity.

The public and private keys exhibit several key properties:

- It is computationally challenging to infer the private key from the public key.
- A message encrypted with a public key is decryptable solely by its corresponding private key, and vice versa.
- The strength of these keys relies on complex mathematical challenges, such as prime factorisation and elliptic curve cryptography, which, with current computing power, require impractical amounts of time to resolve [6].

Thus, deducing the private key from the public key should be prohibitively time-intensive, while verifying a message signed with a private key should be rapid. Underlying mathematical principles maintain this balance. After rigorous mathematical evaluation, encryption methods like RSA and those based on elliptic curves are considered secure for asymmetric encryption.

However, the advent of quantum computing poses a significant threat to this equilibrium. Quantum computers have the potential to solve specific mathematical problems much more efficiently than classical computers, undermining the efficacy of existing cryptographic algorithms. Specifically, quantum computation could simplify extracting a private key from a public key, thereby challenging the security assured by current algorithms.

The rise of quantum computing endangers widely used cryptographic systems, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC). Quantum computers, utilising algorithms like Shor's, could feasibly break RSA and ECDSA (Elliptic Curve Digital Signature Algorithm) in polynomial time, an achievement beyond the reach of classical computing [5]. In response, post-quantum cryptography is being developed to create cryptographic systems resistant to the capabilities of large-scale quantum computers [7].

Blockchain platforms, including Bitcoin, rely on elliptic curve cryptography to safeguard token ownership, ensuring that only the rightful owner can engage in transactions [8]. Without a shift to quantum-resistant cryptographic systems, the ownership of tokens could be jeopardised by anyone with access to a powerful quantum computer. This scenario could severely compromise the foundational trust and security underpinning blockchain technology.

III LIMITATIONS OF CLASSICAL CRYPTOGRAPHY IN BLOCKCHAIN

Blockchain technology, central to establishing a secure and decentralized transaction ledger, fundamentally depends on two cryptographic protocols:

1. Asymmetric digital signatures, such as ECDSA and RSA, are integral to public-key cryptography.
2. Hashing functions like SHA-256, essential for implementing consensus mechanisms.

Though challenging for classical algorithms, these protocols are not intrinsically secure against advancements in quantum computing. Shor's algorithm, in particular, poses a significant threat to the integrity of classical asymmetric digital signatures by undermining their trapdoor functions [9]. Additionally, Grover's algorithm can substantially accelerate the Proof of Work (PoW) algorithm, increasing the likelihood of a quantum node dominating the consensus process [10].

The emergence of quantum computing presents a formidable challenge to traditional cryptographic protocols

such as RSA and ECDSA. These protocols rely on the computational complexity of the Integer Factorization (IF) problem and the Elliptic Curve Discrete Logarithm Problem (ECDLP), which quantum computers can resolve much more rapidly [9]. The prevalent use of ECDSA in blockchain digital signature schemes makes them particularly susceptible to quantum attacks.

Shor's algorithm can solve problems like integer factorization and ECDLP in polynomial time [9], a critical risk for public-key cryptography systems depending on RSA or ECDSA. Classical computers require exponentially more time to solve these problems. Furthermore, quantum computers using Grover's algorithm could hasten hash generation, potentially enabling the reconstitution of an entire blockchain. Grover's algorithm might also be adapted to identify hash collisions, permitting the substitution of blockchain blocks without compromising the system's integrity [10].

Consider Bitcoin as a case in point: its network transactions are vulnerable to quantum attacks. Bitcoin addresses are initially just hashed values of the user's public key, concealing both the private and public keys. However, when a transaction is broadcast on the network, the user's public key is exposed for verification [11]. With quantum adversaries capable of easily breaking ECDSA, they could infer the user's private key from the public key. This would enable an adversary to forge the user's digital signature, authorizing unauthorized transactions. They could impersonate the user, initiating transactions to transfer funds, acting without the user's consent or knowledge. If such unauthorized transactions are confirmed and added to the blockchain before the legitimate ones, they would be erroneously accepted, hijacking genuine transactions [12].

As quantum computers become more accessible, advancing cryptographic systems and digital signature schemes to be quantum-resistant is crucial, ensuring blockchain-based systems' continued security and integrity.

IV POST-QUANTUM CRYPTOGRAPHY IN BLOCKCHAIN

The emergence of quantum computing necessitates a fundamental shift in the cryptographic foundations of blockchain technology. To fortify blockchain systems against quantum threats, a thorough reassessment and evolution of cryptographic primitives are essential. This section delves into signature methods devised to counteract vulnerabilities inherent in public-key cryptography in the quantum age. These methods are based on various mathematical principles, each providing a distinct strategy for securing blockchain against quantum computing challenges.

1 Lattice-Based Cryptography

Lattice-based cryptography is notable for its resilience to quantum computing attacks. It is predicated on the complexity of solving problems in n-dimensional lattice spaces, which are presumed to be unsolvable by quantum computers. This type of cryptography underlies several proposed quantum-resistant algorithms, including New Hope, NTRU, and LWE (Learning with Errors), each promising robust security against quantum threats.

2 Code-Based Cryptography

Originating from the McEliece cryptosystem, code-based cryptography depends on the difficulty of decoding random linear codes. The security principle of this method is anchored in the complexity of solving the Generalized Syndrome Decoding (GSD) problem, a task that quantum algorithms have yet to solve efficiently. This approach is known for its rapid encryption and decryption processes, albeit often resulting in larger key sizes than other cryptographic methods.

3 Multivariate Polynomial Cryptography

Cryptography employs multivariate polynomials over finite fields to create public keys. Its security is contingent upon the difficulty of solving systems of multivariate quadratic equations, known as the MQ problem, which remains an arduous task for quantum computers. This method is especially efficient in generating and verifying signatures.

4 Hash-Based Signatures

Hash-based signatures are among the earliest examples of post-quantum cryptography. Their security is derived entirely from cryptographic hash functions currently considered quantum-resistant. While they provide strong security assurances, hash-based signatures typically face limitations regarding key usage and have larger signature sizes.

5 Isogeny-Based Cryptography

A recent development, isogeny-based cryptography, concentrates on the computational challenge of identifying isogenies between elliptic curves. The security of this method relies on the difficulty of certain problems in elliptic curve theory, which quantum algorithms have not effectively addressed yet.

6 Quantum Key Distribution

Quantum Key Distribution (QKD) utilizes quantum mechanics to secure communication channels. It facilitates the secure exchange of cryptographic keys, making any eavesdropping detectable. While not a direct application

in blockchain, QKD exemplifies a broader spectrum of quantum-resistant cryptographic practices.

In conclusion, post-quantum cryptography is varied, with each approach offering unique advantages and facing distinct challenges. Integrating these cryptographic techniques into blockchain technology is vital for ensuring its durability and security in the forthcoming quantum computing era. As research continues, selecting and adopting these post-quantum cryptographic methods will be critical in protecting blockchain against quantum computing threats.

V ADAPTING BLOCKCHAIN TECHNOLOGY FOR QUANTUM RESILIENCE

The advent of quantum computing necessitates a critical reassessment of the cryptographic infrastructure currently employed in blockchain technology, which is adept at countering conventional computational attacks. This reassessment involves re-evaluating the bit security level metric, a measure traditionally used to gauge the effort required by classical computers to mount a brute-force attack. For example, a 1024-bit RSA key implies a security level equivalent to brute-forcing a key of the same bit length. However, the introduction of quantum computing significantly alters this security paradigm.

Quantum computers fundamentally transform the security landscape. While a classical brute-force attack on an 80-bit security cryptosystem might incur costs ranging from tens of thousands to hundreds of millions of dollars, quantum computers pose a more severe threat. A quantum computer with 1000 qubits could potentially compromise 160-bit elliptic curves, and a 2000-qubit quantum computer might breach a 1024-bit RSA key. This vulnerability extends to systems based on integer factorization and elliptic curves and those reliant on discrete logarithm problems, which Shor's algorithm can efficiently solve.

Conversely, hash functions generally exhibit greater resilience to quantum attacks due to the challenges in developing quantum algorithms for NP-hard problems. Nevertheless, to counter quantum threats, especially from Grover's algorithm, which enhances brute-force capabilities quadratically, the output lengths of hash functions may need to be extended. For instance, a hash function ensuring an n-bit security level in a quantum environment should yield outputs of at least 3*n bits.

Furthermore, Grover's algorithm could potentially hasten mining processes in blockchains like Bitcoin, resulting in faster block generation and potential integrity concerns. Shor's algorithm presents an additional risk by enabling quantum adversaries to forge digital signatures, thus jeopardizing user identities and assets.

In response to these quantum developments, the National Institute of Standards and Technology (NIST) initiated a project in 2016 to establish future post-quantum cryptography standards. By 2017, 59 encryption schemes were submitted, leading to the selection of three digital signature algorithms: Falcon, Dilithium, and SPHINCS+.

Post-quantum cryptosystems intended for blockchain frameworks must exhibit certain characteristics for optimal functionality: small key sizes to ensure efficient storage and management; concise signatures and hashes to prevent blockchain bloat; fast execution speeds to support high transaction volumes; low computational complexity for compatibility across a wide range of hardware; and minimal energy consumption to be environmentally sustainable.

Transitioning to quantum-resistant blockchains is not just a technical challenge but a pivotal step in safeguarding the future of digital transactions in the era of quantum computing.

VI CHALLENGES AND OPPORTUNITIES IN IMPLEMENTING POST-QUANTUM CRYPTOGRAPHY IN BLOCKCHAIN

Integrating post-quantum cryptographic algorithms into established blockchain systems presents significant challenges and opportunities. Successfully navigating these challenges and leveraging the opportunities is crucial for strengthening blockchain systems against the looming quantum computing threat. This section explores the key challenges and opportunities associated with the integration of post-quantum cryptography in blockchain technology.

Integration with Existing Systems: A primary challenge is integrating post-quantum cryptography into blockchain systems that currently rely on classical cryptographic principles. Selecting suitable post-quantum schemes is essential for a smooth transition without compromising security or disrupting ongoing operations. Assessing performance and compatibility with existing systems is imperative. Furthermore, developing new protocols and software tools that support post-quantum cryptography is vital for its efficient integration into blockchain architectures.

Performance Trade-offs: Post-quantum cryptographic algorithms often entail larger key sizes, extended signature lengths, and increased computational demands compared to their classical counterparts. These factors can influence the efficiency, latency, and scalability of blockchain systems. Addressing these issues requires continuous research to refine post-quantum algorithms, exploring hybrid cryptographic solutions, and investigating innovative implementation techniques that maintain security in blockchain systems.

Scalability and Network Efficiency: Blockchain networks need to manage growing transaction volumes and participant numbers efficiently. The larger key and signature

sizes inherent in post-quantum cryptographic schemes could exacerbate scalability challenges by increasing storage and bandwidth requirements. Research into key and signature compression, reducing storage overhead, and minimizing the impact of post-quantum cryptography on network performance is essential to mitigate these challenges.

Standardization Efforts and Regulatory Considerations: Standardizing post-quantum cryptographic algorithms is a critical aspect of their adoption in blockchain systems. Organizations such as NIST are instrumental in evaluating and endorsing post-quantum schemes for widespread use. Developers and organizations must adapt to these new standards and modify their systems accordingly as standardisation progresses. Additionally, evolving regulations regarding data protection, privacy, and cybersecurity must be considered in implementing post-quantum cryptography, as these regulations can influence the adoption of new cryptographic technologies in blockchain systems.

In summary, the shift to post-quantum cryptography in blockchain systems entails various challenges and opportunities that require careful consideration and strategic action. Collaborative efforts among researchers and developers are crucial to ensure blockchain technology's long-term security and resilience in the era of post-quantum computing, focusing on effective integration, performance optimization, scalability, and compliance with emerging standards.

VII STRATEGIES FOR POST-QUANTUM INTEGRATION IN BLOCKCHAIN SYSTEMS

Integrating post-quantum cryptographic algorithms into existing blockchain systems is a crucial and complex task that demands a strategic and systematic approach. This section outlines various strategies to facilitate the seamless incorporation of post-quantum cryptography into blockchain technology, thus protecting these systems from potential quantum computing threats.

Gradual Transition to Post-Quantum Cryptography: A phased transition from classical cryptographic protocols to post-quantum alternatives is recommended to minimize disruptions. This step-by-step approach entails updating cryptographic primitives and protocols in stages, maintaining backward compatibility with existing systems. Hybrid cryptographic schemes, which merge classical and post-quantum algorithms during this transitional phase, can provide enhanced security and flexibility.

Thorough Testing and Validation: Rigorous testing and validation of post-quantum cryptographic algorithms are imperative before integrating them into blockchain infrastructures. Assessments should focus on the algorithms' resilience to quantum attacks, their computational and communication efficiency, and compliance with established standards. Additionally, the potential impact of these new algorithms on overall system performance and user experience should be meticulously evaluated and mitigated.

Ensuring Interoperability and Standardization: Effective integration of post-quantum cryptography in blockchain systems necessitates ensuring interoperability across various implementations and platforms. Embracing standardized post-quantum cryptographic algorithms and protocols facilitates smooth interactions and communication between diverse blockchain networks. Collaboration with standardizing bodies, like NIST, is vital for adhering to international guidelines and promoting the adoption of secure and reliable post-quantum solutions.

Education and Awareness: Increasing awareness among developers, users, and stakeholders about quantum computing's implications and the need for quantum-resistant solutions is fundamental to successful integration. Initiatives aimed at education, training, and disseminating research findings are key in accentuating the benefits and challenges of implementing post-quantum cryptography in blockchain systems. A well-informed community is better prepared to make decisions regarding adopting and integrating these advanced technologies.

Ongoing Research and Development: The landscape of post-quantum cryptography is continuously evolving, introducing new algorithms and methods to address emerging challenges and improve existing solutions. Persistent research and development are vital to keep pace with advancements in quantum computing and post-quantum cryptography. Staying informed about the latest developments and actively participating in research endeavours ensures that blockchain systems remain secure and updated in the face of evolving quantum threats.

In summary, integrating post-quantum cryptographic algorithms into blockchain systems necessitates a comprehensive strategic approach encompassing gradual transition, rigorous testing, a focus on interoperability, educational initiatives, and ongoing research. By embracing these strategies, the blockchain community can collaboratively ensure blockchain technology's long-term security and viability in the quantum computing era.

VIII CONCLUSION AND FUTURE DIRECTIONS

In conclusion, integrating post-quantum cryptography into blockchain technology is a precautionary measure and a necessary evolution to safeguard against the impending quantum computing era. This paper has outlined the vulnerabilities of current cryptographic methods in blockchain systems to quantum computing threats and emphasized the importance of transitioning to post-quantum cryptography. Strategies for implementing this transition have been discussed, focus-

ing on the gradual integration of new cryptographic methods, rigorous testing and validation, ensuring interoperability and standardization, raising awareness and education, and the need for continuous research and development.

As we look to the future, several key directions emerge:

Advancements in Quantum-Resistant Algorithms: Ongoing research into developing more efficient and robust quantum-resistant algorithms is paramount. This includes improving the performance of existing algorithms and discovering new cryptographic approaches that may offer enhanced security and efficiency.

Collaborative Standardization Efforts: The role of international standardization bodies like NIST will become increasingly crucial as they set the benchmarks for post-quantum cryptographic methods. Collaboration among academia, industry, and regulatory bodies will be essential to establish and adopt these standards globally.

Blockchain Infrastructure Evolution: Blockchain technology itself must evolve to accommodate new cryptographic standards. This evolution involves both software and hardware aspects, ensuring that blockchain platforms can implement and run post-quantum cryptographic algorithms efficiently.

Education and Training: As the blockchain and quantum computing fields rapidly evolve, the need for specialized knowledge and skills in these areas will grow. Educational institutions and industry leaders should focus on developing curricula and training programs that equip the next generation of professionals with the necessary expertise.

Monitoring Quantum Computing Developments: The blockchain community must stay vigilant regarding the progress in quantum computing. Understanding the advancements in quantum technologies will be crucial for timely responses and updates to cryptographic practices.

Exploring Hybrid Solutions: Investigating and developing hybrid solutions that combine the strengths of classical and quantum-resistant cryptographic methods could provide an effective interim solution while fully quantum-resistant technologies are perfected.

The journey towards quantum-resistant blockchain systems is both challenging and exciting. It presents opportunities for innovation, collaboration, and the development of technologies that could redefine the security landscape in the digital world. The blockchain community, therefore, must remain proactive, adaptive, and collaborative in addressing these challenges and embracing the opportunities that lie ahead in the quantum computing era.

IX References

[1] "What is ethereum?" [Online]. Available: https://ethereum.org

[2] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, vol. 3, no. 37, pp. 2–1, 2014.

[3] "Erc725 alliance." [Online]. Available: https://erc725alliance.org/

[4] M.I. Mehar, C.L. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H. M. Kim, and M. Laskowski, "Understanding a revolutionary and flawed grand experiment in blockchain: the dao attack," Journal of Cases on Information Technology (JCIT), vol. 21, no. 1, pp. 19–32, 2019.

[5] T.M. Fern´andez-Caram‘es and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," IEEE Access, vol. 8, pp. 21 091–21 116, 2020.

[6] J.-S. Coron, "What is cryptography?" IEEE Security & Privacy, vol. 4, no. 1, pp. 70–73, 2006.

[7] D.J. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, no. 7671, pp. 188–194, 2017.

[8] "Transactions — bitcoin." [Online]. Available: https://developer.bitcoin.org/devguide/transactions.html

[9] P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997.

[10] L.K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," Physical Review Letters, vol. 79, no. 2, pp. 325–328, 1997.

[11] A.M. Antonopoulos, Mastering Bitcoin, 2nd Edition. O'Reilly Media, Inc., 2017.

[12] J.J. Kearney and C. A. Perez-Delgado, "Vulnerability of blockchain technologies to quantum attacks," Array, vol. 10, no. November 2020, p. 100065, 2021. [Online]. Available: https://doi.org/10.1016/j.array.2021.100065