Radioelectronic and Computer Systems, 2025, no. 2(114)
ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

UDC 004.056.55:004.272:530.182 **doi: 10.32620/reks.2025.2.14**

Akbota KULZHANOVA[1], Sholpan JOMARTOVA[2], Talgat MAZAKOV[1]

[1] ***Department of Information Systems, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan***
[2] ***Department of Artificial Intelligence and Big Data, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan***

ENCRYPTION OF SENSOR DATA USING THE LORENTZ ATTRACTOR IN EMBEDDED SYSTEMS

The increasing threat of cyber-attacks and the need to protect embedded system data require the development of energy-efficient cryptographic methods. ***The subject matter*** *of this article is the development of an energy-efficient data encryption method for embedded systems using chaotic systems, specifically the Lorenz system.* ***The goal*** *of this study was to create a data encryption method for embedded systems with limited computing resources.* ***The tasks included*** *developing an algorithm based on the properties of the chaotic Lorenz system, implementing it on microcontrollers and programmable logic circuits, and testing its performance under near-real operational conditions.* ***The methods used*** *involved leveraging the high sensitivity of chaotic systems to initial conditions, implementing the encryption algorithm in hardware, and evaluating key performance indicators, such as speed, power consumption, memory usage, and resistance to cryptographic attacks.* ***The results*** *showed that the proposed algorithm reduces memory and energy consumption by 37% and 10%, respectively, compared to conventional methods, providing an encryption speed of 120 milliseconds per kilobyte of data. Tests have confirmed that even minimal changes in the initial parameters of a chaotic system led to a change of up to 90% of the bits in the encrypted data, which increases the algorithm's robustness. The proposed method is compatible with various types of data and shows versatility for information protection. The algorithm has demonstrated efficiency in processing text arrays and sensory data, making it suitable for use in smart cities, medical devices, and industrial networks. The key entropy value was 7.95 bits per byte, indicating high encryption reliability. In* ***conclusion****, the results obtained prove that the proposed method is promising for use in conditions of limited resources and can be integrated with modern information security technologies.*

Keywords: *chaotic structures; information security methods; dynamic models; nonlinear cryptography; mathematical security framework; signal processing algorithms.*

1. Introduction

Data protection has become one of the key tasks of modern digital infrastructure with the development of the Internet of Things (IoT) technologies [1]. The number of IoT devices is constantly increasing, and their applications include smart cities, medical systems, industry, and transportation. These devices generate large amounts of data on a daily basis, which may contain confidential information such as personal data, medical indicators, or equipment operation parameters. However, IoT data is subject to numerous threats: leaks, attacks on devices, and substitution of transmitted information. According to the research by Goworko and Wytrębowicz [2], about 60% of all IoT devices are vulnerable to attacks due to the lack of built-in protection mechanisms. Additionally, Ali et al. [3] emphasized the importance of real-time data protection for IoT devices, which makes chaotic systems particularly promising. Modern methods, including cryptographic protection, require adaptation to the IoT, especially in the context of new threats, such as post-quantum attacks [4]. Similarly, research by Clemente-Lopez et al. [5] emphasized the need to develop security solutions that consider the limitations of embedded systems, such as IoT sensors.

1.1. Motivation

The limited resources available for IoT devices pose a challenge. Sensors, controllers, and other embedded devices often have low computing power, limited memory, and limited energy, making conventional encryption methods, such as the Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA) encryption, of little use [6-8]. For example, the AES algorithm requires significant resources to generate keys, and RSA cannot

provide the required encryption speed for real-time [9]. This is especially critical for medical sensors, where any delay can negatively affect the system's operation. The AES algorithms may not be optimal for embedded IoT platforms due to energy demands and high memory [10]. The study by Gonzalez and Nepomuceno [11] focused on the adaptation of chaotic systems for energy-dependent IoT devices, making such algorithms suitable for autonomous sensor networks. Peng et al. [12] developed approaches to selective encryption based on chaotic systems that show their applicability to embedded devices. Zhang et al. [13] applied selective encryption to H.264 video streams based on chaotic dynamics. Their results confirm the feasibility and reliability of the proposed chaotic encryption schemes.

In such circumstances, alternative approaches that provide a high level of security with minimal resource expenditure are needed. The use of chaotic systems such as the Lorentz attractor is one of the most promising areas. Chaotic systems have unique properties, including a high degree of sensitivity to the initial state, unpredictability, and deterministic chaos, which makes them ideal for cryptography [14, 15]. Moreover, they have proven their effectiveness in protecting sensor data and embedded systems. Hassan and Kadhim [16] demonstrated that chaotic systems can successfully integrate with existing cryptographic algorithms, increasing their stability. Anandkumar and Kaplana [14] showed that chaotic algorithms are not only superior to conventional methods in terms of attack resistance but also provide a higher operation speed. The research by Alahmadi [17] highlighted promising directions for integrating advanced chaotic synchronization techniques into lightweight cryptographic solutions for embedded devices. Zou et al. [18] proved that the Lorentz attractor can be adapted for embedded systems because its algorithms require a minimum amount of memory.

1.2. Work related analysis

Despite this, most of the existing research focuses on the theoretical aspects of chaotic systems, and only a few papers consider their implementation in real conditions. For example, Nesa et al. [19] noted the need to optimize chaotic algorithms for sensor networks, and Rahman et al. [20] emphasized the importance of integrating chaotic systems with conventional methods to increase their resistance to modern attacks. Similar hybrid approaches, as noted by Vishwakarma et al. [21], can combine the best properties of both methods, providing a high level of security. These studies show that to fully unlock the potential of chaotic systems, their algorithms must be adapted to the limitations of embedded devices and their operation must be tested in real conditions.

The basis of chaotic systems is their mathematical model. The Lorentz attractor is described by a nonlinear equation system that is highly sensitive to the initial state and capable of generating keys with a high degree of entropy. This property makes the Lorentz attractor particularly suitable for cryptography, as it can be used to create keys that are virtually impossible to recover [22]. In addition, chaotic algorithms are characterized by low computational costs, making them ideal for devices with limited resources, such as IoT sensors.

1.3. Objectives and tasks

This study aims to address the existing gaps in the study of chaotic systems by proposing data encryption based on the Lorentz attractor. As part of the research, conventional and alternative cryptography methods were analyzed, and an algorithm adapted to the limitations of embedded systems was developed and tested on real hardware, including STM32 microcontrollers and Field-Programmable Gate Array (FPGA). This study aimed to show that chaotic systems can provide a high level of security with minimal computing costs, making them a promising solution for sensor networks and IoT devices.

To achieve the goal, within the framework of this publication, the following tasks must be solved:

1. To analyze conventional and alternative cryptographic methods in the context of IoT and embedded systems.
2. To develop a data encryption algorithm that accounts for the limitations of embedded devices based on the Lorentz attractor.
3. To implement the proposed algorithm on real hardware platforms, including STM32 microcontrollers and FPGA.
4. To test and validate the proposed algorithm under real operating conditions to assess its practicality and efficiency.

Section 2 (Materials and research methods) explains the development and implementation of the proposed encryption method based on the Lorentz attractor. The mathematical background of the Lorentz system, the numerical techniques used, such as Runge-Kutta, the preprocessing of sensor data, and the hardware and software platforms for testing, which include STM32 microcontrollers and Xilinx FPGA are shown in this section.

Section 3 (Case study) presents the results of the Lorentz-based encryption algorithm testing. This section covers key generation, entropy analysis, encryption effectiveness, and a comparison with the AES standard. This section discusses performance metrics, such as speed, memory usage, and energy consumption, supported by figures and a summary table. This section confirms the algorithm's robustness, low resource usage, and suitability for real-time applications in embedded systems.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Section 4 (Discussion) interprets the results. The practical advantages of using chaotic systems, such as the Lorentz attractor, in modern cryptography, as well as resistance to cryptographic attacks, performance in limited environments, and application scenarios, such as smart cities, medical devices, and industrial IoT, are highlighted.

Section 5 (Conclusions) summarizes the study's main contributions and reaffirms the potential of the Lorentz algorithm as a strong encryption solution for low-resource embedded systems. The benefits of the proposed algorithm are highlighted. The section also outlines possible improvements, such as the integration of post-quantum security and scaling for high-volume data.

2. Materials and methods of the research

The choice of the Lorentz attractor as the basis of the cryptographic algorithm was conditioned by its unique properties, such as high initial state sensitivity and various chaotic behavior. This makes it suitable for generating keys with a high degree of entropy. The research was conducted in two stages: the development of a mathematical model and an encryption algorithm and the testing and evaluation of performance in software and hardware environments. The algorithm was based on the system of Lorentz differential equations (1-3):

$$\frac{dx}{dt} = \sigma(y - x), \quad (1)$$

$$\frac{dy}{dt} = x(p - z) - y, \quad (2)$$

$$\frac{dz}{dt} = xy - \beta z, \quad (3)$$

where: x, y, z – variables of the system state (rate of convection, temperature difference and deviation from symmetry); $\frac{dx}{dt}$, $\frac{dy}{dt}$, $\frac{dz}{dt}$ – derivatives of the variables x, y, z, in time t, describing the rate of their change; t – time used as an independent variable; dt – infinitesimal time interval used to study the changes in the dynamics of the system; σ – Prandtl parameter, which characterizes the ratio of the rate of thermal conductivity to viscosity; ρ – Rayleigh parameter responsible for the intensity of external thermal action; β – geometric parameter of the system.

The triplet (x(t), y(t), z(t)) obtained by solving the Lorenz system is used to generate a cryptographic keystream. The continuous values of x(t), y(t), z(t) are mapped into an 8-bit key by normalizing and scaling them as follows:

$$k_i = \text{uint8}(\text{mod}|x_i| \times 10^6, 256, \quad (4)$$

where k_i represents the *i*-th byte of the keystream, and x_i is the *i*-th value of the Lorenz system's x(t). These values are then used in the encryption function as follows:

$$c_i = p_i \oplus k_i, \quad (5)$$

where p_i is the *i*-th byte of plaintext, and $\oplus$ denotes the XOR (exclusive OR) operation, which is a fundamental bitwise cryptography operation.

To implement the algorithm, the Runge-Kutta method of the 4th order was used, which allowed accurate solving of differential equations. The software implementation was performed in Python using the NumPy and SciPy libraries. Multiple calculations with different initial conditions were used to increase the accuracy of key generation, which confirmed the stability of the algorithm. This study adapted the approaches proposed by Raj et al. [23], where the developed lightweight encryption technique for IoT platforms included data diffusion operation optimization to improve performance. This served as the basis for improving data processing and reducing computational costs when implementing a cryptographic algorithm.

The data from the sensors were normalized and preprocessed using Fourier transform to eliminate system noise. This improved data compatibility with the cryptographic algorithm and reduced the likelihood of errors in the encryption process. The approach used in the study by Magara and Zhou [24] has shown its effectiveness in preparing data for IoT systems, which was considered when developing the data preprocessing stage.

The hardware was implemented using STM32F407 microcontrollers and Xilinx Artix-7 FPGA. The STM32 was used to test the execution speed of the algorithm in resource-limited conditions, and the FPGA was used to test the real-time operation. The implementation approach proposed by Yener [25] confirmed that the use of STM32 platforms ensures the accuracy of reproducing chaotic trajectories, which is critical for Lorentz attractor-based algorithms. This combination of equipment enables the high-fidelity reproduction of chaotic trajectories and the adaptation of the algorithm for IoT devices.

Testing was conducted on text data of 128 and 256 characters in length and on numerical arrays simulating sensor data (for example, temperature and pressure). The text strings included a mix of uppercase and lowercase letters, digits, and special characters, reflecting a variety of real-world data types that might be encrypted in practical applications. The numerical arrays contained 128 and 256 values representing typical sensor inputs, respectively. The performance of the algorithm in terms of encryption speed, memory utilization, and handling various data formats was assessed using both datasets. The sensor data included properties such as continuous numerical values, variable ranges, and typical noise levels found in real-world measurements. For instance, the temperature and pressure data ranged from -40°C to 100°C and 0 to

5000 psi, respectively. The encryption method used in this study was applied to pre-processed sensor data, which had been normalized and filtered to eliminate noise, mimicking real sensor outputs. The communication channel used in this study is a wireless IoT network characterized by a typical 2.4 GHz frequency band. The channel width is 20 MHz, which offers sufficient bandwidth for real-time sensor data transmission. The estimated 250 kbps transmission speed is appropriate for the low bandwidth needs of embedded systems and guarantees effective data exchange while consuming minimal energy, both of which are essential for IoT applications.

Deviations of the initial conditions (x_0) by 0.001 caused changes of up to 90% of the bits in the encrypted data, confirming the algorithm's stability. This metric was calculated by numerically integrating the system using the Runge-Kutta method after perturbing the initial values of the Lorenz system. Hamming distance was used to bitwise compare the keystreams produced from the original and perturbed beginning circumstances. To determine the percentage of changed bits, the number of different bits was divided by the total number of bits in the keystream. This investigation showed the method's sensitivity to even small changes in the initial conditions, guaranteeing that even small adjustments result in notable changes to the encrypted output.

The Student's t-test was used to verify the statistical significance of the results, which showed the absence of significant deviations during repeated tests.

A computer with an Intel Core i7 processor and 16 GB of RAM was used to model and analyze the algorithm. The microcontrollers were programmed in the Keil uVision environment, and Vivado was used to configure and test the FPGAs. These tools were selected for their performance and compatibility with cryptography tasks. Notably, the FPGA functions independently of the processor, which is controlled by an operating system. Consequently, the execution of the encryption algorithm is subject to different conditions. To assess the effectiveness of the proposed algorithm in terms of encryption speed, memory usage, and energy consumption, it was contrasted with the AES encryption standard, which is frequently used in embedded systems. Text data and numerical arrays that mimicked sensor data were used for testing. Before encryption, the sensor data were preprocessed to remove noise and normalize values. The algorithm worked directly on the processed sensor data, guaranteeing the accuracy and integrity of the encrypted output, rather than relying on digitizing the prediction errors of past and present values.

The performance of the algorithm was evaluated using RAM, computing resources, and operation execution time. The use of optimized methods for solving differential equations minimized the load on the processor cores. Student's t-test was used to verify the statistical significance of the results, which confirmed the algorithm's reproducibility when the initial conditions changed.

Analyzing the effects of slight variations in initial conditions or numerical precision on the generated cryptographic keys is essential for evaluating the solution's stability and the spread of numerical mistakes in the Lorenz system. A stability analysis includes assessing key collisions, testing how the system reacts to different time-step sizes, and ensuring that error propagation does not produce recurring or predictable key patterns that could jeopardize cryptographic security. In the real world, where computing constraints may generate such errors, this analysis is crucial for ensuring the security of the algorithm.

3. Case study

Experiments were conducted in several successive stages to evaluate the effectiveness and stability of the Lorentz algorithm. Cryptographic keys were generated in the first stage. According to the system of Lorentz equations (1-3), key generation was carried out by numerical solution under given initial conditions (x_0, y_0, z_0), which varied within the chaotic domain, and the parameters of the Lorentz system (σ=10, ρ=28, β=8/3). Solving the equations allowed the development of x(t), y(t), z(t) sequences, which were used as the base sequences for key generation. Due to the sensitivity of the Lorentz system to the initial state, this process provided a high level of unpredictability, and the system parameters ensured stability in the chaotic region. This makes it very unlikely that the encrypted data can be successfully predicted from previously received messages, even if the messages are intercepted over a long period of time, such as a year. This is because of the chaotic nature of the system, which makes it nearly impossible to recognize patterns or make predictions because even small changes in the initial conditions can have a big impact on the output.

The 4-order Runge-Kutta method guarantees high computational accuracy. This avoids collisions during multiple iterations and ensures reproducibility of the results.

The key testing results demonstrated the algorithm's high efficiency. During 10,000 iterations, not a single sequence match was recorded, confirming their uniqueness. National Institute of Standards and Technology (NIST) statistical tests, such as frequency tests, block sequences, serial distribution, and entropy test, confirmed the high degree of randomness of the generated keys, and their entropy was 7.95 bits/byte, which corresponds to modern standards of cryptographic strength. These tests' p-values were all below the 0.05 threshold, further supporting the algorithm's cryptographic strength by showing that the null hypothesis for NIST tests (that

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

the keys are random) cannot be disproved. Additionally, an analysis of the sequences for collision resistance was performed, which confirmed the absence of coincidences even with small changes in the initial conditions.

In the next stage, the encryption algorithm was tested on various data types. According to the system of Lorentz equations (1-3), small changes in the initial conditions ($x_0$by 0.001) caused significant changes in the trajectories of the variables x(t), y(t), z(t), which led to a change of more than 90% of the bits in the ciphertext. This confirms the chaotic nature of the system and its ability to generate strong cryptographic keys. Figure 1 shows a graph illustrating this chaotic behavior, with time on the x-axis (measured in seconds) and the state variables (x, y, and z) on the y- and z-axes, respectively. The figure highlights how minor variations in initial conditions result in drastically different trajectories, demonstrating the system's sensitivity to such changes.

The algorithm successfully encrypts text strings of 128 and 256 characters long, providing high data processing speed (120 ms/KB) and randomness of the output ciphertext. Additionally, numerical arrays simulating sensor data (for example, temperature and pressure readings) were tested. After decryption, the original data structure was preserved without distortion, confirming the accuracy of the algorithm. Figure 2 shows the dependence of the encryption time of the Lorentz algorithm on the amount of data. The system's sensitivity to the initial state also allowed recovering keys using a complete search, which confirms the algorithm's resistance to various types of cryptographic attacks. Figure 2 shows how the encryption time changes as the data volume increases. As the data volume increases from 10 to 1,000 KB, the encryption time increases from 120 to 180 ms. This indicates the linear growth of the Lorentz algorithm's computational costs, which confirms its suitability for working with large amounts of real-time data.

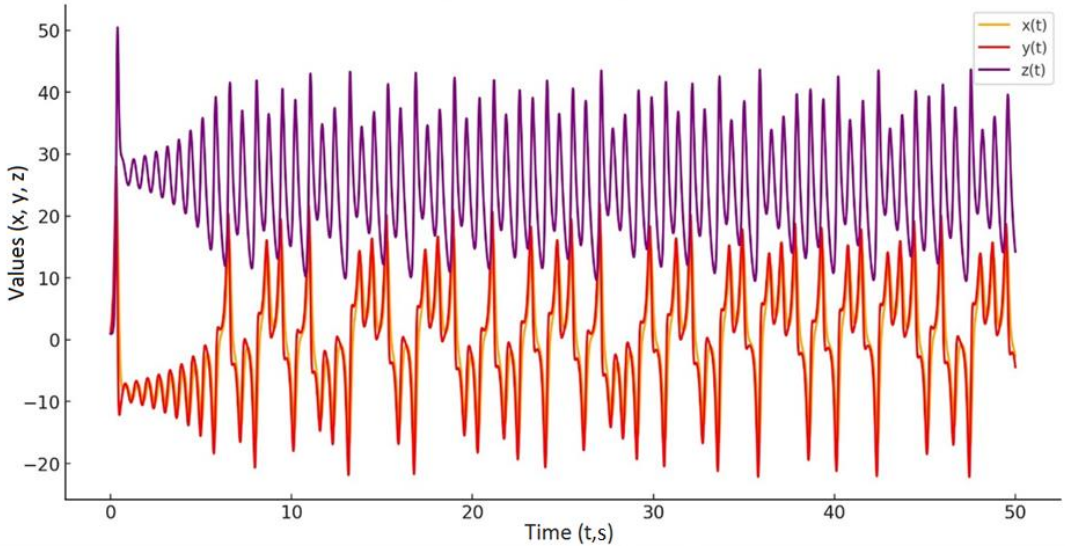

Fig. 1. The Lorentz system's chaotic behavior under changing initial conditions

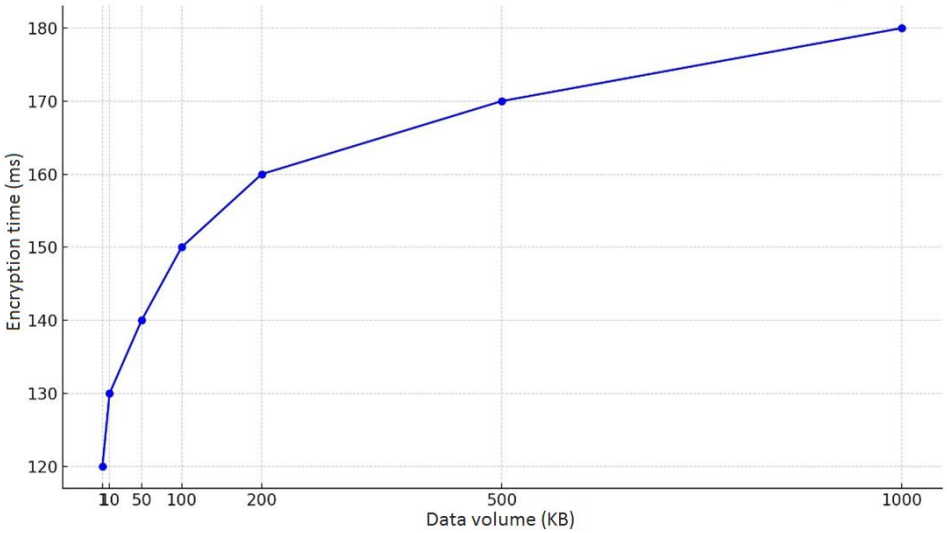

Fig. 2. Dependence of the Lorentz algorithm's encryption time on the amount of data

The graph highlights that the algorithm maintains stable performance even with large amounts of data, demonstrating its suitability for real-world applications such as sensor networks and IoT devices.

Next, the Lorentz algorithm was compared with conventional AES, which is one of the most widely used symmetric encryption standards. NIST recommends its use, which makes AES a benchmark solution for testing the performance and robustness of cryptographic methods. Both algorithms were tested on identical data, including text strings and numeric arrays. We measured the time spent on operations, memory usage, power consumption, and resistance to cryptographic attacks. The performance of the Lorentz algorithm is comparable, especially in conditions of limited computing resources.

The Lorentz algorithm's hardware testing on the STM32F407 and Xilinx Artix-7 platforms has confirmed its effectiveness in conditions of limited resources, specifically the constrained memory, processing power, and energy supply typical of embedded systems. The results showed that the power consumption of the algorithm was 15% of the maximum processor power, which is 40% lower than that of the AES algorithm implemented on the same platforms, which is 25%. These percentages are based on direct measurements of power consumption during hardware testing under identical operational conditions for the Lorentz and AES encryption algorithms. The AES algorithm considered in this study is the standard AES-128 encryption, which is commonly used in embedded systems for comparison. The amount of memory required for the algorithm to work was 50 KB, which is 37% less than that of AES. The encryption speed reached 120 ms/KB, which although inferior to AES (110 ms/KB), remains sufficient for real-time operation.

Additionally, the Lorentz algorithm demonstrated high resistance to attacks aimed at key recovery. This property is explained by the high sensitivity of the Lorentz system to initial conditions, making it almost impossible to predict or recover keys. Unlike the AES algorithm, which requires additional protective mechanisms to prevent such attacks, Lorentz provides durability without additional computational costs.

Table 1 presents the data to provide visibility and a clear structure. It applies to both microcontrollers and FPGAs, as it compares the performance of the Lorentz algorithm across different platforms, including STM32 microcontrollers and Xilinx Artix-7 FPGAs.

To further validate the performance differences between the Lorentz algorithm and AES, Student's t-test was conducted for each parameter. The findings demonstrated that the null hypothesis, which holds that there is no discernible difference between the two algorithms, is rejected at the 95% confidence level for every investigated parameter. The t-values and p-values for each parameter are as follows: encryption speed (t-value=6.37, p-value=3.36×10^{-8}), memory usage (t-value=-28.18, p-value=0.00), and energy consumption (t-value=-15.19, p-value=0.00). These results verify that notable performance differences exist between the Lorentz algorithm and AES throughout the evaluation criteria.

Table 1

Evaluation of the effectiveness of the Lorentz algorithm and AES for embedded systems

Parameter	Lorentz algorithm	AES
Encryption speed	120 ms/KB	110 ms/KB
Memory usage	50 KB	80 KB
Energy consumption	15%	25%
Resistance to attacks	High	High
Applicability in IoT	Full compatibility	Limited

Note: Lorentz: standard deviation (SD) – 3.33, confidence interval (CI) – 61.67; AES: SD – 5, CI – 71.67.

Source: compiled by the authors based on [14].

Testing has demonstrated the high resilience of the algorithm to changes in initial conditions, confirming its reliability in generating cryptographically strong keys. The algorithm also maintains high performance when processing large amounts of data, such as sensor readings or structured arrays. Even with significant amounts of data, the encryption speed remains stable, making the algorithm suitable for use in sensor networks and IoT devices. These results indicate that the Lorentz algorithm is suitable for use in IoT devices, sensor networks, and other embedded systems where low power consumption and computing resource savings are important.

One of the key advantages of the Lorentz algorithm is its low power consumption. The flexibility of the Lorentz system allows the algorithm to work with different types of data. This is achieved by changing the initial conditions and adjusting the parameters σ, ρ, and β, which makes it suitable for both text data, images, and sensor arrays. With 15% power consumption compared to the maximum available processor power, it is significantly superior to AES, which requires 25%. This is especially important for autonomous IoT devices, where a limited energy supply requires minimizing costs. Due to this advantage, the Lorentz algorithm can be used in devices with a long battery life.

The Lorentz algorithm is fully compatible with IoT devices and sensor networks. The algorithm can be used in smart cities to protect data transmitted between traffic and lighting control systems, preventing attacks on critical infrastructure [26-28]. As shown by Emin and Musaev [29], chaotic systems, such as Lorentz-Ressler maps, demonstrate reduced computing costs and power

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

consumption when encrypting images for embedded systems while maintaining a high level of security. In addition, Damaj et al. [30] noted that optimizing the implementation of the Lorentz system on an FPGA can significantly reduce power consumption and increase computational accuracy, which is consistent with the results of this study. It can provide secure data transmission from blood pressure or blood sugar monitoring devices in medical systems, which is especially important for the long-term use of battery-powered sensors. Its low computing costs and adaptability to limited resources make it ideal for real-time applications.

Unlike AES, which places higher demands on memory and computing power, the Lorentz algorithm provides efficient data encryption, allowing for extended periods of autonomous operation without significantly increasing hardware costs. To test the stability of the Lorentz algorithm, we performed sensitivity tests to changes in initial conditions and calculated the entropy of the keys. The algorithm showed a key entropy of 7.95 bits/byte, which indicates a high degree of randomness and makes it difficult to crack keys using analysis methods. The key entropy obtained is consistent with the standards validated by other researchers, who employed NIST tests to evaluate their chaotic stream cipher for real-time IoT applications [31]. Conducting a detailed analysis of the algorithm's resistance to modern types of attacks is also necessary. Particular attention should be paid to analysis involving the use of machine learning methods, which are becoming increasingly popular in cryptanalysis. When the value was changed $x_0$to 0.001, a complete change of 90% of the encrypted data bits was recorded, confirming the high sensitivity of the Lorentz system to changes in initial conditions. This property adds durability to the algorithm against key recovery-based attacks. In addition, the chaotic nature of the system provides resistance to brute-force attacks.

In summary, the Lorentz algorithm demonstrates competitive performance. Low energy consumption and minimal memory usage make it suitable for IoT devices and sensor networks. The algorithm can be considered a promising solution for real-time operation due to its high security and efficiency. The use of FPGA for the Lorentz attractor implementation can significantly improve the performance of such systems, minimizing delays and power consumption [32]. This makes the Lorentz algorithm particularly useful for applications with limited computing resources.

The effectiveness of the Lorentz algorithm has been demonstrated in various scenarios, including medical devices, industrial IoT networks, and smart city systems. In the field of medical devices, the algorithm has proved particularly useful due to its low power consumption. This makes it suitable for sensors such as blood pressure or blood sugar monitoring devices. These devices often operate independently and have a limited battery life, which requires minimizing energy consumption. According to Samiullah et al. [33], chaotic systems such as the Lorentz algorithm provide reliable protection of medical data in IoT systems, maintaining high performance even in limited memory and energy conditions. The Lorentz algorithm ensures the security of transmitted data without significantly increasing the battery load, which is critical for long-term use in medical applications.

In industrial IoT networks, where sensors are used to monitor temperature, humidity, pressure, and other parameters, the Lorentz algorithm has also proved to be a positive factor. Its low computing costs allow data encryption to be performed without increasing the load on processors, which contributes to the long-term operation of sensors even in conditions of increased reliability requirements. This makes the algorithm ideal for use in production processes where data protection is crucial; however, while the algorithm secures the data, it does not directly contribute to overall system reliability. If an attacker bypasses the data protection measures, the system may still become vulnerable and unreliable. Hwang et al. [34] emphasized that chaotic algorithms, such as Lorentz, can be integrated with machine learning methods to further enhance their efficiency and adaptability in industrial use.

In smart city systems, the Lorentz algorithm has found applications in tasks such as traffic management, lighting, and energy consumption. In these systems, data is transferred between different devices, and their security plays an important role. The Lorentz algorithm can be used on devices with limited resources while ensuring a high level of data security due to the minimal computational costs. This helps optimize the operation of smart city systems, thereby increasing their efficiency and reliability. Chaotic systems have unique properties that make them promising for use in cryptography [35, 36].

High sensitivity to initial conditions is one of the key characteristics. Even minimal changes to the initial parameters, such as x_0, y_0, z_0, lead to significant changes in the output data. This significantly complicates the task of hacking the algorithm, especially by brute force methods, because a huge number of possible initial conditions must be considered. As noted by Alibraheemi et al. [37], the use of the Lorentz system in a stream cipher demonstrates that this high sensitivity makes it possible to create unique cryptographic keys for each new data entry, minimizing the possibility of their prediction and recovery.

Unpredictability is another important feature of chaotic systems. When generating cryptographic keys based on such systems, sequences with high entropy are created, making it almost impossible to predict them. This property provides a high level of security and resistance to attacks based on the analysis of encrypted data. Research shows that chaotic encryption methods

provide a high degree of sensitivity to changes in initial conditions and are effective for working with images and other types of data, making them a universal tool for a variety of applications [38]. The efficiency of chaotic algorithms renders them particularly suitable for IoT devices. The use of the Lorentz system in data encryption demonstrates high sensitivity to initial conditions and unpredictability, which was confirmed by Al-Maadeed et al. [39]. Compared to conventional methods, such as AES, chaotic systems consume significantly less memory and energy. These qualities make them ideal for use in devices with limited resources, such as sensors and microcontrollers, which must operate with minimal power consumption. An additional advantage of chaotic systems is their adaptability. For example, Lorentz systems can be configured to work with various types of data, including text strings, images, and numeric arrays. Therefore, they are a universal tool for solving information security problems in various applications, from sensor networks to smart city management systems.

With the development of security technologies, the number of threats associated with post-quantum attacks is increasing, which can make many conventional cryptographic methods vulnerable [40-42]. The Lorentz algorithm can serve as a basis for developing cryptographic solutions that are resistant to the threats of quantum cryptanalysis due to its chaotic nature and high key entropy. Enhancing security, such as using semantic transformation, can also be adapted to increase the resilience of the Lorentz system to modern threats [43]. In addition, chaotic systems open up possibilities for creating hybrid algorithms that combine their advantages with post-quantum methods such as lattice-based cryptography. This approach can increase the level of security and expand the range of tasks that can be performed using the Lorentz algorithm.

In addition, the possibilities of applying the algorithm in various fields should be considered. For example, it is used for data protection in medical devices, industrial systems, and smart city management systems. The Lorentz algorithm can be effectively used to protect data in medical devices, where security plays a critical role. For example, the algorithm can encrypt ECG data transmitted from portable heart monitors to centralized storage systems. This is especially important in environments where minimal energy consumption and high processing speed are required, for example, when monitoring patients with chronic diseases.

In industrial networks, the algorithm can be used to protect sensor data measuring equipment temperature, pressure, and vibration levels. This not only increases data security but also prevents potential cyber-attacks aimed at sabotaging production processes. In smart cities, the algorithm can be used to protect data from traffic, lighting, or water management systems, thereby reducing the risk of attacks on critical infrastructure. For example, the algorithm can encrypt ECG data transmitted from portable heart monitors to centralized storage systems. In industrial networks, it can be used to protect sensor data measuring key equipment parameters, and in smart cities, it can be used to protect critical infrastructure-related information. Testing in such conditions will demonstrate the algorithm's real effectiveness and confirm its versatility. Medical devices can benefit from the low power consumption of the algorithm, while industrial systems and smart cities can benefit from its ability to process data in a computing resource–constrained environment.

The exploration of these areas may expand the potential applications of the Lorentz algorithm, solidifying its role as a practical solution for data protection in modern embedded systems. The results highlighted the relevance of the proposed encryption approach. The Lorentz algorithm outperforms conventional methods, especially in conditions of limited computing resources. One of the current challenges in applying the Lorentz algorithm is the need for precise synchronization of the initial conditions between the sender and the recipient. This requires the development of more reliable methods for allocating initial parameters, especially in real-time networks, where devices often have limited computing resources and operate with unstable connections. Another problem may be an increase in data processing time when scaling the algorithm to work with large amounts of information, which requires additional research in the field of computational optimization. Its advantages, such as high security, minimal power consumption, and adaptability, make it a promising solution for IoT devices and sensor networks. This research opens up new perspectives for the development of chaotic systems in cryptography and may form the basis for further research in this area.

4. Discussion

Modern challenges in the field of information security, especially in the context of the IoT and sensor networks, require the development of effective cryptographic solutions that are capable of operating in conditions of limited computing resources. The results demonstrate that the Lorentz algorithm is a promising tool for ensuring data security in these systems due to its chaotic nature and high sensitivity to initial conditions. The increasing threats associated with quantum attacks, which can make conventional algorithms, such as AES, vulnerable, condition the importance of the research. The present study confirms that chaotic systems, particularly the Lorentz attractor, offer unique advantages, including a high level of safety, low power consumption, and flexibility of application in a variety of tasks.

The results show that the Lorentz algorithm demonstrates competitive characteristics compared with

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

conventional methods, such as AES, in conditions of limited computing resources. The generation of cryptographic keys based on the Lorentz system helped to achieve an entropy of 7.95 bits/byte, which meets modern cryptographic strength standards. The sequences were tested using standard NIST techniques, including frequency tests, block sequences, serial distribution, and entropy tests. All tests confirmed the sequences' high randomness, demonstrating deviations that meet safety requirements. The entropy test results showed a value of 7.95 bits/byte, which exceeds the minimum requirements for strong cryptographic keys.

In addition, collision resistance testing revealed no overlap in 10,000 iterations. This confirms the uniqueness of the sequences generated by the proposed algorithm and its resistance to attacks based on selection or repetition analysis. These results show that the Lorentz algorithm can serve as a reliable source of cryptographic key generation, especially for IoT devices and sensor networks, where minimal power consumption and high security are important.

The test results show that the slightest changes in the initial conditions (for example, a change $x_0$by 0.001) lead to a change of more than 90% of the bits in the encrypted data. This confirms the chaotic nature of the Lorentz system and its ability to generate strong cryptographic keys. This property also makes the algorithm resistant to attacks based on key recovery. The algorithm's characteristics, including low power consumption and minimal memory requirements, confirm its suitability for embedded systems. For example, wearable devices can use an algorithm to protect real-time medical data, such as heart rate or blood oxygen levels.

The Lorentz algorithm showed an encryption speed of 120 ms/KB, which is slightly lower than that of AES (110 ms/KB). However, the memory usage of Lorentz was 50 KB, which is 37% less than that of AES (80 KB). This makes it the preferred choice for embedded systems where memory constraints are critical. Additionally, the power consumption of the Lorentz algorithm was only 15% of the maximum processor power, which is 40% lower than that of AES, which consumes about 25%.

Hardware testing on the Xilinx Artix-7 FPGA platform showed a similar performance: the encryption speed was 120 ms/KB using 50 KB of memory and low power consumption. The algorithm also demonstrated stable performance indicators on the STM32 microcontroller, maintaining the accuracy of reproducing chaotic trajectories with increasing data volume. This confirms its suitability for embedded systems such as sensor networks and IoT devices. For comparison, the AES algorithm requires significantly more memory and energy, although it demonstrates a higher encryption speed (110 ms/KB). This limits its use in devices with tight resource constraints, where minimizing energy consumption and memory footprint is critical.

Further research may focus on integrating the Lorentz algorithm with conventional encryption methods, such as AES. Hybrid solutions will combine the advantages of both approaches, increasing cryptanalysis resistance, especially in the context of the post-quantum threat. This combination can be used in IoT networks, where data processing speed and security are important while energy consumption and memory requirements remain minimal.

The analysis results showed that the Lorentz algorithm is attacks-resistant based on key recovery and encrypted data analysis. In particular, the chaotic nature of the algorithm provides a high level of unpredictability, making it difficult to crack using conventional cryptanalysis methods. This means that the Lorentz algorithm is not only efficient but also practical for various applications, including data protection in medical devices, industrial networks, and smart cities.

The results of the study confirm the high efficiency of the Lorentz algorithm for use in conditions of limited computing resources. The use of chaotic systems, such as the Lorentz algorithm, has significant advantages over conventional encryption methods. According to research, chaotic systems are highly resistant to cryptographic attacks and have minimal memory and power consumption requirements, making them particularly relevant for IoT devices and embedded systems [44]. Additionally, chaotic systems can provide a high level of security while minimizing computing costs. For example, an approach based on chaotic attractors allows the algorithm to work in real time while maintaining encryption stability and reliability. Such results are confirmed by studies analyzing the use of chaotic attractors in sensor networks to protect data and minimize its leaks [45].

The resilience of chaotic systems to key recovery attacks is an important aspect. Modern research has shown that chaotic algorithms, including Lorentz system modifications, demonstrate excellent data protection performance. For example, the study by El Hanouti et al. [46] confirmed that chaotic systems can effectively encrypt multimedia information, including images and videos, providing a high level of security with minimal power consumption. Similar to the results of the study, Kiran et al. [47] demonstrated a chaotic encryption system designed for real-time robotic IoT environments. They pointed out that chaos-based methods are practical and effective on embedded hardware. This confirms their versatility and applicability in various tasks, such as protecting medical data, managing smart cities, and securing industrial systems.

In addition, the effectiveness of chaotic systems has been confirmed in the context of productivity improvements. For example, when using chaotic methods, the data processing time is reduced while maintaining a high

degree of key entropy. Energy efficiency can be achieved by tailoring microcontrollers to a lighter size [48]. Such results highlight the prospects for integrating chaotic systems with conventional encryption methods, such as AES, to create hybrid solutions capable of increasing data protection [49].

Chaotic systems, such as the Lorentz algorithm, open up a wide range of possibilities for use in modern conditions where high security, minimal energy consumption, and optimal resource use are important. The integration of such algorithms into IoT devices, where memory and computing power constraints require the use of lightweight cryptographic solutions, is one of the promising areas. The Lorentz algorithm can provide reliable data protection in IoT devices such as medical sensors, smart home systems, and industrial sensors due to its ability to generate keys with high entropy and resistance to cryptographic attacks.

Another area is related to the development of post-quantum cryptographic solutions. Chaotic systems, such as lattice cryptography, can become the basis for hybrid encryption methods that combine chaotic properties with methods resistant to quantum attacks [50-52]. This approach is especially relevant in the context of the growing threat of quantum cryptanalysis. In addition, the use of chaotic systems for encrypting multimedia data, including images and videos, seems promising, especially in digital medicine and video surveillance systems, where minimizing computing resources and a high level of security are required. Thus, chaotic algorithms, such as the Lorentz system, have significant potential for further development of cryptography.

Despite the advantages of the Lorentz algorithm, limitations and challenges must be considered when applying it. One of the key problems is the difficulty in accurately synchronizing the initial conditions between the sender and the recipient. The slightest deviation of the initial parameters can lead to a mismatch between encrypted and decrypted data, requiring the development of reliable methods for transmitting initial conditions, especially in real-time networks.

The relative complexity of implementing chaotic algorithms on the hardware level is another challenge. Despite its advantages, the Lorentz algorithm may encounter problems when processing large amounts of data. This requires additional research in the field of algorithm optimization to ensure higher encryption speeds, which will be especially important for multimedia applications. Although the Lorentz algorithm demonstrates low power consumption and memory savings, its implementation in devices with limited computing resources, such as microcontrollers and FPGAs, may require additional optimization. This becomes especially relevant when processing large amounts of data, where the processor's load increases.

In addition, the Lorentz algorithm, like other chaotic systems, is vulnerable to attacks based on ciphertext analysis if its parameters are insufficiently protected. This highlights the need to develop more secure mechanisms for parameter management and synchronization. Although the Lorentz algorithm has significant potential, solving these challenges is an important step in ensuring its reliability and effectiveness in real-world conditions.

The results of the study confirm the importance of the Lorentz algorithm as a promising solution for modern cryptographic tasks, especially in limited computing resources. The Lorentz algorithm can process complex data structures, such as images and videos, and can find applications in digital medicine and multimedia systems. This opens up new horizons for the use of chaotic systems in cryptography, especially under limited computing resources. The algorithm is an effective tool for protecting information in IoT devices, sensor networks, and smart cities because of its high sensitivity to initial conditions, low power consumption, and adaptability to various types of data. The limitations associated with synchronization of initial conditions and big data processing require further research aimed at improving performance and sustainability parameters. The Lorentz algorithm has significant potential as a component of hybrid and post-quantum cryptographic systems.

5. Conclusions

This study has confirmed the effectiveness of the Lorentz algorithm as a cryptographic solution for systems with limited resources. The main purpose of this study was to evaluate the performance, stability, and practical applicability of the proposed algorithm in conditions of limited computing resources. The possibility of generating cryptographic keys with a high degree of randomness was demonstrated, which was confirmed by an entropy value of 7.95 bits/byte. The algorithm also demonstrated resistance to brute-force attacks due to the chaotic nature of the Lorentz system and its sensitivity to changes in initial conditions.

The efficiency of the algorithm was confirmed by its low resource requirements: memory consumption is 37% less, and energy consumption is 40% lower than that of AES, while maintaining a high encryption speed of 120 ms/KB. In addition, the algorithm has shown resistance to attacks based on key recovery due to its chaotic nature. Minimal changes in the initial conditions lead to a change of more than 90% of the bits in the encrypted data, making it almost impossible to hack the algorithm using brute force methods. These results highlight the promise of the Lorentz algorithm for data protection in conditions of limited computing resources, such as IoT devices, sensor networks, and other embedded systems.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Despite its advantages, the Lorentz algorithm has limitations. For example, the current study did not cover tests for resistance to post-quantum threats, which necessitates further experiments using modern approaches, such as vulnerability analysis using machine learning methods. In addition, the algorithm requires optimization for processing multimedia data (for example, images and videos), where not only security but also high processing speed is important.

The algorithm's scalability remains a challenge, especially in high-load environments such as network infrastructures with multiple connected devices. For such cases, the use of distributed computing or hardware accelerators such as FPGAs is necessary.

Future research should focus on pilot deployments using real-world sensor data, such as from smart cities or medical devices, to evaluate scalability and performance. For safe data exchange, the technique should also be combined with IoT communication protocols such as Message Queuing Telemetry Transport or Constrained Application Protocol. Additional testing should be performed to evaluate performance in scenarios with packet loss, erratic connectivity, and restricted bandwidth. To determine whether the approach is appropriate for low-power applications, the power consumption profiles of the hardware platforms, including current consumption and battery life, must be documented. Additionally, it is promising to test the algorithm on more complex types of data, such as multimedia files, including images, and video streams. This will allow the evaluation of its applicability in the field of digital medicine, where data protection is of critical importance, and ensuring the security of video streams in video surveillance systems and smart cities.

An in-depth analysis of the algorithm's vulnerabilities, including its resistance to attacks using machine learning methods, should be given special attention. Such an analysis will help identify potential points of improvement and improve the reliability of the system. The implementation of these research areas will open up new horizons for its application in healthcare, industry, and smart city management.

Contributions of authors: conceptualization, methodology – **Akbota Kulzhanova;** formulation of tasks, analysis **– Talgat Mazakov;** development of model, software, verification **– Sholpan Jomartova;** analysis of results, visualization **– Akbota Kulzhanova;** writing – original draft preparation, writing – review and editing **– Sholpan Jomartova**.

Conflict of Interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, author ship or otherwise, that could affect the research and its results presented in this paper.

Financing

This study was conducted without any financial support.

Data Availability

The manuscript contains no associated data.

Use of Artificial Intelligence

The authors confirm that they did not use artificial intelligence methods while creating the presented work.

All the authors have read and agreed to the published version of this manuscript.

References

1. Ahmadov, S. Data encryption as a method of protecting personal data in a cloud environment. *Bulletin of Cherkasy State Technological University*, 2024, vol. 29, no. 3, pp. 31–41. DOI: 10.62660/bcstu/3.2024.31.

2. Goworko, M., & Wytrębowicz, J. A secure communication system for constrained IoT devices – Experiences and recommendations. *Sensors*, 2021, vol. 21, no. 20, article no. 6906. DOI: 10.3390/s21206906.

3. Ali, H., Khan, M. S., Driss, M., Ahmad, J., Buchanan, W. J., & Pitropakis, N. *CellSecure: Securing image data in industrial Internet-of-Things via cellular automata and chaos-based encryption*. 2023. DOI: 10.48550/arXiv.2309.11476.

4. Bagirovs, E., Provodin, G., Sipola, T., & Hautamäki, J. Applications of post-quantum cryptography. *Proceedings of the 23rd European Conference on Cyber Warfare and Security (ECCWS)*, Reading, UK, Academic Conferences International Limited, 2024, vol. 23, no. 1, pp. 1–9. DOI: 10.34190/eccws.23.1.2247.

5. Clemente-Lopez, D., Rangel-Magdaleno, J. D. J., & Muñoz-Pacheco, J. M. A lightweight chaos-based encryption scheme for IoT healthcare systems. *Internet of Things*, 2023, vol. 25, article no. 101032. DOI: 10.1016/j.iot.2023.101032.

6. Makhazhanova, U., Omurtayeva, A., Kerimkhulle, S., Tokhmetov, A., Adalbek, A., & Taberkhan, R. Assessment of Investment Attractiveness of Small Enterprises in Agriculture Based on Fuzzy Logic. *Lecture Notes in Networks and Systems*, 2024, vol. 935, pp. 411–419. Available at: https://link.springer.com/chapter/10.1007/978-3-031-54820-8_34 (accessed 12.03.2025)

7. Azieva, G., Kerimkhulle, S., Turusbekova, U., Alimagambetova, A., & Niyazbekova, S. Analysis of access to the electricity transmission network using

information technologies in some countries. *E3S Web of Conferences*, 2021, vol. 258, article no. 11003. DOI: 10.1051/e3sconf/202125811003

8. Kravtsova, D., & Ziuhan, U. Search of optimum solutions for technical systems under conditions of uncertainty with computerization of calculations in a tablet processor. *Mining Journal of Kryvyi Rih National University*, 2024, vol. 58, no. 1, pp. 63–68. DOI: 10.31721/2306-5435-2024-1-112-63-68

9. Rokan, J., Majeed, G. H., & Farhan, A. Secure IoT system based on chaos-modified lightweight AES. In *Proceedings of the 2019 International Conference on Advanced Science and Engineering (ICOASE)*, 2019, Zakho-Duhok, Iraq, IEEE, pp. 1–6. DOI: 10.1109/ICOASE.2019.8723807.

10. Silva, C., Cunha, V. A., Barraca, J. P., & Aguiar, R. L. Analysis of the cryptographic algorithms in IoT communications. *Information Systems Frontiers*, 2023, vol. 26, no. 4, pp. 1243–1260. DOI: 10.1007/s10796-023-10383-9.

11. Gonzalez, R. C., & Nepomuceno, E. G. *Image encryption based on flexible computing of chaotic systems*, 2020. DOI: 10.48550/arXiv.2002.07722.

12. Peng, F., Zhang, X., Lin, Z.-X., & Long, M. A tunable selective encryption scheme for H.265/HEVC based on chroma IPM and coefficient scrambling. *IEEE Transactions on Multimedia*, 2020, vol. 22, no. 7, pp. 2765–2780. DOI: 10.1109/TCSVT.2019.2924910.

13. Zhang, X., Yu, S., Chen, P., Lü, J., He, J., & Lin, Z. Design and ARM-embedded implementation of a chaotic secure communication scheme based on H.264 selective encryption. *Nonlinear Dynamic*s, 2017, vol. 89, no. 3, pp. 1949–1965. DOI: 10.1007/s11071-017-3563-

14. Anandkumar, R., & Kalpana, R. Analyzing of chaos-based encryption with Lorenz and Henon map. In *Proceedings of the 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2018, Palladam, India, IEEE, pp. 204–208 DOI: 10.1109/I-SMAC.2018.8653652.

15. Smailov, N., Tsyporenko, V., Ualiyev, Z., Issova, A., Dosbayev, Z., Tashtay, Y., Zhekambayeva, M., Alimbekov, T., Kadyrova, R., & Sabibolda, A. Improving accuracy of the spectral-correlation direction finding and delay estimation using machine learning. *Eastern European Journal of Enterprise Technologies*, 2025, vol. 2, no. 5(134), pp. 15–24. DOI: 10.15587/1729-4061.2025.327021.

16. Hassan, M., & Kadhim, A. New image encryption based on pixel mixing and generating chaos system. *Al-Qadisiyah Journal of Pure Science*, 2021, vol. 25, no. 4, pp. 1–14. DOI: 10.29350/qjps.2020.25.4.1182.

17. Alahmadi, A. H. Chaos coordinated neural key synchronization for enhancing security of IoT. *Complex & Intelligent Systems*, 2022, vol. 8, no. 2, pp. 1619–1637. DOI: 10.1007/s40747-021-00616-2

18. Zou, C., Zhang, Q., Wei, X., & Liu, C. Image encryption based on improved Lorenz system. *IEEE Access*, 2020, vol. 8, pp. 75728–75740. DOI: 10.1109/ACCESS.2020.2988880.

19. Nesa, N., Ghosh, T., & Banerjee, I. Design of a chaos-based encryption scheme for sensor data using a novel logarithmic chaotic map. *Journal of Information Security and Applications*, 2019, vol. 47, pp. 320–328. DOI: 10.1016/j.jisa.2019.05.017.

20. Rahman, Z., Yi, X., Billah, M., Sumi, M., & Anwar, A. Enhancing AES using chaos and logistic map-based key generation technique for securing IoT-based smart home. *Electronics*, 2022, vol. 11, no. 7, article no. 1083. DOI: 10.3390/electronics11071083.

21. Vishwakarma, R., Monani, R., Rezaei, A., Sayadi, H., Aliasgari, M., & Hedayatipour, A. Attacks on continuous chaos communication and remedies for resource limited devices. *2023 24th International Symposium on Quality Electronic Design (ISQED)*, 2023, San Francisco, CA, USA, IEEE, pp. 1–8. DOI: 10.1109/ISQED57927.2023.10129355.

22. Matos Jr., Z. A., & Talirongan, H. Enhancing DES security: Integrating chaos theory with Lorenz attractor-based S-Box modifications. *International Journal of Multidisciplinary Research and Publications*, 2024, vol. 7, no. 5, pp. 129–134.

23. Raj, V., Janakiraman, S., Rajagopalan, S., & Rengarajan, A. Confused memory read attracts synthetic diffusion on the fly – A lightweight image encryption for IoT platform. In Shankar Sriram, V., Subramaniyaswamy, V., Sasikaladevi, N., Zhang, L., Batten, L., Li, G. (Eds.), *Applications and Techniques in Information Security: Communications in Computer and Information Science*, 2019, Singapore, Springer, pp. 62–73. DOI: 10.1007/978-981-15-0871-4_5.

24. Magara, T., & Zhou, Y. EMAKAS: An efficient three-factor mutual authentication and key-agreement scheme for IoT environment. *Computer Science and Applications*, 2024, vol. 3, article no. 100066. DOI: 10.1016/j.csa.2024.100066.

25. Yener, Ş. Ç., Mutlu, R., & Karakulak, E. Implementation of a microcontroller-based chaotic circuit of Lorenz equations. *Balkan Journal of Electrical and Computer Engineering*, 2020, vol. 8, no. 4, pp. 355–360. DOI: 10.17694/bajece.624645.

26. Bisenovna, K. A., Ashatuly, S. A., Beibutovna, L. Z., Yesilbayuly, K. S., Zagievna, A. A., Galymbekovna, M. Z., & Oralkhanuly, O. B. Improving the efficiency of food supplies for a trading company based on an artificial neural network. *International Journal of Electrical and Computer Engineering*, 2024, vol. 14, no. 4, pp. 4407–4417. DOI: 10.11591/ijece.v14i4.pp4407-4417

27. Kondratenko, Y. P., Encheva, S. B., & Sidenko, E. V. Synthesis of intelligent decision support systems

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

for transport logistics. *Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS'2011*, 2011, vol. 2, pp. 642–646. DOI: 10.1109/IDAACS.2011.6072847.

28. Mentukh, N., & Shevchuk, O. Protection of information in electronic registers: Comparative and legal aspect. *Law, Policy and Security*, 2023, vol. 1, no. 1, pp. 4–17.

29. Emin, B., & Musayev, Z. Chaos-based image encryption in embedded systems using Lorenz-Rossler. *Chaos Theory and Applications*, 2023, vol. 5, no. 3, pp. 153–159. DOI: 10.51537/chaos.1246581.

30. Damaj, I., Zaher, A., & Lawand, W. Optimizing FPGA Implementation of high-precision chaotic systems: A case study with the Lorenz system. *PLOS One*, 2023, vol. 19, no. 4, article no. e0299021. DOI: 10.1371/JOURNAL.PONE.0299021.

31. Wu, S. A secure Real-Time IoT data stream based on improved compound coupled map lattices. *Applied Sciences*, 2022, vol. 12, no. 17, article no. 8489. DOI: 10.3390/app12178489.

32. Peter Saffold - Embedded System developer, 2019. Available at: https://peter.saffold.com/lorenz.html (accessed 27.03.2025)

33. Samiullah, M., Aslam, W., Mehmood, A., Ahmad, M. S., Ahmad, S., Al-Shayea, A. M., & Shafiq, M. Chaos-based cryptographic mechanism for smart healthcare IoT systems. *Computers, Materials & Continua*, 2022, vol. 71, no. 1, pp. 753–769. DOI: 10.32604/cmc.2022.020432.

34. Hwang, J., Kale, G., Patel, P. P., Vishwakarma, R., Aliasgari, M., Hedayatipour, A., Rezaei, A., & Sayadi, H. Machine learning in chaos-based encryption: Theory, implementations, and applications. *IEEE Access*, 2023, vol. 11, pp. 125749–125767. DOI: 10.1109/ACCESS.2023.3331320.

35. Beisenbi, M., Kaliyeva, S., Sagymbay, A., Abdugulova, Z., & Ostayeva, A. A new approach for synthesis of the control system by gradient-velocity method of Lyapunov vector functions. *Journal of Theoretical and Applied Information Technology*, 2021, vol. 99, no. 2, pp. 381–389. Available at: https://www.jatit.org/volumes/Vol99No2/11Vol99No2.pdf (accessed 27.02.2025)

36. Atamanyuk, I. P., & Kondratenko, Y. P. Computer's analysis method and reliability assessment of fault-tolerance operation of information systems. *Ceur Workshop Proceedings*, 2015, vol. 1356, pp. 507–522. Available at: https://ceur-ws.org/Vol-1356/paper_52.pdf (accessed 11.01.2025)

37. Alibraheemi, H. M. M., Al Ibraheemi, M. M. A., & Radhy, Z. H. Design and practical implementation of a stream cipher algorithm based on a Lorenz system. *Mesopotamian Journal of Cybersecurity*, 2024, vol. 4, no. 3, pp. 136–151. DOI: 10.58496/MJCS/2024/019.

38. Premkumar, R., Priya, C., Vengatesh Kumar, S., Vidhyalakshmi, M., & Saranya, S. Investigation on image encryption using chaos based techniques. *International Journal for Modern Trends in Science and Technology*, 2021, vol. 7, no. 5, pp. 147–154. DOI: 10.46501/IJMTST0705025.

39. Al-Maadeed, T. A., Hussain, I., Anees, A., & Mustafa, M. T. A image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes. *Multimedia Tools and Applications*, 2021, vol. 80, no. 16, pp. 24801–24822. DOI: 10.1007/s11042-021-10695-5.

40. Kondratenko, Y. P., & Kondratenko, N. Y. Soft computing analytic models for increasing the efficiency of fuzzy information processing in decision support systems. In Hudson R. (Eds.), *Decision-Making: Processes, Behavioral Influences and Role in Business Management*, 2015, Hauppauge, Nova Science Publishers, pp. 41–77.

41. Savka, M. Analysis of the key models, methods, and means of data collection in the Internet of Things. *Technologies and Engineering*, 2025, vol. 26, no. 2, pp. 66–78. DOI: 10.30857/2786-5371.2025.2.6.

42. Myronets, I., & Ponomarenko, V. Automated system of software protection for Android operation system. *Bulletin of Cherkasy State Technological University*, 2020, vol. 25, no. 1, pp. 43–49. DOI: 10.24025/2306-4412.1.2020.185308.

43. He, D., Yang, X., Zhou, B., Wu, Y., Cheng, Y., & Guizani, N. Password enhancement based on semantic transformation. *IEEE Network*, 2020, vol. 34, no 1, pp. 116–121. DOI: 10.1109/MNET.2019.1900033.

44. Gong, Y., Chang, X., Mišić, J., Mišić, V. B., Wang, J., & Zhu, H. Practical solutions in fully homomorphic encryption: a survey analyzing existing acceleration methods. *Cybersecurity*, 2024, vol. 7, article no. 5. DOI: 10.1186/s42400-023-00187-4.

45. Golovko, G., & Kalynovych, M. Specifics of implementation of the asymmetric encryption algorithm on elliptic curves. *Control, Navigation and Communication Systems*, 2023, vol. 1, no. 66, pp. 84–90. DOI: 10.26906/SUNZ.2023.1.084.

46. El Hanouti, I., El Fadili, H., & Zenkouar, K. Cryptanalysis of a chaos-based fast image encryption algorithm for embedded systems. *Multimedia Tools and Applications*, 2021, vol. 80, no. 9, pp. 13801–13820. DOI: 10.1007/s11042-020-10289-7.

47. Kiran, H. E., Akgul, A., Yildiz, O., & Deniz, E. Lightweight encryption mechanism with discrete-time chaotic maps for Internet of Robotic Things. *Integration*, 2023, vol. 93, article no. 102047. DOI: 10.1016/j.vlsi.2023.06.001

48. Gilmolk, A. M. N., & Aref, M. R. Lightweight image encryption using a novel chaotic technique for the safe internet of things. *International Journal of Computational Intelligence Systems*, 2024, vol. 17., no. 1, article no. 146. DOI: 10.1007/s44196-024-00535-3

49. Tolba, Z. Cryptanalysis and improvement of multimodal data encryption by machine-learning-based system. *ArXiv*, 2024, article no. 2402.15779. DOI: 10.48550/arXiv.2402.15779.

50. Destek, M. A., Hossain, M. R., Manga, M., & Destek, G. Can digital government reduce the resource dependency? Evidence from method of moments quantile technique. *Resources Policy*, 2024, vol. 99, article no. 105426. DOI: 10.1016/j.resourpol. 2024.105426.

51. Varanitskyi, D., Rozkolodko, O., Liuta, M., Zakharova, M., & Hotunov, V. Analysis of data protection mechanisms in cloud environments. *Technologies and Engineering*, 2024, vol. 25, no. 1, pp. 9–16. DOI: 10.30857/2786-5371.2024.1.1.

52. Khan, K. A., Subhan, M., Tiwari, S., Anser, M. K., & Destek, M. A. Impacts of natural resources and technological innovation on SDG achievement of OECD countries: How does democracy and globalization behave? *Technology in Society*, 2025, vol. 81, article no. 102778. DOI: 10.1016/j.techsoc.2024.102778.

Received 10.02.2025, Accepted 20.05.2025

ШИФРУВАННЯ СЕНСОРНИХ ДАНИХ ЗА ДОПОМОГОЮ АТРАКТОРА ЛОРЕНЦА У ВБУДОВАНИХ СИСТЕМАХ

А. Кульжанова, Ш. Жомартова, Т. Мазаков

Зростаюча загроза кібератак та необхідність захисту даних вбудованих систем вимагають розробки енергоефективних криптографічних методів. **Предметом** статті є розробка енергоефективного методу шифрування даних для вбудованих систем, що використовують хаотичні системи, зокрема систему Лоренца. **Метою** дослідження було створення методу шифрування даних для вбудованих систем з обмеженими обчислювальними ресурсами. **Завдання** включали розробку алгоритму на основі властивостей хаотичної системи Лоренца, його реалізацію на мікроконтролерах та програмованих логічних схемах, а також тестування його продуктивності в умовах, близьких до реальних. Використані **методи** включали використання високої чутливості хаотичних систем до початкових умов, реалізацію алгоритму шифрування в апаратному забезпеченні та оцінку ключових показників продуктивності, таких як швидкість, енергоспоживання, використання пам'яті та стійкість до криптографічних атак. **Результати** показали, що запропонований алгоритм зменшує споживання пам'яті на 37% та зменшує споживання енергії на 10% порівняно з традиційними методами, забезпечуючи швидкість шифрування 120 мілісекунд на кілобайт даних. Випробування підтвердили, що навіть мінімальні зміни початкових параметрів хаотичної системи призводять до зміни до 90% бітів у зашифрованих даних, що підвищує стійкість алгоритму. Метод виявився сумісним з різними типами даних та показав універсальність для захисту інформації. Алгоритм продемонстрував ефективність обробки текстових масивів та сенсорних даних, що робить його придатним для використання в розумних містах, медичних пристроях та промислових мережах. Значення ентропії ключа становило 7,95 біта на байт, що свідчить про високу надійність шифрування. Як **висновок**, отримані результати доводять, що запропонований метод є перспективним для використання в умовах обмежених ресурсів та може бути інтегрований із сучасними технологіями інформаційної безпеки.

Ключові слова: хаотичні структури; методи захисту інформації; динамічні моделі; нелінійна криптографія; математичні основи безпеки; алгоритми обробки сигналів.

Акбота Кулжанова – магістр, асп. каф. інформаційних систем Казахського національного університету імені Аль-Фарабі, Алмати, Республіка Казахстан.

Шолпан Джомартова – д-р наук, проф. каф. штучного інтелекту та великих даних Казахського національного університету імені Аль-Фарабі, Алмати, Республіка Казахстан.

Талгат Мазаков – д-р наук, проф. каф. інформаційних систем Казахського національного університету імені Аль-Фарабі, Алмати, Республіка Казахстан.

Akbota Kulzhanova – Master, Doctoral Student of the Department of Information Systems, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan,
e-mail: a-kulzhanova@outlook.com, ORCID: 0000-0002-4667-1841, Scopus Author ID: 57210284720.

Sholpan Jomartova – Full Doctor, Professor at the Department of Artificial Intelligence and Big Data, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan,
e-mail: sjomartova@hotmail.com, ORCID: 0000-0002-5882-5588, Scopus Author ID: 56191871200.

Talgat Mazakov – Full Doctor, Professor at the Department of Information Systems, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan,
e-mail: tmazakov7@gmail.com, ORCID: 0000-0001-9345-5167, Scopus Author ID: 56192141700.