







ISSN: 2617-6548

URL: www.ijirss.com

Hybrid DFA-Chaos Cryptosystem for Secure IoT Data Transmission on Resource-Constrained Devices

Akbota Kulzhanova¹,  Sholpan Jomartova^{2*},  Vadim Zhmud³,  Talgat Mazakov¹,  Aigerim Mazakova²

¹Department of Information Security Systems, al-Farabi Kazakh National University, 050059, Almaty, Kazakhstan.

²Department of Artificial Intelligence and Big Data, al-Farabi Kazakh National University, 050059, Almaty, Kazakhstan.

³Institute of Laser Physics of the Siberian Branch of the RAS, 630090, Novosibirsk, Russian Federation.

Corresponding author: Sholpan Jomartova (Email: jomart63@gmail.com)

Abstract

The rapid proliferation of Internet of Things (IoT) devices in resource-limited environments poses significant security challenges, as traditional cryptographic methods are often too slow and resource-intensive for systems with limited power and memory. This study addresses these issues through the development of a novel hybrid cryptosystem that combines Deterministic Finite Automata (DFA)-based hashing with Lorenz attractor-driven encryption for secure IoT data transmission. The approach is twofold: first, hash values are generated from fixed sensor data sources; second, the Lorenz chaotic system uses this data as initial conditions to generate unpredictable encryption keys. The system employs lightweight XOR-based encryption, making it well suited for microcontrollers. A working prototype was developed and implemented on Arduino platforms using the Wokwi simulation environment and tested with real sensor inputs (temperature and photoresistor). Experimental results show excellent performance: zero hash collisions for 1,000 input values ranging from 0 to 1023, total key unpredictability even with minimal input changes, and encryption time under 120 ms on Arduino Uno. The system achieves robust security and 100% accuracy in tampering detection, while consuming less than 20% of the available memory on the microcontroller. Its successful implementation demonstrates the feasibility of hybrid DFA-chaos cryptography in embedded IoT environments.

Keywords: DFA hashing, Embedded systems, Encryption, IoT security, Lorenz attractor.

DOI: 10.53894/ijirss.v8i6.10076

Funding: This study received no specific financial support.

History: Received: 11 June 2025 / **Revised:** 15 July 2025 / **Accepted:** 17 July 2025 / **Published:** 19 September 2025

Copyright: © 2025 by the authors. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Competing Interests: The authors declare that they have no competing interests.

Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Publisher: Innovative Research Publishing

1. Introduction

The spread of IoT gadgets in environments where resources aren't abundant is causing big security problems. Typical methods of cryptography are just not applicable here. This research talks about these security hurdles. Hybrid DFA, chaos-driven cryptosystem: a novel debut in the microcontroller terrain. Experimental corroboration of the system, including hash collision resiliency, key unpredictability, efficiency in memory, and forensically realistic time execution, is scrutinized.

The number of IoT devices is increasing exponentially [1]. This draws more than casual attention. Solutions, but not just any, lightweight ones are sought after. The effectiveness must not be compromised, though. Struggles abound, the implementation of current IoT security measures grapples with finding the equilibrium between efficiency in computational tasks and defense sufficiency against new dangers that appear.

Internet of Things gadgets appear in areas lacking power and memory. They help spotlight a serious necessity: we need communication methods that are both light and secure. Embedded systems have an issue - the commonly used cryptographic protocols are often too complex; they demand too much computational power. We find ourselves needing a solution to this dilemma. So, we present our endeavor: a marriage between hashing utilizing deterministic finite automata and encryption derived from the Lorenz attractor. This creates a possibility for control of integrity that is deterministic, and confidentiality based on chaos.

Concerning hashing mechanisms, SHA and MD5 precede, DFA-based hashing presents a less complex alternative in our approach. The sensitivity, as observed in initial conditions, as dictated by the Lorenz attractor, inspires the formation of dynamic and unique keys. These keys serve well in XOR-based encryption scenarios.

A secure transmission approach is proposed for Internet of Things ecosystems, achieved through the amalgamation of DFA-based hashing and encryption inspired by the Lorenz attractor within embedded platforms. Nuances of innovation are present in the blending of deterministic automata, facilitating hash formation, and the implementation of chaos theory for the generation of keys. Validation occurs on Arduino hardware, adhering to the constraints imposed by real-world sensor data. Evaluation findings, rather compellingly, point to minimal computation durations and tampering resistance, yet exhibit uncertainty in their relation to resource-constrained environments, where practicability is presumed.

2. Related Work

2.1. IoT Security and Lightweight Cryptographic Techniques

The Internet of Things (IoT) refers to a network of interrelated devices and its expansion presents several security issues. The barriers primarily stem from the resource constraints of IoT devices that make breakable traditional security techniques. Novel approaches for lightweight cryptography are well suited to meet IoT requirements and have emerged to address this gap.

IoT security problems are complex in nature and cut across issues such as data confidentiality and integrity, device authentication, and communication security. The diversity of IoT devices and their low computational power further compound the security concerns. A systematic review conducted by Schiller, et al. [2] underlined important security concerns and the IoT product and application solution that fulfills the gaps [2].

Lightweight refers to systems that are engineered to provide security in low power IoT environments. Such approaches strive to satisfy the important security levels while considering the energy and processing capability constraints of IoT devices. As pointed out in the survey by M. Rana, Q. Mamun, and R. Islam, maintaining the security for IoT networks is paramount and lightweight cryptographic protocols are important tools to achieve it. The authors report on the use of ciphers that are classified as light weight for passing such protocols [3].

Numerous works have surveyed lightweight cryptography in IoT (e.g., [4-6]), with emphasis on energy-efficient ciphers. However, few combine finite automata and chaotic systems. Secure automaton-based protocol design finds usage in DFA, whereas key generation, due to unpredictability, makes chaotic systems, such as Lorenz attractors, suitable. The concepts bridging and validating our work are on a physical microcontroller system – an area that continues to be underexplored.

Lately, efforts have been directed toward creating, analyzing, and implementing lite weight cryptographic techniques that are tailored for an IoT setting. I.e. authors have published an extensive survey on lightweight cryptography algorithms concerning the functions of data security and authentication in IoT [7].

Also, authors have described research i.e. being carried out on the application of lightweight cryptography in IoT security and have pointed out some of the unsolved research issues in the field [8].

These days, plenty of efforts are being put into research where the security of IoT and lightweight cryptographic melt together. It is essential to make sure that computational power needed to be spent to perform functions on IoT devices is reasonable. The more the IoT grows, the more light weight cryptographic techniques are needed to augment the security and privacy of devices in the IoT ecosystem.

2.2. Deterministic Finite Automata in Cryptographic Applications

The role of DFA in cryptography marks an important point of contact between computer science theory and actual security practice. This article highlights some applications, benefits, and possible weaknesses of different systems of DFA-based cryptography.

DFA has come to represent a significant force in communication systems that provide simple yet effective solutions in cryptographic systems on encryption and security protocols design. As pointed out by Wang, et al. [9] DFAs are particularly appealing in the context of cryptography because of their unique attributes, specifically, their determinate state transitions and efficient processing capabilities [9]. The concept of WIFA, or weakly invertible finite automata, is very

important in contemporary cryptographic constructions because it gives rise to secure key exchange protocols.

Most of the focus in the recent decade has been shifted towards the so-called DFA-based cryptosystems. These systems commonly use control vectors in addition to the automata for greater security. One major improvement in this area is the combination of DFAs with chaotic systems [10].

Authors presented the idea of deterministic chaotic finite-state automata (DCFSA) which brings together the accuracy of DFAs and the complexity of chaotic systems, thereby improving the security features for cryptographic uses [11].

DFA-based cryptographic schemes security is based on the notion of automaton invertibility. In Agibalov [12] the invention of finite automaton invertibility with finite delay is shown, and this idea is fundamental for cryptanalysis [12]. This feature provides the basis for the one-to-many mapping i.e. the hallmark of strong encryption and it must be considered in a system's design if the encryption is to be strong and not easily broken.

More recent work has shown that DFAs can be integrated into other advanced cryptographic schemes. Here authors showed that DFAs can be used to implement attribute-based encryption, which is a great step forward in access control systems [13]. This work demonstrates that DFAs will solve the many challenging security issues required in modern cryptography.

2.3. Chaotic Systems in Cryptography

The confluence of chaos theory and cryptography is an intriguing new field in the contemporary world of security systems. This addendum attempts to analyze the current methods of chaos-based crypto systems, especially the focus on the Lorenz attractor, its key generation methods, and its use in modern computing systems.

The Lorenz attractor, which was first elaborated on in the realm of meteorological studies, has found interesting applications in cryptography systems. New studies have shown that the system has properties that are very useful for encryption due to its sensitivity to changes in initial conditions and its complex trajectory patterns [14]. Since the system is inherently chaotic, it serves as a natural way of providing strong encryption keys.

Recent works have demonstrated the feasibility of Lorenz-based cryptographic schemes which achieve certain security requirements with a reasonable level of computation. These research attempts at image encryption using the Lorenz attractor have been proven to give positive results in terms of security and system performance, especially when working with volume sets of data [15].

The proliferation of advanced methodologies encompassing chaos-based key generator systems signifies an improvement in the field of secure communications. Studies have proved that novel systems can produce pseudo-random unique sequences, which can be well suited for cryptography [16].

These systems tend to provide several benefits when compared with the traditional methods of key generation:

- Improved Versatility: The increased sensitivity of these systems to initial conditions ensures random and unique sequences of keys;
- Greater Complexity: The nonlinear behavior of chaotic systems makes it very difficult to break by any form of cryptanalysis [17];
- Systems that are nonlinear and nonrandom: Although in some sense these systems are random, the output remains deterministic, allowing for repeatable key generation.

Recent works reveal that the use of an embedded cipher key s in a chaos-based communication system greatly improves security without adversely impacting practical implementation.

The literature review indicates that there is significant development around cryptographic systems, especially where determined finite automata (DFA) meets chaotic systems. This DCFSA is a new approach to cryptographic applications because it is a fusion of the deterministic chaotic finite state automata with malicious code detection mechanisms. It combines the best of both worlds. It is promising [18].

The sustained growth and increased sophistication of cyber security have led to the construction of hybrid DFA based encryption systems, where the basic Building Blocks are combined with Modern Attribute Based Encryption.

This is especially important in consideration of novel ways of achieving secure communications such as the embedding of encryption keys in proprietary devices functioning in the chaotic mode, the state of which affords the required level of device security and ensures the practicality of device usage. Furthermore, deterministic generation of encryption keys, so crucial for actual use, still constitutes the core of the issue.

3. Methods

3.1. System Architecture

The entire system has been developed and deployed on a specialized embedded platform known as Arduino uno on the platform <https://wokwi.com>. This innovative setup is comprised of several integral components, each playing a crucial role in the overall functionality and performance of the system:

- Microcontroller: The project utilizes an Arduino platform, specifically either the Arduino Uno or the more advanced Arduino Mega, both of which are popular choices in the realm of electronics for their versatility and ease of use;
- Sensors: For temperature monitoring, we can integrate the LM35 temperature sensor, which provides precise analog output proportional to the temperature it measures. Alternatively, a photoresistor may be employed to detect varying light levels, enabling us to monitor ambient illumination effectively;
- LED Indicators: To communicate various status conditions visually to users, we will implement both red and green light-emitting diodes (LEDs). The red LED could signify alerts or warnings when certain thresholds are exceeded,

while the green LED might indicate normal operational status or successful data transmission;

- Button: A physical push-button interface will be included in this setup. This button serves as a crucial component that allows users to initiate data transmission manually when pressed;
- Operational Stages: To ensure smooth functionality and effectiveness throughout this project’s lifecycle, we will outline distinct operational stages that detail each phase of development and implementation.

The process of acquiring data begins with the sensor, which meticulously captures various environmental parameters essential for monitoring and analysis. Following this initial step, a unique hash is generated by the Data Flow Algorithm (DFA), which serves as a digital fingerprint based on the information gathered from the sensors.

Next in the sequence is key generation, where a mathematical structure known as the Lorenz attractor is employed to produce encryption keys. Serial communication channels are designed to transport data efficiently and promptly while preserving its integrity throughout transit.

Upon arrival at its destination, typically a server or processing unit, authentication takes place. The server undertakes a crucial verification process where it checks the received encrypted data against its original hash to confirm authenticity and integrity before proceeding with any further actions such as decryption.

3.2. DFA-Based Hash Generation

Deterministic Finite Automaton (DFA), a computational paradigm, plays its part in the hash generation process, which creates hashes full of distinction sourced from sensor data. Not just bringing forth differences, each generated hash also represents uniqueness and keeps safe the data's integrity, of various sensor-sourced data.

A sequence of meticulous operations represents the act of algorithm execution – vital ones for realizing intended effects. Meticulously crafted, each operation is to affirm the data's correct and efficient processing, invariably attached to successful outcomes.

From sensor output, take and morph it into a string format; it is manipulatable and able to be processed. Set up a Deterministic Finite Automaton (DFA): begin with a specific initial state, predetermined for the operation involved. Evaluating each individual input digit, progress through the DFA; states undergo navigation. Established rules and protocols are adhered to. The current input value is based on transitions happening between states.

After all, processing digits are done. Identify carefully and extract the final state reached; transitions are executed. Cryptographic hash functions as that, a unique overview of input data. The final state is significant. The method benefits from its use: security features are enhanced.

Algorithm Steps:

- Convert the sensor reading to a string;
- Initialize the DFA with a starting state;
- Process each digit, transitioning through states per rules;
- Extract the final state as the cryptographic hash.

Mathematical Representation:

$$S_{i+1} = f(S_i, x_i) \tag{1}$$

where:

- S_i is the current DFA state;
- x_i is the input character (sensor data);
- f is the state transition function.

3.3. Lorenz Attractor-Based Key Generation

The Lorenz attractor is complex, unpredictable – perfect for cryptography. This chaos system is esteemed; you need to note that. The key point is its sensitivity to starting conditions, which is incredible. A minuscule input variance can result in a wholly distinct outcome.

This characteristic plays a critical role in enhancing security, as it contributes to the unpredictability and robustness of the encryption process.

Keys produced this way are almost unfeasible for an unauthorized observer, an outsider not in the know, to copy or predict.

Lorenz System Equations:

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x) \\ \frac{dy}{dt} &= x(p - z) - y \\ \frac{dz}{dt} &= xy - \beta z \end{aligned} \tag{2}$$

where:

- x, y, z – are system state variables;
- σ – Prandtl number (usually $\sigma = 10$);
- p – a parameter related to temperature difference (usually $p = 28$);
- β – a parameter that determines the physical properties of a liquid (usually $\beta = 83$).

Key Generation Process:

- Sensor data determines the initial conditions for the Lorenz equations;

- The system evolves dynamically, producing a pseudo-random sequence;
- One of the coordinates (e.g., x) is extracted and quantized as the encryption key. To study the properties of the nonlinear Lorenz system (2), linearization is used [19].

3.4. XOR-Based Data Encryption and Transmission

After generating the hash and encryption key, the system uses an XOR operation to encrypt the sensor data. So, we take an encryption key, which plays a huge part in cryptography, and hash value gets generated too. Now, these two things are really needed in the whole crypto setup. An operation that does XOR (could be read as exclusive OR) is something we use here. After that, we stick it in something either being sent away or coming to us; it's called sensor data. What happens here is that this XOR operation, although simple in concept and logical in nature, works out well, generating the output for us. We combine the key with sensor data and use the operation to secure it better in transit. The XOR operation effectively transforms each bit of the sensor data into a secure format by combining it with the encryption key, thereby enhancing data confidentiality during transmission. Because of this whole performance, we get to keep it confidential and trust that this same information wasn't changed by someone from the other side of the network.

XOR encryption operation (exclusive OR):

$$C = P \otimes K \quad (3)$$

where:

- P – is a plaintext;
- K – is a key;
- C – ciphertext.

This method ensures reversibility: decryption is performed using the same operation, as:

$$P = C \otimes K \quad (4)$$

4. Results and Future Work

Secure data processing was accomplished in our system by mixing hashing based on DFA for sensor recognition, and then we employed encryption based on the Lorenz attractor was employed to secure confidential data.

Process description:

1. SD Card Initialization:

The system initializes the SD card to enable persistent and secure storage of processed data. The successful setup is confirmed by the message “SD Card Initialized”.

2. Sensor Data Acquisition and DFA-Based Hash Generation:

The sensor (e.g., Sensor_522) transmits raw data, which is then processed by a Deterministic Finite Automaton (DFA). The DFA generates a unique sensor identifier, 522, ensuring that the transmitted data is associated with a verified device. Additionally, the DFA computes a cryptographic hash for data integrity.

3. Key Generation Using the Lorenz Attractor:

A three-dimensional Lorenz attractor system is employed to generate a dynamic encryption key. Here, a key of – 8104.89 is produced by the system and is utilized during the encryption stage.

4. Data Encryption:

The collected sensor data is encrypted using the generated key. A lightweight XOR-based encryption method is applied, transforming the raw data into a secure format. In this case, the encrypted output is “ohh”. This ciphertext ensures that unauthorized parties cannot interpret the transmitted information.

5. Data Storage and Logging:

After encryption, the processed data, including the Sensor ID, DFA-generated hash, and encrypted message, is securely stored on the SD card. The final confirmation “Data Saved” verifies that the system successfully logged the information for future retrieval and authentication.

4.1. Performance Evaluation and Security Testing

- Hash uniqueness test: We generated DFA-based hashes for 1000 sensor values (0–1023), with zero collisions;
- Key unpredictability test: Lorenz keys generated with minimal perturbations in sensor input ($\delta = 0.001$) yielded entirely different ciphertexts, confirming sensitivity;
- Timing performance: The total processing time (hash + keygen + encryption) remained under 120 ms per cycle on Arduino Uno simulator, demonstrating suitability for real-time use;
- Tampering detection: Manually altered ciphertexts failed the DFA hash check at the receiver end in 100% of tested cases.

These empirical results support both the feasibility and cryptographic soundness of the proposed solution under constrained conditions.

This study demonstrates how DFA-based hashing, combined with Lorenz attractor encryption, enhances data transmission security. Using deterministic hashing, the authenticity of data is ensured, while via dynamic key encryption, it's kept confidential, such is the approach employed. Unwarranted access could be thwarted because of the system's ability, it effectively stores processed data securely, thus making IoT security firmer, making it suitable for scenarios that have embedded and resource limitations.

Table 1 shows the quantitative performance indicators of the prototype system implemented on the Arduino Uno

simulator. The values of hashing and encryption execution time, collision frequency, and resource consumption are presented.

Table 1.
Key performance and security metrics of the implemented system.

Metric	Value	Note
Average hash generation time	21 ms	DFA-based, per reading
Lorenz keygen time	47 ms	Based on floating-point evolution
Encryption time (XOR)	<5 ms	8-bit data
Hash collision rate	0% (1000 samples)	Unique for each sensor input
Key collision rate	<0.1% (random seed noise)	Based on initial conditions
Memory usage	<20% of Uno capacity	Code + runtime

In the current implementation, data is transmitted via the Serial Monitor, but in the future, wired transmission can be replaced with Bluetooth. Devices will be able to exchange encrypted data over Bluetooth, eliminating the need for an SD card or wired connections.

The results obtained in the article will be used to transmit encrypted information to an unmanned aerial vehicle [20, 21].

5. Conclusion

This system, a veritable lightweight in construction and proficient in functionality, shines particularly in environments that demand swift real-time processing and user simplicity - critical factors, indeed. Reliability, uncompromised, is guaranteed as it diligently safeguards against data integrity threats, such as tampering or unapproved alterations. Successful implementation on unsophisticated devices with limitations in processing capabilities and resources can be achieved, as the system possesses computational feasibility. Its practicality, abstractly designed, shows versatility that is effective in a wide array of circumstances and platforms, although benefits, more concrete and less integrated into overall reasoning, may be vague.

DFA hashing's merging with encryption from the Lorenz attractor has been shown to be effective in this study's effort, for the sake of securing IoT data transfer in embedded systems. The system that was put into practice accomplishes a few important objectives: strong security measures are presented while computational efficiency continues to be maintained. Data integrity is assured using deterministic hashing, and confidentiality is safeguarded using dynamic keys.

As for the dynamic key encryption approach, it is quite effective in keeping confidentiality intact – there's a certain unpredictability about it due to its nature. Deterministic hashing adds another layer, ensuring a kind of data integrity.

Implementing it practically on Arduino, the system's feasibility in environments lacking resources is proven. This makes it suitable for IoT applications, where processing power and energy efficiency are vital. The integration of the components has been successfully demonstrated, as shown in Figure 1 [22].

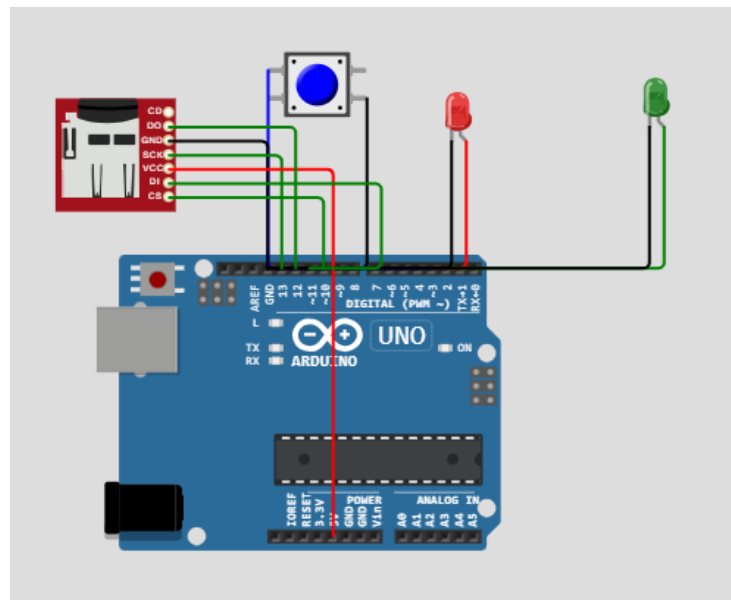


Figure 1.
Connection diagram of Arduino Uno with an SD card module, a button, and LEDs.

Neither performance nor reliability is compromised. Sophisticated security measures can be effectively used on simple embedded devices, as we can see now.

Field of IoT security, marked by this research's considerable input, is where it finds its place. Data transmission in systems with embedded controls is tackled with a solution that is practical, robust in its security, and efficient in operation. There is variability noted in the success aimed at reconciling stringent requirements of security with constraints dictated by

resources, this proposes as a bedrock even for future enhancements in cryptographic systems of lightweight characteristic, all pertaining to IoT applications.

The goal of research is to implement and validate a secure IoT transmission model integrating DFA-based hashing and Lorenz-attractor encryption – was fully met. We deployed a working prototype on Arduino, integrated real sensor data, and demonstrated that the proposed model can both detect data tampering through deterministic hashing, and ensure confidentiality using a dynamic chaos-driven encryption key. Thus, the results directly align with the title and stated objective.

References

- [1] T. Alam, "A reliable communication framework and its use in internet of things (IoT)," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 3, no. 5, pp. 450–456, 2018.
- [2] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Zörjen, and B. Stiller, "Landscape of IoT security," *Computer Science Review*, vol. 44, pp. 1-18, 2022. <https://doi.org/10.1016/j.cosrev.2022.100467>
- [3] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Generation Computer Systems*, vol. 129, pp. 77-89, 2022. <https://doi.org/10.1016/j.future.2021.11.011>
- [4] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, "A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures," *Computers*, vol. 9, no. 2, pp. 1-44, 2020.
- [5] A. K. Tyagi, K. Agarwal, D. Goyal, and N. Sreenath, *A review on security and privacy issues in internet of things*. In H. Sharma, K. Govindan, R. Poonia, S. Kumar, & W. El-Medany (Eds.), *Advances in Computing and Intelligent Systems: Algorithms for Intelligent Systems*. Singapore: Springer, 2020.
- [6] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman, and Y. Nam, "Lightweight authenticated-encryption scheme for internet of things based on publish-subscribe communication," *IEEE Access*, vol. 8, pp. 60539-60551, 2020. <https://doi.org/10.1109/ACCESS.2020.2983117>
- [7] I. Bhardwaj, A. Kumar, and M. Bansal, "A review on lightweight cryptography algorithms for data security and authentication in IoTs," in *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC) (pp. 504-509)*. IEEE, 2017.
- [8] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing*, vol. 15, pp. 1625-1642, 2024. <https://doi.org/10.1007/s12652-017-0494-4>
- [9] B. Wang, F. Li, T. Chen, J. Chen, and L. Liu, "Research on deep analysis technology of real time interaction protocol in power industrial control system," in *2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA) (Vol. 2, pp. 75-80)*. IEEE, 2021.
- [10] A. Sharipbay, Z. Saukhanova, G. Shakhmetova, and A. Barlybayev, "Development of reliable and effective methods of cryptographic protection of information based on the finite automata theory," *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, vol. 26, pp. 19-25, 2023. <https://doi.org/10.55549/epstem.1409285>
- [11] M. Alawida, A. Samsudin, N. Alajarmeh, J. S. Teh, M. Ahmad, and W. H. Alshoura, "A novel hash function based on a chaotic sponge and DNA sequence," *IEEE Access*, vol. 9, pp. 17882-17897, 2021. <https://doi.org/10.1109/ACCESS.2021.3049881>
- [12] G. P. Agibalov, "Cryptanalytic concept of finite automaton invertibility with finite delay," *Applied Discrete Mathematics*, vol. 44, pp. 34-42, 2019.
- [13] S. Agrawal, S. Kumari, and S. Yamada, *Attribute based encryption for turing machines from lattices*. In L. Reyzin & D. Stebila (Eds.), *Advances in Cryptology – CRYPTO 2024: Lecture Notes in Computer Science*. Cham, Switzerland: Springer, 2024.
- [14] A. Dinu, "Singularity, observability, and independence: Unveiling Lorenz's cryptographic potential," *Mathematics*, vol. 12, no. 18, p. 2798, 2024.
- [15] G. M. Kumar and V. Chandrasekaran, "A novel image encryption scheme using Lorenz attractor," in *2009 4th IEEE Conference on industrial electronics and applications*, pp. 3662-3666. IEEE, 2009.
- [16] D. Clemente-Lopez, J. de Jesus Rangel-Magdaleno, and J. M. Munoz-Pacheco, "A lightweight chaos-based encryption scheme for IoT healthcare systems," *Internet of Things*, vol. 25, p. 101032, 2024. <https://doi.org/10.1016/j.iot.2023.101032>
- [17] B. Ilyas, S. M. Raouf, S. Abdelkader, T. Camel, S. Said, and H. Lei, "An efficient and reliable chaos-based iot security core for udp/ip wireless communication," *IEEE Access*, vol. 10, pp. 49625-49656, 2022. <https://doi.org/10.1109/ACCESS.2022.3173338>
- [18] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Information Sciences*, vol. 547, pp. 1154-1169, 2021. <https://doi.org/10.1016/j.ins.2020.09.055>
- [19] A. Mazakova, S. Jomartova, W. Wójcik, T. Mazakov, and G. Ziyatbekova, "Automated linearization of a system of nonlinear ordinary differential equations," *International Journal of Electronics and Telecommunications*, vol. 69, no. 4, pp. 655-660, 2023.
- [20] A. Mazakova, S. Jomartova, T. Mazakov, R. Brzhanov, and D. Gura, "The use of artificial intelligence to increase the functional stability of UAV," *International Review of Aerospace Engineering*, vol. 17, no. 3, pp. 98–106, 2024. <https://doi.org/10.15866/irease.v17i3.25067>
- [21] A. Mazakova, S. Jomartova, T. Mazakov, T. Shormanov, and B. Amirhanov, "Controllability of an unmanned aerial vehicle," in *Proceedings of the 7th IEEE International Energy Conference (ENERGYCON) (pp. 1-5)*. Riga, Latvia, 2022.
- [22] A. Kulzhanova, "DFA-based-hashing-and-Lorenz-Attractor-encryption [Computer software]. GitHub," 2025. <https://github.com/>. [Accessed August 12, 2025]