ТЕХНИЧЕСКИЕ НАУКИ
И ТЕХНОЛОГИИ

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
INFORMATION TECHNOLOGY

DOI 10.51885/1561-4212_2023_4_427
IRSTI 81.93.29

G.B. Shakhmetova[1], A.A. Sharipbay[2], Zh.S. Saukhanova[3], A.B. Barlybayev[4]
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
[1]*E-mail: shakhmetova.gb@gmail.com**
[2]*E-mail: sharlt@mail.ru*
[3]*E-mail: saukhanova@mail.ru*
[4]*E-mail: frank-ab@mail.ru*

STUDY OF FINITE AUTOMATES USED IN CRYPTOGRAPHY

КРИПТОГРАФИЯДА ҚОЛДАНЫЛАТЫН АҚЫРЛЫ АВТОМАТТАРДЫ ЗЕРТТЕУ

ИССЛЕДОВАНИЕ КОНЕЧНЫХ АВТОМАТОВ, ПРИМЕНЯЕМЫХ В КРИПТОГРАФИИ

Аңдатпа. *Мақалада соңғы автоматтарға негізделген криптографиялық жүйелерге шолу берілген. Шетелдік басылымдардағы отандық ғалымдардың ақырлы автоматтық криптография бойынша теориялық материалдары зерттелді. Ақырлы автоматтар модельдерінің әртүрлі типтерінің жұмысын жақсырақ түсіну үшін негізгі ұғымдарға анықтамалар берілді: ақырлы автомат – танушы, ақырлы автомат – түрлендіргіш, кідіріспен қайтымдылық, кері автомат, ақырлы автоматтардың ауыстырылуы және құрамы. Әрі қарай мақалада шығусыз автоматтарға негізделген криптографиялық алгоритмдер сипатталды, олардың артықшылықтары мен кемшіліктері атап өтілді. Соңында шығуы бар автоматқа негізделген соңғы автоматтар модельдері туралы ақпарат беріледі. Классикалық криптографияның қолданыстағы алгоритмдерінен соңғы автомат моделінің артықшылықтары ашылды. Зерттеу криптографиялық алгоритмдердің негізі ретінде ақырлы автоматтарды пайдалану перспективалары туралы қорытынды жасауға мүмкіндік береді.*

Түйін сөздер: *криптография; шығысы бар ақырлы автомат; шығыссыз ақырлы автомат; ақырлы автоматтың қайтымдылығы; ақырлы автоматтардың құрамы.*

Abstract. *The article provides an overview of cryptographic systems based on finite automata. Theoretical materials of domestic scientists in foreign publications on finite-automaton cryptography have been studied. For a better understanding of the operation of various types of finite automata models, definitions of the main concepts were given: finite automaton – recognizer, finite automaton - converter, reversibility with a delay, inverse automaton, permutation and composition of finite automata. Further in the article, cryptographic algorithms based on automata without an exit were described, their advantages and disadvantages were noted. At the end, information is given about finite automata models, which are based on an automaton with an exit. The advantages of the finite automaton model over the existing algorithms of classical cryptography are revealed. The study allows us to make a conclusion about the prospects of using finite automata as the basis for cryptographic algorithms.*

Keywords: *cryptography; finite automaton with output; finite automaton without output; reversibility of a finite automaton; composition of finite automata.*

Аннотация. *В статье приведен обзор криптографических систем, в основе которых лежат конечные автоматы. Исследованы теоретические материалы отечественных ученных в зарубежных изданий по конечно-автоматной криптографии. Для лучшего понимания работы различных видов конечно-автоматных моделей были приведены определения основных понятий: конечный автомат – распознаватель, конечный автомат –*

преобразователь, обратимость с задержкой, обратный автомат, перестановочный и композиция конечных автоматов. Далее в статье были описаны криптографические алгоритмы, основанные на автоматах без выхода, отмечены их преимущества и недостатки. В конце приведена информация о конечно-автоматных моделях, в основе которых лежит автомат с выходом. Выявлены преимущества конечно-автоматной модели над существующими алгоритмами классической криптографии. Исследование позволяет сделать заключение о перспективности использования конечных автоматов в качестве основы для криптографических алгоритмов.

Ключевые слова: *криптография; конечный автомат с выходом; конечный автомат без выхода; обратимость конечного автомата; композиция конечных автоматов.*

Introduction. Digital communication can involve three categories of participants: *sender*, *recipient and attacker – a black hat hacker*. To ensure the security of communication, it is necessary to convert an original message into a presentation form that is incomprehensible to an attacker. This can be achieved through cryptography – the science of models and methods of encryption to ensure confidentiality, integrity, and authentication.

Currently, there are various mathematical (formal) models and computational methods of cryptography that are used to ensure the security (reliability) of information exchange.

In the context of cryptography, the original message represented in a human-readable form is called *"plaintext"* while the transformed message in an incomprehensible form is referred to as *"ciphertext"*. The methods used for the process of transformation are called *"encryption and decryption"* methods, which can be called as cryptographic methods [1]. Cryptographic techniques encompass a variety of approaches, including symmetric, asymmetric (or public-key) encryption, and more. These methods are represented through theoretical-numerical models, logarithmic signatures, elliptic curves, and a range of algorithms like 3DES, CAST5, AES, RC4, Serpent, Twofish, Blowfish, IDEA, RSA, PGP, DH, FKE, Elgamal, and homomorphic encryption (HE), among others [2].

The main goal of cryptographic methods is to ensure confidentiality, integrity, authentication, authorization, availability, non-repudiation, and access control [3] when transmitting data over an insecure channel.

As known from [4], many classical cryptographic methods are based on mathematical models such as number theory, bilinear theory, and logarithmic concepts. Implementing such methods can be costly due to the use of a large number of computational resources. For this reason, many researchers are interested in improving existing cryptographic algorithms or creating radically new formal models. As an alternative model for constructing efficient and reliable cryptographic methods, the theory of finite automata is proposed, since finite automata are characterized by the simplicity of their software and hardware implementation, proven by the production of central processors of modern computers. Using various models of finite automata, such as Mile/Moore automata, Robin-Scott model, Glushkov automata, cellular automata and others, alternative methods for creating various cryptosystems have been developed.

This article provides an overview of scientific research on the use of various models of finite automata in the creation of several reliable cryptosystems.

Basic concepts of automata theory. The theory of finite automata is an important area of the theory of formal languages and computing. This theory studies computational models called *finite automata (FA)*, which are abstract devices with limited memory and discrete states. Finite automata, in turn, are divided into two classes: *automata without output* and *automata with output*. FA without output, or automata – recognizer, is a mathematical model that recognizes an incoming sequence of symbols. An abstract discrete device that transforms an incoming sequence of signals into an output sequence of signals is called an FA with output, or an

automata – transducer. These types of automata are widely used in cryptographic systems for modeling and implementing various protocols and algorithms. They can be used for data encryption and decryption, key management, integrity checking, and other cryptographic operations.

Consider the formal definition of a FA. The simplest automaton is an algebraic structure of the form [5]:

$$A = < X, Q, \delta >, \quad (1)$$

where:

$X = \{x_1, x_2, \dots, x_n\}$ – non-empty and finite set of input signal;

$Q = \{q_1, q_2, \dots, q_k\}$ – non-empty and finite set of states;

δ: $Q \times X \to Q$ – transition function.

If an initial state and a set of final states are added to the algebraic structure (1), then the simplest automaton will become a *recognizer automaton* or an *automaton without output with finite memory* and will have the following form:

$$A =< X, q_0, Q, Q_F, \delta >, \quad (2)$$

where:

$q_0 \in Q$ – initial state;

$Q_F \subseteq Q$ – set of final states.

It should be noted that the initial state q_0 can be simultaneously the final state.

Similarly, if a non–empty and finite set of the output alphabet and an output function are added to the structure (2), then *automata without output with finite memory* will become *an automata – transducer* or an *automaton with output and finite memory* and will have the following form:

$$A =< X, Y, q_0, Q, Q_F, \delta, \lambda >, \quad (3)$$

where:

Y – non-empty and finite set of output signal;

λ: $Q \times X \to Y$– output function.

Automata without output, as well as automaton with output, are classified into deterministic (DFA) and non-deterministic FA (NFA).

In DFA, each combination of the current state and the input symbol defines a single next transition and state. This means that for each state and input symbol, there is only one next state. A deterministic automaton does not allow ambiguity in determining the next state. An example of DFA is the Robin-Scott model.

Unlike a deterministic finite automata, a nondeterministic automata can have multiple possible next states for each state and input symbol. This means that upon receiving a specific input symbol in the current state, the automaton can transition to one of several states or even remain in the current state.

If system (1) is extended with the output alphabet $Y = \{y_1, y_2, \dots, y_m\}$ and, as a consequence, with the output function λ: $Q \times X \to Y$, then the simplest automaton will become *an automata- transducers* or *an automata with output* and will have the following form: $A =< X, Y, Q, \delta, \lambda >$.

Automata- transducers include Mealy/Moore automata [6]:

Mili Machine: $\begin{cases} q(t+1) = \delta(q(t), x(t)) \\ y(t) = \lambda(q(t), x(t)) \end{cases}$, t=0,1,2,…

Moore Machine: $\begin{cases} q(t+1) = \delta(q(t), x(t)) \\ y(t) = \lambda(q(t)) \end{cases}$, t=0,1,2,…

The main property that influenced the application of FA in cryptographic algorithms is the invertibility of finite automata with a finite delay τ. The study of invertibility of FA with output was initiated by the cryptologist Renji Tao in the early 1980s, who is considered the founder of Finite Automata Cryptography (FAC). FAC is the integration of finite automata with the concept of cryptography, and this concept was introduced in the work [7]. R. Tao proved that automata with output possess the invertibility property and demonstrated the possibility of constructing inverse automata [8].

A finite automata - transducer is called an invertible FA with a finite delay τ, if, having an output sequence and an initial state, it is possible to restore the input sequence with a delay τ. In other words [9]:

The finite automata - transducer $A = < X, Y, Q, \delta, \lambda >$ is *invertible with delay* τ, or τ - *invertible*, where $\tau \in N_0$, if $\forall q \in Q, \forall x, x' \in X, \forall \alpha, \alpha' \in X^{\tau}$, $\lambda(q, x\alpha) = \lambda(q, x'\alpha')$. It follows that $x = x'$. In another formulation, we can say that for $\forall\ q \in Q, x \in X$, и $\forall\ \alpha \in X^{\tau}$, x can be uniquely determined using the state q and the output function $\lambda(q, x\alpha)$.

For finite automata without output to be *invertible*, it is necessary and sufficient that its transition table be *permutable*. This means that each row of the transition table must contain a different state. This important property ensures that the ciphertext is unambiguous. For security, it is also assumed that all columns of the transition table form a permutation of the state set [7].

Automaton $A = < X, Q, \delta >$ is a *permutation or Glushkov automaton*, when for each pair $b \in Q, x \in X$, there is only one $a \in Q$ such that $\delta(a, x) = b$ [5].

The main idea behind the applicability of FA in cryptography is that invertible finite automata act as encoders for plaintext, while their inverses FA as decoders for ciphertext. Definitions for inverse finite automata with output and without output are:

Automaton - transducer A′ is called *inverse with delay τ* to automaton A, if $\forall q \in Q\ \exists\ q' \in$ Q′ such that (q′, q) is a τ-pair in A′×A.

For $\forall q \in Q$ and $\forall q' \in Q'$, if $\forall a \in X^{\omega}, \exists a_0 \in X^k$: $\lambda'\big(q', \lambda(q, a)\big) = a_0 a$ и $|\alpha 0| = \tau$, then (q', q) it is called a *pair with a delay of* τ (*τ-pair*) or in other words, q' corresponds to q with delay τ [18].

Automaton – recognizer $A^{-1} = < X, Q, \delta^{-1} >$, with transition function $\delta^{-1}(b, x) = a$, where $a, b \in Q, x \in X$ is called *inverse* to the automaton $A = < X, Q, \delta >$ if and only if $\delta(a, x) = b$.

Then, for $\forall a, b \in Q\ (a \neq b)$ and for $\forall x \in X^*$ the equality $A^{-1}\big(A(x)\big) = x$ holds [9].

It should be noted that in finite automata cryptography, the concept of *composition of finite automata* with output is encountered. Let's consider its definition:

Let two automata be given $A_1 =< X_1, Y_1, Q_1, \delta_1, \lambda_1 >$ and $A_2 =< X_2, Y_2, Q_2, \delta_2, \lambda_2 >$, where *X2 = Y1*. Then *the composition* of two automata is defined as:

$$C(A_1, A) =< X_1, Y_2, Q_1 \times Q_2, \delta, \lambda >,$$

where,

$$\delta(< q_1, q_2 >, x) =< \delta_1(q_1, x), \delta_2\big(q_2, \lambda_1(q_1, x)\big) >, \lambda(< q_1, q_2 >, x) = \lambda_2\big(q_2, \lambda_1(q_1, x)\big),$$

$$x \in X_1, q_1 \in Q_1, q_2 \in Q_2.$$

Finite automata without output in cryptography. The aforementioned FA without output had found their application in cryptography. Various cryptographic systems have been built based on them (Fig. 1).

The initiator of the application of finite automata - recognizer in cryptographic systems was

the scientist R. Dömösi [7]. In 2008, he proposed a new stream ciphering method based on the mathematical model of Robin-Scott. However, this cryptographic system was compromised in 2010 by cryptologists Z. Kovács and A. Pénzes. The cryptoanalysis of the Dömösi system, where an automaton equivalent to the key automaton of the cryptographic system was broken. After extensive work on improving the compromised cryptographic system, in 2015 R. Dömösi and G. Horváth implemented a new block cipher, where keys were the Glushkov automata product (permutation automaton). In 2016, Khaleel G. et al described proposed modifications to the Dömösi cryptographic system in their works [11].

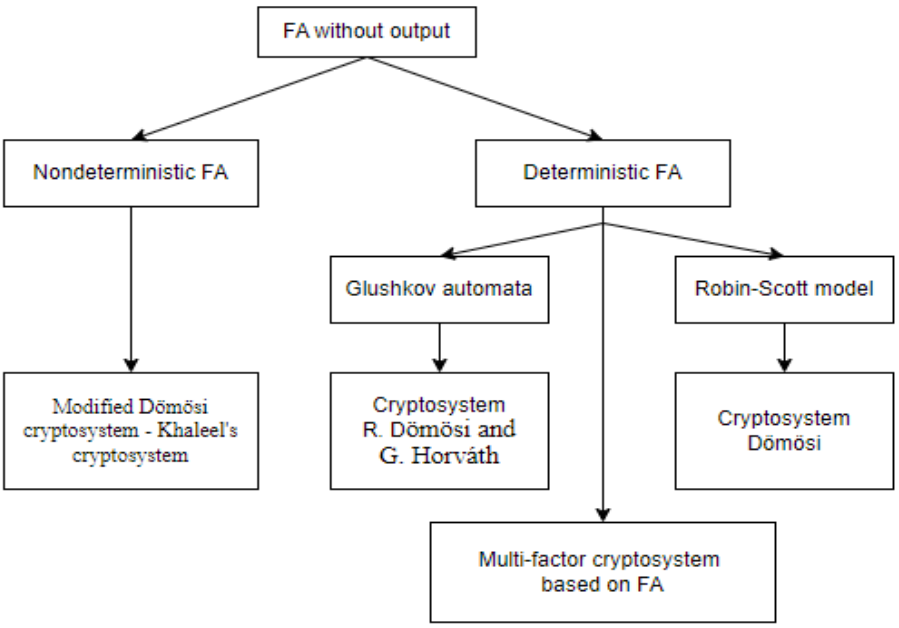

Figure 1. Cryptosystems based on FA without output

Interest in Finite Automata Cryptography (FAC) continues to evolve, as evidenced by the proposed multi-factor cryptographic system using a recognizer automaton in [10].

In the symmetric cryptographic system proposed by Dömösi, the FA without output serves as the key that is used to encrypt the plaintext and decrypt the ciphertext. The essence of the operation is as follows: each element of the set of plaintext symbols is assigned one or several final states of the key automata, and each final state is assigned to one and only one element of the set of symbols. During the encryption process, the key automata read the plaintext symbol by symbol, starting from the initial state. Each text symbol is assigned a character string within a specified range. The encrypted text is the concatenation of these character strings. During the decryption process, the key automaton starts from the initial state and reads the encrypted text symbol by symbol. During decryption, the input signals associated with the corresponding final states are combined, leading to the restoration of the original message in its initial form [11].

The symmetric streaming cryptosystem Dömösi has a number of advantages: a key-independent random number generator, weak reversibility of automata that does not affect the cryptosystem, a set of keys containing more than 256! randomly generated automata - keys. But, unfortunately, it has a drawback - the ciphertext is many times longer than the plaintext [5].

As mentioned earlier, after the compromise of the Dömösi cryptosystem, a new block cipher based on Glushkov automata was proposed by Dömösi P and Horváth G. A. In the proposed

cryptosystem, the same key automata and the same pseudorandom number generator act as both the encoder and decoder. The cryptosystem consists of two main blocks: the pseudorandom number generator block (PNGB) and the set of permutation automata block (SPAB). To obtain the plaintext from the ciphertext, the same PNGB must be used, and it should be kept secret and secure. Modern block ciphers ensure that encrypting the same plaintext results in distinct ciphertexts. This is achieved by altering the initial value of the PNGB during each encryption operation. Specifically, the PNGB generates two blocks: one remains constant and confidential, serving as a part of the key (known as the main vector), while the other block changes with each encryption, becoming the first block of the ciphertext (referred to as the initialization vector). The final initial value can be calculated as a function of these two blocks. The encoding process relies on an encryption function designed to bolster the security of the cryptographic system. This function takes three parameters into account: the plaintext block and two pseudorandom blocks. Through multiple rounds of this function, the encrypted text is produced. The decoding process employs the same function but with different parameters: the ciphertext block and two pseudorandom blocks [12].

The block cipher system under discussion boasts high-speed encryption and decryption capabilities. Performance testing has revealed that it can achieve encoding speeds exceeding 7 megabytes per second. Furthermore, the system demonstrates an ideal avalanche effect. Additionally, a notable advantage of this system is that the number of possible key automata is equal to 256!65536. This provides a significantly strong defense against brute force attacks.

The identified drawbacks of the Dömösi stream cipher system prompted researchers G. Khaleel and Turaev Sh. to modify the system and propose an enhanced cryptographic algorithm, known as Modified Dömösi cryptosystem. In the suggested approach, an additional control mechanism is employed to prevent rollback within the encryption algorithm. This control system generates two vectors by considering the current state, input symbols, and final states. The control system comprises two phases: initialization and utilization. Thanks to this alteration, which effectively mitigates inverse search challenges, the encrypted text is generated in linear time relative to the maximum length of the encrypted text blocks. Importantly, this modified cryptosystem maintains an equivalent level of security against attacks as the original Dömösi cryptosystem [11].

A notable advantage of the modified Dömösi cryptosystem is that the use of NFA introduces non-determinism to the system. This, in turn, allows the system to avoid the reversibility of a FA. As a result, a cryptosystem based on NFA cannot be compromised using reversibility.

It is worth noting that finite automata can be applied as a component in any cryptographic system. For example, in the paper [10], it is demonstrated how the RSA cryptosystem can be improved by adding a recognizer automata. The essence of the proposed multi-factor cryptosystem with an automata is as follows: the message Recipient generates key pairs and then sends a list of public keys (r) to the Sender, where the value of r ranges from 50 to 100 or 1000. The Sender selects the public key from the list r, then sets the input alphabet Σ, determines the formal language L over the alphabet Σ and builds a FA without output - M, which recognizes the specified language L. Next, the Sender encrypts any sequence of characters of the language L using the selected public key, and sends a set containing the encrypted element of the language L and the constructed automatic recognizer M. After receiving this set, the Recipient decrypts the encrypted element of the language using all r secret keys, and receives an r – set of decrypted elements of the language L, which is fed to the input machine M. In the case where the automaton M accepts more than one of the decrypted elements of the language, the Recipient asks the Sender to repeat the procedures described above. Once the Recipient receives only one decrypted element, they memorize the ID of the

private key used to identify the decrypted element accepted by automaton M. Recipient indicate that the Sender can start sending the encrypted message. Upon receiving instructions, the Sender encrypts the message using the chosen public key and sends it to the Recipient, who then decrypts it using the corresponding known private key.

It should be noted that the proposed multi-factor cryptosystem has a higher cryptographic strength than the classical asymmetric cryptosystem RSA. This is due to the fact that in one session a large set of public and private key pairs is generated between the Sender and the Recipient, which can mislead a third party, since the attacker has no idea which of the list of public keys was selected.

Finite automata with output in cryptography. The previous section discussed the use of automaton models without output in cryptography, highlighting the advantages and drawbacks of such models, such as the Dömösi cryptosystem and its enhanced version. However, there is also interest in automata with output. Therefore, many scientific papers have been studied and analyzed [7], where the concept of finite automata cryptography was introduced, which is integration of the theory of automata and cryptography.

Knowledge about the representation of FAC has been systematized and described using a constructed ontology, which provides a clear understanding of the application of finite automata in this field. As a practical example, the ontology of the FAPKC (Finite Automation Public Key Cryptosystems) was created - a stream cipher with an open key based on finite automata, proposed by R. Tao [9]. This ontology demonstrated the process of enhancing FAPKC from version FAPKC0 to FAPKC4.

Asymmetric cryptosystem based on FA is interesting because it uses a public key, which is a composition of reversible automata, to encrypt plaintext and verify signatures. While the private key used to decrypt and sign messages consists of inverses of these automata. This method particularly noteworthy because reversing the sequence of the automata is a difficult task, especially without knowing the secret key. In number theory, a large number can be decomposed into prime factors and their order in the product does not matter, in FA theory, the order of the placement of FAs in the composition is of great importance. In other words, the composition of a FA does not have the property of commutativity. Therefore, decomposing the composition of FA into their constituent components is as difficult as decomposing the product of two large numbers. Thus, the decomposition of FA into primitive automata is the key to building highly reliable information security systems. [7].

As it is known, the key property of finite automata that determines their application in information encryption/decryption is invertibility. Therefore, research has been conducted on the verification of automaton invertibility and the algorithms for constructing automata, which have been presented in works [13, 14]. In these works, the problems of invertibility of several FA models (FAM) were considered, such as the invertibility of FA with input-output memory and the invertibility of automata storing information, which confirms the need to study the problem of reversibility and other FAM.

In 2010, S. Chopuryan and G. Makarov proposed an improved FAPKC system that can withstand such types of attacks as an attack based on the selected plaintext and based only on ciphertext [7]. One of the drawbacks of existing finite automata public key systems is that they rely on easily invertible nonlinear automata with zero delay and easily invertible linear automata with delay τ. To create more secure FAPKC algorithm, the authors S. Chopuryan and G. Margarov proposed increasing the delay τ of the encryption finite automaton. To achieve this goal, they presented two methods. The first way is to modify the non-linear automata to easily invertible non-linear automata with a delay $\tau 1$, where the delay $\tau 1$ is proportional to the number of states of the easily invertible linear automata. The second way is to add new states between

two states of an easily invertible linear automaton. The resulting new linear automaton is equivalent to the initial automaton, but has a large clock delay.

It is known that besides FAPKC, there are other FAM in cryptography. For example, the application of automata in a cryptosystem based on a 128-bit key using the key generation algorithm based on DAFA (DES Augmented Finite Automaton cryptosystem) and DES (Data Encryption Standard). Also exist new cryptographic algorithms based on Mealy/Moore automata and recursive functions. One of the components in the proposed system is automata that are part of the secret key. Recursive functions such as a recurrent matrix, generating function, and graph are used, and their reversibility is defined.

The research in [15] delved into a comprehensive examination of the properties of LFT (Linear Finite Transducers) and their invertibility. Additionally, a novel structural FA with Memory known as PILT (Post Initial Linear Transducer) which is extend of LFT was introduced in the same context. These studies extensively examined the properties and reversibility of LFT, providing various examples to illustrate the proposed methods and concepts in a visual manner. The works delved into the specifics of formalizing the process of injectivity verification and developing memory-based inverse finite transducers, including both linear and quasi-linear models.

Conclusion. There are numerous well-known cryptographic ciphers that are successfully used for information security and demonstrate high computational efficiency. However, the rapid progress and development of quantum computers have increased the probability of solving many classically hard problems, while advancements in cryptanalysis have spurred the development of new methods to break classical cryptographic systems. For example, 1024-bit RSA encryption was cracked by researchers from the United States, the Netherlands, and Australia, who discovered a serious vulnerability in the cryptographic library implemented in GnuPG. Such instances stimulate the development of new cryptographic systems or the improvement of existing ones using alternative mathematical models.

Thus, the growing threat of cryptanalysis and the development of quantum computers drive the creation of new cryptographic systems that are resistant to new methods of attacks and ensure a high level of information security. From the research conducted by scientists and published in international and Kazakhstani journals, it can be concluded that finite automata show promise as a foundation for cryptographic algorithms. Further research on the construction methods of such crypto-algorithms and their analysis methods remains highly relevant tasks.

Acknowledgements. Within the framework of the project AP19677422 “Development of reliable and effective methods of cryptographic protection of information based on the finite automata theory” on grant funding for scientific and (or) scientific and technical projects for 2023-2025 (Ministry of Science and Higher Education of the Republic of Kazakhstan)

Список литературы

1. Buchanan, W. (2017). Cryptography. Denmark: River Publishers.
2. Hamza, A., Kumar, B. (2020). A Review Paper on DES, AES, RSA Encryption Standards. Proceedings in 9th International Conference on System Modeling & Advancement in Research Trends. India. (p 333-338).
3. Alemami, Y., Afendee, Mohamed M., Atiewi, S. (2019). Research on Various Cryptography Techniques. International Journal of Recent Technology and Engineering (IJRTE). 8(2S3), p 395-405.
4. Kodada, B.B., D’Mello, D.A. (2021). Symmetric Key Cryptosystem based on Sequential State Machine. IOP Conf. Series: Materials Science and Engineering. (pp 1-10).
5. Шахметова Г.Б., Шарипбай А.А., Сауханова Ж.С. Применение конечных автоматов без выхода в криптографических алгоритмах // Вестник Государственного университета им.

Шакарима. №1 (85), 2019, стр 138-142
6. Pavithrana, P., Mathewa, Sh, Namasudrab, S, Lorenzc, P. (2021) A novel cryptosystem based on DNA cryptography and randomly generated mealy machine. Computers & security.104.
7. Шарипбай А.А., Сауханова Ж.С., Шахметова Г.Б., Сауханова М.С. Онтология конечно-автоматной криптографии. Онтология проектирования. – 2019. – Т. 9, №1(31). - С. 36-49
8. Navalakhe, R. Atre, H. (2023). Implementation of cryptographic algorithms using moore machine and recurrence matrix. Punjab University Journal of Mathematics. 55(3). (p. 89-98)
9. Tao, R.J. (2009) Finite Automata and Application to Cryptography. Tsinghua University Press.
10. Jawaharlal, S. M., Narayanan, A., Santhar, S., Sivaramalingam, B. (31 March 2020). Cryptography using muli-factor key system and finite state machine. Patetnt No US10609003B2.
11. Жукабаева Т., Абдилдаева А., Тураев Ш., Марденов Е. Разработка модифицированных криптосистем на основе конечных автоматов // Матер. IV междунар. науч.-практ. конф. «Информатика и прикладная математика». – Алматы, 2019. – Ч.1. – С.239-247.
12. Khaleel, G., Turaev, S. I. Al-Shaikhli, Mohd Tamrin, M.I. (2016). An overview of cryptosystems based on finite automata. Journal of Advanced Review on Scientific Research. 27(1). (p 1-7).
13. Sharipbay, A.A., Saukhanova, Zh.S., Shakhmetova, G.B., Saukhanov, N.S. (2019) Application of finite automata in cryptography. International Conference on Engineering & MIS – 2019. ENU.
14. Шахметова Г.Б., Сауханова Ж.С., Шарипбай А.А., Улюкова Г.Б.Использование обратимых автоматов в асимметричных криптосистемах // Вестник АУЭС №1(48), 2020, сс. 118-123
15. Amorim, I.(2016). Linear Finite Transducers Towards a Public Key Cryptographic System. PhD thesis. Portugal.

References

1. Buchanan, W. (2017). Cryptography. Denmark: River Publishers.
2. Hamza, A., Kumar, B. (2020). A Review Paper on DES, AES, RSA Encryption Standards. Proceedings in 9th International Conference on System Modeling & Advancement in Research Trends. India. (p. 333-338).
3. Alemami, Y., Afendee, Mohamed M., Atiewi, S. (2019). Research on Various Cryptography Techniques. International Journal of Recent Technology and Engineering (IJRTE). 8(2S3), p 395-405.
4. Kodada, B.B., D'Mello, D.A. (2021). Symmetric Key Cryptosystem based on Sequential State Machine. IOP Conf. Series: Materials Science and Engineering. (pp 1-10).
5. Shakhmetova G.B., Sharipbay A.A., Saukhanova Sh.S. Application of finite state machines without output in cryptographic algorithms // Bulletin of the State University named after. Shakarima. №1 (85), 2019, p. 138-142
6. Pavithrana, P., Mathewa, Sh, Namasudrab, S, Lorenzc, P. (2021) A novel cryptosystem based on DNA cryptography and randomly generated mealy machine. Computers & security.104.
7. Sharipbay A.A., Saukhanova Zh.S., Shakhmetova G.B., Saukhanova M.S. Ontology of finite-automata cryptography. Design ontology. – 2019. – T. 9, №1(31). - p. 36-49
8. Navalakhe, R. Atre, H. (2023). Implementation of cryptographic algorithms using moore machine and recurrence matrix. Punjab University Journal of Mathematics. 55(3). (p. 89-98)
9. Tao, R.J. (2009) Finite Automata and Application to Cryptography. Tsinghua University Press.
10. Jawaharlal, S. M., Narayanan, A., Santhar, S., Sivaramalingam, B. (31 March 2020). Cryptography using muli-factor key system and finite state machine. Patetnt No US10609003B2.
11. Zhukabaeva T., Abdildaeva A., Turaev Sh., Mardenov E. Development of modified cryptosystems based on finite state machines//IV international scientific-practical conf. "Informatics and applied mathematics." – Almaty, 2019. – Part 1. – P.239-247.
12. Khaleel, G., Turaev, S. I. Al-Shaikhli, Mohd Tamrin, M.I. (2016). An overview of cryptosystems based on finite automata. Journal of Advanced Review on Scientific Research. 27(1). (p 1-7).
13. Sharipbay, A.A., Saukhanova, Zh.S., Shakhmetova, G.B., Saukhanov, N.S. (2019) Application of finite automata in cryptography. International Conference on Engineering & MIS – 2019. ENU.
14. Shakhmetova G.B., Saukhanova Zh.S., Sharipbay A.A., Ulyukova G.B. Use of reversible automata in asymmetric cryptosystems // Bulletin of AUES No. 1(48), 2020, p. 118-123
15. Amorim, I.(2016). Linear Finite Transducers Towards a Public Key Cryptographic System. PhD thesis. Portugal.