The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2023

Volume 26, Pages 19-25

IConTES 2023: International Conference on Technology, Engineering and Science

Development of Reliable and Effective Methods of Cryptographic Protection of Information Based on the Finite Automata Theory

Altynbek Sharipbay
L.N. Gumilyov Eurasian National University

Zhanat Saukhanova
L.N. Gumilyov Eurasian National University

Gulmira Shakhmetova
L.N. Gumilyov Eurasian National University

Alibek Barlybayev
L.N. Gumilyov Eurasian National University

Abstract: This paper describes project to conduct study of cryptographic protection of information on publications in publications and development of methods for reliable and efficient cryptographic protection of information based on finite automaton models-FAM, preparation of additions to standards and management of dissertations of undergraduates and doctoral students on information security and information protection. To achieve this goal, following tasks will be solved: 1. Study of mathematical foundations of cryptology and analysis of standards for cryptographi. Results: Theory of finite fields, models of FA, descriptions of requirements of standards, proposals to standards. 2. Study of applicability of various FA models in construction of reliable and efficient cryptoalgorithms. Results: Algorithm for obtaining an inverse FA from given FA - proving applicability of FA in cryptosystem, algorithm for composing several FA - proving increase in reliability of cryptosystem using composite FA with increased number of states, algorithm for constructing equivalent FA – proving increase in efficiency of cryptosystems using equivalent FA with reduced number of states. 3. Development and verification of programs for reliable and efficient cryptosystem based on KA. Results: FA cryptographic programs and their applications in steganography, verification and testing protocols for developed programs.

Keywords: Cryptography, Information security, Finite automata, Reversibility of finite automata, Information security standards

Introduction

In era of active use of Internet, ensuring security of information becomes serious problem. Therefore, special attention is paid to ensuring confidentiality, availability and integrity of information using cryptographic methods. During COVID 19 demand for online services has increased. This led to increase in attacks and hacks (Boranbayev et al., 2018). In 2022, outside attacks on communication infrastructures have become more frequent, which required an increase in the quality of information protection. Security of every citizen and entire country depends on reliability and effectiveness of cryptographic protection. Therefore, cryptographic information protection tools developed on basis of specific methods are required.

Kazakhstan uses foreign software products (Seilova et al., 2021). State programs and Concepts (Kassymzhanova et al., 2022) require the development (Aktayeva et al., 2018) of domestic software products (Mukanov, 2023).

- Selection and peer-review under responsibility of the Organizing Committee of the Conference

Based on these documents, project executors are engaged in cryptographic information protection and have certain scientific background (Shakhmetova et al., 2021; Sharipbaev et al., 2004; Sharipbaev et al., 2004; Andasova et al., 2009; Satybaldina et al., 2009; Abdymanapov et al., 2021; Sharipbay et al., 2013).

In (Sharipbaev et al., 2006; Satybaldina et al., 2009; Sharipbay et al., 2016; Sharipbay et al., 2017; Sharipbay et al., 2016), applications of finite automata (FA) in cryptography and general idea of information encryption by means of FA with output and FA without output were described. In (Shakhmetova, 2018; Shakhmetova et al., 2019), issues of using automata models without exit in cryptography were discussed, advantages and disadvantages of such models as the Domosi cryptosystem and its improved version were presented. But there was interest in FA with release (Shakhmetova et al., 2018). Many scientific papers (Sharipbay et al., 2019) have been studied and analyzed, where concept of finite automaton cryptography (FAC) was introduced.

All knowledge about FAC is presented with help of ontology, which is built for first time and provides clear understanding of using FA in cryptography and systematizes the information about this subject area obtained during study. As practical example, FAPKC ontology (Finite Automation Public Key Cryptosystems) was constructed - public key streaming cryptosystem based on FA, proposed by Tau (2008). In this ontology, process of improving FAPKC from version FAPKC0 to FAPKC4 was shown. Based on these studies, the following problems were identified:

- Absence of algorithm for constructing composition of PILT - automata.
- Large key size. For example, key length for algorithm security achieved with 512-bit RSA key is 2792 bits for FAPKC.
- Lack of evidence base for correctness of cryptographic algorithms.

Considering all weaknesses of previous cryptosystems (Bao & Igarashi, 1995; Meskanen, 2001), R. Tau proposed new asymmetric encryption algorithm FAPKC4 (Tao & Chen, 1999). It is interesting in that public key is used to encrypt plaintext and verify signature, which consists of sequential composition of reversible automata, while inverse automata are part of the private key, which is used to decrypt and sign the message. It's believed that without knowledge of secret key it's difficult to invert sequence of automata composition (Satybaldina et al., 2011). In contrast to number theory, where large number can always be decomposed into simple factors, for which order of their mutual arrangement in product is not important, in theory of FA in composition of reversible automata, both their set and the order of the mutual arrangement of reversible automata in composition matter. In other words, composition of FA from primitive automata doesn't have the commutativity property. Therefore, the task of decomposing FA composition into its constituent components is same difficult task as factoring the product of two large numbers (Sharipbay et al., 2019). Therefore, decomposition of FA into primitive automata allows you to create ultra-reliable information security systems.

As is known, main property of FA, which determines its use in encryption/decryption of information, is its reversibility. Therefore, issues of checking the reversibility of FA, algorithms for constructing FA, which were presented in works (Shakhmetova et al., 2020; Shakhmetova & Saukhanova, 2020), were investigated. In these works, problems of reversibility of several FAM were considered, such as reversibility of input-output FA and reversibility of automata that stores information, which confirms need to study problem of reversibility of other FAM as well.

It is known that in addition to FAPKC, there are other FAM in cryptography. In Abubaker (2011), it was proposed to use FA in a cryptosystem based on 128-bit key using key generation algorithm based on (DAFA - DES Augmented Finite Automaton cryptosystem, DES - Data Encryption Standard). The paper (Srilakshmi, 2012) proposes new cryptographic algorithms based on Mealy/Moore automata and recursive functions. In (da Cruz Amorim, 2016; Vieira, 2017), all characteristics of linear FA and their reversibility were studied, and new structural FAM was also presented, called PILT - Post Initial Linear Tranducer.

There are also studies in this subject area in Russia and Kazakhstan. So in works (Agibalov, 2009; Kovalev & Trenkaev, 2011; Kovalev, 2014) implementation of FAPKC on FPGAs is shown, scientists from L.N. Gumilyov ENU proposed hardware implementation of FA-cryptosystem with public key (Satybaldina et al., 2011; Satybaldina et al., 2011).

Today, there are many well-known cryptographic ciphers that have proven themselves well in information security environment, and they undoubtedly have high efficiency from computational point of view. However, rapid growth and improvement of quantum computers has increased likelihood of solving most classically difficult problems, and constant improvement of cryptanalysis has influenced development of new algorithms for breaking classical cryptographic systems. If we take 1024-bit RSA encryption as example, then it was cracked by scientists from USA, Netherlands and Australia, who found serious vulnerability in cryptographic library implemented in GnuPG (Bernstein et al., 2017). This trend gives impetus to development of new cryptographic systems or the improvement of existing ones, using alternative mathematical models.

As result of studies of publications of domestic scientists in foreign and Kazakh publications, it can be concluded that such studies are mainly carried out as memristive cryptography (James, 2019), cryptography based on elliptic curves (Muratbekov et al., 2014; Kulmamirov et al., 2018), improvement of classical cryptographic algorithms (Gnatyuk et al., 2020; Gnatyuk et al., 2020; Biyashev et al., 2021), neural networks in cryptography (Fenina, 2021), which indicates that in Kazakhstan, research in FAC is carried out only by project executors, as described in the backlog of the project. Consequently, there are no software implementations of finite-automatic methods of cryptographic information protection, except for those that were discussed in review of existing works. Therefore, fundamental differences between project idea and existing analogues are that:

- For FAM based on PILT-automata, algorithm for constructing composition of reversible PILT-automata will developed and implemented.
- FAM will used in steganography, to protect secret text in stegacontainer, as well as in encoding/decoding of binary data.
- Proofs of correctness of cryptographic algorithms and protocols are carried out not by testing methods on specific data, but by formal proofs of verification conditions formulated in logical language.

This project provides for creation of reliable and efficient cryptosystem based on FAM, where encryption is carried out by a composition of reversible FA, and decryption by reverse sequence of reverse FA. Decomposition of an automata-encoder into simple components has exponential complexity (Agibalov, 2009), and its performance doesn’t depend on the size of its transition table. Therefore, cryptographic systems based on FAM will have a significant advantage, both in terms of throughput and performance, over cryptographic methods based on numerical operations. In addition, development and verification of necessary cryptoprotocols will carried out using specification language with expressive power equivalent to expressive power of FA, which ensures correctness of created formalisms, constructiveness of algorithms and provability of their correctness. These arguments prove scientific novelty, importance and prospects of developing FAM, confirm significance of such cryptographic methods on national and international scale, and prove high scientific and technical level of proposed project, which will make significant contribution to formation of domestic scientific and technological potential.

Significance of the Project

In digital society, correct creation, use and protection of information resource ensures increase in degree of organization, and therefore, efficiency of functioning of economic systems. In turn, information resources today acquire characteristics of commodity and capital, actively participate in commodity-money relations. Therefore, urgent problem has arisen of creating domestic models and methods for protecting information resources from illegal actions that can lead to loss or distortion of valuable data and cause enormous material damage to their owners and society as a whole. In solving this problem, one cannot ignore time factor, when loss of time leads to a country lagging behind other countries. Issues of economic and national security of country depend on this. Without correct and timely solution to problem of protecting information resources, any country has no future. Results of project will be of economic and industrial interest, and will also cause great social demand among scientists and specialists working in field of information security.

For successful implementation of project, it’s required to combine scientific results obtained earlier in direction of study area and results of project participants themselves into single integrated finite-automata technology for cryptographic information protection, which will include software implementation of information protection methods, teaching aid, training course and recommendations for improving state standards in field of cryptographic information protection.

Research in project is interdisciplinary, which requires knowledge in field of algebra to justify factorization of numbers, automata theory for modeling algorithms for encryption and decryption of information, mathematical logic for formulating and proving verification conditions for cryptographic algorithms and protocols, as well as information technology for programming encryption and decryption algorithms information, and standardization to prepare recommendations for improving state standards in the field of cryptographic information protection.

Due to fact that in Kazakhstan information security must be ensured, without any doubt, only by domestic cryptosystems.

Research Methods

The main scientific issue is the problem of developing reliable and efficient methods of cryptographic information protection based on the theory of finite automata, which requires a consistent study of the mathematical foundations of cryptography and the analysis of standards for the subject area of the project and the study of the applicability of various FA models in solving the problem of cryptography based on the construction of reverse FA, as well as the development and software implementation of cryptographic methods for protecting information based FA and verification of implemented programs. To study the mathematical foundations of cryptology and analyze the standards for the subject area of the project, descriptive research methods are used, and to solve other issues, the following experimental studies and works are sequentially performed: choosing a specific FA model; constructing a reverse FA to the selected FA; building a composition of the FA from a specific model; development and software implementation of data encryption methods based on various FA models; verification of programs and evaluation of their complexity, reliability and efficiency. To assess the applicability of the given FA to solve the problem of creating a reliable and efficient method of cryptographic information protection, experimental methods, software design methods, program testing methods, and formal program verification methods are used.

The most important experiments are: development and verification of the program for constructing the reverse FA given by the FA in order to determine their applicability to the creation of the required cryptosystem; development and verification of a program for constructing a composition of given FA in order to increase the reliability of the developed cryptosystem based on an increase in the number of FA and states of the resulting FA; development and verification of a program for constructing a FA equivalent to a given FA in order to increase the efficiency of the developed cryptosystem by reducing the number of states of the resulting FA.

The research used in the project as a substantiation of ways to achieve the goal of developing methods for reliable and effective cryptographic protection of information should use descriptive studies of the mathematical foundations of cryptology and analysis of standards for the subject area of the project, as well as the following experimental studies: development and verification of a program for constructing a reverse FA by given FA; development and verification of a program for constructing a composition of given FA; development and verification of a program for constructing a FA equivalent to a given FA. In addition to these methods, the project will use the methods of number theory, automata theory, the theory of algorithms and the theory of information encryption, as well as methods for constructing and verifying algorithms, methods for developing and testing software, and methods for graphical presentation of analysis results.

Methods for collecting primary information are searching the Internet and scientific and technical libraries for scientific publications and publications on models and methods of cryptology, as well as the texts of international and domestic standards and other legal documents on information security and cryptographic protection of information, specifications of cryptographic programs (possibly with online demonstration) that can be used in solving some tasks of the project with references to them. The methods of data processing are comparison with the contents of the available scientific, practical and regulatory materials, and in the absence of the latter, the found materials will be studied and stored in computer memory or in the cloud, indicating their IP addresses or mailing addresses of sources. Participants have a sufficiently high level of knowledge and experience in the subject area of the project to ensure reliability and reproducibility. They can hold scientific seminars, participate in scientific conferences and other events dedicated to the scientific direction of the project.

Conclusion

Main results of the project will be:

- correspond to international level of scientific and technical development, as they will published in rating international editions;
- ensure information security in field of information and communication technology, since reliability of created cryptosystems on KAM will be proven using composite automata;

- have a high degree of readiness for commercialization, since effectiveness of created cryptosystems on KAM will be proved by using an equivalent automaton with a minimum number of states, facilitating its software and hardware implementation;
- participate in training of highly qualified young specialists and scientists, involving bachelors, masters and PhD students in EP "Computer Science", "Artificial Intelligence Technology" and "Information Security" to solve individual project tasks as topics of their diploma and dissertation works, which is scientifically confirmed-practical significance and impact on the development of science: computer science and artificial intelligence.

In general, results of project contribute to solution of urgent tasks of socio-economic and scientific and technical development of RK, provided for in following state programs:

- "Digital Kazakhstan", which provides for the task "Ensuring information security in the field of ICT";
- "Development of Education and Science of the Republic of Kazakhstan", which provides for tasks to ensure a safe and convenient learning environment; increasing the effectiveness of R&D and integration into the global educational and scientific space.

Scientific Ethics Declaration

The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

Acknowledgements

* This article was presented as an oral presentation at the International Conference on Technology, Engineering and Science (www.icontes.net) held in Antalya/Turkey on November 16-19, 2023.

* This research is funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP19677422).

References

Abdymanapov, S. A., Muratbekov, M., Altynbek, S., & Barlybayev, A. (2021). Fuzzy expert system of Information security risk assessment on the example of analysis learning management systems. *IEEE Access, 9,* 156556-156565.

Abubaker, S. (2011). *Probabilistic, lightweight cryptosystems based on finite automata*. (Doctoral dissertation).

Agibalov, G. P. (2009). *Finite automata in cryptography. Prikladnaya Diskretnaya Matematika, 11,* 43-73.

Aktayeva, A., Niyazova, R., Muradilova, G., Makatov, Y., & Kusainova, U. (2018). Cognitive computing cybersecurity: social network analysis. In *International Conference on Convergent Cognitive Information Technologies* (pp. 28-43). Cham: Springer International Publishing.

Andasova, B. Z., Satybaldina, D. Zh., & Sharipbaev, A. A. (2009). Analysis of cryptographic protocols based on modal logics. *Bulletin of ENU. L.N. Gumilyov, 4*(71), 50-57.

Bao, F., & Igarashi, Y. (1995). Break finite automata public key cryptosystem. In *International Colloquium on Automata, Languages, and Programming* (pp. 147-158). Berlin, Heidelberg: Springer

Bernstein, D. J., Breitner, J., Genkin, D., Groot Bruinderink, L., Heninger, N., Lange, T., ... & Yarom, Y. (2017). Sliding right into disaster: Left-to-right sliding windows leak. In Proceeding 19th *International Conference, Cryptographic Hardware and Embedded Systems–CHES 2017* (pp. 555-576). Taipei, Taiwan.

Biyashev, R. G., Kapalova, N. A., Dyusenbayev, D. S., Algazy, K. T., Wojcik, W., & Smolarz, A. (2021). Development and analysis of symmetric encryption algorithm Qamal based on a substitution-permutation network. *International Journal of Electronics and Telecommunications, 67*(1), 127-132.

Boranbayev, A., Boranbayev, S., Nurusheva, A., & Yersakhanov, K. (2018). The modern state and the further development prospects of information security in the Republic of Kazakhstan. In *Information Technology-New Generations: 15th International Conference on Information Technology* (pp. 33-38). Springer International Publishing.

da Cruz Amorim, I. D. F. (2016). *Linear finite transducers towards a public key cryptographic system* (Doctoral dissertation.) Universidade do Porto (Portugal)

Fenina, O. (2021). The application of neural networks in cryptography. In Proceedings of the *4th International Conference on Mathematics and Statistics* (pp. 48-58).

Gnatyuk, S., Akhmetov, B., Kozlovskyi, V., Kinzeryavyy, V., Aleksander, M., & Prysiazhnyi, D. (2020). *New secure block cipher for critical applications: Design, implementation, speed and security analysis. In Advances in artificial systems for medicine and education III* (pp. 93-104). Springer International Publishing.

Gnatyuk, S., Kinzeryavyy, V., Iavich, M., Odarchenko, R., Berdibayev, R., & Burmak, Y. (2020*). Studies on cryptographic security and speed analysis of new advanced block cipher* (pp. 202-213). ICST

James, A. P. (2019). An overview of memristive cryptography. *The European Physical Journal Special Topics, 228*(10), 2301-2312.

Kassymzhanova, A. A., Usseinova, G. R., Baimakhanova, D. M., Ibrayeva, A. S., & Ibrayev, N. S. (2022). Legal framework for external security of the Republic of Kazakhstan. *International Journal of Electronic Security and Digital Forensics, 14*(2), 209-222.

Kovalev, D. S. (2014). Optimization of FPGA implementations of finite-automatic cipher systems. In *Collection of Scientific Articles of the All-Russian Scientific and Practical Conference* (pp. 38-44). Barnaul: FPGAs, Signal Processing Systems.

Kovalev, D. S., & Trenkaev, V. N. (2011). FPGA implementation of finite automata public key cryptosystem. *Prikladnaya Diskretnaya Matematika, 13*, 33-34.

Kulmamirov, S. A., & Aksholak, G. I. (2018). Analysis of encrypted digital signature algorithms based on elliptic curves. In Proceedings of the *International Practical Internet Conference "Actual Problems of Science*

Meskanen, T. (2001). *On finite automaton public key cryptosystems.* Turku Centre for Computer Science.

Mukanov, A. (2023). The main indicators of the state program digital Kazakhstan. In Proceedings of the *7 th International Scientific and Practical Conference Current Issues and Prospects for the Development of Scientific Research, 32* (151), 25-38.

Muratbekov, M. M., Abdymanapov, S. A., & Altynbek, S. A. (2014). Using the properties of Abelian groups to build cryptosystems on elliptic curves of odd order. *Bulletin of KazUEFMT, 1*, 105-109.

Satybaldina, D. Zh., & Sharipbaev, A. A. (2009). Application of fuzzy set theory to information Security Risk Analysis. In Abstracts of the *Third Congress of the World Mathematical Society of Turkic Countries,* (p. 216).

Satybaldina, D. Zh., & Sharipbaev, A. A. (2009). Information security risk assessment based on fuzzy logic. In Proceedings of the *II All-Russian Conference "Knowledge - Ontologies – Theories* (pp. 216-220). Novosibirsk.

Satybaldina, D. Zh., Sadykov, A. A., & Adamova, A. D. (2011). Hardware-software implementation of a cryptosystem based on finite automata. *Bulletin of L.N. Gumilyov atyndagy ENU Khabarshysy*, (2).

Satybaldina, D., Sharipbayev, A., & Adamova, A. (2011). *Implementation of the finite automaton public key cryptosystem on FPGA.* (pp. 167-173). WOSIS.

Satybaldina, D., Sharipbayev, A., Sadykov, A., & Adamova, A. (2011). FPGA implementation of the Finite Automaton Public Key Cryptosystem. In Book of abstracts of the *Third International Conference on Control and Optimization with Industrial Applications* (COIA 2011) (pp. 42-43). Ankara, Turkey.

Seilova, N., Kungozhin, A., Ibrayev, R., Gorlov, L., Ospanov, Z., Itemirov, R., & Kiyashko, I. (2021). About cryptographic properties of the Qalqan encryption algorithm. In *Ceur Workshop Proceedings "Cybersecurity Providing in Information and Telecommunication Systems II—CPITS-II*, 206-215.

Shakhmetova, G. B. (2018). Automata without exit in cryptography. In *XIII International Scientific Conference of Students and Young Scientists Science and Education* (pp. 767-770).

Shakhmetova, G. B., & Saukhanova, Zh. S. (2020). On algorithms that determine reversible finite automata with memory. In *XV International Scientific Conference* (pp. 496-500). Ǵylym Jáne Bilim-2020 Shakhmetova, G. B., Saukhanova, Zh. S., & Sharipbay, A. A. (2019). The use of finite automata without exit in information encryption. *Bulletin of the State University, 1*(85), 138-143.

Shakhmetova, G. B., Saukhanova, Zh. S., Sharipbay, A. A., & Ulyukova, G. B. (2020). The use of reversible automata in asymmetric cryptosystems. *Bulletin of AUPET, 1*(48), 118-123.

Shakhmetova, G. B., Sharipbay, A. A., Saukhanova, Zh. S., & Isabaeva, G. Zh. (2018). The use of finite automata for the development of asymmetric ciphers. *In Proceedings of the V International Scientific and practical conference "intelligent information and communication technologies - a means of implementing the third industrial revolution in the light of the strategy* (pp. 286-288).

Shakhmetova, G., Saukhanova, Z., Udzir, N. I., Sharipbay, A., & Saukhanov, N. (2021). Application of pseudo-memory finite automata for information encryption. In *IntelITSIS*, 330-339.

Sharipbaev, A. A., & Satybaldina, D. Zh. (2006). On finite-automatic models for the design of cryptosystems. In Proceedings of the *11th International Interuniversity in Mathematics and Mechanics, dedicated to the 10th anniversary of the ENU. L.N.* (p.214). Gumilyov Kazakhstan, Astana.

Sharipbaev, A. A., Bekbulatova, K., & Satybaldina, D. Zh. (2004). Security of public key algorithms. In Proceedings of *the International Scientific and Practical Conference Valikhanov Readings-9* (Volume 4, pp. 149-152). Kokshetau.

Sharipbaev, A. A., Kaplina, S. A., & Satybaldina, D. Zh. (2004). Methods for designing block ciphers. In Proceedings of the *International Scientific and Practical Conference Valikhanov Readings-9* (Volume 4, pp. 164-167). Kokshetau.

Sharipbay, A. A. (2016). Automatic models in cryptography. *Bulletin of KazNU Series of Mathematics, Mechanics, Computer Science, 3-1* (90), 96-104.

Sharipbay, A. A. (2016). Automatic models of encoders in electronics and cryptography. In Proceedings of the *V International Scientific and Practical Conference Informatization of Society* (pp. 402-411). Astana

Sharipbay, A. A. (2017). Genetic cryptographic algorithm of asymmetric information encryption. *In International Scientific Conference Computer Science and Applied Mathematics Part II,* Almaty (pp. 144-151).

Sharipbay, A. A., Omarbekova, A. S., & Niyazova, R. S. (2013). Cryptology. *MYURK, 1413*

Sharipbay, A. A., Saukhanova, Z. S., Shakhmetova, G. B., & Saukhanov, N. S. (2019). Application of finite automata in cryptography. In Proceedings of the *5th International Conference on Engineering and MIS,* 1-3.

Sharipbay, A. A., Saukhanova, Zh., Shakhmetova, G. B., & Saukhanova, M. S. (2019). Ontology of finite automaton cryptography. *Ontology of Design, 9*(1), 36-49.

Srilakshmi, S. (2012). On finite state machines and recursive functions application to cryptosystems.

Tao, R. (2008). *Finite automata and application to cryptography.* Chicago: Springer.

Tao, R., & Chen, S. (1999). The generalization of public key cryptosystem FAPKC4. *Chinese Science Bulletin, 44,* 784-790.

Vieira, J. B. (2017). *Finite transducers in public key cryptography.* Universidade do Porto (Portugal)

Author Information

Altynbek Sharipbay
L.N. Gumilyov Eurasian National University
Pushkin street 11, Astana, Kazakhstan
Contact e-mail: *sharalt@mail.ru*

Zhanat Saukhanova
L.N. Gumilyov Eurasian National University
Pushkin street 11, Astana, Kazakhstan

Gulmira Shakhmetova
L.N. Gumilyov Eurasian National University
Pushkin street 11, Astana, Kazakhstan

Alibek Barlybayev
L.N. Gumilyov Eurasian National University
Pushkin street 11, Astana, Kazakhstan

To cite this article:

Sharipbay, A., Saukhanova, Z., Shakhmetova, G., & Barlybayev, A. (2023). Development of reliable and effective methods of cryptographic protection of information based on the finite automata theory. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 26,* 19-25.