

Research on the criteria of cryptographic resistant of continuous encryption algorithms

Davlatali Akbarov¹, Shukhratjon Umarov^{2}, Mamirjon Turdimatov², Husniddin Sotvoldiyev², Abdulhay Abduqodirov², and Ulmasbek Karimov³*

¹ Kokand State Pedagogical Institute, Kokand, Uzbekistan

² Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Fergana, Uzbekistan

³ Fergana State University, Fergana, Uzbekistan

Abstract. The article examines the features of the criteria for the strength of continuous encryption algorithms. The general properties of the models of algorithms of the continuous encryption class are revealed. On their basis, the corresponding requirements are formulated in the form of criteria that determine the necessary conditions for cryptographic resistant. The totality of these criteria is formulated as a statement.

1 Introduction

Ideally strong encryption algorithms are reliable for cryptographic protection of information. However, when used in practical applications, there are some inconveniences. In particular, the length of the key block has a large character sequence. This property, for example, can cause problems with storing and transferring keys [1].

With the intensive development of modern computer technology and technology, in addition to the binary number system in calculations, logical operations that carry out bit comparisons have a special place.

Currently, globalization in all spheres of life, the development of methods and means, ensuring the protection of information: stored, processed and exchanged in information and communication networks, is especially significant and relevant [2].

2 Formulation

Research on the way of eliminating the inconvenience due to the large volume of the key length naturally led to the problem of the need to develop a more convenient encryption algorithm, while maintaining the basic properties of an ideally strong encryption algorithm [3]. The proposed article formulates the necessary conditions for the security of continuous encryption algorithms in the form of a statement.

* Corresponding author: sh.umarov81@mail.ru

3 Solution

It is known that the problem is solved on the basis of generators generating pseudo-random sequences. Generators of pseudo-random sequences for the original key with a length of at least 256 characters, based on one-way (irreversible) transformations, such as: independently transforming bits, nibbles and bytes, compression tables, matrix expansions with proportional rows and columns, logical operations and table replacement with uniform distribution elements in the truth table, a combination of pseudo-random sequence generator models, etc. [4-5].

With an initial key of relatively small length, but currently at least 256 characters, with a pseudo-random sequence generator, based on one-way transformations, a sequence of sufficiently large length is generated, the elements of which, with some operation, are converted (gammed) with the characters of the encrypted message. Thus, a continuous encryption algorithm is being developed.

The conducted system studies and scientific observations of the authors made it possible to formulate the following statement as necessary conditions for the criteria for assessing the strength of continuous encryption algorithms.

4 Statement

In order for the continuous encryption algorithm to be cryptographically strong, the following conditions must be met [6]:

1) The algorithm must be open, its cryptographic resistant depends not only on the unknown key, but also on the key length, it must be at least 256 bits:

$$k = k_1 k_2 \dots k_N, \quad k_i \in \{0,1\}, \quad N = 32 \times l, \quad l = 8,9,\dots < \infty$$

2) The operations used in the transformation of the algorithm must correspond to the effective use in microprocessors, microcontrollers and computer computing systems;

3) The properties of effective mixing and propagation of basic transformations are provided: nonlinearity, one-sidedness, equilibrium, regularity, avalanche effect, flexibility in relation to correlation;

4) The algorithm must ensure the generation of a sufficiently large length of the period of the pseudo-random sequence based on the original key during the implementation of the encryption process;

5) The generated blocks of the pseudo-random sequence must have the property of uniform distribution over bits, two bits, etc.;

6) All gamma elements (bits, nibbles, bytes and arc subblocks) of a pseudo-random sequence should be obtained under the influence of other elements (as a pseudo-random sequence generated on the basis of shift registers), i.e., effective mixing is carried out;

7) Gamma elements (bits, nibbles, bytes and other sub-blocks) of a pseudo-random sequence must have the properties of a sufficiently high randomness.

Proof: If the continuous encryption algorithm is cryptographically strong, then the conditions given in the statement are fulfilled. The necessary cryptographic characteristics of these conditions are justified by the fact that their non-fulfillment can be the basis, negatively affecting the strength of the algorithm. The cryptographic features of the conditions given in the statement are substantiated below.

1. The requirement of the first condition ensures that there is no doubt about the strength of the encryption algorithm on the part of users of various kinds, thereby observing the generally accepted principle of Kirchhoff.

Key symbols are determined based on the principle of using the encryption algorithm in the transformations. In this case, the length of the original key, at present, must be at least 256 characters:

a) if transformations are performed on bits, then the length of the original key is not less than 256 bits;

b) if conversions are performed on nibbles or bytes, then the length of the original key is not less than 256 nibbles or bytes, respectively.

2. The second requirement, continuous encryption algorithms should contain transformations, not complex computable operations, allowing them to be widely and conveniently implemented in hardware [7].

Otherwise, i.e., ineffectiveness of operations of transformations of the encryption algorithm in applications of microprocessors, microcontrollers, computers and other computing devices of information technology, will limit their widespread use. The application of a table-swap operation, with a truth table with uniformly distributed elements, is advisable.

3. The third requirement is necessary in order to ensure the resistance of the algorithm transformation to cryptographic attacks. If basic transformations are carried out by operations on bits or their unions, then without ensuring effective mixing and sifting, they can be the basis for modeling various types of crypto attacks, based on the results of statistical analysis:

a) The properties of effective mixing and scattering of transformations at input blocks $(x_1^i, x_2^i, \dots, x_n^i)$, $i = 0, \dots, 2^{n-1}$ and output blocks, where $n \geq m$, are checked and, as a result, are determined by a uniform distribution of output blocks in their truth table;

b) The independence of the set of output blocks relative to the set of input blocks - the property of pseudo randomness will ensure the nonlinearity of the transformation.

The fulfillment of condition a) will provide the properties of transformations, such as: equilibrium, regularity, avalanche effect, correlation immunity, etc.

4. The fourth requirement will provide properties of resilience of transformations against attacks using inverse transformations of the algorithm. In particular, it will limit the cryptographic attack: knowing some part of the cryptograms, one can find the initial key of the generator of the pseudo-random sequence algorithm.

If the basic transformations of the generator and the algorithm do not have one-way transformations, then using inverse transformations it is possible to simulate means of a cryptographic attack to disclose the necessary information.

From a theoretical point of view, it is possible to compile a truth table for any transformation based on possible input blocks and corresponding output blocks, based on Zhegalkin polynomials [8]. But the properties of the multivalued replacement of the basic transformations of continuous encryption, from a practical point of view, complicate the modeling of inverse transformations.

5. The fifth requirement ensures that the gamma key is of sufficient length. As a result, it is achieved that the power of the set of symbols in the table of cipher designations will be large enough and efficient implementation of encryption of multivalued substitution will be ensured.

The case when the algorithm does not generate a pseudo-random sequence of sufficiently long length is the basis for ineffective implementation of multivalued substitution in the encryption process. Checking the period of the length of the pseudo-random sequence $c_1 c_2 c_3 c_4 \dots c_8 c_9 \dots$ is carried out as follows: a block of pseudo-random sequence elements up to a certain number $i = N$, $i = 2, 3, \dots, N < \infty$, i.e., the block $c_1 c_2 \dots c_N$ is not identically repeated by the next block $c_{N+1} c_{N+2} \dots c_{2N}$. The lower bound of the value determines the key length period.

6. The sixth requirement will ensure the stability of the generated pseudo-random sequence as a gamma key with some operation, symbols of the encrypted message with symbols of the pseudo-random sequence.

In a block generated by a pseudo-random sequence with a continuous encryption algorithm generator, its sub blocks: with one, two, three, etc. elements must be repeated randomly. This feature is checked by statistical tests of randomness, for example, "Chi-square" test.

7. The seventh requirement will ensure that the sub-blocks of the pseudo-random sequence are sufficiently random.

If the elements (with one, two, three and etc.) are not formed with the participation of other parts, then the parts of the generated pseudo-random sequence do not possess the properties of sufficient randomness.

The use of "Chi-square" criterion to determine the degree of randomness of the distribution of elements and combinations of elements as part of a pseudo-random sequence is carried out as follows.

Let the results of some process be in quantity $k: y_1, y_2, \dots, y_k$ and this process is independently performed n times. In this case, n is a somewhat sufficient number of times larger than the number k , that is, $n > k$. In this case, the problem is solved: the repetition of the results y_1, y_2, \dots, y_k how much they deviate from the uniform $Y_1 = Y_2 = \dots = Y_k$ repetitions, where $Y_s, s = 1, 2, \dots, k$ means the number of repetitions of the results y_1, y_2, \dots, y_k , respectively, with an independent product of the process n many times, relative to k the number of results.

For this, the following designations are introduced:

p_s - Probability that the result of the process will be y_s , where $s = 1, 2, \dots, k$;

Y_s - the number of results of the process y_s , when carrying out the process independently n times.

According to these designations, the formula of the so-called "Chi-square" criterion, which expresses the standard deviation of the results of a certain process from the uniform distribution of its results, looks like [9]:

$$V = \sum_{s=1}^k \frac{(Y_s - np_s)^2}{np_s}$$

If the observed process is independently performed many times and the results of the process y_1, y_2, \dots, y_k are always repeated in the same quantity, i.e., $Y_1 = Y_2 = \dots = Y_k$, then the relations hold $p_1 = p_2 = \dots = p_k = \frac{1}{k}$, hence the equalities

$$V = \sum_{s=1}^k \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \sum_{s=1}^k \frac{\left(\frac{n}{k} - \frac{n}{k}\right)^2}{\frac{n}{k}} = 0$$

But, in most real practical cases, such a circumstance is not observed. Suppose that when the process is independently carried out a sufficiently large number of n times, the probability that the results of the process y_1, y_2, \dots, y_k are equal, i.e., $p_1 = p_2 = \dots = p_k = \frac{1}{k}$ in addition, the values for the number of repetitions $Y_s, s = 1, 2, \dots, k$ are not equal. Then, the following formula

$$V = \sum_{s=1}^k \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \frac{k}{n} \sum_{s=1}^k \left(Y_s - \frac{n}{k}\right)^2$$

Expresses the standard deviation from a uniform distribution $Y_1 = Y_2 = \dots = Y_k = \frac{n}{k}$, an uneven distribution Y_1, Y_2, \dots, Y_k . In this last formula, the expression $\left(Y_s - \frac{n}{k}\right)$ is limited to some constant, i.e., $\left|Y_s - \frac{n}{k}\right| \leq C = \text{const}$. Therefore, having an adequate model of the process flow, the following can be done. In the appropriate way: determining the values of its parameters, automating the necessary calculations by software, carrying out in a large number ($n \rightarrow \infty$) independent processes for generating elements of a pseudo-random sequence, we obtain the ratio:

$$V = \sum_{s=1}^k \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \frac{k}{n} \sum_{s=1}^k \left(Y_s - \frac{n}{k}\right)^2 \leq \frac{k}{n} \sum_{s=1}^k C^2 = \frac{(kC)^2}{n} \rightarrow 0.$$

This means that if a sufficiently large number of independent processes have been carried out to generate elements of a pseudo-random sequence and at the same time bits, nibbles, bytes and other parts are distributed almost evenly in the sequence block, then the value of the "Chi-square" criterion of the distribution tends to zero. Therefore, it is concluded that the degree of randomness of the generated pseudo-random sequence is quite high.

The calculated value V determines the degree of randomness of the generated sequence. To do this, we will use the table of critical points "Chi-square" of the criterion for the distribution of random variables. The row of this table $N = k - 1 = 2 - 1 = 1$ contains the interval where the value V is located. If this value lies between $p=25\%$ and $p=75\%$, then the generated pseudo-random sequence is taken as random. For completeness, the table of critical points "Chi-square" of the criterion for the distribution of random variables is given [10].

Table 1. "Chi-square" criterion table

	$p=1\%$	$p=5\%$	$p=25\%$	$p=50\%$	$p=75\%$	$p=95\%$	$p=99\%$
$N=1$	0.00016	0.00393	0.1015	0.4549	1.323	3.841	6.635
$N=2$	0.02010	0.1026	0.5754	1.386	2.773	5.991	9.210
$N=3$	0.1148	0.3518	1.213	2.366	4.108	7.815	11.34
$N=4$	0.2971	0.7107	1.923	3.357	5.385	9.488	13.28
$N=5$	0.5543	1.1455	2.675	4.351	6.626	11.07	15.09
$N=6$	0.8721	1.635	3.455	5.348	7.841	12.59	16.81
$N=7$	1.239	2.167	4.255	6.346	9.037	14.07	18.48
$N=8$	1.646	2.733	5.071	7.344	10.22	15.21	20.09
$N=9$	2.088	3.325	5.899	8.343	11.39	16.92	21.67

$N=10$	2.558	3.940	6.737	9.342	12.55	18.31	23.21
$N=11$	3.053	4.575	7.584	10.34	13.70	19.68	24.72
$N=12$	3.571	5.226	8.438	11.34	14.85	21.03	26.22
$N=15$	5.229	7.261	11.04	14.34	18.25	25.00	30.58
$N=20$	8.260	10.585	15.45	19.34	23.83	31.41	37.57
$N=30$	14.95	18.49	24.48	29.34	34.80	43.77	50.89
$N=50$	29.71	34.76	42.94	49.33	56.33	67.50	76.15
$N > 50$	$v + \sqrt{2vx_p} + \frac{2}{3}x_p^2 - \frac{2}{3} + O\left(\frac{1}{\sqrt{v}}\right)$						
$x_p=8$	-2.33	-1.36	-0.674	0.00	0.674	1.64	2.33

Let a pseudo-random sequence of bits with a period $\lambda = 2^t$ be generated, where t – number is determined by the number of bits, depending on the length of the period.

To check the degree of randomness of the bits in a pseudo-random sequence block, the following is first defined:

1. The possible elements contained in the pseudo-random bit sequence are “0” and “1”, i.e. (s): 0, 1;
2. The probability that these elements are contained / appear in a block of a pseudo-random sequence are
(p_s): $\frac{1}{2}, \frac{1}{2}$;
3. Observed number (Y_s): N_0, N_1 ; where N_0 and N_1 ; where and the number of zeros "0" and ones "1" in the original block of bits with the length $\lambda = 2^t$ of the pseudo-random sequence $c_1c_2c_3c_4 \dots c_8c_9 \dots$ and equality $N_0 + N_1 = \lambda$ takes place;
4. Observed number (λp_s): $\frac{\lambda}{2}, \frac{\lambda}{2}$; in tabular form is expressed

s	0	1
p_s	$\frac{1}{2}$	$\frac{1}{2}$
Y_s	N_0	N_1
λp_s	$\frac{\lambda}{2}$	$\frac{\lambda}{2}$

The "Chi-square" value of the distribution is calculated by the formula:

$$V = \sum_{s=0}^{k-1} \frac{(Y_s - np_s)^2}{np_s}$$

In this case: $k = 2$; $s \in \{0;1\}$; $p_0 = p_1 = \frac{1}{2}$; $Y_0 = N_0$; $Y_1 = N_1$; $n = \lambda = 2^t$; therefore,

according to the formula, there is
$$V = \frac{(Y_0 - 2^{t-1})^2 + (Y_1 - 2^{t-1})^2}{2^{t-1}}.$$

Although, on the basis of the "Chi-square" criterion, a positive result was obtained by chance, it will not be superfluous to check for other tests. The more positive answers the better [11].

Let us briefly stop to check the degree of randomness of a pair of bits in the gamma key sequence block. For this, the following parameters are first defined:

1. Possible elements contained in the pseudo-random sequence of a pair of bits are "00", "01", "10" and "11", i.e. (s): 00, 01, 10, 11;
2. The probability that these elements are contained / appear in a block of a pseudo-random sequence are (P_s): $\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}$;
3. Observed number (Y_s): $N_{00}, N_{01}, N_{10}, N_{11}$; where N_{00}, N_{01} and N_{11} – is the number of elements "00", "01", "10" and "11" in the original block of bits with the length $\lambda = 2^t$ of the pseudo-random sequence $c_1c_2c_3c_4 \dots c_8c_9 \dots$, and equality $N_{00} + N_{01} + N_{10} + N_{11} = \frac{\lambda}{2}$ takes place;
4. Observed number (λp_s): $\frac{\lambda}{8}, \frac{\lambda}{8}, \frac{\lambda}{8}, \frac{\lambda}{8}$; in tabular form is expressed

s	0	1	2	3
p_s	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
Y_s	N_{00}	N_{01}	N_{10}	N_{11}
$\frac{\lambda}{2} p_s$	$\frac{\lambda}{8}$	$\frac{\lambda}{8}$	$\frac{\lambda}{8}$	$\frac{\lambda}{8}$

Having the following parameter values:

$$k = 4; s \in \{00; 01; 10; 11\}; \quad p_0 = p_1 = p_2 = p_3 = \frac{1}{4}; \quad Y_0 = N_{00}; Y_1 = N_{01}; Y_2 = N_{10};$$

$$Y_3 = N_{11}; \quad n = \frac{\lambda}{2} = 2^{t-1}; \quad N = k - 1 = 4 - 1 = 3; \text{ it is possible to implement the application of}$$

"Chi-square" criterion to determine the degree of randomness, the sequence of a pair of bits in a block of a pseudo-random sequence, similarly as above.

5 Analysis of the obtained results

Thus, the necessary conditions for ensuring the strength of continuous encryption algorithms, their substantiated properties, mathematical approaches and models for checking the given necessary strength conditions, the proposed cryptographic principles and tools allow for correct research of algorithm transformations.

A method for finding the length of the period of a pseudo-random sequence has been determined.

A model of the method of practical application "Chi-square" of the criterion for determining the degree of randomness of elements or their combinations in the block of the generated pseudo-random sequence has been developed [12-18].

6 Conclusion

1. Having determined the number of all kinds of logical operations on bits and analyzing their features, those that have the properties of cryptographic resistant were identified;
2. Based on the transformation of table replacement: two, three, nibble, byte, etc. connections of the encrypted message and the key block, the necessary and sufficient conditions and methods for the development of classes of cryptographic algorithms have been established;
3. The conditions for cryptographic resistant of the transformation of a table replacement are justified by the regularity of their truth table and replacement, ie. with uniform distribution of cipher values in the corresponding tables;
4. A universal method (rule) for constructing a model of Boolean functions according to a truth table with Zhegalkin polynomials has been determined, in the case of one-to-one and multiple-valued inputs and outputs of transformations;
5. The effectiveness of the proposed new cryptographic algorithms is confirmed by the following: work without interruption, convenient and inexpensive implementation in hardware and software.

The results obtained make it possible to effectively and scientifically study the strength of continuous encryption algorithms. Mathematical approaches, methods and models, cryptographic principles and tools, allow you to study cryptographic transformations according to appropriate criteria.

The analysis of the transformations of the algorithms of the continuous encryption class according to the criteria of the formulated assertion in a systematic manner is periodically deepened and expanded with the development of achievements in science, computer technology and the development of technologies.

References

1. Alferov, A. P., Zubov, A. Y., Kuzmin, A. S., & Cheremushkin, A. V. (2002). *Foundations of cryptography*. Gelios ARB, Moscow.
2. Kharin, Y. S., Bernik, V. I., Matveev, G. V., & Agievich, S. V. (2003). *Mathematical and Computer Foundations of Cryptology*. Novoye Znaniye, Minsk.
3. Akbarov, D., & Abdukadirov, A. (2022, June). Research of general mathematical characteristics of logical operations and table replacements in cryptographic transformations. In *AIP Conference Proceedings* **2432**, **1**.
4. Moldovyan, A. A., Moldovyan, N. A., & Sovetov, B. Y. (2001). *Cryptography. Speed Ciphers*, 496.
5. Sobti, R., & Geetha, G. (2012). Cryptographic hash functions: a review. *International Journal of Computer Science Issues (IJCSI)*, **9(2)**, 461.
6. Wang, M., Duan, M., & Zhu, J. (2018, May). Research on the security criteria of hash functions in the blockchain. In *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts* (pp. 47-55).
7. Akbarov, D., Umarov, S., Turdimatov, M., Sotvoldiyev, K., Ibrokhimov, N., & Sadirova, K. (2024, November). *E3S Web of Conferences* **508**, 03009.
8. Umarov, S. (2024, May). *AIP Conference Proceedings* **3147**, **1**.

9. Alfrhan, A., Moulahi, T., & Alabdulatif, A. (2021). Comparative study on hash functions for lightweight blockchain in Internet of Things (IoT). *Blockchain: Research and Applications*, **2(4)**, 100036.
10. Turdimatov, M., Xusanova, M., Sadirova, X., Abdurakhmonov, S., & Bilolov, I. (2024, November). On the method of approximation and quantization of information transmission through communication channels. In *E3S Web of Conferences* (Vol. **508**, p. 03007). EDP Sciences.
11. Turdimatov, M., Mukhtarov, F., Ibrokhimov, N., Umarov, S., Mirzayev, J., & Rakhmatov, R. (2024). Mathematical approximator based on basic spline approximation. In *E3S Web of Conferences* (Vol. **508**, p. 04010). EDP Sciences.
12. Windarta, S., Suryadi, S., Ramli, K., Pranggono, B., & Gunawan, T. S. (2022). Lightweight cryptographic hash functions: design trends, comparative study, and future directions. *IEEE Access*, **10**, 82272-82294.
13. Madaliev, M., Usmonov, M., Fayzullaev, J., Khusanov, Y., Radjapov, K., Sattorov, A., & Jalilov, I. (2024). Numerical study of 2D and 3D flow after NASA 4412 airfoil. In *E3S Web of Conferences* (Vol. **538**, p. 01012). EDP Sciences.
14. Madaliev, M., Usmonov, M., Ismoilov, M., Bilolov, I., Israilov, S., Abdullajonova, N., & Rajabova, K. (2024). Analysis of jet currents using the SST turbulence model. In *E3S Web of Conferences* (Vol. **538**, p. 01019). EDP Sciences.
15. Madaliev, M., Usmonov, M., Umirzakov, Z., Usmonov, S., Ismoilov, M., Adilov, Z., & Alimova, N. (2024). Comparison modern of turbulence models for the 2D NASA wall-mounted hump separated flow problem. In *E3S Web of Conferences* (Vol. **538**, p. 01013). EDP Sciences.
16. Madaliev, M., Usmonov, M., Soliyev, O., Otajonov, J., Kadirov, K., Otakhanova, Z., & Mavlonova, D. (2024). Comparison of turbulence models for the axisymmetrical separated boundary layer problem. In *E3S Web of Conferences* (Vol. **538**, p. 01018). EDP Sciences.
17. Ismoilov, M. M., Obidova, G., Juraeva, M., Meliqo'ziev, A., Maxkamova, D., Toshpo'latova, M. (2024) *E3S Web of Conferences* **508**, 06002.
<https://doi.org/10.1051/e3sconf/202450806002>
18. Rayimdjhanov, O., Mukhtarov, F., Ismoilov, M. M., Abdusamatov, H., Abdullaeva, M., Madaminov, M. (2024) *E3S Web of Conferences* **508**, 01004.
<https://doi.org/10.1051/e3sconf/202450801004>
19. Payzullaxanov, M. S., Salomov, U., Kuchkarov, A., Mamatov, O., & Xolmatov, A. (2024). Crystal structure and magnetic properties ferrites Ba-Fe-O, Bi-Fe-O, synthesized in NGO "Physics-Sun". In *BIO Web of Conferences* (Vol. **84**, p. 05030). EDP Sciences.
20. Abdulkhaev, Z. E., Madraximov, M. M., Orzimatov, J. T., & Abdurazaqov, A. M. (2023). Transition processes during the start-up of the pumping unit of happ. In *E3S Web of Conferences* (Vol. **420**, p. 07023). EDP Sciences.
21. Abdivakhidova, N., & Salomov, U. (2024, March). Topological modeling and simulation of large-scale natural gas network. In *AIP Conference Proceedings* (Vol. **3045**, **1**). AIP Publishing.
22. Khujaev, P., Abdulkhaev, Z., Numonjonov, S., Karimov, N., & Akhunov, K. (2024). Modernization of existing infrastructure, heat supply systems. In *E3S Web of Conferences* (Vol. **538**, p. 01010). EDP Sciences.
23. Abdulkhaev, Z., Madraximov, M., Abdujalilova, S., Mirzababayeva, S., Otakulov, B., Sattorov, A., & Umirzakov, Z. (2023). Flow trajectory analysis and velocity

- coefficients for fluid dynamics in tubes and holes. In E3S Web of Conferences (Vol. **452**, p. 02010). EDP Sciences.
24. Madraximov, M., Abdulkhaev, Z., Ibrokhimov, A., & Mirababaeva, S. (2024, June). Numerical simulation of laminar symmetric flow of viscous fluids. In AIP Conference Proceedings (Vol. **3119**, **1**). AIP Publishing.
 25. Khujaev, P., Bokiev, B., Kholmurotov, T., Murodov, P., Yakubov, A., & Said, M. T. (2024). Innovative approaches to the feasibility study of options for calculation schemes of water supply. In E3S Web of Conferences (Vol. **538**, p. 03019). EDP Sciences.