computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

# STUDIES ON STATISTICAL ANALYSIS AND PERFORMANCE EVALUATION FOR SOME STREAM CIPHERS

Ivan Gorbenko [1,2], Alexandr Kuznetsov [1,2], Yurii Gorbenko [1,2], Serhii Vdovenko [3], Vladyslav Tymchenko [1,2], Maria Lutsenko [1,2]

[1] V. N. Karazin Kharkiv National University, Svobody sq., 6, Kharkiv, 61022, Ukraine
[2] JSC "Institute of Information Technologies", Bakulin St., 12, Kharkiv, 61166, Ukraine, gorbenkoi@iit.kharkov.ua, kuznetsov@karazin.ua, gorbenkou@iit.kharkov.ua, tvlad.tyma@gmail.com, lutsenko.maria.kh@gmail.com
[3] Ivan Chernyakhovsky National Defense University of Ukraine, Povitroflotsky avenue, 28, Kyiv-049, 03049, Ukraine

**Paper history:**
Received 20 November 2018
Received in revised form 17 March 2019
Accepted 22 March 2019
Available online 31 March 2019

**Keywords:**
stream cipher;
encryption;
pseudorandom sequence;
statistical analysis;
performance evaluation.

**Abstract:** This paper presents the results of the comparative analysis of safety statistics and performance of encryption, the Strumok stream symmetric cipher (proposed for the national encryption standard of Ukraine) with other known cryptographic transformation algorithms, such as SALSA20, SNOW2.0, HC, AES with usages in stream mode, etc. They are accepted as national, international standards or are presented by the New European Schemes for Signatures, Integrity, and Encryptions (NESSI), Cryptography Research and Evaluation Committees (CRYPTREC) and others. The result of safety statistics is an analysis of the cryptographic properties of the output sequences using statistical test sets developed by the National Institute of Standards and Technology (NIST STS) and the DIEHARD tests. The result of the study of performance is the evaluation of the use of central processing unit (CPU) time to convert one octet of data to 64-bit computing platforms, following the test profile used in the eSTREAM contest.

## 1. INTRODUCTION

Today, due to intensive development and improvement of technology, society has more opportunities for social interaction, processing, and transmission of information that can serve the interests of individuals, corporations or states. Therefore, in today's world, knowledge in various fields of activity and a person's life plays an important role that requires multiple means of protection, provided service privacy policy in information and telecommunication systems.

Currently, in cryptography, there are several groups of cryptographic transformations, namely, symmetric and asymmetric encryption. The cryptographic primitives of symmetric encryption use cryptographic conversion methods for open text and the same secret key for cipher text (for example, block and stream algorithms), while cryptographic primitives for asymmetric encryption use a pair of keys that are interconnected [1].

Special attention has been paid to stream cryptographic transformations that are designed to protect information and telecommunication systems and technologies in most cryptographic applications, including generation of pseudorandom sequences, encryption for information and telecommunication systems, as well as for ensuring the confidentiality and integrity of information for cryptographic authentication protocols, electronic signatures and other services [2]. Implementation of international projects such as eSTREAM [3], NESSIE, CRYPTREC (in Japan) [4] proves this. They are aimed at the development and research of encryption algorithms that would provide a high level of cryptographic stability, high performance and function on various computing platforms. Because of these projects, national and international standards for cryptographic transformation were adopted.

The list of studied stream cryptographic transformation algorithms is shown in Table 1, which provides brief information on ciphers and membership of relevant standards or projects. For comparison, symmetric block ciphers such as AES are also attached, which can be used in stream mode.

## 2. STATISTICAL PROPERTIES

### 2.1 GENERAL DESCRIPTION

One of the critical indicators of stream ciphers is cryptographic resistance – a maximum period generating pseudorandom sequences, as the availability period of a pseudorandom sequence is a significant drawback to the statistical random sequences. For example, if a cipher has a small generation period, then it is evident that its value may be easily predicted; hence, the sequence period should be large and much larger than the expected length of the open message [15].

For the experimental research of cryptographic properties, statistical tests were used, such as NIST STS [16] and DIEHARD [17], for values of output sequences.

They aim to verify the hypothesis of the random nature of the original sequence of the studied cryptographic algorithm that generates the data, which is not different in a statistical sense from some hypothetical "random" sequence.

**Table 1. List of studied algorithms for stream cryptographic transformation**

| The name of the cipher | Specified | State size, bit | Key size, bit | The size of the initialization vector, bit |
|---|---|---|---|---|
| AES | FIPS-197, CRYPTREC, ISO/IEC 18033-3 [5] | 128 | 128 | 128 |
| | | 256 | 256 | 256 |
| CRYPTMT3 | eSTREAM | 128 | 128 | 64 |
| DECIM | ISO/IEC 18033-4 [6], eSTREAM | 288 | 128 | 128 |
| ENOCORO [7] | CRYPTREC | 272 | 128 | 64 |
| GRAIN [8] | eSTREAM | 128 | 128 | 96 |
| HC [9] | eSTREAM | 128 | 128 | 128 |
| | | 256 | 256 | 256 |
| KCIPHER-2 | CRYPTREC, ISO/IEC 18033-4 | 640 | 128 | 128 |
| MICKEY2 [10] | eSTREAM | 160 | 128 | 128 |
| MUGI | ISO/IEC 18033-4 | 128 | 128 | 128 |
| RABBIT [11] | eSTREAM, ISO/IEC 18033-4 | 513 | 128 | 64 |
| RC4 | IETF | 256 | 256 | – |
| SALSA20 | eSTREAM | 512 | 128 | 64 |
| SNOW2.0 [12] | NESSIE, ISO/IEC 18033-4 | 512 | 128 | 128 |
| | | | 256 | 256 |
| SOSEMANUK | eSTREAM | 512 | 128 | 128 |
| STRUMOK | IEEE International Conference on Dependable Systems [13, 14] | 1024 | 256 | 256 |
| | | | 512 | |
| TRIVIUM | eSTREAM | 288 | 80 | 80 |

### 2.2 NIST STS

The NIST STS package was designed during the AES competition for the study of random or pseudo-random numbers generators and is the most common tool for assessing the statistical security of cryptographic primitives. Using this package allows us to determine how closely the cryptographic algorithms are compared with the generators of "random" sequences, that is, with a high probability to confirm whether the resulting series is statistically safe.

The package contains 15 tests [18], but in reality, depends on the input parameters, 188 probabilities ($P_1$,$P_2$,...,$P_{188}$) are calculated that can be considered as the result of the work of individual tests. For statistical testing of pairs (the random key and initialisation vector), 100 sequences in length of $10^6$ bits are generated. The mathematical expectation of the number of passed tests by the studied generator is shown in Tables 2 and 3, where:

M – the evaluation of the mathematical expectation of the number of passed tests;

S – the assessment of the average deviation of the results testing the number of passed tests.

Their high cryptographic properties confirm the given results of testing of different ciphers. In particular, all cryptographic transformations studied showed a large number of successfully passed tests: between 130 and 135 tests for probabilities $P_j \geq 0.99$, and from 186 to 188 for expectations $P_j \geq 0.96$ (except CRYPTMT, which received the result of 159).

**Table 2. Results of the NIST STS by criterion $P_j \geq 0.99$**

| The name of the cipher | $M_{099}$ | $S_{099}$ |
|---|---|---|
| AES-128 | 127.07 | 4.44 |
| CRYPTMT | 130.89 | 7.28 |
| DECIM | 132.44 | 4.40 |
| ENOCORO | 132.92 | 7.16 |
| GRAIN | 132.36 | 7.57 |
| HC-256 | 133.75 | 6.04 |
| KCIPHER-2 | 131.29 | 3.32 |
| MICKEY2 | 133.53 | 7.85 |
| MUGI | 132.23 | 7.33 |
| RABBIT | 132.65 | 4.02 |
| RC4 | 133.70 | 8.19 |
| SALSA20 | 134.16 | 5.27 |
| SNOW2.0 | 132.78 | 4.89 |
| SOSEMANUK | 131.73 | 6.99 |
| STRUMOK-256 | 130.01 | 4.86 |
| STRUMOK-512 | 132.83 | 7.52 |
| TRIVIUM | 130.24 | 9.94 |

It is necessary to note high statistical parameters of the Strumok algorithm, which shows specific properties to the random bits generator. In particular, according to the results of Table 2, it is seen that formed pseudorandom sequences in their properties are not inferior to the world-known stream cryptographic algorithms.

## 2.3 DIEHARD

George Marsaglia proposed a set of the DIEHARD statistical tests in 1995. The DIEHARD is considered as a set of experiments with the most stringent criteria for the sequence properties and is intended to characterise the randomness (or lack thereof) in a sequence of integers formed by a specific pseudorandom sequence generator.

**Table 3. Results of the NIST STS by criterion $P_j \geq 0.96$**

| The name of the cipher | $M_{096}$ | $S_{096}$ |
|---|---|---|
| AES-128 | 186.63 | 0.55 |
| CRYPTMT | 158.56 | 2.30 |
| DECIM | 186.44 | 0.96 |
| ENOCORO | 187.17 | 0.89 |
| GRAIN | 186.92 | 1.19 |
| HC-256 | 186.66 | 1.38 |
| KCIPHER-2 | 186.71 | 0.70 |
| MICKEY2 | 186.60 | 1.51 |
| MUGI | 186.50 | 0.99 |
| RABBIT | 187.22 | 0.66 |
| RC4 | 186.30 | 1.27 |
| SALSA20 | 187.00 | 0.99 |
| SNOW2.0 | 186.79 | 0.66 |
| SOSEMANUK | 186.80 | 1.49 |
| STRUMOK-256 | 186.45 | 1.21 |
| STRUMOK-512 | 186.90 | 0.90 |
| TRIVIUM | 187.15 | 1.21 |

A specific feature of the DIEHARD system is the practical orientation of the tests, that is, the basis of some criteria are not theoretical calculations of statistical safety assessment, but the evaluation of the results based on earlier author's practice tests.

In the program implementation of the DIEHARD, depending on the input data, 215 tests are included (the results are seen in Table 4).

**Table 4. Results of the DIEHARD**

| The name of the cipher | Probabilities | | | | |
|---|---|---|---|---|---|
| | $P_j \leq 0.1$ | $0.1 < P_j \leq 0.25$ | $0.25 < P_j \leq 0.75$ | $0.75 < P_j \leq 0.9$ | $P_j > 0.9$ |
| AES-128 | 16 | 37 | 109 | 28 | 25 |
| AES-256 | 15 | 33 | 115 | 31 | 21 |
| CRYPTMT | 21 | 34 | 99 | 36 | 25 |
| DECIM | 25 | 29 | 93 | 42 | 26 |
| ENOCORO | 18 | 36 | 102 | 43 | 16 |
| GRAIN | 17 | 26 | 122 | 31 | 19 |
| HC-128 | 17 | 37 | 103 | 36 | 22 |
| HC-256 | 25 | 33 | 109 | 30 | 18 |
| KCIPHER-2 | 25 | 41 | 90 | 39 | 20 |
| MICKEY2 | 21 | 35 | 104 | 32 | 23 |
| MUGI | 25 | 33 | 107 | 27 | 23 |
| RC4 | 23 | 21 | 104 | 35 | 32 |
| SALSA20 | 17 | 33 | 106 | 27 | 32 |
| SNOW2.0 | 21 | 31 | 112 | 33 | 18 |
| SOSEMANUK | 13 | 25 | 126 | 34 | 17 |
| STRUMOK-256 | 20 | 29 | 113 | 35 | 18 |
| STRUMOK-512 | 26 | 26 | 113 | 28 | 22 |
| TRIVIUM | 24 | 27 | 107 | 35 | 22 |

Even though the Sosemanuk cipher, based on the results of the distribution of probabilities for uniform, shows insignificant, but a little higher, unlike other ciphers, deviation from the uniform distribution, according to the results of the last test, it occupies a leading position. It should be noted that according to statistical analyses of the NIST STS package, KCipher-2 has a high position, but in the DIEHARD test, it takes the last place.

## 3. PERFORMANCE EVALUATION

The stream encryption of a long sequence has the most significant potential advantage over block cryptographic transformations [3, 6, 19-24], which is essential for many applications [25-37].

To test the algorithms the equipment with Intel Core i7-7700 3.6GHz processor was used (first level 64KB cache and second level 1024KB), 32GB DDR3 2133MHz RAM and OS Windows 10. By the chosen method of studying the speed of stream cryptographic transformation in this work, the following parameters are used:

- the rate of encryption of a long sequence (1GB) without taking into account the time of setting the key and the initialisation vector (the results are shown in Table 5);

- the speed of encryption of small data packets (40, 576 and 1500 bytes), taking into account the establishment of a particular value of the initialisation vector (the results see in Tables 6 – 8);

- the speed of initialisation key parameters (the key and the initialisation vector $IV$, the results can be seen in Table 9).

**Table 5. The rate of encryption 1GB data**

| The name of the cipher | Cycles per byte | Mbps |
|---|---|---|
| AES-128 | 9 | 3290 |
| AES-256 | 12 | 2321 |
| DECIM | 1519 | 19 |
| HC-128 | 2 | 15044 |
| HC-256 | 5 | 6152 |
| MICKEY2 | 310 | 93 |
| RABBIT | 6 | 4943 |
| SALSA20 | 8 | 3624 |
| SNOW2.0-128 | 3 | 10663 |
| SNOW2.0-256 | 3 | 10580 |
| SOSEMANUK | 4 | 6476 |
| STRUMOK-256 | 2 | 17406 |
| STRUMOK-512 | 2 | 17631 |
| TRIVIUM | 6 | 5069 |

The results obtained from encryption of long sequences, which are carried out for each algorithm on a key, are shown in Table 5. From the data in the table, it follows that stream ciphers have an undeniable advantage over blocks.

Among the stream algorithms, HC-128, Strumok-256 and Strumok-512 are the fastest.

**Table 6. The speed of encryption by 350 packets of 40 bytes**

| The name of the cipher | Cycles per byte | Mbps |
|---|---|---|
| AES-128 | 13 | 2240 |
| AES-256 | 18 | 1600 |
| DECIM | 2294 | 13 |
| HC-128 | 299 | 97 |
| HC-256 | 1832 | 16 |
| MICKEY2 | 737 | 39 |
| RABBIT | 17 | 1672 |
| SALSA20 | 13 | 2286 |
| SNOW2.0-128 | 13 | 2196 |
| SNOW2.0-256 | 13 | 2154 |
| SOSEMANUK | 16 | 1750 |
| STRUMOK-256 | 17 | 1723 |
| STRUMOK-512 | 17 | 1697 |
| TRIVIUM | 27 | 1057 |

**Table 7. The speed of encryption by 120 packets of 576 bytes**

| The name of the cipher | Cycles per byte | Mbps |
|---|---|---|
| AES-128 | 9 | 3291 |
| AES-256 | 13 | 2160 |
| DECIM | 1600 | 18 |
| HC-128 | 22 | 1280 |
| HC-256 | 130 | 221 |
| MICKEY2 | 342 | 84 |
| RABBIT | 7 | 4424 |
| SALSA20 | 8 | 3477 |
| SNOW2.0-128 | 3 | 8919 |
| SNOW2.0-256 | 3 | 8777 |
| SOSEMANUK | 4 | 6430 |
| STRUMOK-256 | 3 | 9216 |
| STRUMOK-512 | 3 | 10842 |
| TRIVIUM | 8 | 3814 |

**Table 8. The speed of encryption by 50 packets of 1500 bytes**

| The name of the cipher | Cycles per byte | Mbps |
|---|---|---|
| AES-128 | 9 | 3297 |
| AES-256 | 13 | 2247 |
| DECIM | 1569 | 18 |
| HC-128 | 10 | 2941 |
| HC-256 | 53 | 545 |
| MICKEY2 | 323 | 89 |
| RABBIT | 6 | 3953 |
| SALSA20 | 8 | 3429 |
| SNOW2.0-128 | 3 | 9836 |
| SNOW2.0-256 | 3 | 9836 |
| SOSEMANUK | 4 | 7595 |
| STRUMOK-256 | 2 | 11538 |
| STRUMOK-512 | 2 | 14634 |
| TRIVIUM | 6 | 4478 |

Analysing the results presented in Tables 6–8, it should be noted that the advantage of the speed of encryption stream algorithms maintained for packets size of more than 40 bytes. For small packets, the time of internal state initialisation begins to play a significant part in the stream algorithms. As for the comparison of the speed of stream algorithms, it should be emphasised on the advantage of the SNOW2.0 and Strumok generators.

**Table 9. The speed of initialisation key parameters**

| The name of the cipher | Cycles per installation | |
|---|---|---|
| | *Key* | *IV* |
| AES-128 | 0.27 | 50000000 |
| AES-256 | 0.21 | 64285714 |
| DECIM | 34393 | 104668 |
| HC-128 | 11831 | 304321 |
| HC-256 | 72435 | 49697 |
| MICKEY2 | 16751 | 214961 |
| RABBIT | 343 | 10638298 |
| SALSA20 | 1 | 5000000000 |
| SNOW2.0-128 | 320 | 11363636 |
| SNOW2.0-256 | 319 | 11363636 |
| SOSEMANUK | 422 | 8474576 |
| STRUMOK-256 | 407 | 8771930 |
| STRUMOK-512 | 394 | 9090909 |
| TRIVIUM | 834 | 4310345 |

According to the results of the studies presented in Table 9, it should be noted the advantage of the Salsa20 cipher. The HC algorithm, which showed good results of the speed, it has the shortest time of installation a key, but the time it takes to initialise the vector, is the most. The Strumok algorithm has average values for this criterion.

## 4. CONCLUSIONS

The symmetric stream ciphers play an essential role in the processes of cryptographic protection of information. They have a high speed of cryptographic transformation, especially for use with large encryption amounts of the input data.

The results obtained from comparative studies have shown that the stream algorithms significantly exceed block ciphers by the speed of encryption in large packets. Among the stream algorithms, the Strumok generator, whose structure is targeted at applications in a modern 64-bit computing system, has the advantage of giving the highest values. In particular, the Intel Core i7-7700 3.6GHz and OS Windows 10 have reached 16 – 18Gbps encryption speeds.

With small encryption packets, the computational efficiency of the stream ciphers decreases, and for packets size of 40 bytes block ciphers become faster. When comparing the stream algorithms, the Strumok generator that stably shows a high encryption speeds has the advantage.

The study of the initialisation time of cryptographic algorithms didn't show the advantage of block or stream algorithms. And although with the increased size of processed data, the initialisation time plays a tiny part in the process of encryption, this parameter should also to be given attention. In particular, according to our research, the most significant advantage over the initialisation time has the Salsa20 cipher.

Generalising the results, it should be noted that the Strumok keystream generator in most cases showed better results. When implemented on a 64-bit computing platform, it provides a tremendous speed of encryption and can be recommended for practical application in the modern information and telecommunication systems.

## 7. REFERENCES

[1] N. Ferguson, B. Schneier, *Practical Cryptography*, John Wiley & Sons, 2003, 432p.

[2] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997, 794 p.

[3] *The eSTREAM Project*, 2004, [Online]. Available: http://www.ecrypt.eu.org

[4] *Cryptography Research and Evaluation Committees*, CRYPTREC, 2005, [Online]. Available: http://www.cryptrec.go.jp

[5] *ISO/IEC 18033-3:2010. Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*, 2012. [Online]. Available: https://www.iso.org

[6] *ISO/IEC 18033-4:2011. Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers*, 2012. [Online]. Available: http://www.iso.org

[7] *ISO/IEC 29192-3:2012. Information technology-Security techniques-Lightweight cryptography-Part 3: Stream ciphers*, [Online]. Available: https://www.iso.org

[8] *The eSTREAM Project – eSTREAM Phase 3. Grain (Portfolio Profile 2)*. [Online]. Available: http://www.ecrypt.eu.org

[9] *The eSTREAM Project - eSTREAM Phase 3. HC (Portfolio Profile 1)*. [Online]. Available: http://www.ecrypt.eu.org

[10] *The eSTREAM Project - eSTREAM Phase 3. MICKEY (Portfolio Profile 2)*. [Online]. Available: http://www.ecrypt.eu.org

[11] *The eSTREAM Project - eSTREAM Phase 3. Rabbit (Portfolio Profile 1)*. [Online]. Available: http://www.ecrypt.eu.org

[12] *The eSTREAM Project - eSTREAM Phase 3. Salsa20 (Portfolio Profile 1)*. [Online]. Available: http://www.ecrypt.eu.org

[13] I. Gorbenko, O. Kuznetsov, Y. Gorbenko, A. Alekseychuk, V. Tymchenko, "Strumok keystream generator," *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kiev, 2018, pp. 294-299.

[14] D. D. Ismoyo, R. W. Wardhani, "Block cipher and stream cipher algorithm performance comparison in a personal VPN gateway," *Proceedings of the 2016 International Seminar on Application for Technology of Information and Communication (ISemantic)*, Semarang, 2016, pp. 207-210.

[15] I. Gorbenko, A. Kuznetsov, M. Lutsenko, D. Ivanenko, "The research of modern stream ciphers," *Proceedings of the 4th International Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, 2017, pp. 207-210.

[16] D. Moody, "Post-quantum cryptography: NIST's plan for the future," *Proceedings of the Seventh International Conference on Post Quantum Cryptography*, Japan, 2016. [Online]. Available: https://pqcrypto2016.jp

[17] *The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness*. [Online]. Available: http://stat.fsu.edu/pub/diehard

[18] Special Publication 800-22. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. [Online]. Available: http://csrc.nist.gov

[19] *eSTREAM Optimized Code HOWTO*, 2005. [Online]. Available: http://www.ecrypt.eu.org

[20] A. Andrushkevych, Y. Gorbenko, O. Kuznetsov, R. Oliynykov, M. Rodinko, "Prospective lightweight block cipher for green IT engineering," in: V. Kharchenko, Y. Kondratenko, J. Kacprzyk (eds) *Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control*, vol 171, Springer, Cham, 2019, pp. 95-112.

[21] M. Robshaw, O. Billet, *New stream cipher designs: The eSTREAM Finalists*, Berlin, 2008.

[22] O. Kuznetsov, O. Potii, A. Perepelitsyn, D. Ivanenko, N. Poluyanenko, "Lightweight stream ciphers for green IT engineering," In: V. Kharchenko, Y. Kondratenko, J. Kacprzyk (eds) *Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control*, vol 171. Springer, Cham, 2019, pp. 113-137.

[23] V.I. Dolgov, I.V.Lisitska, K.Ye. Lisitskyi, "The new concept of block symmetric ciphers design," *Telecommunications and Radio Engineering*, vol. 76, issue 2, pp. 157-184, 2017.

[24] A. A. Zadeh, H. M. Heys, "Application of simple power analysis to stream ciphers constructed using feedback shift registers," *The Computer Journal*, vol. 58, no. 4, pp. 961-972, April 2015.

[25] O. Potii, Y. Gorbenko, K. Isirova, "Post quantum hash based digital signatures comparative analysis. Features of their implementation and using in public key infrastructure," *Proceedings of the 2017 4th International Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 105-109.

[26] K. Lisickiy, V. Dolgov, I. Lisickaya, "Cipher with improved dynamic indicators of the condition of a random substitution," *Proceedings of the 2017 4th International Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 396-399.

[27] A. Vambol, V. Kharchenko, O. Potii, N. Bardis, "McEliece and Niederreiter cryptosystems analysis in the context of postquantum network security," *Proceedings of the 2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)*, Corfu, 2017, pp. 134-137.

[28] A. Yanko, S. Koshman, V. Krasnobayev, "Algorithms of data processing in the residual classes system," *Proceedings of the 2017 4th International Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 117-121.

[29] C. Carlet et al., "Analysis of the algebraic side channel attack," *Journal of Cryptographic Engineering*, vol. 1, no. 2, pp. 45-62, 2012.

[30] V. Krasnobayev, A. Kuznetsov, S. Koshman, S. Moroz, "Improved method of determining the alternative set of numbers in residue number system," In: O. Chertov, T. Mylovanov, Y. Kondratenko, J. Kacprzyk, V. Kreinovich, V. Stefanuk (eds) *Recent Developments in Data Science and Intelligent Analysis of Information. ICDSIAI 2018. Advances in Intelligent Systems and Computing*, vol. 836, Springer, Cham, 5 August 2018, pp. 319-328.

[31] A. R. Kazmi, M. Afzal, M. F. Amjad, A. Rashdi, "Combining algebraic and side channel attacks on stream ciphers," *Proceedings of the 2017 International Conference on Communication Technologies (ComTech)*, Rawalpindi, 2017, pp. 138-142.

[32] S. Rassomakhin, A. Kuznetsov, V. Shlokin, I. Belozertsev, R. Serhiienko, "Mathematical model for the probabilistic minutia distribution

in biometric fingerprint images," *Proceedings of the 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP)*, Lviv, Ukraine, 2018, pp. 514-518.

[33] T. Grinenko, O. Nariezhnii, "The method of constructing the randomness extractor of a quantum random number generator on the basis of multimodulo transformation," *Proceedings of the 2017 4th International Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 167-172.

[34] D. P. Upadhyay, P. Sharma, S. Valiveti, "Randomness analysis of A5/1 Stream Cipher for secure mobile communication," *International Journal of Computer Science & Communication*, vol. 3, pp. 95-100, 2014.

[35] K. Isirova, O. Potii, "Decentralized public key infrastructure development principles," *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kiev, 2018, pp. 305-310.

[36] D. Upadhyay, T. Shah, P. Sharma, "Cryptanalysis of hardware based stream ciphers and implementation of GSM stream cipher to propose a novel approach for designing n-bit LFSR stream cipher," *Proceedings of the 2015 19th International Symposium on VLSI Design and Test*, Ahmedabad, 2015, pp. 1-6.

[37] P. Pillai, S. Pote, "Physical layer security using stream cipher for LTE," *Proceedings of the 2015 IEEE Bombay Section Symposium (IBSS)*, Mumbai, 2015, pp. 1-5.

***Ivan D. Gorbenko,*** *Doctor of Sciences (Engineering), Full Professor, Academician of the Academy of Applied Radio-electronics Sciences, Professor of the V. N. Karazin Kharkiv National University. Areas of scientific interests: applied cryptology, post-quantum cryptography and authentication.*

***Alexandr A. Kuznetsov,*** *Doctor of Sciences (Engineering), Full Professor, Academician of the Academy of Applied Radio-electronics Sciences, Professor of the V. N. Karazin Kharkiv National University. Areas of scientific interests: cryptography, coding and steganography.*

***Yurii I. Gorbenko,*** *Candidate of Sciences (Engineering), Researcher, Academician of the Academy of Applied Radio-electronics Sciences, Researcher of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: applied cryptology, methods of information security in computer systems.*

***Serhii G. Vdovenko,*** *Associate Professor of the Communication and Information Systems Department of Information Technologies Institute, Ivan Chernyakhovsky National Defense University of Ukraine, colonel. Science interest: information security, information security, countermeasures against the electronic warfare, cybersecurity and cyber warfare.*

***Vladyslav A. Tymchenko,*** *Master of Technology degrees in Cybersecurity with Honours from V. N. Karazin Kharkiv National University in 2018. Researcher of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Science interest: post-quantum cryptography, network, artificial intelligence.*

***Maria S. Lutsenko,*** *Master of Technology degrees in Cybersecurity with Honours from V. N. Karazin Kharkiv National University in 2019. Researcher of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Science interest: post-quantum cryptography and authentication, security information systems and technologies.*