UDC 003.26:004.056.55
DOI https://doi.org/10.32689/maup.it.2023.1.3

Nikolai VASILENKO
Doctor of Physical and Mathematical Sciences, Doctor of Law, Full Professor, Professor at the Department of Cybersecurity, National University "Odessa Law Academy", 28 Richelevskaya St., Odessa, Ukraine, postal code 65011 (vasylenko.it@journals.maup.kiev.ua)
ORCID: 0000-0002-8555-5712

Anton SYSOIENKO
Ph. D. Student at the Department of Information Security and Computer Engineering, Cherkasy State Technological University, 460 Shevchenko Blvd., Cherkasy, Ukraine, postal code 18006 (Ampere859@gmail.com)
ORCID: 0000-0002-6154-8411

Микола ВАСИЛЕНКО
доктор фізико-математичних наук, доктор юридичних наук, професор, професор кафедри кібербезпеки, Національний університет «Одеська юридична академія», вул. Рішельєвська, 28, Одеса, Україна, індекс 65011 (vasylenko.it@journals.maup.kiev.ua)

Антон СИСОЄНКО
аспірант кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, б-р Шевченка, 460, Черкаси, Україна, індекс 18006 (Ampere859@gmail.com)

Bibliographic description of the article: Vasilenko, M., Sysoienko, A. (2023). Metod pidvyshchennia stiikosti psevdovypadkovykh poslidovnostei, syntezovanykh na osnovi operatsii dodavannia za modulem [Method for increasing the stability of pseudorandom sequences synthesized on the basis of modulo addition operations]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 1 (7), 21–28. DOI: https://doi.org/10.32689/maup.it.2023.1.3

Бібліографічний опис статті: Василенко, М., Сисоєнко, А. Метод підвищення стійкості псевдовипадкових послідовностей, синтезованих на основі операцій додавання за модулем. *Інформаційні технології та суспільство.* 2023. Вип. 1 (7), 21–28. DOI: https://doi.org/10.32689/maup.it.2023.1.3

METHOD FOR INCREASING THE STABILITY OF PSEUDORANDOM SEQUENCES SYNTHESIZED ON THE BASIS OF MODULO ADDITION OPERATIONS

Problems of security and integrity of information in computer systems and networks require special approaches to their solution. Data exchange processes have become much simpler, faster, and some of them are free. Making important decisions in industry, financial and government spheres is no longer possible without processing gigantic arrays of information. Due to the recent events in Ukraine and the world and the increase in the number of attacks on computer systems, it is necessary to solve new tasks of information protection, which are faced by relevant specialists. At the same time, the danger of interference in the operation of information systems for unauthorized reading of information begins to grow. Currently, there is a global transition to an information society, the development of which is inextricably linked with the intensification of information processes, the need to collect, process and transmit huge amounts of information. Informatization has affected all spheres of human activity as a whole: public administration, finance, economy, education, production, etc. A special place in the field of information protection is occupied by tasks, the solution of which has important scientific, technical and national importance. One of these tasks is to increase the efficiency of computer cryptography algorithms due to the development of new microcrypto primitives. Cryptography is one of the ways to combat cybercrime. Various cryptographic encryption methods, which are used to protect information resources that are processed, stored and transmitted in modern information and communication systems and networks, make it possible to sufficiently reliably and effectively protect information from unauthorized access and familiarization with it. Cryptographic protection, that is, the use of text encryption procedure with the help of complex mathematical algorithms, is gaining more and more popularity. The solution of this task will make it possible to improve the existing crypto algorithms and create new ones, the main advantages of which will be high speed and crypto resistance due to the increase in the variability of the encryption process. The paper provides a theoretical substantiation of the effect of improving the quality of statistical characteristics of the resulting pseudorandom sequence, built on the basis of modulo addition of the results of two-bit operations of cryptographic transformation of information. The obtained results are confirmed by statistical portraits of the testing of the studied pseudorandom sequences. The constructed portraits for various parameters of sequence generation have been analyzed.

Key words: *pseudorandom sequence, modulo addition operations, cryptographic transformation, cryptanalysis.*

МЕТОД ПІДВИЩЕННЯ СТІЙКОСТІ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ, СИНТЕЗОВАНИХ НА ОСНОВІ ОПЕРАЦІЙ ДОДАВАННЯ ЗА МОДУЛЕМ

Проблеми захищеності та цілісності інформації в комп'ютерних системах та мережах потребують особливих підходів до їх вирішення. Процеси обміну даними стали набагато простішими, швидшими, а деякі з них – безкоштовними. Прийняття важливих рішень у промисловості, фінансовій і державній сферах уже неможливе без обробки гігантських масивів інформації. У зв'язку з останніми подіями в Україні та світі, збільшенням кількості атак на комп'ютерні системи необхідно вирішувати нові задачі захисту інформації, які постають перед відповідними фахівцями. Водночас почала зростати небезпека втручання в роботу інформаційних систем для несанкціонованого зчитування інформації. Нині відбувається глобальний перехід до інформаційного суспільства, розвиток якого нерозривно пов'язаний з інтенсифікацією інформаційних процесів, необхідністю збору, обробки і передавання величезних обсягів інформації. Інформатизація торкнулася всіх сфер діяльності людини в цілому: державного управління, фінансів, економіки, освіти, виробництва та ін. Особливе місце у сфері захисту інформації посідають задачі, вирішення яких має важливе науково-технічне й загальнодержавне значення. Однією з таких задач є підвищення ефективності алгоритмів комп'ютерної криптографії за рахунок розробки нових мікрокриптопримітивів. Одним із шляхів боротьби з кіберзлочинністю є криптографія. Різноманітні криптографічні методи шифрування, які використовують з метою захисту інформаційних ресурсів, що обробляються, зберігаються та передаються в сучасних інформаційно-комунікаційних системах та мережах, дозволяють досить надійно та ефективно захищати інформацію від несанкціонованого доступу та ознайомлення з нею. Криптографічний захист, тобто використання процедури шифрування тексту за допомогою складних математичних алгоритмів, завойовує все більшу популярність. Вирішення цієї задачі дозволить вдосконалити існуючі криптоалгоритми та створити нові, основними перевагами яких будуть висока швидкість та криптостійкість, обумовлена збільшенням варіативності процесу шифрування. У роботі проведено теоретичне обґрунтування ефекту підвищення якості статистичних характеристик результуючої псевдовипадкової послідовності, побудованої на основі додавання за модулем результатів дворозрядних операцій криптографічного перетворення інформації. Отримані результати підтверджені статистичними портретами тестування досліджуваних псевдовипадкових послідовностей. Виконано аналіз побудованих портретів для різних параметрів формування послідовностей.

Ключові слова: *псевдовипадкова послідовність, операції додавання за модулем, криптоперетворення, криптоаналіз.*

The problem statement. Information today is considered as a strategic product. A significant increase in volumes of information flows in all areas of social relations, which are processed, transmitted and stored with the help of computer systems, is associated with the processing of gigantic arrays of information. Problems of security and integrity of information in computer systems and networks require special approaches to their solution.

Nowadays, technologies for processing and transmitting large volumes of information are gaining more and more importance. If this information belongs to the category of information with limited access, there is an additional requirement for the need to protect it. Cryptographic methods and means of information protection form the basis of ensuring information security in information and telecommunication systems. Uncontrolled distribution and use of software leads to the loss of confidentiality of information resources of citizens and the state as a whole. As a result, the development of information resources is inextricably linked with their security and protection.

It should be taken into account that the most reliable protection is provided only with the help of integrated approach, and the solution of the task of information security should be a set of organizational, technical and cryptographic measures. Thus, the urgency of the problem of ensuring information protection in all spheres of life of a person, society and the state (social, political, economic, military, ecological, scientific and technological, informational ones, etc.) serves as a basis for creating new developments in the field of information security and is considered one of the promising areas of scientific research.

Analysis of recent research and publications. Cryptographic protection is one of the promising areas of scientific research both in our country and abroad in the field of information protection.

A significant contribution to the improvement of existing and development of new methods and means of cryptographic protection of information has been made by the following foreign and domestic scientists: C.E. Shannon, B. Schneier, G. Brassard, J.L. Massey, W. Diffie, M.E. Hellman, R.L. Rivest, A. Shamir, N. Koblitz, O.A. Moldovian, M.A. Moldovian, V.M. Rudnytskyi, I.D. Horbenko, V.K. Zadiraka, M.A. Ivanov, A.N. Fionov, V.V. Yashchenko, O.O. Logachov, B.Ya. Riabko, A.M. Oleksiichuk, L.V. Kovalchuk, A.Ya. Biletskyi, O.H. Korchenko et al.

However, in connection with the development of computer systems, the tasks of increasing the level of information protection and reducing the encryption time have always been and will remain unsolved. The main characteristics of cryptographic systems are stability, speed and reliability of cryptographic transformation, which must be constantly improved. The use of the latest technologies increases the requirements for the quality of original sequences of pseudorandom numbers, which are the basis of ensuring data confidentiality in the development of new methods for cryptographic protection of information for computer cryptography systems [1, 2]. Pseudorandom sequence (PRS) is widely used in modern computer systems to solve such tasks as protection of information from unauthorized access, control of information integrity, generation of signals that provide hidden data transmission, simulation of complex systems and objects [3–5]. The term "random sequence" will mean a sequence generated by a physical process, the result of which is unpredictable and cannot be reproduced. By a pseudorandom sequence of numbers, we will understand a reproducible sequence generated with the help of deterministic algorithm (regardless of the method of its implementation), which has statistical properties with a specified accuracy that repeat all or part of statistical properties of random sequences.

Currently, a number of methods for the synthesis of operations of direct, inverse and mutual cryptographic transformation have been developed [6, 7, 8]. The main advantage of cryptographic transformation is high speed of implementation of crypto algorithms. However, all the possibilities of increasing the stability of cryptographic systems based on cryptographic transformation operations have not been exhausted at the moment. Therefore, there is a need to conduct additional research aimed at developing algorithms for the synthesis of pseudorandom sequences based on the use of cryptographic transformation operations.

Based on quality indicators of pseudorandom sequences specified in [9–11], the assessment of the quality of a pseudorandom sequence synthesized on the basis of operations of cryptographic transformation of information and modulo two addition has been carried out.

In articles [3, 12–15], a study of a pseudorandom number generator based on the use of modulo addition operation of some number *M* of two or more pseudorandom sequences (the period of which is mutually simple), which shows that the combination of sequences leads to an increase in the period and improvement of statistical properties of the resulting pseudorandom sequence, has been conducted.

In articles [16–18], a procedure for the synthesis of pseudorandom sequences based on the use of modulo *M* {2;4} addition operation of $Q \in \{2;3;4;5\}$ results of random two-bit operations of cryptographic transformation of information is considered and experimentally investigated. As a result of these studies, the probability of degeneracy of the resulting transformation operation, which leads to an increase in the stability of cryptographic systems, is empirically determined, and a quantitative indicator of the assessment of the quality of pseudorandom sequence construction according to the specified principle is also proposed.

In works [10, 19, 20] based on quality indicators of pseudorandom sequences, an analysis of methods for assessing the quality of pseudorandom sequences, the synthesis of which was conducted based on the use of operations of modulo two addition for computer cryptography systems, has been carried out.

In [21, 22], it is shown that for practical implementation of a cryptographic algorithm based on the use of the proposed information-driven permutation operations, it is necessary to determine practical cryptographic stability of the algorithm, which directly depends on the password length and the number of operations used to encrypt information.

In [23], the entire sequence of mathematical transformations, which provides the synthesis of a formalized model of the operation, suitable for practical use in crypto primitives, is considered.

The study of the quality of a pseudorandom sequence synthesized on the basis of operations of cryptographic transformation of information is an urgent problem of the modern development of information technologies [24].

The purpose of the article is the theoretical substantiation of the effect of improving the quality of statistical characteristics of the resulting pseudorandom sequence, built on the basis of modulo addition of the results of two-bit operations of cryptographic transformation of information.

Results and discussion. After conducting an analysis of scientific studies of the received sequences for theoretical substantiation of the reasons for the change in their quality, let's formalize the obtained results. For this, we introduce the following notations.

Let $Z = \bigcup z_j$ be a binary information sequence that is divided into combinations of pairs of binary symbols z_j, $j = 1,2,\ldots j$. Coding operations are determined by commands, the number *Q* and the sequence number *i* of which correspond to the number and sequence number of independent cryptographic transformations. Let's denote the operation of two-bit encoding of the *j*-th combination of information sequence for the *i*-th team by $F_{i;Q}^{k}\left(z_j\right)$. Then for $Q = 2$ commands: $F_{1;2}^{k}\left(z_1\right)$ is an operation of two-bit encoding of the first sequence combination for the first command; $F_{2;2}^{k}\left(z_1\right)$ is an operation of two-bit encoding of the first sequence combination for the second command; $F_{1;2}^{k}\left(z_2\right)$ is an operation of two-bit encoding of the second sequence combination for the first command; $F_{2;2}^{k}\left(z_2\right)$ is an operation of two-bit encoding of the second sequence combination for the second command.

Based on the given notations, let's formalize the algorithm for constructing a pseudorandom sequence based on the use of operations of modulo two addition of two transformation results.

Let's denote the operation of two-bit decoding of the *j*-th combination of the sequence for the *i*-th command by $F_{i;Q}^{d}\left(z_j\right)$, and the operations of two-bit encoding and decoding of the *j*-th combination of the sequence by $F_{Q}^{k}\left(z_j\right)$ and $F_{Q}^{d}\left(z_j\right)$. Then for $Q = 2$:

1) if $F_{1;2}^{d}\left(z_1\right) = F_{1;2}^{-k}\left(z_1\right) : F_{1;2}^{k}\left(z_1\right) \times F_{1;2}^{d}\left(z_1\right) = \mathrm{E}$, where E is an unary operator, and $F_{2;2}^{d}\left(z_1\right) = F_{2;2}^{-k}\left(z_1\right) : F_{2;2}^{k}\left(z_1\right) \times F_{2;2}^{d}\left(z_1\right) = \mathrm{E}$, then for $F_{2}^{k}\left(z_1\right) = F_{1;2}^{k}\left(z_1\right) \oplus F_{2;2}^{k}\left(z_1\right)$ and $F_{2}^{d}\left(z_1\right) = F_{2}^{-k}\left(z_1\right)$ it holds: $F_{2}^{k}\left(z_1\right) \times F_{2}^{d}\left(z_1\right) \neq \mathrm{E}$;

2) if $F_{1;2}^{d}(z_2)=F_{1;2}^{-k}(z_2):F_{1;2}^{k}(z_2)\times F_{1;2}^{d}(z_2)=\mathrm{E}$, $F_{2;2}^{d}(z_2)=F_{2;2}^{-k}(z_2):F_{2;2}^{k}(z_2)\times F_{2;2}^{d}(z_2)=\mathrm{E}$, then for $F_{2}^{k}(z_2)=F_{1;2}^{k}(z_2)\oplus F_{2;2}^{k}(z_2)$ and $F_{2}^{d}(z_2)=F_{2}^{-k}(z_2)$ it holds: $F_{2}^{k}(z_2)\times F_{2}^{d}(z_2)\neq \mathrm{E}$;

3) if $F_{1;2}^{d}(z_3)=F_{1;2}^{-k}(z_3):F_{1;2}^{k}(z_3)\times F_{1;2}^{d}(z_3)=\mathrm{E}$, $F_{2;2}^{d}(z_3)=F_{2;2}^{-k}(z_3):F_{2;2}^{k}(z_3)\times F_{2;2}^{d}(z_3)=\mathrm{E}$, then for $F_{2}^{k}(z_3)=F_{1;2}^{k}(z_3)\oplus F_{2;2}^{k}(z_3)$ and $F_{2}^{d}(z_3)=F_{2}^{-k}(z_3)$ it holds: $F_{2}^{k}(z_3)\times F_{2}^{d}(z_3)\neq \mathrm{E}$, etc.

In general case, if $F_{1;2}^{d}(z_j)=F_{1;2}^{-k}(z_j):F_{1;2}^{k}(z_j)\times F_{1;2}^{d}(z_j)=\mathrm{E}$, $F_{2;2}^{d}(z_j)=F_{2;2}^{-k}(z_j):F_{2;2}^{k}(z_j)\times F_{2;2}^{d}(z_j)=\mathrm{E}$, then for $F_{2}^{k}(z_j)=F_{1;2}^{k}(z_j)\oplus F_{2;2}^{k}(z_j)$ and $F_{2}^{d}(z_j)=F_{2}^{-k}(z_j)$ it holds: $F_{2}^{k}(z_j)\times F_{2}^{d}(z_j)\neq \mathrm{E}$.

Let's formalize the algorithm for constructing a pseudorandom sequence based on the use of operations of modulo two addition of three transformation results. Then for $Q=3$:

1) if $F_{1;3}^{d}(z_1)=F_{1;3}^{-k}(z_1):F_{1;3}^{k}(z_1)\times F_{1;3}^{d}(z_1)=\mathrm{E}$, $F_{2;3}^{d}(z_1)=F_{2;3}^{-k}(z_1):F_{2;3}^{k}(z_1)\times F_{2;3}^{d}(z_1)=\mathrm{E}$, $F_{3;3}^{d}(z_1)=F_{3;3}^{-k}(z_1):F_{3;3}^{k}(z_1)\times F_{3;3}^{d}(z_1)=\mathrm{E}$, then for $F_{3}^{k}(z_1)=F_{1;3}^{k}(z_1)\oplus F_{2;3}^{k}(z_1)\oplus F_{3;3}^{k}(z_1)$ and $F_{3}^{d}(z_1)=F_{3}^{-k}(z_1)$ it holds: $F_{3}^{k}(z_1)\times F_{3}^{d}(z_1)\neq \mathrm{E}$;

2) if $F_{1;3}^{d}(z_2)=F_{1;3}^{-k}(z_2):F_{1;3}^{k}(z_2)\times F_{1;3}^{d}(z_2)=\mathrm{E}$, $F_{2;3}^{d}(z_2)=F_{2;3}^{-k}(z_2):F_{2;3}^{k}(z_2)\times F_{2;3}^{d}(z_2)=\mathrm{E}$, $F_{3;3}^{d}(z_2)=F_{3;3}^{-k}(z_2):F_{3;3}^{k}(z_2)\times F_{3;3}^{d}(z_2)=\mathrm{E}$, then for $F_{3}^{k}(z_2)=F_{1;3}^{k}(z_2)\oplus F_{2;3}^{k}(z_2)\oplus F_{3;3}^{k}(z_2)$ and $F_{3}^{d}(z_2)=F_{3}^{-k}(z_2)$ it holds: $F_{3}^{k}(z_2)\times F_{3}^{d}(z_2)\neq \mathrm{E}$;

3) if $F_{1;3}^{d}(z_3)=F_{1;3}^{-k}(z_3):F_{1;3}^{k}(z_3)\times F_{1;3}^{d}(z_3)=\mathrm{E}$, $F_{2;3}^{d}(z_3)=F_{2;3}^{-k}(z_3):F_{2;3}^{k}(z_3)\times F_{2;3}^{d}(z_3)=\mathrm{E}$, $F_{3;3}^{d}(z_3)=F_{3;3}^{-k}(z_3):F_{3;3}^{k}(z_3)\times F_{3;3}^{d}(z_3)=\mathrm{E}$, then for $F_{3}^{k}(z_3)=F_{1;3}^{k}(z_3)\oplus F_{2;3}^{k}(z_3)\oplus F_{3;3}^{k}(z_3)$ and $F_{3}^{d}(z_3)=F_{3}^{-k}(z_3)$ it holds: $F_{3}^{k}(z_3)\times F_{3}^{d}(z_3)\neq \mathrm{E}$, etc.

In general case, if $F_{1;3}^{d}(z_j)=F_{1;3}^{-k}(z_j):F_{1;3}^{k}(z_j)\times F_{1;3}^{d}(z_j)=\mathrm{E}$, $F_{2;3}^{d}(z_j)=F_{2;3}^{-k}(z_j):F_{2;3}^{k}(z_j)\times F_{2;3}^{d}(z_j)=\mathrm{E}$, $F_{3;3}^{d}(z_j)=F_{3;3}^{-k}(z_j):F_{3;3}^{k}(z_j)\times F_{3;3}^{d}(z_j)=\mathrm{E}$, then for $F_{3}^{k}(z_j)=F_{1;3}^{k}(z_j)\oplus F_{2;3}^{k}(z_j)\oplus F_{3;3}^{k}(z_j)$ and $F_{3}^{d}(z_j)=F_{3}^{-k}(z_j)$ it holds: $F_{3}^{k}(z_j)\times F_{3}^{d}(z_j)\neq \mathrm{E}$.

Let's formalize the algorithm for constructing a pseudorandom sequence based on operations of modulo two addition of *Q* transformation results:

1) if for $\forall i\leq Q$ $F_{i;Q}^{d}(z_1)=F_{i;Q}^{-k}(z_1):F_{i;Q}^{k}(z_1)\times F_{i;Q}^{d}(z_1)=\mathrm{E}$, then for $F_{Q}^{k}(z_1)=F_{1;Q}^{k}(z_1)\oplus F_{2;Q}^{k}(z_1)\oplus\ldots\oplus F_{Q;Q}^{k}(z_1)$ and $F_{Q}^{d}(z_1)=F_{Q}^{-k}(z_1)$ it holds: $F_{Q}^{k}(z_1)\times F_{Q}^{d}(z_1)\neq \mathrm{E}$;

2) if for $\forall i\leq Q$ $F_{i;Q}^{d}(z_2)=F_{i;Q}^{-k}(z_2):F_{i;Q}^{k}(z_2)\times F_{i;Q}^{d}(z_2)=\mathrm{E}$, then for $F_{Q}^{k}(z_2)=F_{1;Q}^{k}(z_2)\oplus F_{2;Q}^{k}(z_2)\oplus\ldots\oplus F_{Q;Q}^{k}(z_2)$ and $F_{Q}^{d}(z_2)=F_{Q}^{-k}(z_2)$ it holds: $F_{Q}^{k}(z_2)\times F_{Q}^{d}(z_2)\neq \mathrm{E}$;

3) if for $\forall i\leq Q$ $F_{i;Q}^{d}(z_3)=F_{i;Q}^{-k}(z_3):F_{i;Q}^{k}(z_3)\times F_{i;Q}^{d}(z_3)=\mathrm{E}$, then for $F_{Q}^{k}(z_3)=F_{1;Q}^{k}(z_3)\oplus F_{2;Q}^{k}(z_3)\oplus\ldots\oplus F_{Q;Q}^{k}(z_3)$ and $F_{Q}^{d}(z_3)=F_{Q}^{-k}(z_3)$ it holds: $F_{Q}^{k}(z_3)\times F_{Q}^{d}(z_3)\neq \mathrm{E}$, etc.

In general case, if for $\forall i\leq Q$ $F_{i;Q}^{d}(z_j)=F_{i;Q}^{-k}(z_j):F_{i;Q}^{k}(z_j)\times F_{i;Q}^{d}(z_j)=\mathrm{E}$, then for $F_{Q}^{k}(z_j)=F_{1;Q}^{k}(z_j)\oplus F_{2;Q}^{k}(z_j)\oplus\ldots\oplus F_{Q;Q}^{k}(z_j)$ and $F_{Q}^{d}(z_j)=F_{Q}^{-k}(z_j)$ it holds: $F_{Q}^{k}(z_j)\times F_{Q}^{d}(z_j)\neq \mathrm{E}$.

Thus, as a result of the formalization of algorithms for constructing pseudorandom sequences based on the use of operations of modulo *M* addition of *Q* results of the transformation, dependencies are obtained that confirm the degeneracy of the result regardless of *Q* and *M* values.

Experimental studies have shown that for $Q\in\{2;3;4;5\}$ the values of relative coefficient of the quality of pseudorandom sequence construction reach the values suitable for its practical use.

The essence of the method for increasing the stability of pseudorandom sequences to linear cryptanalysis is due to the following: $F_{Q}^{k}(z_j)\times F_{Q}^{d}(z_j)\neq \mathrm{E}$, where $F_{Q}^{k}(z_j)=F_{1;Q}^{k}(z_j)\oplus F_{2;Q}^{k}(z_j)\oplus\ldots\oplus F_{Q;Q}^{k}(z_j)$, $F_{Q}^{d}(z_j)=F_{Q}^{-k}(z_j)$, and for $\forall i\leq Q$ $F_{i;Q}^{d}(z_j)=F_{i;Q}^{-k}(z_j):F_{i;Q}^{k}(z_j)\times F_{i;Q}^{d}(z_j)=\mathrm{E}$.

Let's check the quality of pseudorandom sequences for resistance to linear cryptanalysis attacks using the system for evaluation of NIST STS statistical properties [25].

Statistical portraits of the results of testing of pseudorandom sequences, obtained on the basis of independent two-bit random operations of the information sequence cryptotransformation followed by modulo two and four addition of the obtained results, are shown in Figures 1–2.

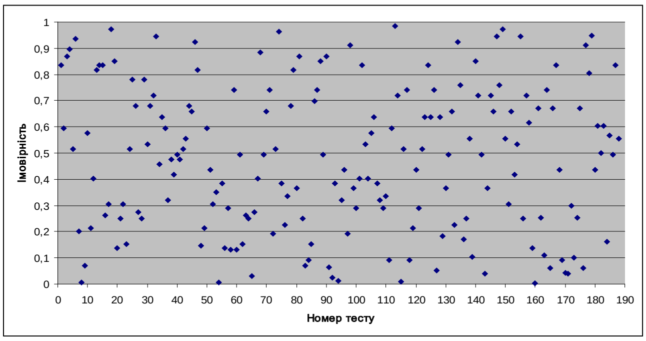

Fig. 1. Statistical portrait of the software implementation of the algorithm of pseudorandom sequence generation for M=2

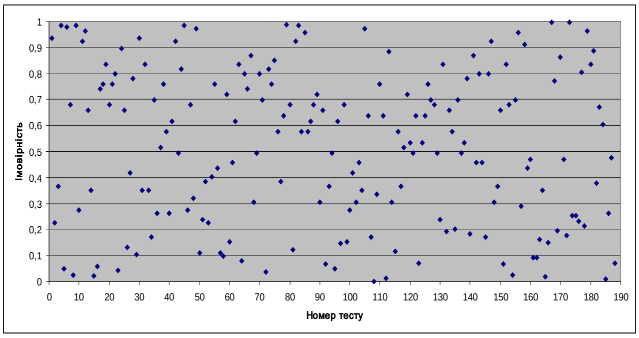

Fig. 2. Statistical portrait of the software implementation of the algorithm of pseudorandom sequence generation for M=4

The analysis of statistical portraits presented in Figures 1 and 2 shows that the pseudorandom sequence obtained on the basis of independent crypto transformation operations with subsequent modulo two addition of the obtained results has slight advantages in terms of resistance to linear cryptanalysis compared to the pseudorandom sequence obtained on the basis of modulo four addition of the results of independent two-bit operations of cryptographic transformation.

An increase in the number of crypto transformation operations leads to a sharp significant decrease in the share of degenerate resulting operations (for *Q*=3) followed by a gradual increase in this share (for *Q*=4 and *Q*=5).

Conclusions and prospects for further research. The presented research has made it possible to obtain the following results:

– algorithms for constructing pseudorandom sequences based on the use of modulo *M* addition operations of *Q* results of independent two-bit cryptographic transformations of the sequence have been formalized;

– dependences that confirm the degeneracy of the result of the synthesis of such sequences regardless of *Q* and *M* values have been obtained;

– the essence of the method for increasing the resistance of the obtained pseudorandom sequences to linear cryptanalysis has been presented, and their testing with the help of NIST tests has also been performed.

Further studies will be conducted to further confirm the improvement of the quality of the obtained result and the possibility of establishing the dependence between the input information and PRS results, as well as the possibility of establishing the dependence of PRS construction. If the dependence is not established, then the built PRS can be used as a damping sequence.

This method will be proposed to be used in further scientific research to solve the task of constructing a discrete model of the synthesis of pseudorandom sequence using available computing tools. In further research, the assessment of the quality of developed method of increasing the stability of pseudorandom sequences to linear cryptanalysis with additional damping and a given number of primary pseudorandom sequences of the transformation will be carried out.

Bibliography:

1. Рудницький В.М., Лада Н.В., Бабенко В.Г. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія / Черкас. держ. технол. ун-т. Харків: ДІСА ПЛЮС, 2018. 184 с.

2. Method for developing pseudo-random number generators for cryptographic applications in 5g networks / S. Gnatyuk, Y. Burmak, R. Berdibayev et al. *Cybersecurity: Education, Science, Technique*: Electronic scientific publication. 2021. No. 4 (12). P. 151–162. URL: https://doi.org/10.28925/2663-4023.2021.12.151162.

3. Фауре Э.В., Щерба А.И., Лавданский А.А. Анализ корреляционных свойств последовательностей (псевдо) случайных чисел. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. № 1 (18) С. 142–150. URL: http://nbuv.gov.ua/j-pdf/Nitps_2015_1_32.pdf.

4. Faure E., Myronets I., Lavdanskyi A. Autocorrelation criterion for quality assessment of random number sequences. *3rd International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020),* (Zaporizhzhia, Apr. 27, 2020 – May 1, 2020). P. 675–689. ISSN: 1613-0073. URL: https://doi.org/10.32782/cmis/2608-52.

5. Faure E., Fedorov E., Myronets I., Sysoienko S. Method for generating pseudorandom sequence of permutations based on linear congruential generator. *Fifth International Workshop on Computer Modeling and Intelligent Systems (CMIS-2022)*, (Zaporizhzhia, May 12, 2022). P. 175–185. ISSN: 1613-0073. URL: https://doi.org/10.32782/cmis/3137-15.

6. Рудницький В.М., Бабенко В.Г., Стабецька Т.А. Узагальнений метод синтезу обернених нелінійних операцій розширеного матричного криптографічного перетворення. *Системи обробки інформації*: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2014. Вип. 6 (122). С. 118–121.

7. Наукоемкие технологии в инфокоммуникациях: обработка и защита информации: кол. монография / под ред. В.М. Безрука, В.В. Баранника. Харьков: Компания СМИТ, 2013. 398 с.

8. Бабенко В.Г., Мельник О.Г., Стабецкая Т.А. Построение нелинейных операций расширенного матричного криптографического преобразования. Криптографическое кодирование: кол. монография / под ред. В.Н. Рудницкого, В.Я. Мильчевича. Харьков: Щедрая усадьба плюс, 2014. С. 41–55.

9. Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. March 2010. 384 p. ISBN: 978-0-470-47424-2.

10. L'Ecuyer P., Simard R., Chen E.J, Kelton W.D. An object-oriented random-number package with many long streams and substreams. *Operations research*. 2002. Vol. 50. No. 6. P. 1073–1075.

11. Буценко Ю., Розоринов Г., Савченко Ю. Общее и селективное тестирование псевдослучайных битовых последовательностей. *Сучасний захист інформації*: наук.-техн. журн. 2014. № 2. С. 16–21.

12. Лавданский А.А. Фауре Э.В. Оценка статистических свойств последовательностей на выходе комбинационного генератора с помощью графических тестов. *Системні дослідження та інформаційні технології*. Київ, 2015. № 2. С. 39–50.

13. Лавданский А.А., Фауре Э.В. Комбинационный метод формирования последовательности псевдослучайных чисел. *Системний аналіз та інформаційні технології (SAIT-2014)*: матеріали 16-ї Міжнар. наук.-техн. конф., (Київ, 26-30 трав. 2014 р.). Київ: ННК «ІПСА» НТУУ «КПІ», 2014. С. 403–404.

14. Фауре Э.В., Щерба А.И., Лавданский А.А. Оценка статистических характеристик последовательности псевдослучайных чисел, порожденной комбинационным генератором. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво.* 2015. № 18. С. 165–171.

15. Лавданський А.О. Оцінка часу формування послідовності псевдовипадкових чисел. *Проблеми інформатизації*: матеріали Четвертої міжнар. наук.-техн. конф., (Черкаси – Баку – Бельсько-Бяла – Полтава). Черкаси: ЧДТУ, 2016. С. 71.

16. Ланських Є.В., Сисоєнко С.В., Пустовіт М.О. Оцінка якості псевдовипадкових послідовностей на основі використання операцій додавання за модулем два. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. № 4 (21). С. 147–150.

17. Фауре Е.В., Сисоєнко С.В., Миронюк Т.В. Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення. *Системи управління, навігації та зв'язку*. Полтава: ПНТУ, 2015. № 4 (36). С. 130–133.

18. Фауре Е.В., Сисоєнко С.В. Оцінка якості псевдовипадкових послідовностей на основі додавання за модулем. *Вісник інженерної академії України*. Київ, 2016. № 3. С. 165–172.

19. Сисоєнко С.В., Сисоєнко А.А. Дослідження та аналіз псевдовипадкових послідовностей для систем комп'ютерної криптографії. *Проблеми інформатизації*: тези доп. сьомої міжнар. наук.-техн. конф., (Черкаси: ЧДТУ; Харків: НТУ «ХПІ», ДП «ПД ПКНДІ АП»; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН, 13–15 листоп. 2019 р.). 2019. Т. 3: секції 5–7. С. 67.

20. Sysoienko A.A., Sysoienko S.V. Investigation of the quality of pseudorandom sequences synthesized on the basis of modulo two addition operations. *Десята міжнародна науково-технічна конференція*: тези доп., (Черкаси: ЧДТУ; Харків: НТУ «ХПІ», ДП «ПД ПКНДІ АП»; Баку: ВА ЗС АР; Бельсько-Бяла, 24–25 листоп. 2022 р.). 2022. Т. 1. С. 85.

21. Бабенко В.Г., Миронюк Т.В., Кривоус Г.В. Алгоритми застосування операцій перестановок, керованих інформацією, для реалізації криптоперетворення інформації. *Вісник Черкаського державного технологічного університету*. 2021. № 3. С. 44–58. URL: https://doi.org/10.24025/2306-4412.3.2021.247252.

22. Захист інформації на основі операцій перестановок, керованих інформацією: монографія / Т.В. Миронюк, С.В. Сисоєнко, В.Г. Бабенко та ін.; Черкас. держ. технол. ун-т. Черкаси: видавець Гордієнко Є.І., 2021. С. 103–164. ISBN: 978-966-97302-2-0.

23. Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation / V. Rudnitsky, R. Berdibayev, R. Breus et al. *Сучасні інформаційні системи*. 2019. Т. 3. № 4. С. 109–114. doi: 10.20998/2522-9052.2019.4.16.

24. Криптографічне кодування: обробка та захист інформації: кол. монографія / під ред. В.М. Рудницького; Черкас. держ. технол. ун-т. Харків: Діса Плюс, 2018. 139 с.

25. Богданов В.В., Паламарчук Н.А. Навчальний комплекс статистичної оцінки псевдовипадкових і текстових послідовностей. *Збірник наукових праць Військового інституту телекомунікацій та інформатизації Національного технічного університету України «КПІ»*. Київ: ВІТІ НТУУ «КПІ», 2007. Вип. 3. С. 17–26.

References:

1. Rudnytskyi, V.M., Lada, N.V., Babenko, V.H. (2018). Kryptohrafichne koduvannia: syntez operatsii potokovoho shyfruvannia z tochnistiu do perestanovky: monohrafiia [Cryptographic Coding: Synthesis of Stream Encryption Operations with Permutation Accuracy: monograph], Cherkasy State Technological University. Kharkiv: DISA PLIuS, 184 p. [in Ukrainian].

2. Gnatyuk, S., Burmak, Y., Berdibayev, R. et al. (2021). Method for developing pseudo-random number generators for cryptographic applications in 5g networks. *Cybersecurity: Education, Science, Technique*: Electronic scientific publication, 4 (12), 151–162. Retrieved from https://doi.org/10.28925/2663-4023.2021.12.151162.

3. Faure, E.V., Shcherba, A.I., Lavdanskij, A.A. (2015). Analiz korrelyacionnyh svojstv posledovatel'nostej (psevdo) sluchajnyh chisel [Analysis of correlation properties of sequences of (pseudo) random numbers]. *Nauka i tekhnika*

Povitrianykh Syl Zbroinykh Syl Ukrainy – Science and Technology of the Air Force of the Armed Forces of Ukraine, 1 (18), 142–150. Retrieved from http://nbuv.gov.ua/j-pdf/Nitps_2015_1_32.pdf

4. Faure, E., Myronets, I., Lavdanskyi, A. (2020). Autocorrelation criterion for quality assessment of random number sequences. *3rd International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020),* (Zaporizhzhia, Apr. 27 – May 1), 675–689. ISSN: 1613-0073. Retrieved from https://doi.org/10.32782/cmis/2608-52.

5. Faure, E., Fedorov, E., Myronets, I., Sysoienko, S. (2022). Method for generating pseudorandom sequence of permutations based on linear congruential generator. *Fifth International Workshop on Computer Modeling and Intelligent Systems (CMIS-2022)*, (Zaporizhzhia, May 12), 175–185. ISSN: 1613-0073. Retrieved from https://doi.org/10.32782/cmis/3137-15.

6. Rudnytskyi, V.M., Babenko, V.H., Stabetska, T.A. (2014). Uzahalnenyi metod syntezu obernenykh neliniinykh operatsii rozshyrenoho matrychnoho kryptohrafichnoho peretvorennia [Generalized method of synthesis of inverse nonlinear operations of extended matrix cryptographic transformation]. *Systemy obrobky informatsii – Information Processing Systems*. Kharkiv: KhUPS im. I. Kozheduba, 6 (122), 118–121 [in Ukrainian].

7. Naukoemkie tekhnologii v infokommunikaciyah: obrabotka i zashchita informacii: kol. monografiya [Science-Intensive Technologies in Infocommunications: Processing and Protection of Information: coll. monograph], V.M. Bezruk, V.V. Barannik (eds.) (2013). Kharkiv: Kompaniya SMIT, 398 p.

8. Babenko, V.G., Mel'nik, O.G., Stabec'kaya, T.A. (2014). Postroenie nelinejnyh operacij rasshirennogo matrichnogo kriptograficheskogo preobrazovaniya. Kriptograficheskoe kodirovanie: koll. monografiya [Construction of Non-Linear Operations of Extended Matrix Cryptographic Transformation. Cryptographic Coding: coll. monograph], V.N. Rudnitsky, V.Ya. Milchevich (eds.). Kharkov: Shchedraya usad'ba plyus, 41–55

9. Ferguson, N., Schneier, B., Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. ISBN: 978-0-470-47424-2, March, 384 p.

10. L'Ecuyer, P., Simard, R., Chen, E.J, Kelton, W.D. (2002). An object-oriented random-number package with many long streams and substreams. *Operations research*, 50 (6), 1073–1075.

11. Bucenko, Yu., Rozorinov, G., Savchenko, Yu. (2014). Obshchee i selektivnoe testirovanie psevdosluchajnyh bitovyh posledovatel'nostej [General and selective testing of pseudo-random bit sequences]. *Suchasnyi zakhyst informatsii – Modern Information Protection*, 2, 16–21

12. Lavdanskij, A.A., Faure, E.V. (2015). Ocenka statisticheskih svojstv posledovatel'nostej na vyhode kombinacionnogo generatora s pomoshch'yu graficheskih testov [Evaluation of statistical properties of sequences at the output of a combinational generator using graphic tests]. *Systemni doslidzhennia ta informatsiini tekhnolohii – System Research and Information Technologies*, 2, 39–50.

13. Lavdanskij, A.A., Faure, E.V. (2014). Kombinacionnyj metod formirovaniya posledovatel'nosti psevdosluchajnyh chisel [Combination method for generating a sequence of pseudo-random numbers]. *Systemnyi analiz ta informatsiini tekhnolohii – System Analysis and Information Technologies*: materials of the 16th Int. Sci. and Tech. Conf. (SAIT-2014), (Kyiv, May 26–30). Kyiv: NNK "IPSA" NTUU "KPI", 403–404.

14. Faure, E.V., Shcherba, A.I., Lavdanskij, A.A. (2015). Ocenka statisticheskih harakteristik posledovatel'nosti psevdosluchajnyh chisel, porozhdennoj kombinacionnym generatorom [Estimation of statistical characteristics of a sequence of pseudorandom numbers generated by a combination generator]. *Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo – Computer-Integrated Technologies: Education, Science, Manufacturing*, 18, 165–171.

15. Lavdanskyi, A.O. (2016). Otsinka chasu formuvannia poslidovnosti psevdovypadkovykh chysel [Estimation of the formation time of a sequence of pseudorandom numbers]. *Problemy informatyzatsii – Informatization Problems:* Proc. of the Fourth Int. Sci. and Tech. Conf. (Cherkasy – Baku – Belsko-Biala – Poltava). Cherkasy: ChDTU, 71 [in Ukrainian].

16. Lanskykh, Ye.V., Sysoienko, S.V., Pustovit, M.O. (2015). Otsinka yakosti psevdovypadkovykh poslidovnostei na osnovi vykorystannia operatsii dodavannia za modulem dva [Evaluation of the quality of pseudorandom sequences based on the use of modulo two addition operations]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy – Science and Technology of the Air Force of the Armed Forces of Ukraine*, 4 (21), 147–150 [in Ukrainian].

17. Faure, E.V., Sysoienko, S.V., Myroniuk, T.V. (2015). Syntez i analiz psevdovypadkovykh poslidovnostei na osnovi operatsii kryptohrafichnoho peretvorennia [Synthesis and analysis of pseudorandom sequences based on cryptographic transformation operations]. *Systemy upravlinnia, navihatsii ta zviazku – Control, Navigation and Communication Systems*. Poltava: PNTU, 4 (36), 130–133 [in Ukrainian].

18. Faure, E.V., Sysoienko, S.V. (2016). Otsinka yakosti psevdovypadkovykh poslidovnostei na osnovi dodavannia za modulem [Quality assessment of pseudorandom sequences based on modulo addition]. *Visnyk inzhenernoi akademii Ukrainy – Bulletin of the Engineering Academy of Ukraine.* 3, 165–172 [in Ukrainian].

19. Sysoienko, S.V., Sysoienko, A.A. (2019). Doslidzhennia ta analiz psevdovypadkovykh poslidovnostei dlia system komp'iuternoi kryptohrafii [Research and analysis of pseudorandom sequences for computer cryptography systems]. *Problemy informatyzatsii – Problems of Informatization*: abstracts of reports of the Seventh Int. Sci. and Tech. Conf. (Cherkasy: ChDTU; Kharkiv: NTU "KhPI", DP "PD PKNDI AP"; Baku: VA ZS AR; Belsko-Biala: UTiHN, Nov. 13–15), 3 (5–7), 67 [in Ukrainian].

20. Sysoienko, A.A., Sysoienko, S.V. (2022). Investigation of the quality of pseudorandom sequences synthesized on the basis of modulo two addition operations. *Deciata mizhnarodna naukovo-tekhnichna konferentsiia – Tenth International Scientific and Technical Conference*: abstracts, (Cherkasy: ChDTU; Kharkiv: NTU "KhPI", DP "PD PKNDI AP"; Baku: VA ZS AR; Belsko-Biala, Nov. 24–25), 1, 85.

21. Babenko, V.H., Myroniuk, T.V., Kryvous, H.V. (2021). Alhorytmy zastosuvannia operatsii perestanovok, kerovanykh informatsiieiu, dlia realizatsii kryptoperetvorennia informatsii [Algorithms for the application of information-driven permutation operations for the implementation of cryptographic transformation of information]. *Visnyk Cherkaskogo derzhavnogo tekhnolohichnogo universytetu – Bulletin of the Cherkasy State Technological University*, 3, 44–58. Retrieved from https://doi.org/10.24025/2306-4412.3.2021.247252 [in Ukrainian].

22. Myroniuk, T.V., Sysoienko, S.V, Babenko, V.H. et al. (2021). Zakhyst informatsii na osnovi operatsii perestanovok, kerovanykh informatsiieiu: monohrafiia [Information Protection Based on Information-Driven Permutation Operations: a monograph]; Cherkasy State Technol. Univ. Cherkasy: vydavets Hordiienko Ye.I., 103–164. ISBN: 978-966-97302-2-0 [in Ukrainian].

23. Rudnitsky, V., Berdibayev, R., Breus, R. et al. (2019). Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation. *Suchasni informatsiini systemy – Modern information systems*, 3 (4), 109–114. doi: 10.20998/2522-9052.2019.4.16.

24. Kryptohrafichne koduvannia: obrobka ta zakhyst informatsii: kol. monohrafiia, [Cryptographic Coding: Information Processing and Protection: coll. monograph] (2018). V.M. Rudnytskyi (ed.), Cherkasy State Technol. Univ. Kharkiv: Disa Plius, 139 p. [in Ukrainian].

25. Bohdanov, V.V., Palamarchuk, N.A. (2007). Navchalnyi kompleks statystychnoi otsinky psevdovypadkovykh i tekstovykh poslidovnostei [Educational complex of statistical evaluation of pseudo-random and textual sequences]. *Zbirnyk naukovykh prats Viiskovoho instytutu telekomunikatsii ta informatyzatsii Natsionalnoho tekhnichnoho universytetu Ukrainy «KPI» – Collection of scientific works of the Military Institute of Telecommunications and Informatization of the National Technical University of Ukraine "KPI".* Kyiv: VITI NTUU "KPI", 3, 17–26 [in Ukrainian].