DOI 10.31891/2307-5732-2025-347-37
УДК 004.032:621.391

KYCHAK VASYL
Vinnytsia National Technical University
https://orcid.org/0000-0001-7013-3261
e-mail: vmkychak@gmail.com
KRASILENKO VLADIMIR
Vinnytsia National Agrarian University;
https://orcid.org/0000-0001-6528-3150
e-mail: krasvg@i.ua
NIKITOVYCH DIANA
Vinnytsia National Technical University
https://orcid.org/0000-0002-8907-1221
e-mail: diananikitovych@gmail.com

SIMULATION OF A COOPERATIVE CRYPTOGRAPHIC PROTOCOL FOR CREATING A JOINT SECRET KEY- PERMUTATION OF A SIGNIFICANT DIMENSION

The significant growth of information volumes, the rapid development of mass communications, telecommunication networks, the latest tools and means of information technology have led to the increasingly widespread use of image and video processing technologies. Since video processing is the most general and promising area of image processing in the latest research and development of such equipment, in this work we will focus our attention on advanced technologies of masking, encryption-decryption of images and frames of video files, which require the creation of appropriate secret keys for their joint use by a certain group of users. The paper considers the issues of creating a so-called cooperative protocol for the negotiation of secret keys-permutations of significant dimension by a group of user parties. Various possible types of representations of such keys are considered and the advantages and features of their new isomorphic matrix representations are shown. The need to create such secret keys-permutations is justified to increase the cryptographic stability of matrix affine-permutation ciphers and other cryptosystems of a new matrix type is justified. The results of modeling the main procedures of the proposed protocol for the negotiation of keys in the form of isomorphic permutations of significant dimension are presented, namely, the processes of generating permutation matrices and their matrix exponents. Model experiments of the protocol as a whole are described and demonstrated, including accelerated methods of matrix raising permutations to significant powers. For such methods, sets of fixed permutation matrices were used, which are matrix exponents of the main permutation matrix. Matrices, i.e. permutation keys, and all procedures over them were given and visualized in their isomorphic representations. The values of fixed matrix exponents correspond to the corresponding weights of the bits of the binary or other code representation of the selected random numbers. The results of the simulation modeling of the protocol demonstrated the adequacy and advantages of using isomorphic representations of such permutation keys and the processes of creating a shared secret permutation key agreed upon by the parties using the proposed protocol.

Keywords: matrix-algebraic model, matrix representations, isomorphic permutation key, cryptogram, cryptographic transformations, affine-permutation cipher, protocol, matrix-type cryptosystem.

КИЧАК ВАСИЛЬ
Вінницький національний технічний університет
КРАСИЛЕНКО ВОЛОДИМИР
Вінницький національний аграрний університет
НІКІТОВИЧ ДІАНА
Вінницький національний технічний університет

СИМУЛЮВАННЯ КООПЕРАТИВНОГО КРИПТОГРАФІЧНОГО ПРОТОКОЛУ ДЛЯ СТВОРЕННЯ СПІЛЬНОГО СЕКРЕТНОГО КЛЮЧА-ПЕРЕСТАНОВКИ ЗНАЧНОГО ВИМІРУ

Значне зростання обсягів інформації, стрімкий розвиток засобів масової комунікації, телекомунікаційних мереж, новітніх засобів і засобів інформаційних технологій зумовили все більш широке використання технологій обробки зображень і відео. Оскільки обробка відео є найбільш загальним і перспективним напрямком обробки зображень у новітніх дослідженнях і розробках такого обладнання, у цій роботі ми зосередимо увагу на прогресивних технологіях маскування, шифрування-дешифрування зображень і кадрів відеофайлів, які потребують створення відповідних секретних ключів для їх спільного використання певною групою користувачів. У статті розглядаються питання створення, так званого, кооперативного протоколу для узгодження секретних ключів-перестановок значного розміру групою користувачів. Розглянуто різні можливі типи представлень таких ключів і показано переваги та особливості їх нових ізоморфних матричних представлень. Обґрунтовано необхідність створення таких секретних ключів-перестановок для підвищення криптографічної стійкості матричних афінно-перестановочних шифрів та інших криптосистем нового матричного типу. Наведено результати моделювання основних процедур запропонованого протоколу узгодження ключів у вигляді ізоморфних перестановок суттєвої розмірності, а саме процесів генерації матриць перестановок та їх матричних степенів. Описано та продемонстровано модельні експерименти протоколу в цілому, включаючи прискорені методи піднесення матриць перестановок до значних степенів. Для таких методів використовували набори фіксованих матриць перестановок, які є деякими фіксованими степенями головної матриці перестановок. Матриці, тобто ключі перестановки, і всі процедури над ними були задані та візуалізовані в їх ізоморфних представленнях. Значення фіксованих степенів матриці відповідають відповідним вагам бітів двійкового або іншого кодового представлення вибраних випадкових чисел. Результати імітаційного моделювання протоколу продемонстрували адекватність і переваги використання ізоморфних представлень таких ключів перестановки та процесів створення загального секретного ключа перестановки, узгодженого деякою групою сторін (більше двох) за допомогою запропонованого кооперативного протоколу.

Ключові слова: матрично-алгебраїчна модель, матричні представлення, ізоморфний ключ перестановки, криптограма, криптографічні перетворення, афінно-перестановочний шифр, протокол, криптосистема матричного типу.

Introduction

The accelerated development of information technology, artificial intelligence, smart technologies in medicine, the military, telecommunication networks and systems and in many other areas, including Internet of Things (IoT) technologies, has made it critically important to protect information from various devices, especially devices with limited resources. The risk of illegal access to secret or confidential data during the implementation of data collection, storage and transmission processes is becoming increasingly noticeable and significant. For example, medical data, and very often it is not only text documents, but a set of images of various formats, contain confidential information about patients, and therefore, after their leakage or distortion through interference, they can violate the confidentiality of patients, cause threats, and cause serious harm to the legitimate rights and interests of patients. Therefore, the basis and key to improving the quality of treatment, to establishing harmonious relations between the doctor and the patient is an effective and reliable mechanism for protecting confidentiality. Partly traditional encryption methods can provide some protection of information, but they cannot balance the protection of special data, for example, images, video files, the analysis and processing of which by traditional methods are not suitable for intelligent environments, neural network methods and tools, do not take into account their specifics. Intellectual processing, medical and technical diagnostics, classification, clustering, segmentation of fragments in images, etc., require increasingly accurate solutions and forecasts.

The significant growth of information volumes, the rapid development of mass communications, telecommunication networks, the latest tools and means of information technology have led to the increasingly widespread use of image and video processing technologies. Especially against the background of Russia's armed aggression against Ukraine, a new era of development of high-precision, highly reliable means of protection and armament has begun, the effectiveness of which is determined primarily by the state of radio-electronic technical means, especially communications, and the reliability, stability, and other characteristics of masking algorithms, encryption of messages of various types and formats. And the effectiveness of solving the tasks assigned to a radio-electronic means depends on the class and type of signals used, on which the range of action, resolution according to various parameters, probability of detection, quality of communication, control capabilities, concealment and coding-encryption depend. Since video processing is the most general and promising area of image processing in the latest research and development of such equipment, in this work we will focus our attention on advanced technologies of masking, encryption-decryption of images and frames of video files, which require the creation of appropriate secret keys for their joint use by a certain group of users.

Overview and analysis of publications

Generalization of known cryptosystems [1-7] with scalar-type data formats to the cases of matrix-tensor formats, emergence and research of a new class of matrix-type cryptosystems (MTCs) [8-11] based on their matrix-algebraic models (MAM) of cryptographic transformations (CTs) 2D (3D) - arrays, images (Is), which have a number of significant advantages, contributed to the intensification of MTC, MAM research and the demonstration of a number of new improvements and applications [11-16]. Hardware implementations of MAMs have the following advantages: they are easier to display on matrix processors, have extended functionality, improved crypto-resistance, allow checking the integrity of cryptograms of black and white, color images [12], and the presence of distortions in them [11], create block ones [13], parametric [13], multi-page [14] models with their significant stability [15]. Generalized MAMs, matrix affine and affine-permutation ciphers (MAPCs), their modifications, as can be seen from [8, 10, 13, 16, 17] have been widely studied and used, including in the creation of blind and other advanced digital signatures in [15, 18, 19].

For cryptographic transformations (CTs) in matrix models of permutations (MM_Ps), with their basic procedures of matrix multiplication and some other element-by-element modulo operations on matrices, byte matrices formed from rows, columns, vectors, which in unitary or other codes display symbols, codes, bytes, must be multiplied by the permutation matrix (PM) [10, 11, 20, 21]. Procedures for rearranging bits, bytes or their groups are the most common and mandatory for almost all known and newly created algorithms and ciphers. To increase the entropy of cryptograms images with their CTs based on MM_Ps and change their histograms, the decomposition of R, G, B components and their bit slices and several matrix keys (MKs) of the PM type are necessary [10, 11, 14, 20, 21]. A number of such pseudo-random (current, step-by-step, frame-by-frame) MKs, which would meet the requirements and be quickly generated, is also needed for masking, CT of video files or stream of blocks from files, images with their significant sizes. Secret key generation protocols for such ciphers were partially considered in works [22-24], including in works [22, 23] some matrix modifications of known key agreement protocols were proposed.

Formulation of the problem

From the above, we can conclude that for MAM it is necessary to form a series-stream of MKs of the PMs type, and precisely those that, along with the main MK key, would satisfy the set of necessary requirements. The issue of creating a general-type master MK (MMK) was considered in [25, 26], but not MK of the PM type, and moreover, not sequences of PMs. Methods for generating a stream of MK-permutations from the main MK (MMK) were partially considered in [27], but only for small-sized bit MKs (256*256) and did not concern the creation of a common one for several (three or more!) user parties. Therefore, the purpose of the work is to propose, highlight and study precisely the joint (cooperative) protocol for agreeing on a secret (main) MK in the form of a large-sized PM, i.e. the main PM (MPM), which is needed to improve and adapt the type and structure of MPMs of such or even larger sizes to the image format and accelerated high-speed hardware implementations

of the protocol and cryptographic transformation procedures based on such a key. It is necessary to model this protocol and show in the future the prospects for using such an MPM key for the processes of forming a PM string-stream with a significant length from it, which are required by progressive MAMs CTs in MT systems. In addition, the above review and analysis of publications allows us to identify several more important tasks, namely the need to develop and model such MAMs STs, that would be best suited for their implementation based on vector-matrix or matrix-matrix multipliers, multi-functional devices of matrix multi-valued logic [28], multiport architectures of neural-net associative memory [29], advanced high-performance sensor systems [30] with MIMO structure and reconfigurable universal logical elements [31], that significantly parallelize the computational processes of cryptographic transformations, and the need to determine, taking into account estimates and criteria, the characteristics and indicators of such models and their implementations for comparison with other known approaches.

Presentation of the main material and research results

In works [11, 13, 14, 15] it is shown that to increase the cryptographic strength of cryptographic transformations based on matrix affine permutation ciphers (MAPCs) or vector affine permutation ciphers (VAPCs), their blocked or paged modifications, especially for blocked MAMs, it is advisable for some types of text-graphic documents (TGDs) and images (I) to use a series-stream of PM-type MKs, which are generated in the encryption-decryption processes from one main MK (MMK) and are dynamic and change for each subsequent block or video frame, and to increase the dimension of the permutation keys. At the same time, the review and analysis of matrix-type ciphers, especially multifunctional parametric block ciphers [10], showed that for large-scale permutation keys it is better and more expedient to use isomorphism of different representations of permutations (matrices or vectors), which play the role of the master key (MMK) and block (and/or) step-by-step, iterative sub keys (SKs). All these keys are similar to permutation matrices PM (the main permutation matrix MMP or its functional transformation, for example, the matrix exponents of the main one!) or vectors that are isomorphic to these matrices and correspond to more traditional mappings of general permutations. And therefore, an important task is to create protocols for agreeing on a secret large-scale MMK of the PM-type in its isomorphic representation by matrices, and especially in a situation where such a secret key must be created immediately for a group of users who are subjects of the processes of classified communication and data transmission.

Without wishing to discuss them exhaustively, we will give a brief introduction to the main cryptographic key establishment methods. We will begin with the Diffie-Hellman protocol, which we consider the starting point for subsequent protocols. Diffie-Hellman (DH) key exchange [32] works over a ring Z_p with large order p. The module p and the generator g, which is primitive root in $\mathrm{Z_p}$ are publicly shared. Alice chooses randomly an exponent integer x_a and computes $k_a = g^{x_a} \bmod p$ which she sends to Bob. Similarly, Bob obtains and responds to Alice with $k_b = g^{x_b} \bmod p$. Then each of them performs exponentiation using the received number as incoming, such that Alice's computes $(g^{x_b} \bmod p)^{x_a} \bmod p = g^{x_b x_a} \bmod p$ and Bob's computes $(g^{x_a} \bmod p)^{x_b} \bmod p = g^{x_a x_b} \bmod p$ (see Fig. 1). Both numbers are equal because modular exponentiation follows the normal rules of ordinary exponentiation. The eavesdropper, Eve, would try to recover g^{ab} from (g, G, g^a, g^b). The Diffie-Hellman algorithm is defined by $F(g, G, g^a, g^b) = g^{ab}$. We say that a group G with large order p satisfies the Computational Diffie-Hellman (CDH) assumption if no efficient algorithm exists to compute $F(g, G, g^a, g^b) = g^{ab}$ [33].

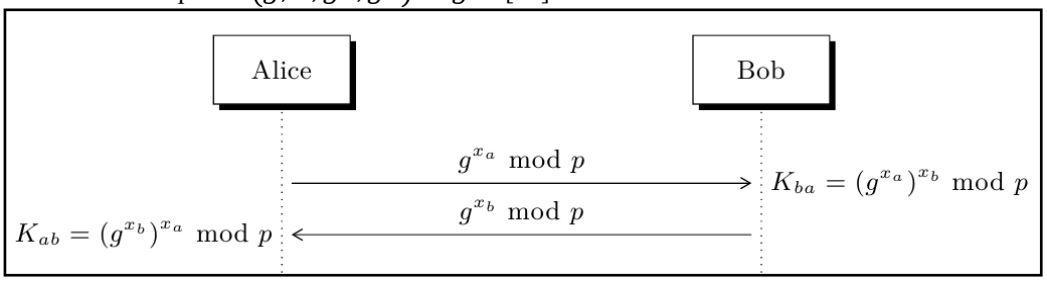

Fig.1. Diffie-Hellman protocol

Closely related to the Computational Diffie-Hellman (CDH) assumption is the Discrete Logarithm Problem (DLP) which is defined as recovering x given g and $g^x \bmod p$.

Now we will try to generalize this well-known protocol to a group of four parties who wish to create a shared secret key for further use to encrypt and decrypt confidential data and transmit it in their communications over open communication channels.

Let us first consider a simplified scheme of a cooperative protocol that creates a scalar key of small size for four parties who want to have such a secret shared key. Fig. 2. shows the essence of such a protocol, which consists in the fact that the parties, having a public base, namely the number "601", and a modulus "257", choose their secret, randomly chosen numbers and known only separately to each party, for example, the numbers "2, 5, 3, 4", respectively, raise the base to these exponents by modulus and transmit the remainders they found along the agreed chain to their neighbors. With the numbers received from their neighbors, see Fig. 2, the line of

numbers "92, 116, 37, 69", each party in the second step and the following repeats the actions similar to the first step. As can be seen from the scheme, in the fourth step all parties will receive the same key, namely the number "121". The results of modeling the cooperative protocol for the three-party case, but for creating a secret shared permutation key (matrix), i.e. of a different type, are shown in Fig. 4. For clarity and ease of visualization, here we show the essence of the functioning of such a protocol, only as an example, for permutation keys of small size, namely (7*7). For a better perception and understanding of the following material, we will consider the essence of isomorphism and variants of isomorphic representations of keys-permutations. It is especially important to choose the most optimal isomorphic representation of this type of keys with significant sizes, especially taking into account the data formats for cryptographic transformations and the computational procedures necessary for implementing the protocol. Fig. 3 shows that the permutation in the traditional vector form (row 2 on the left) uniquely corresponds to the matrix P_b, and accordingly its matrix exponents (column of numbers 2, 3, 4....16) correspond to vector representations in the form of rows (their set is on the right).

	A	B	C	D	E	F
2						
3	Key	Публічні		Основа		Модуль
4				601		257
5						
6	Key_prot	Секретні	Особисті	Матричні	Скаляр, Матриці	
7	Сторони	a	б	c	д	
8		Xa	Xб	Xc	Xд	
9		2	5	3	4	
10	1 крок	116	37	69	92	
11	1-передача	92	116	37	69	
12						
13	2 крок	240	84	24	235	
14	2-передача	235	240	84	24	
15						
16	3 крок	227	68	62	246	
17	3-передача	246	227	68	62	
18						
19	4 крок	121	121	121	121	
20	4-передача					

Fig. 2. A simplified scheme of a cooperative protocol for creating a shared secret scalar key

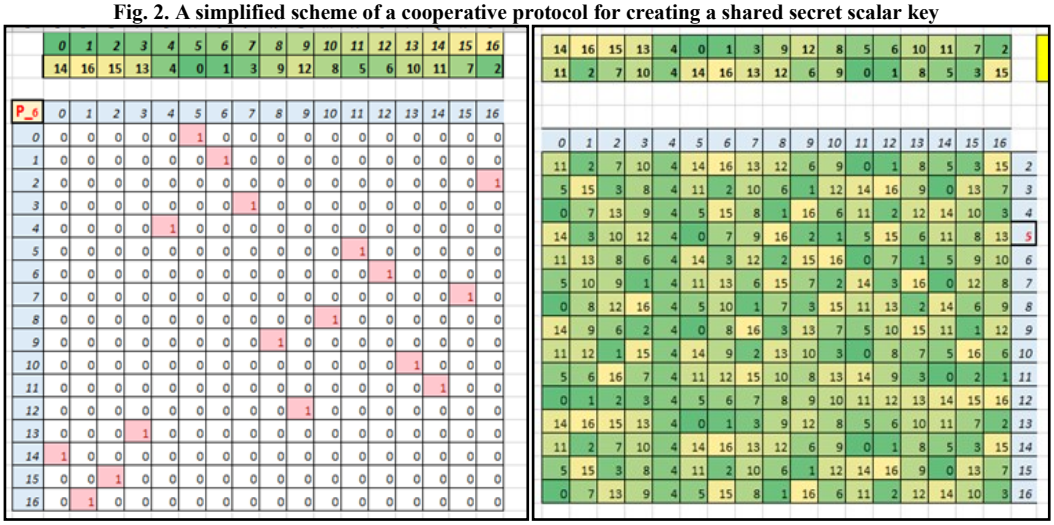

Fig. 3. Examples of isomorphic representations of key-permutations

The basic permutation matrix **P** is shown in Fig. 4 on the right in the first row and formatted in green. The first row, corresponding to the first procedural step, also shows three permutation matrices created by the three parties, namely: (Alisa, Bob, David). They are created by raising the public permutation matrix **P** to some exponent, i.e. to the corresponding random secret numbers chosen by them: (3, 6, 2). The parties exchange the resulting matrices in a specified direction, for example, cyclically to the right in the first step. Over the resulting matrices, each party in the following steps again performs similar calculations and procedures, using the same secret numbers. As can be seen, in the third step all three parties will receive identical permutation matrices **Key**, which are formatted in green in the bottom row. That is, they will essentially receive one and the same key **(Key)**, which is also essentially a permutation matrix. The proposed principle allows the protocol to be generalized to the required and larger number of parties involved in such a cooperative protocol. The parties cannot know about the secret power numbers of the other parties, but this does not prevent them from forming the necessary common secret key in the form of a permutation matrix. To find the key, the attacker must intercept all matrices transmitted by all parties, at all steps, and therefore, with sufficiently large permutation matrices and sufficiently large secret

numbers (exponents), this significantly complicates his attack and unauthorized access. In addition, if the sequence of serial numbers of the parties participating in the protocol in the chain of step-by-step mutual transfers is kept secret, then this also complicates possible attacks. And such a sequence can be additionally agreed upon by the parties, although in the generally accepted version of the protocol it can be completely public.

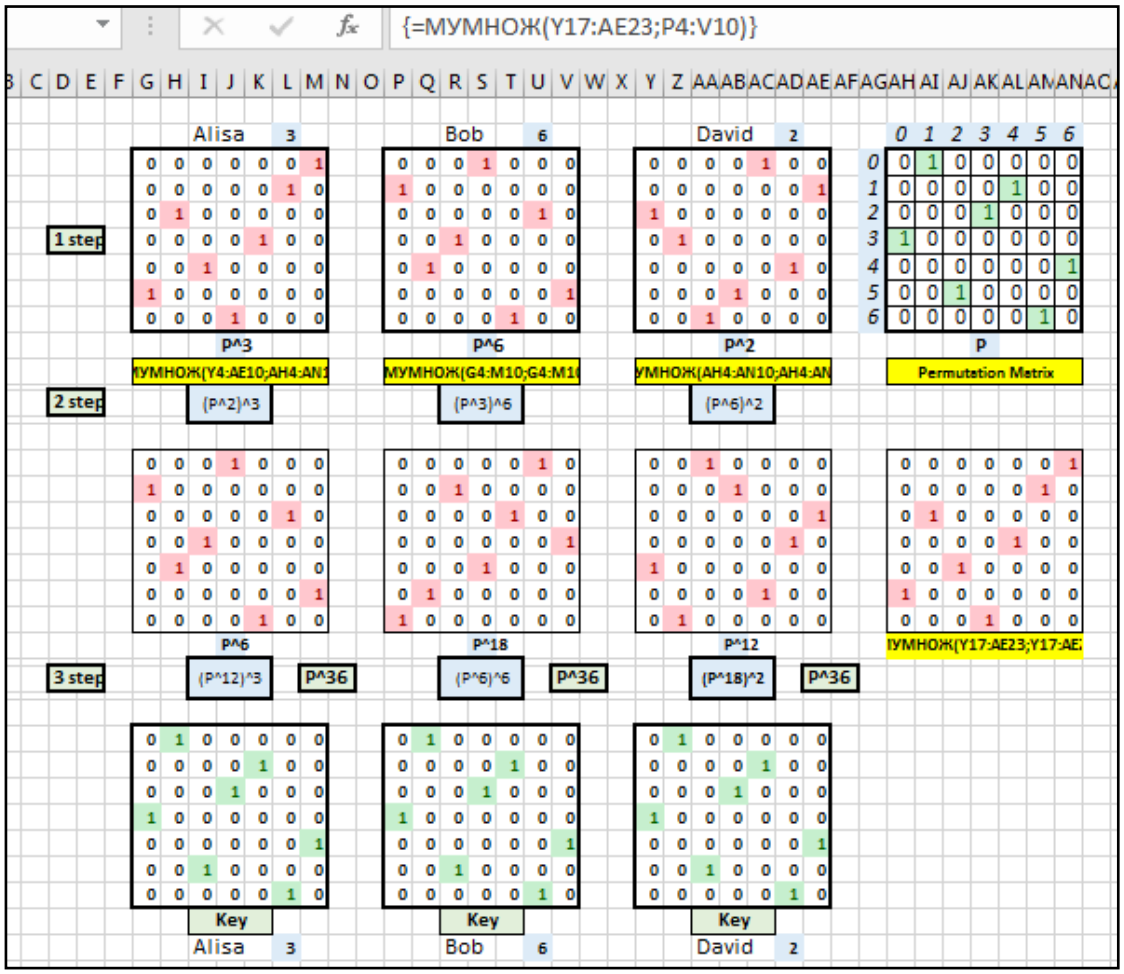

Fig. 4. A simplified scheme of a cooperative protocol for creating a shared secret scalar key

Unlike the protocols in [25, 26], in [34] the so-called cooperative protocol was considered, but it concerned the creation-agreement of MK of the image type (MK_Im-type), and in this work we are interested in the protocol for the case of creating MK of the type of permutation matrices (MK_P-type) or simply traditional permutations P. From the above in the introduction and statement of the tasks, it becomes clear that generating a series of permutation keys (type MK_P) obtained from the main key of the matrix (MMK_P) with significantly increased dimensions, i.e. large-sized, successfully solves the problem of cryptographic stability. Therefore, in the future, we will consider the protocol for agreeing on a large-sized secret master key (type MK_P), and specifically a cooperative one, i.e. for a group of participants, since the solution of this task is relevant and important. The results of modeling and research of the cryptographic cooperative protocol for agreeing on a shared secret MK_P for matrix-algebraic CT models based on the application of new isomorphic representations of MK_P and analysis of protocol procedures will be presented below.

Let us consider a situation, where the file body, any set of data bytes, subject to the encryption process is divided into blocks of significant size, where the length of the blocks is 256*256 bytes. Each of such blocks can therefore be represented as a matrix of a black-and-white image. Suppose it is necessary to rearrange all the bytes of the block according to the permutation matrix, i.e. to the MK_P type. In this case, MK_P in the form generally accepted for permutations should be a vector with N components, each of which is some single (without repetitions) number from the range 0-65535 or a square of N*N elements ("0" or "1"), where N=2^16=65536. The power of the set of possible such MK_P, i.e. their number, is estimated as N! = 65536! which gives colossal values for this N. Let us note an interesting aspect, namely, that each byte address of a block can be represented by two bytes indicating two coordinates (row and column) of the block. This gives us the opportunity to represent any permutation by two blocks (256*256 elements) of bytes, setting in each identical address of these blocks the corresponding high byte (in the first block) and low byte (in the second block) of the new corresponding coordinate of the byte address that is selected for permutation and is given by MK_P.

Fig. 5 shows the appearance of the software module in Mathcad for generating the basic (main) MK_P (MMK_P) and the appearance of its components KeyA and KeyB in the format of two images. Thus, any MK_P

can be uniquely represented by two matrices of size 256*256, the elements of which take values in the range 0-255, with the peculiarity that each of their 256 intensity gradations in each of these two matrices (images) is repeated exactly 256 times. The histograms of the MK_P components KeyA and KeyB have the form of horizontal lines. Note that such an isomorphic representation of the PM in the form of two images gives us the opportunity to use these components KeyA and KeyB as two secret MKs of a general type, for example, as additive and multiplicative keys in MAPC or other MAMs.

In paper [27], the results of modeling the cipher-text of an image (Im) using MAPC using the proposed key and its components as keys are presented. It shows the matrices of the explicit image (Im), its cryptogram (Cmap), verified and difference images, their histograms, the comparative appearance of which and the entropy-histogram analysis confirm the prospects of using the proposed cipher based on the generated Key. These experiments confirmed, that the CT MAPC with the existing 2 components of the PM give high-quality cryptograms, whose histograms are so close to the uniform distribution law that even for image (Im) with an entropy of 0.738, the entropy of cryptograms going all the way up 7.999 and differs from the theoretical maximum (8 bits) by just a fraction of a percent.

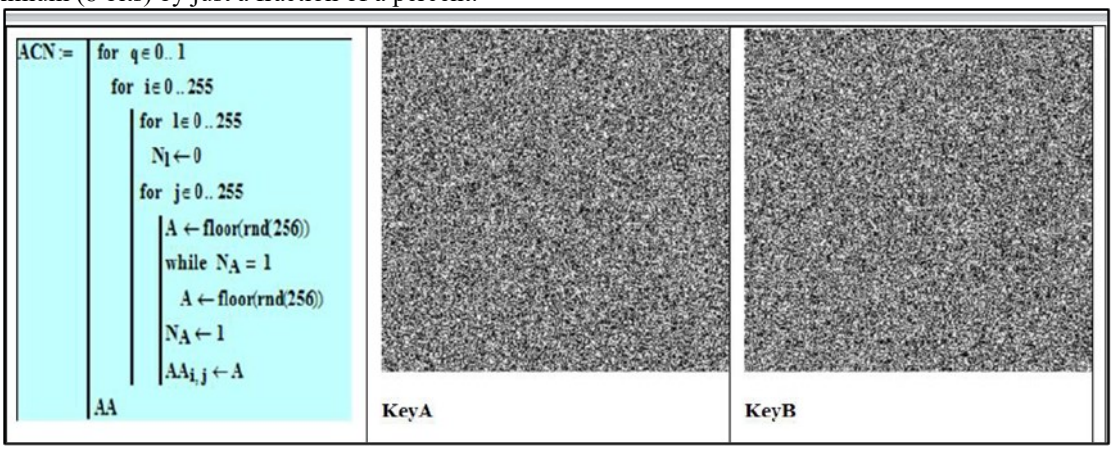

Fig. 5. Mathcad window: Software module for generating the base (main) MK_P and the appearance of its two components, KeyA and KeyB, in the format of two black-and-white images

The results of the simulation of the MAPC and multi-step MAPC [27] for different cases, when the components of affine transformations are first performed in a different sequence and with different or one MK from the PM, and then permutation using the PM, or vice versa, also proved similar qualitative CTs, when applying the proposed representations of the PM. But for all modifications of the MAM with such permutation matrices PMs, the power of the set of which is estimated by a significant value N! = (256*256)! , the primary issue is the agreement on the shared secret master permutation matrix MPM.

For simulation modeling of the cooperative protocol and all its step-by-step procedures, we used a software module we created, which implements the procedure of iterative permutations in MK_P, isomorphic to raising the permutation matrix to the desired exponent, and is shown in Fig. 6 (copies from the Mathcad window).

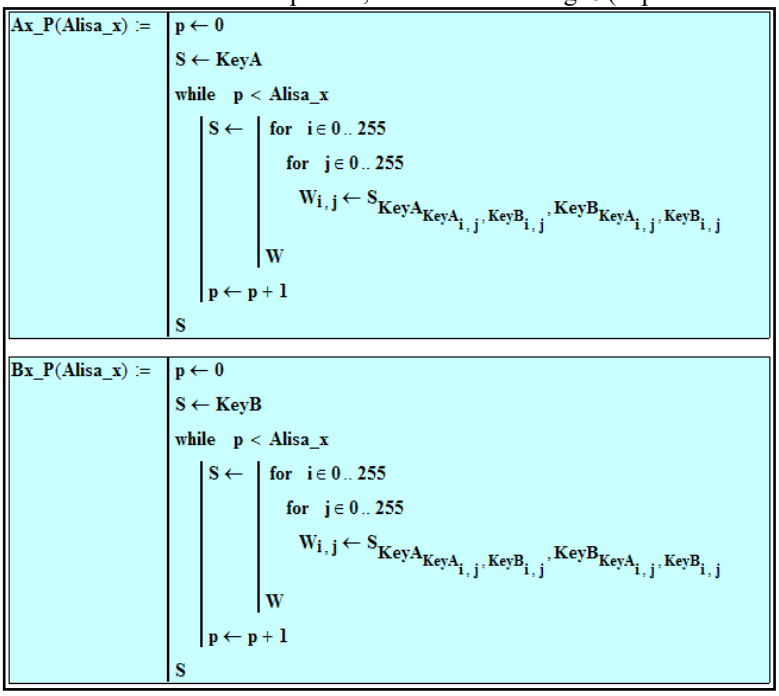

Fig. 6. Software modules (from Mathcad) reflecting the procedure of iterative permutations in MP, isomorphic to raising the MP to the desired exponent by side x

Isomorphic representation of large-sized bit permutation matrices by halftone image matrices, which coincide in format with blocks of files or any data being encrypted, facilitates and accelerates the process of raising permutation matrices MK_P (N*N binary, where N=2^16), replaces the matrix multiplication operation with equivalent fast permutations, which can additionally be even more accelerated at significant exponents by using some basic set of fixed (fixed powers of MMK_P) and their specific sequence. The adequacy and advantages of such accelerated algorithms for isomorphic formation of exponents of matrix permutations were verified by simulations, which, taking into account the limitations, are not given here, but have already been partially covered in [27]. To do this, bit matrices raised to a matrix exponent, after converting them into isomorphic form, were compared with matrices obtained by various iterative or accelerated permutation methods.

The simulation results of the cooperative protocol for the three-party case are shown in Fig. 7-8. The protocol is implemented as follows. Each of the parties x, y, z (Alisa, Bob, David) chooses as a basis a common MK_P, isomorphically represented by its components (KeyA, KeyB) and a path of successive transmissions of the intermediate MK_Ps formed by them at each step, which are formed as exponents of the basis depending on the selected secret identifiers-numbers: Alisa_x, Bob_y, David_z using the permutation software modules described and shown in Fig. 7-8. Each of the parties in the first step raises the GMK_P isomorphically to its chosen secret exponent, which is usually in practice a fairly large pseudo-random number of the order of typical values used today in cryptography to significantly increase the complexity of calculations in brute force attacks on one-way functions. After that, each party sends the new MK_P to the other party along the selected transmission path. Then, in the following steps, the parties similarly raise the new MK_Ps they receive to their same random secret exponents and transmit the resulting permutations (images) along the path again. The generated secret key MK_P (two matrices of size 256x256 bytes) is transmitted by each side to its neighbors along the path, and then the received MK_P are again raised to the appropriate exponents, as shown in Fig. 7-8. All protocol actions are performed with the isomorphic form of MK_P, not with scalars.

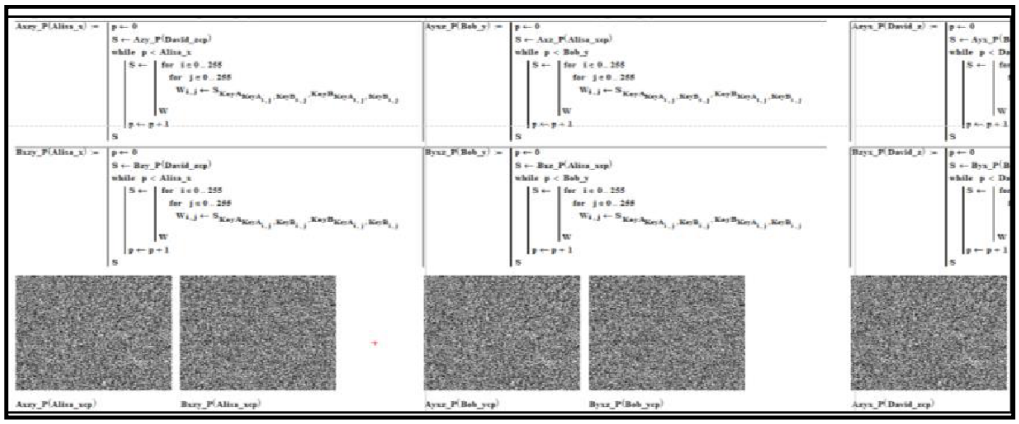

Fig. 7. Fragments from Mathcad for modeling the protocol of forming a shared secret MK_P by three parties: modules for permutations, type of keys

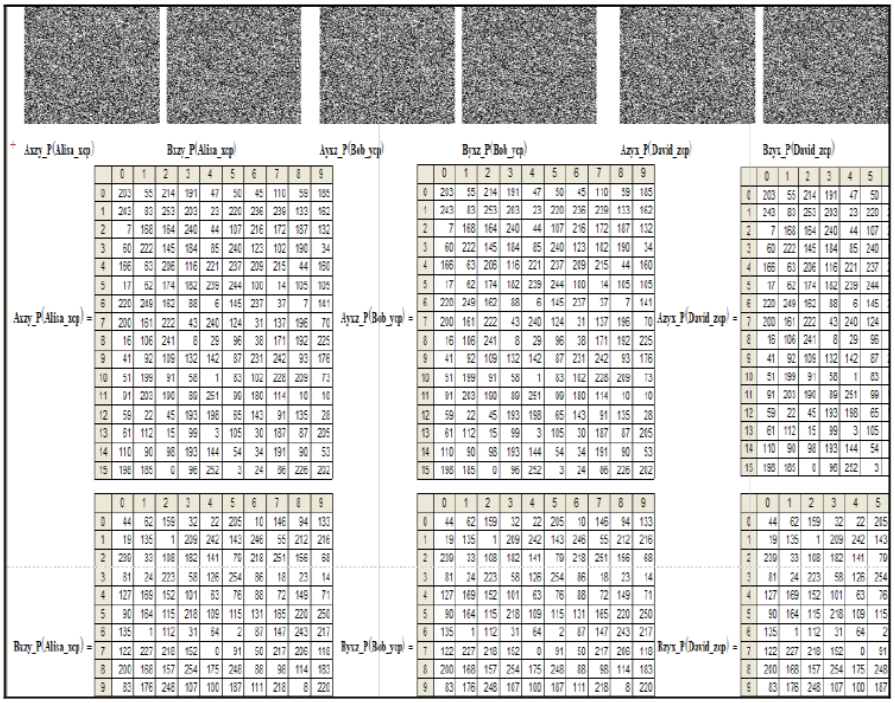

Fig. 8. Mathcad window with identical secret keys MK_Ps formed by three sides in their isomorphic form of two components

The parties do not know the identifiers (powers) of the other parties, but the secret MK_P (isomorphically represented as two images) key they obtain is identical for all group participants. Thus, the result of the protocol is identical keys, a secret MK_P, whose equality is evident (Fig. 8) and ensured for all n parties without knowing each other's identifiers. The correctness of the protocol's operation is confirmed by the simulation results in Mathcad. An analysis of resilience, considering the complexity of the set of large-dimensional MK_Ps generated by this protocol, showed the impossibility of attacks, as for N=2^16, this complexity is estimated to be (2^16)!.

According to the protocol, large-sized permutation matrices must be multiplied many times, i.e., brought to a power, depending on the value (quite large!) of the degrees-identifiers of the parties. And these degrees to which the parties raise these isomorphically represented MPs must be sufficiently significant to ensure the necessary crypto-resistance against attacks. Therefore, taking into account the necessity and expediency of using the above-mentioned accelerated methods of matrix exponentiation, an adequate isomorphic transformation of this procedure into a certain sequence of fixed permutations is shown. Depending on the code in which the degree value is given, the corresponding permutations are selected from the formed set of fixed MPs, the degrees of which correspond to the corresponding weights of the bits of the binary or other code representation of the random numbers chosen by the parties. The results of these simulations, the corresponding formulas, procedures and key fragments, taking into account the limitations on the size of the article and the fact that the results are completely similar, but not for the cooperative protocol, have already been given in works [35, 36], we do not consider them here. A comparison of the elements of the obtained matrices confirmed their complete correspondence and equality. Using the developed functional parametric models of CT using a secret MK_P (PM), consistent with the proposed protocol given above, the correctness of their synthesis and the adequacy of the models using direct and inverse CT images were verified. The results obtained by modeling in Mathcad confirm the correctness of the protocol. Although the initial MPM is known to all parties, the protocol allows, without knowing the secret exponents chosen by the parties, to form a secret key, PM in a similar isomorphic form in a time proportional to the number of fixed permutations. In addition, the stability analysis taking into account the power of the set of the corresponding PM of significant sizes formed by this protocol showed the impossibility of carrying out attacks due to the huge set of possible MPs, which is estimated by the value (**2^16**)!

Note that to combat the attacker's attack, in which he will be able to intercept all the permutations transmitted by the parties in their isomorphic representations in the form of images, at all steps, and due to the publicity of the basic (main) permutation to solve the problem of finding the secret exponents of all parties, several approaches can be proposed. We will consider them in the following works. Here we will indicate only one simple method of combating, which consists in the fact that the parties close the data before transmitting it (encrypt it with a permutation) and open it with it when receiving the data for subsequent calculations. And as a key for this, they use, for example, the permutation key that was obtained by the protocol in the previous session.

Conclusions

A protocol for agreeing on a common cooperative secret key in the form of isomorphic representations of a permutation matrix of significant dimensions has been proposed, its modeling has been performed, and model experiments have been conducted, which have been presented and confirm the adequacy of the functioning of the models and the proposed protocol, methods for generating a series of PMs, the adequacy of algorithmic steps and methods for forming intermediate and final MK_Ps. The models are simple, convenient, adapted to various formats and color images, are better displayed and can be implemented by matrix processors, have high efficiency, stability, and speed. The algorithms for accelerated elevations in significant degrees of permutation matrices with preservation of their isomorphic representations have been tested, and their advantages have been shown.

References

1. Schneier, B. (1996). *Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Inc.

2. Mao, W. (2004). *Modern cryptography: Theory and practice*. Pearson Education.

3. Вербіцький, О. В. (1998). *Вступ до криптології* (248 с.). ВНТЛ.

4. Горбенко, І. Д., & Горбенко, Ю. І. (2012). *Прикладна криптологія. Теорія. Практика. Застосування* (878 с.). Форт.

5. Ємець, В., Мельник, А., & Попович, Р. (2003). *Сучасна криптографія: Основні поняття* (144 с., іл.). БаК.

6. Vostricov, A., Sergeev, M., Balonin, N., & Chernyshev, S. (2017). Digital masking using Mersenne matrices and its special images. *Procedia Computer Science, 112*, 1151-1159.

7. Puteaux, P., & Puech, W. (2021). A recursive reversible data hiding in encrypted images method with a very high payload. *IEEE Trans. Multimedia, 23*, 636-650.

8. Krasilenko, V. G., & Grabovlyak, S. K. (2012). Matrix affine and permutation ciphers for encryption and decryption of images. *Systems of Information Processing, 3*(101), 53-62.

9. Wu, X., et al. (2021). Secure reversible data hiding in encrypted images based on adaptive prediction-error labeling. *Signal Process, 188*, 108200.

10. Krasilenko, V. G., & Dubchak, V. M. (2014). Cryptographic transformations of images based on matrix models of permutations with matrix-bit-map decomposition and their modeling. *Bulletin of Khm. National University. Technical sciences, 1*, 74-79.

11. Krasilenko, V. G., & Nikitovich, D. V. (2016). Modeling and research of cryptographic transformations of images based on their matrix-bit-map decomposition and matrix models of permutations with verification of integrity. *Electronics and Information Technologies, 6*, 111-127.

12. Красиленко, В. Г., Огородник, К. В., & Флавицька, Ю. А. (2010). Моделювання матричних афінних алгоритмів для шифрування кольорових зображень. У *Комп'ютерні технології: наука і освіта: тези доповідей V Всеукр. НПК* (с. 120-124). Київ.

13. Krasilenko, V. G., Lazarev, A. A., & Nikitovich, D. V. (2020). The Block Parametric Matrix Affine-Permutation Ciphers (BP_MAPCs) with Isomorphic Representations and their Research. *Actual Problems of Information Systems and Technologies*, 270-282.

14. Krasilenko, V. G., Lazarev, A. A., & Nikitovich, D. V. (2020). Matrix Models of Cryptographic Transformations of Video Images Transmitted from Aerial-Mobile Robotic Systems. In *Control and Signal Processing Applications for Mobile and Aerial Robotic Systems* (pp. 170-214). Hershey, PA: IGI Global.

15. Красиленко, В. Г., Нікітович, Д. В., Яцковська, Р. О., & Яцковський, В. І. (2019). Моделювання покращених багатокрокових 2D RSA алгоритмів для криптографічних перетворень та сліпого електронного цифрового підпису. *Системи обробки інформації, 1*(156), 92-100.

16. Krasilenko, V. G., Lazarev, A. A., & Nikitovich, D. V. (2020). Models of matrix block affine-permutation ciphers (MBAPCs) for cryptographic transformations and their research. *Збірник матеріалів доповідей та тез III Міжнародної науково-практичної конференції "Проблеми кібербезпеки інформаційно-телекомунікаційних систем"*. Київ: ВПЦ "Київський університет", 314-321. URL: http://ir.lib.vntu.edu.ua//handle/123456789/30700.

17. Krasilenko, V. G., & Nikitovich, D. V. (2018). Поблочні криптографічні перетворення зображень на основі векторних афінно-перестановочних шифрів та їх моделювання. У *Тези доповідей І Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», 19-20 жовтня 2018 р.* (с. 117-121). URL: http://ir.lib.vntu.edu.ua//handle/123456789/23055.

18. Красиленко, В. Г., & Грабовляк, С. К. (2011). Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи. *Системи обробки інформації, 7*, 60-63. URL: http://nbuv.gov.ua/UJRN/soi_2011_7_17.

19. Красиленко, В. Г., Яцковська, Р. О., & Тріфонова, Ю. М. (2013). Демонстрація процесів створення сліпих електронних цифрових підписів на текстографічну документацію на основі моделей матричного типу. *Системи обробки інформації, 3*(110), Т. 2, 18-22.

20. Krasilenko, V. G., & Nikitovich, D. V. (2016). Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітово-зрізовою декомпозиціями. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво, 23*, 31-36.

21. Лужецький, В., & Горбенко, І. (2015). Методи шифрування на основі перестановки блоків змінної довжини. *Захист інформації, 17*(2), 169-175.

22. Білецький, А. Я., Білецький, А. А., & Кандиба, Р. Ю. (2012). Матричні аналоги протоколу Діффі-Хеллмана. *Автоматика, вимірювання та керування: Вісник нац. ун-ту "Львівська політехніка"*, 741, 128-133.

23. Beletskyi, A. Y., Beletskyi, A. A., Stetsenko, D. A. (2010). Modified matrix asymmetric cryptographic algorithm of Diffie–Hellman. *Artificial Intelligence, 3*, 697-705.

24. Квєтний, Р. Н., Титарчук, Є. О., & Гуржій, А. А. (2016). Метод та алгоритм обміну ключами серед груп користувачів на основі асиметричних шифрів ECCта RSA. *Інформаційні технології та комп'ютерна інженерія, 3*, 38-43.

25. Krasilenko, V. G., & Nikitovich, D. V. (2017). Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу. *Системи обробки інформації, 3*(149), 151-157.

26. Krasilenko, V. G., & Nikitovich, D. V. (2017). Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів. *Комп`ютерно-інтегровані технології: освіта, наука, виробництво: науковий журнал*, 26, 111-120.

27. Krasilenko, V. G., & Nikitovich, D. V. (2019). Modeling of methods for generating flows of matrix permutations of significant dimension for cryptographic transformations of images. In *Abstracts of the II All-Ukrainian STC Computer Technologies: Innovations, Problems, Solutions* (pp. 67-77). Zhytomyr: Zhytomyr Polytechnic.

28. Krasilenko, V. G., & Magas, A. T. (1999). Fundamentals of design of multi-functional devices of matrix multi-valued logic with fast programmed adjusting. *Measuring and computer technique in technological processes, 4*, 113-121.

29. Krasilenko, V. G., Lazarev, A. A., Grabovlyak, S. K., & Nikitovich, D. V. (2013). Using a multiport architecture of neural-net associative memory based on the equivalency paradigm for parallel cluster image analysis and self-learning. *Proc. SPIE, 8662*, 86620S.

30. Krasilenko, V. G., Nikolskyy, A. I., Lazarev, A. A. (2015). Designing and simulation smart multifunctional continuous logic device as a basic cell of advanced high-performance sensor systems with MIMO structure. *Proc. SPIE, 9450*, Photonics, Devices, and Systems VI, 94500N. https://doi.org/10.1117/12.2073893.

31. Krasilenko, V. G., Ogorodnik, K. V., Nikolskyy, A. I., & Dubchak, V. N. (2011). Family of optoelectronic photocurrent reconfigurable universal (or multifunctional) logical elements (OPR ULE) on the basis of continuous logic operations (CLO) and current mirrors (CM). *Proc. SPIE, 8001*, International Conference on Applications of Optics and Photonics, 80012Q.

32. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644-654.

33. Kahrobaei, D., Koupparis, C., & Shpilrain, V. (2013). Public key exchange using matrices over group rings. *arXiv preprint arXiv:1302.1625*.

34. Красиленко, В. Г., Нікітович, Д. В. (2018). Кооперативний протокол узгодження спільного секретного матричного ключа. У *Матеріали VII МНПК (ІУСТ), 17-18 вересня 2018 р.* (с. 122-127). Одеса: ОНПУ.

35. Krasilenko, V. G., Yurchuk, N. P., & Nikitovich, D. V. (2021). Застосування ізоморфних матричних представлень для моделювання протоколу узгодження секретних ключів-перестановок значної розмірності. *Вісник Хмельницького національного університету. Серія: Технічні науки, 2*(295), 78-88.

36. Saiko, V., Krasilenko, V., Kiporenko, S., Chikov, I., & Nikitovich, D. (2023). Modeling of a cryptographic protocol for matching a shared secret key-permutation of significant dimension with its isomorphic representations. *CEUR Workshop Proceedings, 3646*, 196-205. https://ceur-ws.org/Vol-3646/Paper_19.pdf.

References

1. Schneier, B. (1996). Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc.
2. Mao, W. (2004). Modern cryptography: Theory and practice. Pearson Education.
3. Verbitskyi, O. V. (1998). Vstup do kryptolohii (248 s.). VNTL.
4. Horbenko, I. D., & Horbenko, Yu. I. (2012). Prykladna kryptolohiia. Teoriia. Praktyka. Zastosuvannia (878 s.). Fort.
5. Yemets, V., Melnyk, A., & Popovych, R. (2003). Suchasna kryptohrafiia: Osnovni poniattia (144 s., il.). BaK.
6. Vostricov, A., Sergeev, M., Balonin, N., & Chernyshev, S. (2017). Digital masking using Mersenne matrices and its special images. Procedia Computer Science, 112, 1151-1159.
7. Puteaux, P., & Puech, W. (2021). A recursive reversible data hiding in encrypted images method with a very high payload. IEEE Trans. Multimedia, 23, 636-650.
8. Krasilenko, V. G., & Grabovlyak, S. K. (2012). Matrix affine and permutation ciphers for encryption and decryption of images. Systems of Information Processing, 3(101), 53-62.
9. Wu, X., et al. (2021). Secure reversible data hiding in encrypted images based on adaptive prediction-error labeling. Signal Process, 188, 108200.
10. Krasilenko, V. G., & Dubchak, V. M. (2014). Cryptographic transformations of images based on matrix models of permutations with matrix-bit-map decomposition and their modeling. Bulletin of Khm. National University. Technical sciences, 1, 74-79.
11. Krasilenko, V. G., & Nikitovich, D. V. (2016). Modeling and research of cryptographic transformations of images based on their matrix-bit-map decomposition and matrix models of permutations with verification of integrity. Electronics and Information Technologies, 6, 111-127.
12. Krasylenko, V. H., Ohorodnyk, K. V., & Flavytska, Yu. A. (2010). Modeliuvannia matrychnykh afinnykh alhorytmiv dlia shyfruvannia kolorovykh zobrazhen. U Kompiuterni tekhnolohii: nauka i osvita: tezy dopovidei V Vseukr. NPK (s. 120-124). Kyiv.
13. Krasilenko, V. G., Lazarev, A. A., & Nikitovich, D. V. (2020). The Block Parametric Matrix Affine-Permutation Ciphers (BP_MAPCs) with Isomorphic Representations and their Research. Actual Problems of Information Systems and Technologies, 270-282.
14. Krasilenko, V. G., Lazarev, A. A., & Nikitovich, D. V. (2020). Matrix Models of Cryptographic Transformations of Video Images Transmitted from Aerial-Mobile Robotic Systems. In Control and Signal Processing Applications for Mobile and Aerial Robotic Systems (pp. 170-214). Hershey, PA: IGI Global.
15. Krasylenko, V. H., Nikitovych, D. V., Yatskovska, R. O., & Yatskovskyi, V. I. (2019). Modeliuvannia pokrashchenykh bahatokrokovykh 2D RSA alhorytmiv dlia kryptohrafichnykh peretvoren ta slipoho elektronnoho tsyfrovoho pidpysu. Systemy obrobky informatsii, 1(156), 92-100.
16. Krasilenko, V. G., Lazarev, A. A., & Nikitovich, D. V. (2020). Models of matrix block affine-permutation ciphers (MBAPCs) for cryptographic transformations and their research. Zbirnyk materialiv dopovidei ta tez III Mizhnarodnoi naukovo-praktychnoi konferentsii "Problemy kiberbezpeky informatsiino-telekomunikatsiinykh system". Kyiv: VPTs "Kyivskyi universytet", 314-321. URL: http://ir.lib.vntu.edu.ua//handle/123456789/30700.
17. Krasilenko, V. G., & Nikitovich, D. V. (2018). Poblochni kryptohrafichni peretvorennia zobrazhen na osnovi vektornykh afinno-perestanovochnykh shyfriv ta yikh modeliuvannia. U Tezy dopovidei I Vseukrainskoi naukovo-tekhnichnoi konferentsii «Kompiuterni tekhnolohii: innovatsii, problemy, rishennia», 19-20 zhovtnia 2018 r. (s. 117-121). URL: http://ir.lib.vntu.edu.ua//handle/123456789/23055.
18. Krasylenko, V. H., & Hrabovliak, S. K. (2011). Matrychni afinni shyfry dlia stvorennia tsyfrovykh slipykh pidpysiv na tekstohrafichni dokumenty. Systemy obrobky informatsii, 7, 60-63. URL: http://nbuv.gov.ua/UJRN/soi_2011_7_17.
19. Krasylenko, V. H., Yatskovska, R. O., & Trifonova, Yu. M. (2013). Demonstratsiia protsesiv stvorennia slipykh elektronnykh tsyfrovykh pidpysiv na tekstohrafichnu dokumentatsiiu na osnovi modelei matrychnoho typu. Systemy obrobky informatsii, 3(110), T. 2, 18-22.
20. Krasilenko, V. G., & Nikitovich, D. V. (2016). Modeliuvannia kryptohrafichnykh peretvoren kolorovykh zobrazhen na osnovi matrychnykh modelei perestanovok zi spektralnoiu ta bitovo-zrizovoiu dekompozytsiiamy. Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo, 23, 31-36.

21. Luzhetskyi, V., & Horbenko, I. (2015). Metody shyfruvannia na osnovi perestanovky blokiv zminnoi dovzhyny. Zakhyst informatsii, 17(2), 169-175.

22. Biletskyi, A. Ya., Biletskyi, A. A., & Kandyba, R. Yu. (2012). Matrychni analohy protokolu Diffi-Khellmana. Avtomatyka, vymiriuvannia ta keruvannia: Visnyk nats. un-tu "Lvivska politekhnika", 741, 128-133.

23. Beletskyi, A. Y., Beletskyi, A. A., Stetsenko, D. A. (2010). Modified matrix asymmetric cryptographic algorithm of Diffie–Hellman. Artificial Intelligence, 3, 697-705.

24. Kvietnyi, R. N., Tytarchuk, Ye. O., & Hurzhii, A. A. (2016). Metod ta alhorytm obminu kliuchamy sered hrup korystuvachiv na osnovi asymetrychnykh shyfriv ECCta RSA. Informatsiini tekhnol

25. Krasilenko, V. G., & Nikitovich, D. V. (2017). Modeliuvannia protokoliv uzghodzhennia sekretnoho matrychnoho kliucha dlia kryptohrafichnykh peretvoren ta system matrychnoho typu. Systemy obrobky informatsii, 3(149), 151-157.

26. Krasilenko, V. G., & Nikitovich, D. V. (2017). Modeliuvannia bahatokrokovykh ta bahatostupenevykh protokoliv uzghodzhennia sekretnykh matrychnykh kliuchiv. Komp`iuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo: naukovyi zhurnal, 26, 111-120.

27. Krasilenko, V. G., & Nikitovich, D. V. (2019). Modeling of methods for generating flows of matrix permutations of significant dimension for cryptographic transformations of images. In Abstracts of the II All-Ukrainian STC Computer Technologies: Innovations, Problems, Solutions (pp. 67-77). Zhytomyr: Zhytomyr Polytechnic.

28. Krasilenko, V. G., & Magas, A. T. (1999). Fundamentals of design of multi-functional devices of matrix multi-valued logic with fast programmed adjusting. Measuring and computer technique in technological processes, 4, 113-121.

29. Krasilenko, V. G., Lazarev, A. A., Grabovlyak, S. K., & Nikitovich, D. V. (2013). Using a multiport architecture of neural-net associative memory based on the equivalency paradigm for parallel cluster image analysis and self-learning. Proc. SPIE, 8662, 86620S.

30. Krasilenko, V. G., Nikolskyy, A. I., Lazarev, A. A. (2015). Designing and simulation smart multifunctional continuous logic device as a basic cell of advanced high-performance sensor systems with MIMO structure. Proc. SPIE, 9450, Photonics, Devices, and Systems VI, 94500N. https://doi.org/10.1117/12.2073893.

31. Krasilenko, V. G., Ogorodnik, K. V., Nikolskyy, A. I., & Dubchak, V. N. (2011). Family of optoelectronic photocurrent reconfigurable universal (or multifunctional) logical elements (OPR ULE) on the basis of continuous logic operations (CLO) and current mirrors (CM). Proc. SPIE, 8001, International Conference on Applications of Optics and Photonics, 80012Q.

32. Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.

33. Kahrobaei, D., Koupparis, C., & Shpilrain, V. (2013). Public key exchange using matrices over group rings. arXiv preprint arXiv:1302.1625.

34. Krasylenko, V. H., Nikitovych, D. V. (2018). Kooperatyvnyi protokol uzghodzhennia spilnoho sekretnoho matrychnoho kliucha. U Materialy VII MNPK (IUST), 17-18 veresnia 2018 r. (s. 122-127). Odesa: ONPU.

35. Krasilenko, V. G., Yurchuk, N. P., & Nikitovich, D. V. (2021). Zastosuvannia izomorfnykh matrychnykh predstavlen dlia modeliuvannia protokolu uzghodzhennia sekretnykh kliuchiv-perestanovok znachnoi rozmirnosti. Visnyk Khmelnytskoho natsionalnoho universytetu. Seriia: Tekhnichni nauky, 2(295), 78-88.

36. Saiko, V., Krasilenko, V., Kiporenko, S., Chikov, I., & Nikitovich, D. (2023). Modeling of a cryptographic protocol for matching a shared secret key-permutation of significant dimension with its isomorphic representations. CEUR Workshop Proceedings, 3646, 196-205. https://ceur-ws.org/Vol-3646/Paper_19.pdf.