Наукові перспективи
Видавнича група

№6(34)
2024

НАУКА і ТЕХНІКА СЬОГОДНІ

серія: право, серія: економіка, серія: педагогіка,
серія: техніка, серія: фізико-математичні науки

З Україною в серці!

Видавнича група «Наукові перспективи»

Громадська наукова організація «Всеукраїнська Асамблея докторів наук із державного управління»

Громадська організація «Асоціація науковців України»

«Наука і техніка сьогодні»

(Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»)

Випуск № 6(34) 2024

Київ – 2024

Publishing Group «Scientific Perspectives»

Public Scientific Organization «Ukrainian Assembly of Doctors of Sciences in Public Administration»

Public organization «Association of Scientists of Ukraine”

"Science and technology today"

("Pedagogy" series, "Law" series, "Economics" series, "Physical and mathematical sciences" series, "Technics" series)

Issue № 6(34) 2024

Kiev – 2024

ISSN 2786-6025 Online
УДК 001.32:1 /3](477)(02)

DOI: https://doi.org/10.52058/2786-6025-2024-6(34)

«Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»)»: журнал. 2024. № 6(34) 2024. С. 1131

Згідно наказу Міністерства освіти і науки України від 07.04.2022 № 320 журналу присвоєно категорію "Б" із економіки та педагогіки (спеціальності – 015 - Педагогічні науки; 076 - Економічні науки)

Згідно наказу Міністерства освіти і науки України від 06.06.2022 № 530 журналу присвоєно категорію "Б" із права (спеціальність – 081 Юридичні науки)

Згідно наказу Міністерства освіти і науки України від 10.10.2022 № 894 журналу присвоєно категорію "Б" із техніки (спеціальність - 122 Комп'ютерні науки)

Журнал видається за підтримки Міждержавної гільдії інженерів консультантів, Інституту філософії та соціології Національної Академії Наук Азербайджану (Баку, Азербайджан), громадської організації «Християнська академія педагогічних наук України» та громадської організації «Всеукраїнська асоціація педагогів і психологів з духовно-морального виховання»

Рекомендовано до видавництва Президією Всеукраїнської Асамблеї докторів наук з державного управління (Рішення від 24.06.2024, № 6/6-24)

Журнал включено до міжнародної наукометричної бази Index Copernicus (IC), міжнародної пошукової системи Google Scholar та до міжнародної наукометричної бази даних Research Bible

- Коваленко Олена Михайлівна - кандидат педагогічних наук, провідний науковий співробітник відділу профільного навчання Інституту педагогіки НАПН України (Київ, Україна)
- Комнатний Сергій Олександрович - докторант кафедри філософії права та юридичної логіки Національної академії внутрішніх справ (Київ, Україна)
- Кравчук Володимир Миколайович — доктор юридичних наук, доцент, доцент кафедри конституційного, адміністративного та міжнародного права Волинського національного університету імені Лесі Українки (Луцьк, Україна)
- Кузьмич Людмила Володимирівна - доктор технічних наук, головний науковий співробітник Інституту водних проблем і меліорації Національної академії аграрних наук України (Київ, Україна)
- Куницький Сергій Олегович - кандидат технічних наук, старший дослідник, провідний науковий співробітник науково-дослідної частини Національного університету водного господарства та природокористування (Рівне, Україна)
- Лук'янчук Олександр Петрович — кандидат технічних наук, доцент, доцент кафедри будівельних, дорожніх, меліоративних, сільськогосподарських машин та обладнання Національного університету водного господарства та природокористування (Рівне, Україна)
- Маджд Світлана Михайлівна - доктор технічних наук, професор, професор кафедри зеленої економіки та економіки природокористування Державної екологічної академії післядипломної освіти та управління (Київ, Україна)
- Мануель Давид Массено - доцент відділу права та захисту даних, старший науковий співробітник і член координаційного комітету лабораторії UbiNET, запрошений член PDPC, член-консультант комісій цифрового права муніципальних адвокатських колегій Кампінаса та Прая-Гранде (Сан-Паулу), а також Комісії з інновацій, управління та технологій муніципальної адвокатської колегії Гуарульюса, коментатор IODA, почесний член IDEIA Institute, член Наукового комітету MICHR, член EDEN, член-кореспондент RedNAC, член UMAU, член-кореспондент UBAU (Португалія)
- Микитин Тарас Миронович - кандидат технічних наук, завідувач кафедри менеджменту Рівненськеого державного гуманітарного університету (Рівне, Україна)
- Миргород-Карпова Валерія Валеріївна - кандидат юридичних наук, заступник директора з наукової роботи, старший викладач кафедри адміністративного, господарського права та фінансово-економічної безпеки Сумського державного університету (Суми, Україна)
- Мізюк Вікторія Анатоліївна – кандидат педагогічних наук, доцент, декан факультету управління, адміністрування та інформаційної діяльності Ізмаїльського державного гуманітарного університету (Ізмаїл, Україна)
- Мірошніченко Валентина Іванівна - доктор педагогічних наук, професор, завдувач кафедри психології, педагогіки та соціально-економічних дисциплін Національної академії Державної прикордонної служби України імені Богдана Хмельницького (Хмельницький, Україна)
- Міхальський Томаш — доктор наук, доцент кафедри географії регіонального розвитку Гданського університету (Польща)
- Огієнко Микола Миколайович - кандидат технічних наук, професор кафедри організації авіаційних робіт та послуг Національного авіаційного університету (Київ, Україна)
- Одарченко Роман Сергійович - завідувач кафедри телекомунікаційних та радіоелектронних систем Національного авіаційного університету (Київ, Україна)
- Оніщенко Наталія Миколаївна - доктор юридичних наук, професор, Заслужений юрист України, академік НАПрН України, завідувач відділу теорії держави і права Інституту держави і права ім. В.М.Корецького НАН України (Київ, Україна)
- Опанасенко Володимир Миколайович — доцент кафедри комп'ютеризованих електротехнічних систем та технологій Національного авіаційного університету (Київ, Україна)
- Охріменко (Жмурко) Тетяна Олександрівна - старший науковий співробітник кафедри комп'ютеризованих систем управління Національного авіаційного університету (Київ, Україна)
- Павлов Костянтин Володимирович — доктор економічних наук, професор, завідувач кафедри підприємництва і маркетингу Волинського національного університету імені Лесі Українки (Луцьк, Україна)
- Паскаль Олена Вікторівна - кандидат педагогічних наук, доцент кафедри педагогічних технологій початкової освіти Державного закладу «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського» (Одеса, Україна)
- Поліщук Віталій Васильович — кандидат сільськогосподарських наук , завідувач відділу зрошення, відділення меліорації Інституту водних проблем і меліорації Національної академії аграрних наук України (Київ, Україна)
- Приходькіна Наталія Олексіївна - доктор педагогічних наук, професор кафедри педагогіки, адміністрування і спеціальної освіти Навчально-наукового інституту менеджменту та психології ДЗВО «Університет менеджменту освіти» НАПН України (Київ, Україна)
- Стахова Анжеліка Петрівна — старший викладач кафедри комп'ютеризованих електротехнічних систем та технологій Національного авіаційного університету (Київ, Україна)
- Турчинова Ганна Володимирівна — кандидат педагогічних наук, доцент, декан факультету природничо-географічної освіти та екології Національного педагогічного університету імені М.П. Драгоманова (Київ, Україна)
- Фесенко Андрій Олексійович - кандидат технічних наук, асистент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. (Київ, Україна)
- Черненко Варвара Петрівна - кандидат фізико-математичних наук, доцент кафедри інформатики і вищої математики Кременчуцького національного університету імені Михайла Остроградського (Кременчук, Україна)
- Чернуха Надія Миколаївна — доктор педагогічних наук, професор, професор кафедри соціальної реабілітації та соціальної педагогіки Київського національного університету імені Тараса Шевченка (Київ, Україна)
- Чумак Оксана Володимирівна - доктор економічних наук, доцент, науковий співробітник відділу статистики і аналітики вищої освіти Державної наукової установи «Інститут освітньої аналітики», (Київ, Україна)
- Шандра Наталія Андріївна - кандидат педагогічних наук, доцент кафедри іноземних мов для природничих факультетів Львівського національного університету імені Івана Франка (Львів, Україна)
- Шеремет Інеса Володимирівна - кандидат педагогічних наук, доцент, доцент кафедри медикобіологічних та валеологічних основ охорони життя і здоров'я Національного педагогічного університету ім. М. П. Драгоманова (Київ, Україна)
- Якимчук Аліна Юріївна - доктор економічних наук, професор, Академік економічних наук України, професор кафедри державного управління, документознавства та інформаційної діяльності Національного університету водного господарства та природокористування (Рівне, Україна)
- Якимчук Олег Феодосійович - керівник групи білінгу Відділу бізнес-систем Департаменту інформаційних технологій ПРаТ «Рівнеобленерго» (Рівне, Україна)
- Яцишин Андрій Васильович - доктор технічних наук, старший науковий співробітник, провідний науковий співробітник Відділу цивільного захисту та інноваційної діяльності Державної установи"Інститут геохімії навколишнього середовища Національної академії наук України" (Київ, Україна)

№ 6(34) 2024
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

ЗМІСТ

СЕРІЯ «Право»

СЕРІЯ «Економіка»

СЕРІЯ «Педагогіка»

СЕРІЯ «Техніка»

СЕРІЯ «Фізико-математичні науки»

№ 6(34) 2024
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

UDC 004.056.55

https://doi.org/10.52058/2786-6025-2024-6(34)-689-703

Krasilenko Volodymyr Grigorovich PhD in Computer Science, Associate Professor, Associate Professor of the Department of Computer Sciences and Economic Cybernetics, Vinnytsia National Agrarian University, St. Sonyachna, 3, Vinnytsia, 21008, tel.: (098) 37-07-440, https://orcid.org/0000-0001-6528-3150

Nikitovich Diana Viktorivna PhD Student, Vinnytsia National Technical University, Khmelnytske shose, 95, Vinnytsia, 21021, tel.: (068) 941-29-72, https://orcid.org/0000-0002-8907-1221

Tytarchuk Yevhenii Oleksandrovich PhD in Computer Science, Senior Lecturer of the Department of Computer Sciences and Economic Cybernetics, Vinnytsia National Agrarian University, St. Sonyachna, 3, Vinnytsia, 21008, tel.: (063) 286-98-73, https://orcid.org/0009-0003-9518-7057

MULTI-PARTY PROTOCOL FOR AGREEMENT OF SHARED SECRET PERMUTATIONS-KEYS OF SIGNIFICANT DIMENSION WITH THEIR ISOMORPHIC REPRESENTATIONS

Abstract. The processes of generating large-dimension permutation matrices and their matrix powers, including in their new isomorphic spaces, are examined, along with their features and advantages for modeling a protocol for the agreement of a main cooperative secret key-permutation by a group of participants. Operations of multiple permutations are proposed instead of raising the corresponding permutation matrices to powers, which are the basic procedures of the proposed cooperative protocol for agreeing on a common secret key-permutation, formed and transmitted in its isomorphic representation. The proposed accelerated methods of raising permutations to significant powers have been verified.

The results of modeling the cooperative protocol for the agreement of the secret key-permutation, its algorithmic steps, and operations have demonstrated the adequacy and advantages of isomorphic representations for describing and functioning processes of matrix models and the proposed protocol. Additionally, the results show that the proposed protocol significantly enhances computational efficiency and security, effectively preventing brute-force attacks even with high-dimensional keys. The practical implications of this work include improved secure communications in distributed systems and potential applications in fields requiring robust cryptographic methods, such as cybersecurity, data protection, and secure communications in IoT networks.

The study demonstrated that isomorphic representations of permutation matrices not only provide high cryptographic strength but also significantly accelerate computational processes, which is critical for applications requiring real-time processing of large data volumes. The verification of the proposed methods confirms their effectiveness and reliability in various usage scenarios.

Keywords: cooperative secret key agreement protocol, matrix models, isomorphic permutation keys, cryptograms, cryptographic transformation

Красиленко Володимир Григорович кандидат технічних наук, с.н.с., доцент, доцент кафедри комп'ютерних наук та економічної кібернетики, Вінницький національний аграрний університет, вул. Сонячна, 3, м. Вінниця, 21008, тел.: (098) 37-07-440, https://orcid.org/0000-0001-6528-3150

Нікітович Діана Вікторівна аспірантка, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021, тел.: (068) 941-29-72, https://orcid.org/0000-0002-8907-1221

Титарчук Євгеній Олександрович кандидат технічних наук, старший викладач кафедри комп'ютерних наук та економічної кібернетики, Вінницький національний аграрний університет, вул. Сонячна, 3, м. Вінниця, 21008, тел.: (063) 286-98-73, https://orcid.org/0009-0003-9518-7057

БАГАТОСТОРОННІЙ ПРОТОКОЛ ДЛЯ УЗГОДЖЕННЯ СПІЛЬНИХ СЕКРЕТНИХ ПЕРЕСТАНОВОК-КЛЮЧІВ ЗНАЧНОГО РОЗМІРУ З ЇХ ІЗОМОРФНИМИ ПРЕДСТАВЛЕННЯМИ

Анотація. Розглядаються процеси генерування матриць перестановок значної розмірності та їх матричних степенів, у тому числі в їх нових ізоморфних просторах, їх особливості та переваги для моделювання протоколу узгодження групою учасників головного кооперативного секретного ключа-перестановки. Запропоновано операції багатократних перестановок замість піднесення відповідних їм матриць перестановок у степені, що є базовими процедурами пропонованого кооперативного протоколу узгодження спільного секретного ключа-перестановки, який формується і передається у його ізоморфному представленні. Верифіковано запропоновані прискорені методи піднесення перестановок у значні степені.

Наведені результати моделювання кооперативного протоколу узгодження секретного ключа-перестановки в цілому, його алгоритмічних кроків, операцій, що продемонстрували адекватність та переваги ізоморфних представлень для опису та процесів функціонування матричних моделей та запропонованого

протоколу. Додатково, результати показують, що запропонований протокол значно покращує обчислювальну ефективність та безпеку, ефективно запобігаючи атакам перебором навіть при використанні ключів високої розмірності. Практичні імплікації цієї роботи включають підвищення безпеки комунікацій у розподілених системах та потенційні застосування в галузях, що потребують надійних криптографічних методів, таких як кібербезпека, захист даних та безпечні комунікації в мережах IoT.

Дослідження продемонструвало, що ізоморфні представлення матричних перестановок не тільки забезпечують високу криптографічну стійкість, але й дозволяють значно прискорити обчислювальні процеси, що є критичним для застосувань, які потребують обробки великих обсягів даних у реальному часі. Верифікація запропонованих методів підтверджує їхню ефективність та надійність у різних сценаріях використання.

Ключові слова: кооперативний протокол узгодження секретного ключа, матричні моделі, ізоморфні ключі-перестановки, криптограми, криптографічне перетворення.

Introduction. In the era of the information society and mass electronic communications, with the widespread use of information technologies (IT), the constant increase in information flow volumes, their significance, and the necessary resilience to potential threats, cryptographic systems hold an important place among the many different technologies, methods, and means of information protection, as they most reliably protect information objects (IO). Over the past two to three decades, the proportion of specific text and graphics documents (TGD) in the form of digital, tabular data, drawings, graphs, diagrams, signatures, visas, resolutions, etc., which are large-dimensional images that need to be transmitted secretly, has significantly increased. Many of them contain information with restricted or closed access, which must be provided as reports to government authorities and certified with digital signatures. Most of the methods and means of cryptographic transformations (CT) of information arrays and images are oriented toward the sequential scalar processing of TGD blocks, converted into digital formats. One of the key issues in the application of cryptography and steganography is the processes (protocols) of agreeing on common secret keys or a series of derived sub-keys. However, most protocols, such as Diffie-Hellman, MTI, STS, etc., as well as most methods of cryptographic transformations of IO, are oriented toward purely scalar keys and sequential block processing. Even for symmetric, widely used algorithms (based on the current AES, IDEA standard, etc.), typical block and key lengths are 256-1024 bits, although for some exceptional ciphers like FEAL, RC6, and other modern modifications of a wide range of known ciphers, these lengths are limited to 1024-2048 bits [1]. The transition from scalar data formats in known systems to more appropriate and natural matrix-tensor formats has intensified the search for

new matrix-algebraic models (MAM) of cryptographic transformations of 2D (3D) arrays, images. The pace of development of cryptanalysis methods and computational tools prompts the increase of key lengths (KL), making the search for new concepts oriented toward parallel matrix processors and matrix-type models (MT) relevant. Based on matrix-algebraic models, a new class of matrix-type cryptosystems (MTC) has emerged [2- 5]. In response to the increasing complexity of the tasks being solved and the amount of information, which more often need to be processed in real-time, the creation of high-performance parallel matrix or multiprocessor computers and algorithms has led to a series of modifications of known CT algorithms and the creation of corresponding matrix-type (MT) models [6-11]. The advantages of such cryptosystems based on matrix-algebraic models, identified in these works, have intensified research on matrix-algebraic models and led to publications [6-10] demonstrating a range of new improvements and proposing extensions of their effective application areas.

Analysis of Recent Research and Publications. Matrix affine and affine-permutation ciphers (MAPC) based on new advanced matrix-algebraic models have been studied and used for cryptographic transformations (CT) of images, creating enhanced electronic digital signatures [11-15], for masking (hiding) images and video files [16-19], and for generating necessary streams of secret matrix keys of various types [20-21]. The use of the proposed matrix approach and matrix-algebraic models has enabled the creation of block [7], parametric [9], and multipage [10] cryptographic models with increased cryptographic strength [10] for 2D arrays, black-and-white, and color images, and to check the integrity of cryptograms and the presence of distortions [5, 6, 8]. The functioning of all such matrix-algebraic models has been confirmed by simulation modeling, demonstrating the advantages of such models and algorithms: expanded functional capabilities and better performance in their hardware implementations on matrix processors.

These facts indicate that traditional processes (protocols) for electronically agreeing on common secret keys [22], or a series of derived sub-keys, should be adapted to new challenges [23-25], including matrix-type cryptosystems [24, 26, 27]. For practically all known algorithms and ciphers, including newly developed ones [5-14], bit, byte, or group permutation procedures are the most common and mandatory. One of the main components of generalized multi-step matrix affine-permutation ciphers is the matrix permutation models (MPM) [3, 5, 6], which have visual simplicity. The modified matrix permutation models with bit-slice decomposition proposed in [27] eliminates the shortcomings of simple MPM but requires two matrix keys (MK) and two vector keys (VK).

The implementation of all the above-mentioned matrix models (MM) requires specific keys in the form of two-dimensional arrays (images). The need for CT over large-dimensional multi-dimensional IO, images, also necessitates not only matrix-algebraic models of CT but also secret matrix keys (MK) [27, 28]. Further

improvements of MM CT for encrypting multi-dimensional signals, multi-spectral images of various physical and aerospace objects, require homogeneous secret matrix keys consistent with their structure, such as matrices (images) [28, 29]. Similar MK are needed for the modified MM CT with cryptogram integrity verification [6]. Additionally, these MK for such MM must account for the specifics and structure of formats and extensions characteristic of black-and-white multi-gradation, color, and multi-spectral images.

Problem Statement. In 2009, for matrix keys of the 1st type in the form of a random (noisy) image, a generalization of the Diffie-Hellman protocol to the matrix case and a method for forming images matrix keys were proposed (MK_I). The improvement of such matrix protocols through the application of enhanced methods for organizing accelerated computations based on parallel matrix logic is addressed in works [26, 27], where the advantages of multi-step, multi-stage protocols for agreeing on a secret MK were confirmed by model experiments. For matrix affine and affine-permutation ciphers, in addition to such MK, it is also necessary to have matrix keys of the 2nd type, namely, a set of binary permutation matrices [3, 6, 26, 27], here denoted as MK_P. The issues of their formation and application were partially addressed in [3, 6, 26], and only in [28] was a protocol for agreeing on MK of the MK_P type proposed. However, it did not consider protocols for cases of agreeing on an MK_P that would be common to all group members, i.e., situations where participants wish to create their cooperative group MK_P.

Unlike the protocols in [26, 27], a so-called cooperative protocol was considered in [29], but it was related to MK_I. It is known from [6, 8] that generating a series of permutation keys (MK_P type) derived from a main matrix key (MMK_P with significantly increased dimensions) successfully addresses the problem of resilience. Therefore, the task of agreeing on a large-dimensional secret main key (MK_P type), specifically cooperative for group participants, is relevant and important. The aim of this work is to develop, model, and study a cryptographic cooperative protocol for agreeing on a common secret MK_P for matrix-algebraic models CT, based on the application of new isomorphic representations of MK_P and the analysis of protocol procedures.

Presentation of Main Results. In our first experiment, the MK_P was a bitwise square matrix (PSAB) with dimensions of 256x256 elements. The simulation of the protocol for the case of raising MK_P to random powers, known only to the parties involved in the exchange (two for clarity), is shown in Figure 1. Even knowing the MK_P—basis, given the significant complexity of the permutation set (N! = 256!, where N is the dimension of MK_P), does not allow the key to be discovered without intercepting both MK_Ps created by the parties.

If the input message is represented as a vector with elements from a chosen range, permutation matrices and vector-matrix procedures can be used to rearrange the components of the vector. By multiplying the matrix corresponding to the

explicit input image on the left and right by the appropriate permutation matrices, the columns and rows of such a matrix are mixed accordingly. This representation of permutation ciphers does not ensure the maximum possible number of permutations, as the elements of rows or columns are shuffled according to the same rules. Permutations can be described by other models as well [1], but in our opinion, the most convenient and adequate for describing cryptographic transformations of images by permuting their pixels are matrix models of the type SPXY=KPX·SI·KPY, where SI is the input message matrix of a given dimension, and KPX and KPY are square permutation matrices along one and the other coordinate respectively, with dimensions consistent with the number of rows and columns. The basis of these models consists of permutation matrices P, which are matrices where each column and each row contains only one element equal to 1, and all other elements are 0 [9, 11]. The cardinality of the set of all possible P matrices of dimension k×k is estimated by the value K = f(k) = k!.

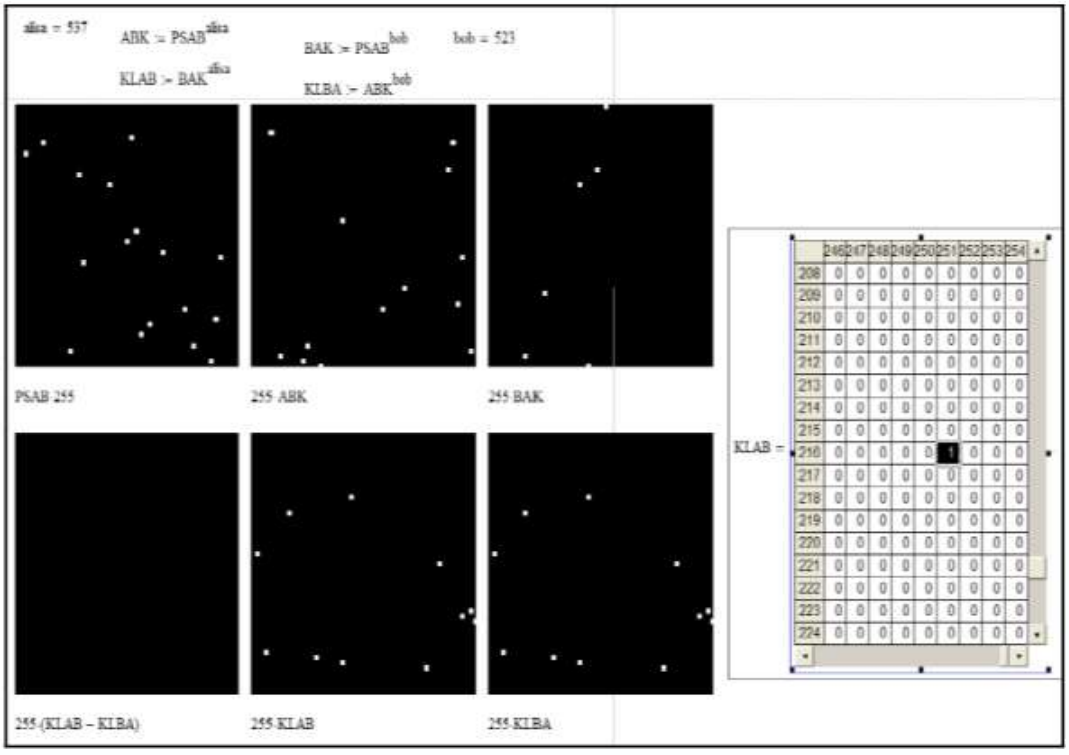

Fig. 1 Fragment of the Mathcad window showing the verification of the modified Diffie-Hellman protocol for the case of raising MK_P to powers (537 and 523), used as the basis. The basis (256x256 PSAB matrix), intermediate MK_Ps (ABK, BAK) exchanged between the parties, and the resulting keys (KLAB, KLBA), which are identical, are displayed.

In the second experiment, the MK_P was a bitwise square matrix with N*N elements ("0" or "1"), where N=2^16, which increased the complexity of the permutation set to (65536!). Thus, any permutation of length 65536 (a 65536×65536

bitwise matrix) can be uniquely isomorphically represented by two matrices of size 256x256, with elements taking values in the range 0-255. The Mathcad window with the module for generating the base (main) MK_P (MMK_P) and the appearance of its components KeyA and KeyB (two halftone images) is shown in Figure 2. The software module (Mathcad copies) that implements the iterative permutation procedure in MK_P, isomorphic to raising the permutation matrix to the required power, is shown in Figure 3. Similar modules were used for all step-by-step procedures in the simulation of the cooperative protocol.

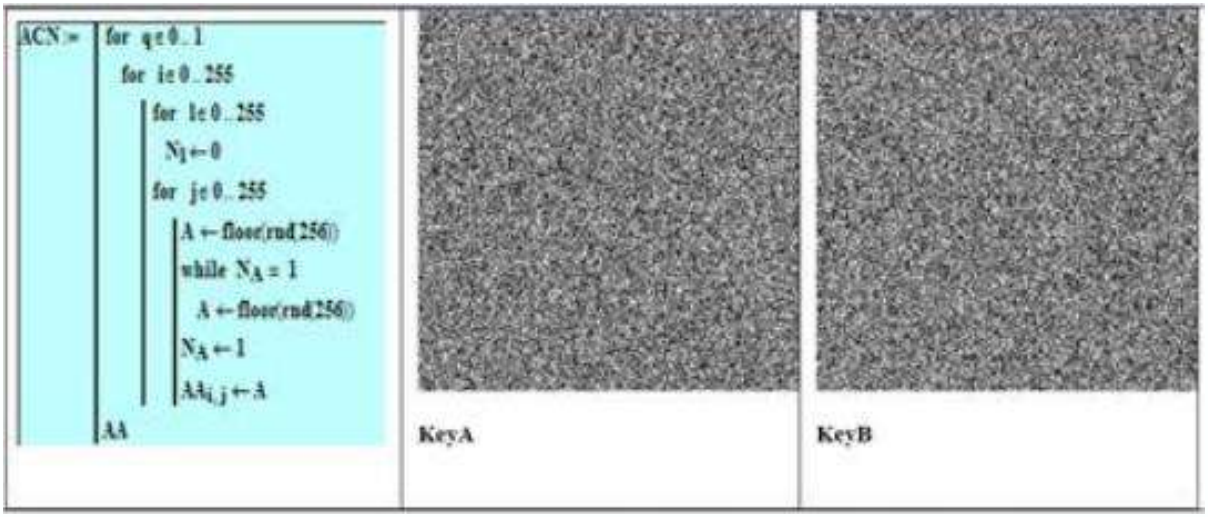

Fig. 2 Software module for generating the base (main) MK_P and the appearance of its two components, KeyA and KeyB, in the format of two black-and-white images (Mathcad window).

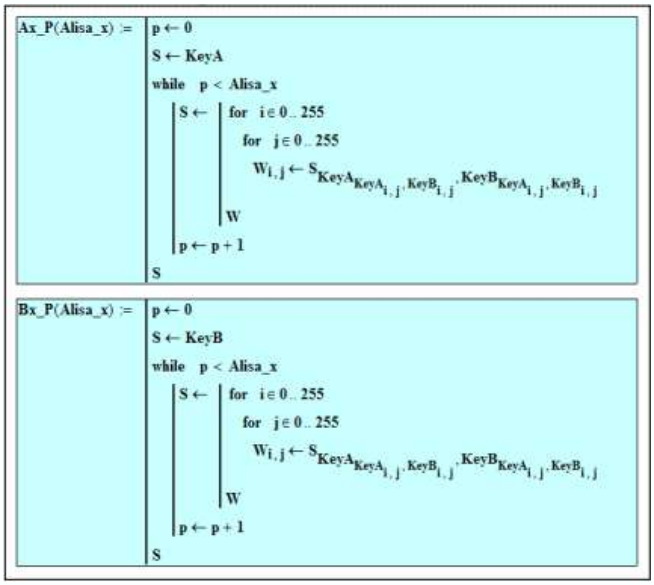

Fig. 3 Software modules (copies from Mathcad) illustrating the iterative permutation procedure in MK_P, isomorphic to raising the permutation matrix to the required power by party x (Alice).

Raising permutation matrices MK_P (N*N binary, where $N = 2^{16}$) is equivalently replaced by fast permutations, which can be further accelerated at significant powers by using a certain basic set of fixed (fixed powers of MMK_P) and specific sequences. We verified the adequacy of the accelerated algorithms for isomorphic formation of matrix permutation powers through modeling. For this purpose, bitwise matrices raised to a matrix power were compared with matrices obtained through fast permutations after being converted to their isomorphic form. The results of modeling the cooperative protocol for the case of three parties are shown in Figures 4-7. The protocol is executed as follows.

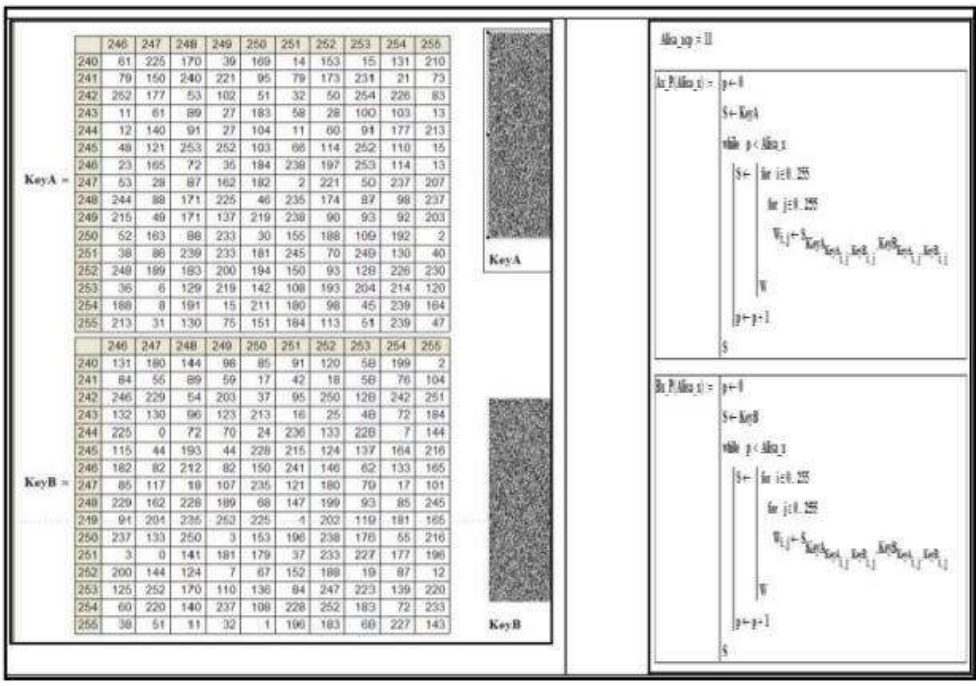

Fig. 4 Mathcad window with the selected large-dimensional MK_P, isomorphically represented by two components (KeyA, KeyB) in digital and visual forms (left), and the software module for multiple permutations (right).

Each party x, y, z (Alice, Bob, David) selects a common MK_P as the basis, isomorphically represented by its components (KeyA, KeyB), and follows a sequential exchange of the intermediate MK_Ps formed at each step. These intermediate MK_Ps are created as powers of the basis, depending on the chosen secret identifiers-numbers: Alice_x, Bob_y, David_z, using the permutation software modules described and shown in Figures 3-4. Each party, in the first step, raises the isomorphic MMK_P to their chosen secret power, which is typically a large pseudorandom number of the order of typical values used today in cryptography to significantly increase the computational complexity in brute-force attacks on one-way functions. After this, each party sends the new MK_P to the other party along the chosen transmission path.

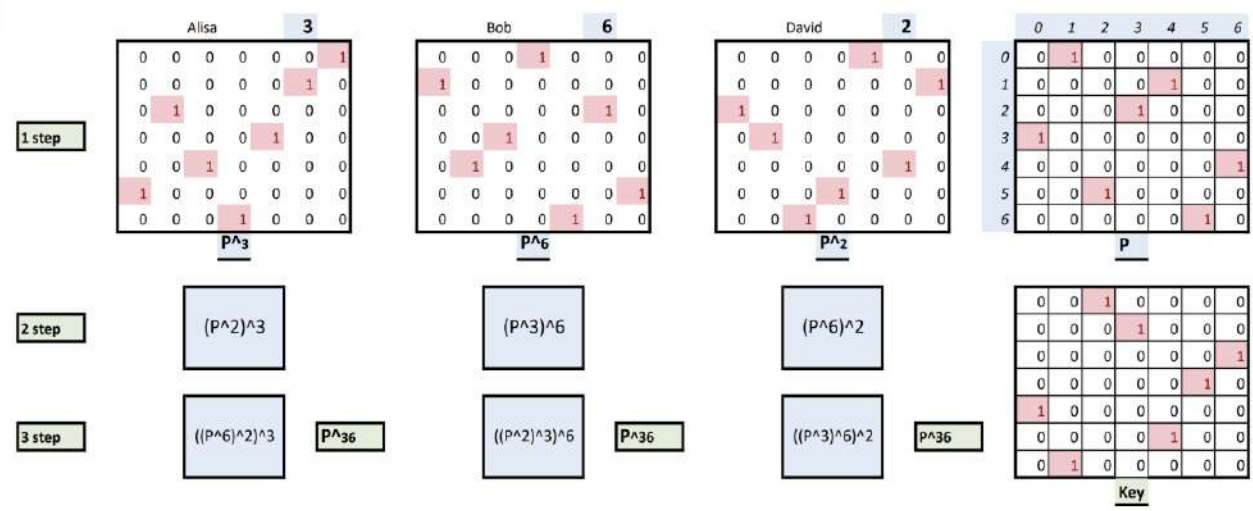

Fig. 5 Scheme of partial key exchange between participants.

To generate a common encryption key, users independently form an asymmetric key pair based on the common parameters of the chosen cryptosystem, and then by exchanging them, they form a shared secret key. Specifically, each participant, responding to another participant's request, raises the matrix P to the power of their chosen secret key and returns the result. This process must be repeated exactly N-1 times; if there are more requests, a Man-in-the-Middle attack may be occurring, and the connection should be terminated. After the final request, each participant multiplies the key by their own private key, thereby forming the shared symmetric encryption key. [25]

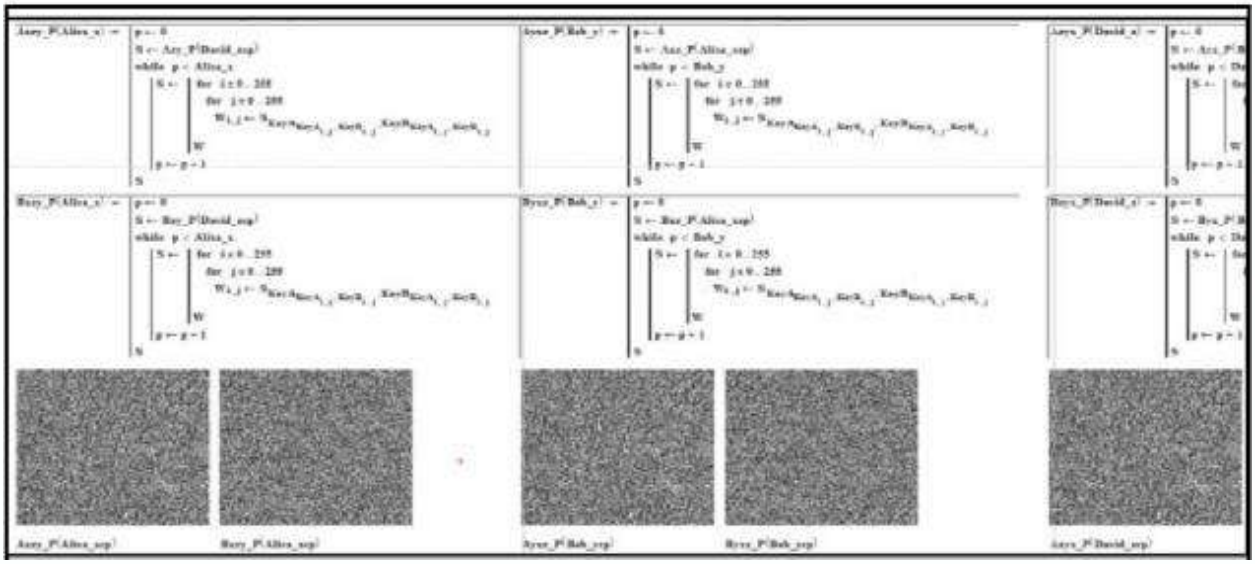

Fig. 6 Fragments of the Mathcad window for modeling the processes of forming the secret MK_P by three parties (Alice, Bob, David): modules for permutations, appearance of the keys.

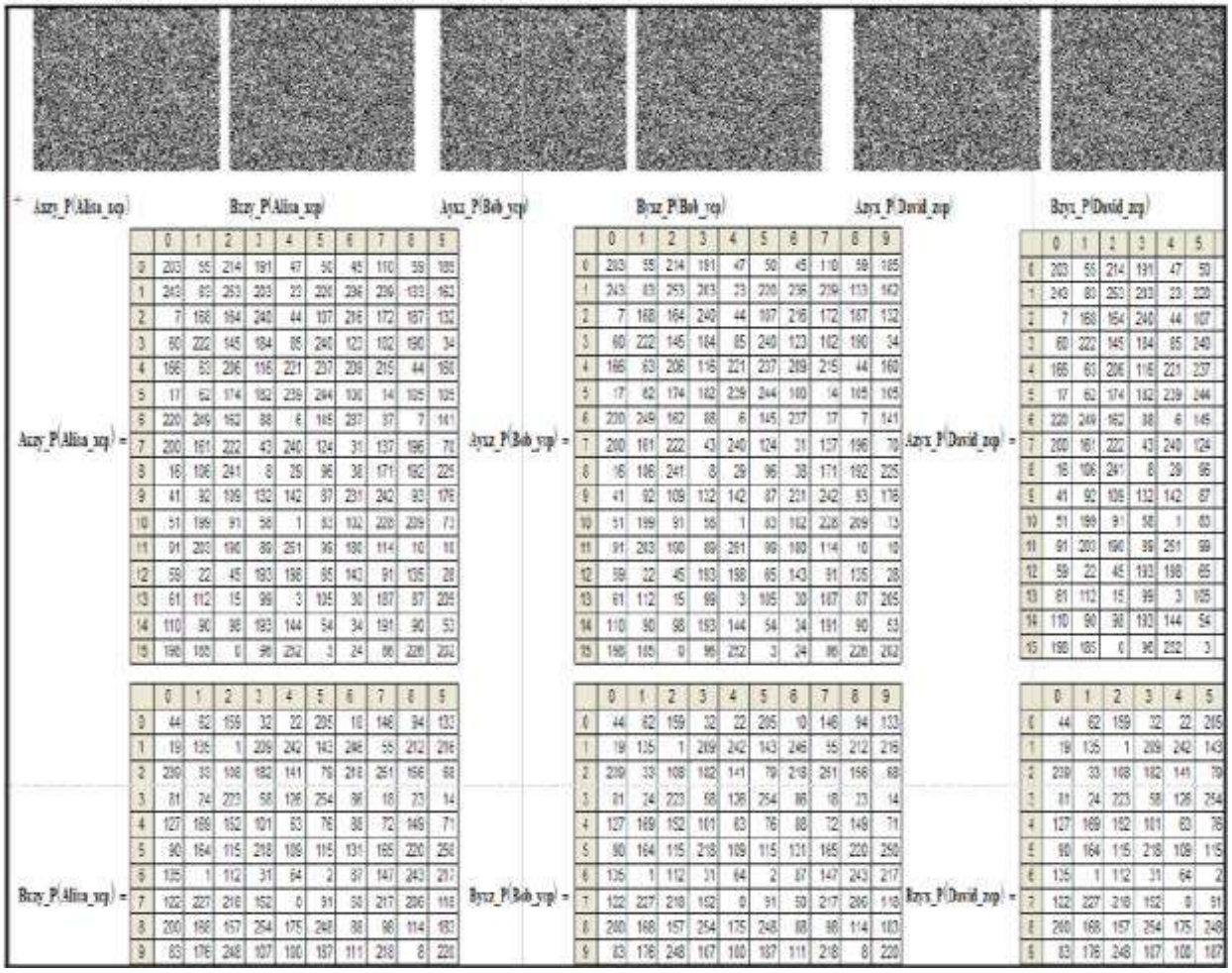

Fig. 6 Copy of the Mathcad window showing the equal secret MK_P keys formed by the three parties, presented as their two isomorphic components.

The formed MK_P (two matrices of 256x256 bytes) are transmitted by each party to their neighbors along the path, and then the received MK_Ps are raised again to their respective powers, as shown in Figures 5-7. All protocol actions are performed with the isomorphic form of MK_P, not with scalars. 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 (Figure 6) 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 $(2^{16})!$.

Conclusions. The modeling of the protocol for agreeing on a cooperative secret large-dimensional permutation key has been completed, confirming its correct

operation and the adequacy of the algorithmic steps and methods for forming the intermediate and final MK_P. The algorithms for accelerated exponentiation of permutation matrices while preserving their isomorphic representations have been verified, demonstrating their advantages.

References:

1. Zeadally, S., Das, A. K., & Sklavos, N. (2019). Cryptographic technologies and protocol standards for Internet of Things. *Internet of Things*. doi: 10.1016/j.iot.2019.100075. Elsevier.

2. Krasilenko, V. H., & Flavytska, Yu. A. (2009). Modelyuvannya matrychnykh alhorytmiv kryptohrafichnoho zakhystu [Modeling of matrix algorithms for cryptographic protection]. *Visnyk NU "Lviv. politekhnika"*, (658), 59-63 [in Ukrainian].

3. Krasilenko, V. H., & Hrabovlyak, S. K. (2012). Matrychni afinno-perestanovochni alhorytmy dlya shyfruvannya ta deshyfruvannya zobrazhen [Matrix affine-permutation algorithms for encryption and decryption of images]. *Systemy obrobky informatsiyi*, 3(2), 53-61 [in Ukrainian].

4. Krasilenko, V. H., & Dubchak, V. M. (2014). Kryptohrafichni peretvorennya zobrazhen na osnovi matrychnykh modelei perestanovok z matrychno-bitovozrizovoyu dekompozytsiyeyu ta yikh modelyuvannya [Cryptographic transformations of images based on matrix permutation models with matrix-bit slice decomposition and their modeling]. *Visnyk KhNU. Tekhnichni nauky*, (1), 74-79 [in Ukrainian].

5. Krasilenko, V. H., Ohornyk, K. V., & Flavytska, Yu. A. (2010). Modelyuvannya matrychnykh afinnykh alhorytmiv dlya shyfruvannya koliorovykh zobrazhen [Modeling of matrix affine algorithms for encrypting color images]. *Komp'yuterni tekhnolohiyi: nauka i osvita: V Vseukr. NPK*, 120-124 [in Ukrainian].

6. Krasilenko, V. H., & Nikitovych, D. V. (2016). Modelyuvannya ta doslidzhennya kryptohrafichnykh peretvoren zobrazhen na osnovi yikh matrychno-bitovo-zrizovoyi dekompozytsiyi ta matrychnykh modelei perestanovok z veryfikatsiyeyu tsilisnosti [Modeling and research of cryptographic transformations of images based on their matrix-bit slice decomposition and matrix permutation models with integrity verification]. *Elektronika ta informatsiyni tekhnolohiyi*, (6), 111-127 [in Ukrainian].

7. Krasilenko, V. H., & Nikitovych, D. V. (2017). Modeli blokovykh matrychnykh afinno-perestanovochnykh shyfriv (MAPSh) dlya kryptohrafichnykh peretvoren ta yikh doslidzhennya [Block matrix affine-permutation ciphers (MAPSh) models for cryptographic transformations and their research]. In *72 NTK: materialy konferentsiyi (13-15 hrudnya 2017 r.)* (pp. 117-122), Odesa: Popov Odesa National Academy of Telecommunications [in Ukrainian].

8. Krasilenko, V. H., & Nikitovych, D. V. (2016). Modelyuvannya kryptohrafichnykh peretvoren koliorovykh zobrazhen na osnovi matrychnykh modelei perestanovok zi spektralnoyu ta bitovo-zrizovoyu dekompozytsiyamy [Modeling of cryptographic transformations of color images based on matrix permutation models with spectral and bit-slice decompositions]. *Komp'yuterno-intehrovani tekhnolohiyi: osvita, nauka, vyrobnytstvo*, (23), 31-36 [in Ukrainian].

9. Krasilenko, V. H., & Nikitovych, D. V. (2017). Bahatofunktsionalni parametrychni matrychno-alhebraichni modeli (MAM) kryptohrafichnykh peretvoren (KP) z operatsiyamy za modulem ta yikh modelyuvannya [Multifunctional parametric matrix-algebraic models (MAM) of cryptographic transformations (KP) with modular operations and their modeling]. In *72 NPK: materialy konferentsiyi (13-15 hrudnya 2017 roku)* (pp. 123-128), Odesa: Popov ONAT [in Ukrainian].

10. Krasilenko, V. H., & Nikitovych, D. V. (2018). Modelyuvannya storinkovykh kryptohrafichnykh peretvoren masyvov koliorovykh zobrazhen na osnovi matrychnykh modelei ta perestanovok [Modeling of paged cryptographic transformations of color image arrays based on matrix models and permutations]. In *Informatsiyno-komp'yuterni tekhnolohiyi – 2018: Zbirnyk tez dopovidey IX Mizhnarodnoyi NTK (20-21 kvitnya 2018 roku)* (pp. 73-77), Zhytomyr: Vyd. O. O. Yevhenok [in Ukrainian].

11. Krasilenko, V. H., & Hrabovlyak, S. K. (2011). Matrychni afinni shyfry dlya stvorennya tsyfrovykh slypykh pidpysiv na tekstohrafichni dokumenty [Matrix affine ciphers for creating digital blind signatures on textographic documents]. *Systemy obrobky informatsiyi*, 7(97), 60-63 [in Ukrainian].

12. Krasilenko, V. H., Yatskovska, R. O., & Trifonova, Yu. M. (2013). Demonstratsiya protsesiv stvorennya slypykh elektronnykh tsyfrovykh pidpysiv na tekstohrafichnu dokumentatsiyu na osnovi modelei matrychnoho typu [Demonstration of processes for creating blind electronic digital signatures on textographic documentation based on matrix-type models]. *Systemy obrobky informatsiyi*, 3(110), T. 2, 18-22 [in Ukrainian].

13. Krasilenko, V. H., & Nikitovych, D. V. (2017). Vdoskonalennya ta modelyuvannya elektronnykh tsyfrovykh pidpysiv matrychnoho typu dlya tekstohrafichnykh dokumentiv [Improvement and modeling of electronic digital signatures of matrix type for textographic documents]. In *Materialy VI MNPK "Informatsiyni upravlyayuchi systemy ta tekhnolohiyi" (IUST-Odesa-2017)* (pp. 312-318), Odesa: VydavInform NU "OMA" [in Ukrainian].

14. Krasilenko, V. H., & Nikitovych, D. V. (2018). Modelyuvannya pokrashchenykh slypykh elektronnykh tsyfrovykh pidpysiv 2D typu [Modeling of improved 2D type blind electronic digital signatures]. In *Informatsiyno komp'yuterni tekhnolohiyi – 2018: Zbirnyk tez dopovidey IX MNPK (April 20-21., 2018)* (pp. 78-82), Zhytomyr: Vyd. O. O. Yevhenok [in Ukrainian].

15. Krasilenko, V. H., Nikitovych, D. V., Yatskovska, R. O., & Yatskovskyi, V. I. (2019). Modelyuvannya pokrashchenykh bahatokrokovykh 2D RSA alhorytmiv dlya kryptohrafichnykh peretvoren ta slypoho elektronnoho tsyfrovoho pidpysu [Modeling of improved multi-step 2D RSA algorithms for cryptographic transformations and blind electronic digital signature]. *Systemy obrobky informatsiyi: zbirnyk naukovykh prats*, 1(156), 92-100 [in Ukrainian].

16. Vostrikov, A., & Sergeev, M. (2015). Expansion of the Quasi-Orthogonal Basis to Mask Images. *Intelligent Interactive Multimedia Systems and Services, Smart Innovations, Systems and Technologies 40*. Springer, 161-168. doi: 10.1007/978-3-319-19830-9_15.

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

18. Krasilenko, V. H., Kychak, V. M., Nikolskyi, A. I., Lazarev, A. A., & Nikitovych, D. V. (2023). Simulation of algorithms for detection, localization and tracking of moving objects in video streams. In *Materialy IX konferentsiyi "Suchasni problemy infokomunikatsiy, radioelektroniky ta nanosystem (SPIRN-2023)"* (pp. 15-17), Vinnytsia. Retrieved from https://conferences.vntu.edu.ua/index.php/spirn/spirn2023/paper/download/19349/16036 [in Ukrainian]

19. Krasilenko, V. H., 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.

20. Krasilenko, V. H., Podlubnyi, V. F., & Nikitovych, D. V. (2023). Modeling a method for generating a stream of secret keys in the form of permutation matrices for encryption-masking of video frames and studying its characteristics. In *2nd International Conference on Innovative Solutions in Software Engineering* (pp. 222-231), Ivano Frankivsk. doi: 10.5281/zenodo.10397356.

21. Krasilenko, V. H., & Nikitovych, D. V. (2018). Modelyuvannya protsesiv heneruvannya matrychnykh klyuchiv [Modeling of matrix key generation processes]. In *Informatsiyni tekhnolohiyi v osviti, nautsi i tekhnitsi (ITONT-2018): Zbirnyk tez dopovidey IV MNPK (17-18 travnya 2018 roku)* (pp. 32-35), Cherkasy: ChDTU [in Ukrainian].

22. Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644-654.

23. Luzhetskyi, V., & Horbenko, I. (2015). Metody shyfruvannya na osnovi perestanovky blokiv zminnoyi dovzhyny [Encryption methods based on variable length block permutation]. *Zakhyst informatsiyi*, 17(2), 169-175 [in Ukrainian].

24. Biletskyi, A. Ya., Biletskyi, A. A., & Kandyba, R. Yu. (2012). Matrychni analohy protokolu Diffie-Hellmana [Matrix analogs of the Diffie-Hellman protocol]. *Avtomatyka, vymiryuvannya ta keruvannya: Visnyk nats. un-tu "Lvivska politekhnika"*, (741), 128-133. [in Ukrainian].

25. Kvietnyi, R. N., Tytarchuk, Ye. O., & Hurzhiy, A. A. (2016). Method and algorithm of key exchange among groups of users based on asymmetric ciphers ECC and RSA. *Informatsiyni tekhnolohiyi ta komp'yuterna inzheneriya*, (3), 38-43 [in Ukrainian].

26. Krasilenko, V. H., & Nikitovych, D. V. (2017). Modelyuvannya protokoliv uzhodzhennya sekretnogo matrychnoho klyucha dlya kryptohrafichnykh peretvoren ta system matrychnoho typu [Modeling protocols for agreeing on a secret matrix key for cryptographic transformations and matrix-type systems]. *Systemy obrobky informatsiyi*, 3(149), 151-157 [in Ukrainian].

27. Krasilenko, V. H., & Nikitovych, D. V. (2017). Modelyuvannya bahatokrokovykh ta bahatostupenevykh protokoliv uzhodzhennya sekretnykh matrychnykh klyuchiv [Modeling of multi-step and multi-level protocols for agreeing on secret matrix keys]. *Komp'yuterno-intehrovani tekhnolohiyi: osvita, nauka, vyrobnytstvo: naukovyy zhurnal*, Lutsk: LNTU, (26), 111-120 [in Ukrainian].

28. Krasilenko, V. H., & Nikitovych, D. V. (2020). Protokoly uzhodzhennya sekretnykh klyuchiv u vyhliadi matrychnykh perestanovok znachnoi rozmirnosti dlya kryptohrafichnykh peretvoren [Protocols for agreeing on secret keys in the form of large-dimension matrix permutations for cryptographic transformations]. In *Tezy dopovidey XI MNPK "IKT – 2020" (April 9-11, 2020 r.)* (pp. 39-49), Zhytomyr. [in Ukrainian]

29. Krasilenko, V. H., & Nikitovych, D. V. (2018). Kooperatyvnyi protokol uzhodzhennya spilnoho sekretnogo matrychnoho klyucha [Cooperative protocol for agreeing on a common secret matrix key]. In *Materialy VII MNPK (IUST) (September 17-18, 2018 r.)* (pp. 122-127), Odesa: Popov ONAT [in Ukrainian].

Література:

1. Zeadally, S., Das, A. K., & Sklavos, N. (2019). Cryptographic technologies and protocol standards for Internet of Things. *Internet of Things*. doi: 10.1016/j.iot.2019.100075. Elsevier.

2. Красиленко, В. Г., & Флавицька, Ю. А. (2009). Моделювання матричних алгоритмів криптографічного захисту. *Вісник НУ «Львів. політехніка»*, (658), 59-63.

3. Красиленко, В. Г., & Грабовляк, С. К. (2012). Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень. *Системи обробки інформації*, 3(2), 53-61.

4. Красиленко, В. Г., & Дубчак, В. М. (2014). Криптографічні перетворення зображень на основі матричних моделей перестановок з матрично-бітовозрізовою декомпозицією та їх моделювання. *Вісник ХНУ. Технічні науки*, (1), 74-79.

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

6. Красиленко, В. Г., & Нікітович, Д. В. (2016). Моделювання та дослідження криптографічних перетворень зображень на основі їхньої матрично-бітово зрізової декомпозиції та матричних моделей перестановок з верифікацією цілісності. *Електроніка та інформаційні технології*, (6), 111-127.

7. Красиленко, В. Г., & Нікітович, Д. В. (2017). Моделі блокових матричних афінно перестановочних шифрів (МАПШ) для криптографічних перетворень та їх дослідження. In *72 НТК: матеріали конференції (13-15 грудня 2017 р.)* (pp. 117-122), Одеса: ОНАЗ ім. Попова

8. Красиленко, В. Г., & Нікітович, Д. В. (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.

9. Красиленко, В. Г., & Нікітович, Д. В. (2017). Багатофункціональні параметричні матрично-алгебраїчні моделі (МАМ) криптографічних перетворень (КП) з операціями за модулем та їх моделювання. In *72 НПК: матеріали конференції (13-15 грудня 2017 року)* (pp. 123-128), Одеса: ОНАЗ ім. О. С. Попова.

10. Красиленко, В. Г., & Нікітович, Д. В. (2018). Моделювання сторінкових криптографічних перетворень масивів кольорових зображень на основі матричних моделей та перестановок. In *Інформаційно-комп'ютерні технології – 2018: Збірник тез доповідей IX Міжнародної НТК (20-21 квітня 2018 року)* (pp. 73-77), Житомир: Вид. О. О. Євенок.

11. Красиленко, В. Г., & Грабовляк, С. К. (2011). Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи. *Системи обробки інформації*, 7(97), 60-63.

12. 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.

13. Красиленко, В. Г., & Нікітович, Д. В. (2017). Вдосконалення та моделювання електронних цифрових підписів матричного типу для текстографічних документів. In *Матеріали VI МНПК «Інформаційні управляючі системи та технології» (ІУСТ-Одеса-2017)* (pp. 312-318), Одеса: ВидавІнформ НУ «ОМА».

14. Красиленко, В. Г., & Нікітович, Д. В. (2018). Моделювання покращених сліпих електронних цифрових підписів 2D типу. In *Інформаційно комп'ютерні технології – 2018: Збірник тез доповідей IX МНПК (20-21 квітня 2018 року)* (pp. 78-82), Житомир: Вид. О. О. Євенок.

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: збірник наукових праць*, 1(156), 92-100.

16. Vostrikov, A., & Sergeev, M. (2015). Expansion of the Quasi-Orthogonal Basis to Mask Images. *Intelligent Interactive Multimedia Systems and Services, Smart Innovations, Systems and Technologies 40*. Springer, 161-168. doi: 10.1007/978-3-319-19830-9_15.

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

18. Красиленко, В. Г., Кичак, В. М., Никольский, А. И., Лазарев, А. А., & Нікітович, Д. В. (2023). Simulation of algorithms for detection, localization and tracking of moving objects in video streams. In *Матеріали IX конференції «Сучасні проблеми інфокомунікацій, радіоелектроніки та наносистем (СПІРН-2023)*, Вінниця, 15-17 листопада 2023 р. Retrieved from https://conferences.vntu.edu.ua/index.php/spirn/spirn2023/paper/download/19349/16036

19. 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.

20. Красиленко, В. Г., Подлубний, В. Ф., & Нікітович, Д. В. (2023). Modeling a method for generating a stream of secret keys in the form of permutation matrices for encryption-masking of video frames and studying its characteristics. In *2nd International Conference on Innovative Solutions in Software Engineering* (pp. 222-231), Ivano Frankivsk. doi: 10.5281/zenodo.10397356.

21. Красиленко, В. Г., & Нікітович, Д. В. (2018). Моделювання процесів генерування матричних ключів. In *Інформаційні технології в освіті, науці і техніці (ІТОНТ 2018): Збірник тез доповідей IV МНПК (17-18 травня 2018 року)* (pp. 32-35), Черкаси: ЧДТУ.

22. Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644-654.

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

24. 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.

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

26. Красиленко, В. Г., & Нікітович, Д. В. (2017). Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу. *Системи обробки інформації*, 3(149), 151-157.

27. Красиленко, В. Г., & Нікітович, Д. В. (2017). Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів. *Комп`ютерно-інтегровані технології: освіта, наука, виробництво: науковий журнал*, Луцьк: ЛНТУ, (26), 111-120.

28. Красиленко, В. Г., & Нікітович, Д. В. (2020). Протоколи узгодження секретних ключів у вигляді матричних перестановок значної розмірності для криптографічних перетворень. In *Тези доповідей XI МНТК «ІКТ – 2020» (9-11 квітня 2020 р.)* (pp. 39-49), Житомир.

29. Красиленко, В. Г., & Нікітович, Д. В. (2018). Кооперативний протокол узгодження спільного секретного матричного ключа. In *Матеріали VII МНПК (ІУСТ) (17-18 вересня 2018 р.)* (pp. 122-127), Одеса: ОНПУ; ред. кол: В. В. Вичужанін.