ISSN 2307-5732
DOI 10.31891/2307-5732

НАУКОВИЙ ЖУРНАЛ

2.2021

ВІСНИК

Хмельницького національного університету

Технічні науки

Technical sciences

SCIENTIFIC JOURNAL
HERALD OF KHMELNYTSKYI NATIONAL UNIVERSITY

2021, Issue 2, Volume 295

Хмельницький

ВІСНИК
ХМЕЛЬНИЦЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
серія: Технічні науки

Затверджений як фахове видання категорії «Б»,
РІШЕННЯ АТЕСТАЦІЙНОЇ КОЛЕГІЇ № 1643 ВІД 28.12.2019 та №409 від 17.03.2020

Засновано в липні 1997 р. ***Виходить 6 разів на рік***

Хмельницький, 2021, № 2(295)

Засновник і видавець: Хмельницький національний університет
(до 2005 р. – Технологічний університет Поділля, м. Хмельницький)

Включено до науково-метричних баз:

Google Scholar	http://scholar.google.com.ua/citations?hl=uk&user=aIUP9OYAAAAJ
Index Copernicus	http://jml2012.indexcopernicus.com/passport.php?id=4538&id_lang=3
Polish Scholarly Bibliography	https://pbn.nauka.gov.pl/journals/46221
CrossRef	http://doi.org/10.31891/2307-5732

Рекомендовано до друку рішенням вченої ради Хмельницького національного університету, протокол № 17 від 27.05.2021 р.

Адреса редакції: редакція журналу "Вісник Хмельницького національного університету"
Хмельницький національний університет
вул. Інститутська, 11, м. Хмельницький, Україна, 29016

☎ (038-2) 67-51-08 **web:** http://journals.khnu.km.ua/vestnik
http://lib.khnu.km.ua/visnyk_tup.htm

e-mail: visnyk.khnu@khmnu.edu.ua
visnyk.khnu@gmail.com

Зареєстровано Міністерством України у справах преси та інформації.
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
Серія КВ № 9722 від 29 березня 2005 року

ЗМІСТ

ЕКОЛОГІЯ

КОМП'ЮТЕРНІ НАУКИ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІ, СИСТЕМНИЙ АНАЛІЗ ТА КІБЕРБЕЗПЕКА

МАШИНОБУДУВАННЯ, МЕХАНІКА ТА МАТЕРІАЛОЗНАВСТВО

ЕЛЕКТРОМЕХАНІКА, ЕЛЕКТРОТЕХНІКА ТА ЕНЕРГЕТИКА

АВТОМАТИЗАЦІЯ, ТЕЛЕКОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

ТЕХНОЛОГІЇ ХІМІЧНОЇ, ХАРЧОВОЇ ТА ЛЕГКОЇ ПРОМИСЛОВОСТІ

DOI 10.31891/2307-5732-2021-293-1-78-88
УДК 637.5.02

В.Г. КРАСИЛЕНКО, Н.П. ЮРЧУК
Вінницький національний аграрний університет
Д.В. НІКІТОВИЧ
Вінницький національний технічний університет

ЗАСТОСУВАННЯ ІЗОМОРФНИХ МАТРИЧНИХ ПРЕДСТАВЛЕНЬ ДЛЯ МОДЕЛЮВАННЯ ПРОТОКОЛУ УЗГОДЖЕННЯ СЕКРЕТНИХ КЛЮЧІВ-ПЕРЕСТАНОВОК ЗНАЧНОЇ РОЗМІРНОСТІ

Для моделювання протоколу узгодження сторонами секретних ключів-перестановок значної розмірності запропоновано їх нові ізоморфні матричні представлення та розглянуто особливості та переваги таких представлень. Наведено результати моделювання процесів генерування матриць перестановок та їх степенів, як базових процедур пропонованого протоколу узгодження ключа у вигляді ізоморфної перестановки значної розмірності. Виконані модельні експерименти, як прискорених методів піднесення перестановок у значні степені, наприклад, з наборами фіксованих матричних представлень, степені яких відповідають відповідним вагам розрядів двійкових чи інших кодових представлень вибраних випадкових чисел, так і протоколу в цілому, продемонстрували адекватність та переваги ізоморфних представлень функціонування моделей та запропонованого протоколу узгодження секретного ключа-перестановки.

Ключові слова: матричні представлення, ізоморфні ключі-перестановки, криптограми, криптографічне перетворення.

VLADIMIR G. KRASILENKO, NATALIYA P. YURCHUK
Vinnytsia National Agrarian University
DIANA V. NIKITOVICH
Vinnytsia National Technical University

THE APPLICATION OF ISOMORPHIC MATRIX REPRESENTATIONS FOR MODELING THE PROTOCOL FOR THE FORMATION OF SECRET KEYS-PERMUTATIONS OF HUGE SIZES

*A The article considers the peculiarities of the application of isomorphic matrix representations for modeling the protocol of matching secret keys-permutations of significant dimension. The situation is considered when for cryptographic transformations of blocks with a length of 256 * 256 bytes, presented in the form of a matrix of a black-and-white image, it is necessary to rearrange all bytes in accordance with the matrix keys. To generate a basic matrix key and the appearance of the components KeyA and KeyB in the format of two black and white images, a software module using engineering mathematical software Mathcad is proposed.*

Simulations are performed, for example, with sets of fixed matrix representations. The essence of the protocol of coordination of the main matrix of permutations by the parties is considered. Also shown are software modules in Mathcad for accelerated methods that display the procedure of iterative permutations in a permutation matrix isomorphic to the elevation of the permutation matrix to the desired degree with a certain side, corresponding to specific bits of bits or other code representations of selected random numbers. It is demonstrated that the parties receive new permutation matrices after the first step of the protocol, those sent to the other party, and the identical new permutation matrices received by the parties after the second step of the protocol, ie the secret permutation matrix.

Similar qualitative cryptographic transformations have been confirmed using the proposed representations of the permutation matrix based on the results of modeling matrix affine-permutation ciphers and multi-step matrix affine-permutation ciphers for different cases when the components of affine transformations are first executed in different sequences. , and then permutation using the permutation matrix, or vice versa. The model experiments performed in the study demonstrated the adequacy of the functioning of the models proposed by the protocol and methods of generating a permutation matrix and demonstrated their advantages.

Keywords: matrix representations, isomorphic permutation keys, cryptograms, cryptographic transformations.

Вступ

Поява та дослідження нового класу криптосистем матричного типу (КМТ) [1-4] на основі їх матрично-алгебраїчних моделей (МАМ) криптографічних перетворень (КП) 2D(3D) - масивів, зображень (З), як узагальнення відомих систем з форматами даних скалярного типу на випадки матрично-тензорних форматів, виявлені їх переваги, сприяли інтенсифікації досліджень КМТ, МАМ та демонстрації цілої низки нових їх покращень та застосувань [5-10]. Низка нових узагальнених МАМ, матричних афінних та афінно-перестановочних шифрів (МАПШ), їх модифікацій досліджувались та використовувались при створенні покращених цифрових підписів у [11-15]. МАМ мають розширені функціональні можливості, покращену крипто-стійкість, при їх апаратних реалізаціях легше відображаються на матричні процесори, дозволяють перевіряти цілісність криптограм чорно-білих, кольорових зображень і наявність у них перекручувань [5,7], створювати блокові [6], параметричні [8], багатосторінкові [9] моделі з їх значною стійкістю [10]. Базовими процедурами КП у матричних моделях перестановок (ММ_П), є множення матриць та деякі інші по-елементні операції за модулем над матрицями. А тому для ММ_П необхідно матриці байтів, утворених з рядків, колонок, векторів, що в унітарних чи інших кодах відображають символи, коди, байти, множити на матриці перестановок (МП). Практично для всіх відомих алгоритмів та шифрів включно з новостворюваними [16-27] процедури переставляння бітів, байтів чи їх груп є найбільш поширеними та обов'язковими. Зауважимо, що для збільшення ентропії криптограм З при їх КП на основі ММ_П та зміни їх гістограм необхідні декомпозиція R,G,B складових і їх бітових зрізів та навіть декілька матричних ключів (МК) типу МП [3-5]. Низка таких (поточних, покрокових, по-фреймових) псевдовипадкових МК, які б

відповідали вимогам, швидко генерувались, потрібна і для маскування, КП відео-файлів чи потоку блоків з файлів, зображень при їх значних розмірах [16-21].

Постановка проблеми

Отже, для КП, МАМ є гостра необхідність формування з головного МК низки МП, які б задовольняли ряду вимог. Оскільки питання узгодження головного МК загального виду розглядались в [28,29], але не послідовності МП, а методи генерування потоку МК перестановок з головного МК частково розглядались в [30], але тільки для бітових МП невеликих розмірів (256*256), то **метою роботи** є спроба не тільки запропонувати, промоделювати, дослідити протокол узгодження секретного (головного) МК (МП значної розмірності), тобто ГМП, але й на основі застосування нових ізоморфних представлень удосконалити та адаптувати вид, структуру ГМП такої чи ще більшої розмірності до формату З і до швидких апаратних рішень, проаналізувати цей протокол, модифікувати та прискорити процес формування потоку МП з такої ГМП для МАМ КП у криптосистемах МТ.

Виклад основного матеріалу

Огляд нових концептуальних підходів при створенні МТ шифрів, особливо багатофункціональних параметричних блочних [4], їх аналіз показав, що доцільно використовувати для досягнення мети ізоморфність різних представлень перестановок (матриць чи векторів), що виступають у ролі головного ключа (ГК) та раундових, покрокових чи по-блокових МК типу МП, тобто під-ключів (ПК), а матриці перестановок Р чи їх необхідні степені у моделях КП формувати та обробляти у ізоморфних просторах, які є більш зручними та адекватними використовуваним засобам. З робіт [6,8,9] відомо, що при КП на основі МАПШ, ВАПШ криптограми для деяких видів текстово-графічних документів (ТГД) і З, особливо для поблочних МАМ, при використанні одного ПК для всіх блоків є недостатніми по стійкості. Та попри це генерація низки ПК типу МП, що створюються з ГК (ГМП зі збільшеною на порядки розмірністю), дозволяє успішно вирішувати цю проблему. А тому актуальною та важливою є задача узгодження секретного ГК типу МП значної розмірності.

Розглянемо ситуацію, коли для КП блоків, кожен з яких представлений у вигляді матриці чорно-білого зображення, що еквівалентно значній довжині блоків у 256*256 байтів, необхідно переставити всі байти блока у відповідності до МП. В цьому випадку МП в загально прийнятому вигляді повинна бути квадратною з N*N елементами («0» чи «1»), де $N=2^{16}$. Потужність множини можливих таких МП, тобто їх кількість оцінюється, як N!, що дає для цього N колосальні значення (**65536 !**), які навіть уявити важко. Зауважимо, що кожну адресу байту блоку можна представити і за допомогою двох байтів, що вказують дві координати (рядок та стовпчик) блоку. Це дає нам можливість двома блоками байтів, тобто двома матрицями (З) розміром 256*256 елементів, представляти будь-яку перестановку, ставлячи в кожній однаковій адресі цих блоків відповідну старшому байту (в першому блоці) та молодшому байту (в другому блоці) координати нової адреси вибраного для перестановки байту. Отже, любу МП можна однозначно ізоморфно відобразити двома матрицями розміром 256*256, елементи яких приймають значення з діапазону 0-255, з тією особливістю, що кожна з 256 їх градацій інтенсивності в кожній з цих двох матриць (З) повторюється рівно по 256 раз. Для перевірки адекватності та особливостей застосування таких запропонованих ізоморфних представлень були виконані модельні експерименти стосовно створення на їх основі протоколу узгодження сторонами секретних ключів-перестановок значної розмірності. На рис. 1 показано вигляд модуля у Mathcad для генерування базового (головного) МК (МП) та вигляд його складових KeyA та KeyB у форматі двох чорно-білих зображень. Гістограми складових KeyA та KeyB МП зображені на рис.2 та мають вигляд горизонтальних ліній, як і очікувалось. Відмітимо, що таке пропоноване ізоморфне у вигляді двох зображень представлення МП дає нам гарну можливість використати ці складові KeyA та KeyB і у якості двох секретних МК загального типу, наприклад, як адитивний та мультиплікативний ключі у МАПШ чи іншій МАМ. Про це свідчать результати моделювання КП зображення (Im) МАПШ за допомогою пропонованої МП та її складових, як ключів, що показані на рис. 3 з матрицями явного З (Im), проміжних, його криптограм (Cmap) та перевірних зображень. А гістограми явного З, його криптограм після кожного КП афінними складовими цієї МП зображені також на рис.2. Вони свідчать про якісні КП навіть дуже специфічних зображень.

Ці та низка інших проведених модельних експериментів підтвердили, що КП зображень і довільних блоків байтів на основі МАПШ наявними 2-ма складовими з ізоморфного вигляду МП дають якісні криптограми CD_ImAa та CD_ImAm, гістограми яких H_CDa та H_CDm настільки близькі до рівномірного закону розподілу, що навіть для З (Im) з ентропією 0,738 ентропія криптограм відрізняється від теоретично максимальної (8 біт) всього на долі відсотка, збільшуючись аж до 7,99.

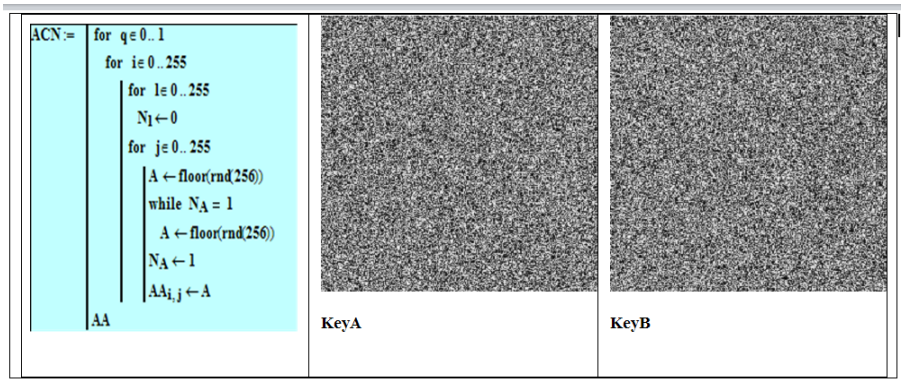

Рис. 1. Вікно Mathcad. Програмний модуль для генерування базового (головного) МК (МП) та вигляд складових KeyA та KeyB у форматі двох чорно-білих зображень

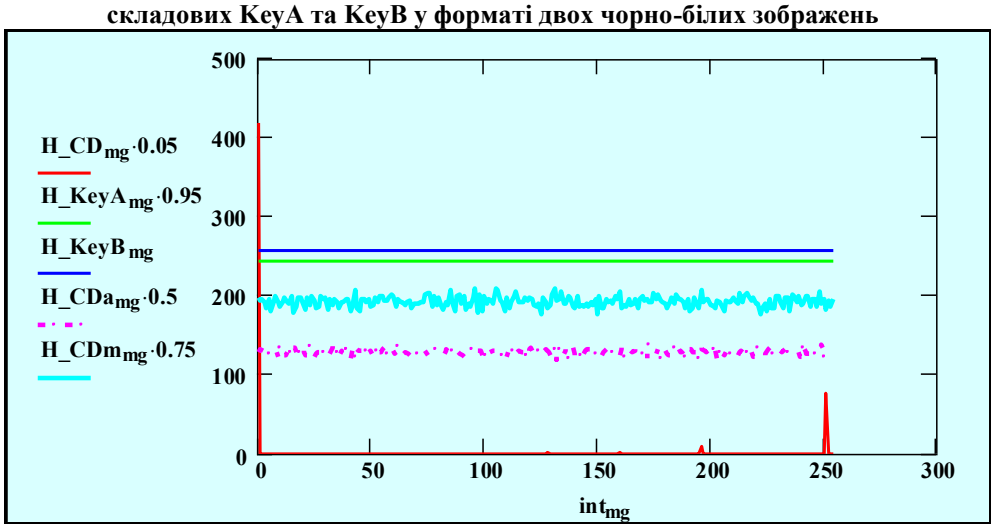

Рис. 2. Гістограми H_KeyA та H_KeyB відповідно складових KeyA та KeyB МП, гістограма H_CD криптограми З (співпадає з гістограмою явного З), відповідні гістограми H_CDa та H_CDm криптограм після адитивної та мультиплікативної афінних КП З за допомогою тих же KeyA та KeyB (Вікно Mathcad)

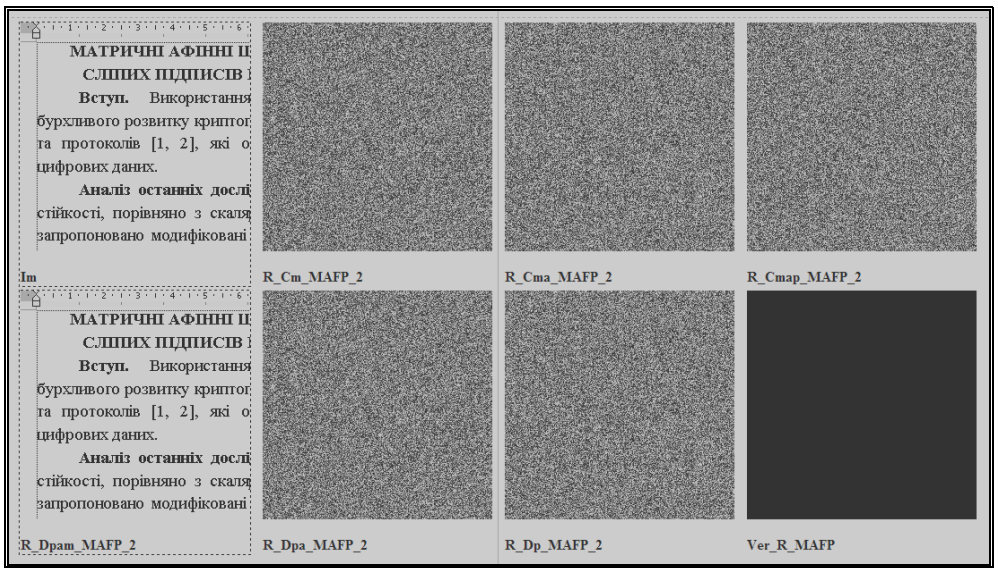

Рис. 3. Результати моделювання МАПШ на основі МП та її складових, як адитивного та мультиплікативного МК. Верхній ряд, зліва направо: явне, після перетворень, криптограма після МАПШ; Нижній ряд: відновлене, проміжні та різницеве (праворуч) зображення ТГД

Результати моделювання МАПШ та багатокрокових МАПШ [2, 6], для різних випадків, коли спочатку виконуються складові афінних перетворень і у іншій послідовності та різними, чи одним МК від МП, а потім перестановка за допомогою МП, чи навпаки, також засвідчили подібні якісні КП при застосуванні пропонованих представлень МП. В той же час для всіх модифікацій МАМ при таких МП зі значною розмірністю, потужність множини яких оцінюється значною величиною N!=(256*256)!, є надважливим питання узгодження сесійної секретної ГМП в аналогічному ізоморфному представленні,

тобто дослідження модифікацій відповідного протоколу з урахуванням особливостей нашого узагальненого підходу. Як попередні [6. 29], так і наведені тут результати експериментів дозволяють, узагальнюючи наш підхід, стверджувати, що і для синтезу ГМП зі значно більшою розмірністю останні можна також однозначно представити за допомогою 3, 4 і т.д. зображень-матриць чи блоків з байтів, аналогічних вищевказаним складовим KeyA та KeyB.

Розглянемо сутність самого протоколу узгодження ГМП сторонами. Нехай є сторони: ***x*** (Alisa) та ***y*** (Bob). Допустимо, що відома одна МП з множини допустимих у вигляді складових KeyA та KeyB, що показана на рис. 4. Крім того, завжди існує матриця зворотної перестановки (МЗП), яка для вибраного представлення має вигляд 2-х З KeyAO та KeyBO. Кожна з сторін на першому кроці підносить ізоморфно ГМП у вибрану ними свою секретну степінь, яка зазвичай на практиці є досить великим випадковим (псевдовипадковим) числом порядку типових величин, що застосовуються сьогодні в криптографії для суттєвого збільшення складності обчислень при перебірних атаках на односторонні функції. Для наочності і спрощення демонстрації у першому експерименті ми вибрали ці степені для сторін, рівні 11 та 17 для прикладу !. Після цього кожна сторона пересилає нову МП іншій стороні та на другому кроці сторони, отримані ними нові МП аналогічно підносять у ті ж свої випадкові секретні степені. Тут аналогія з протоколом Діффі-Хелмана, проте протокольні дії виконуються не зі скалярами, а з ізоморфно представленими МП.

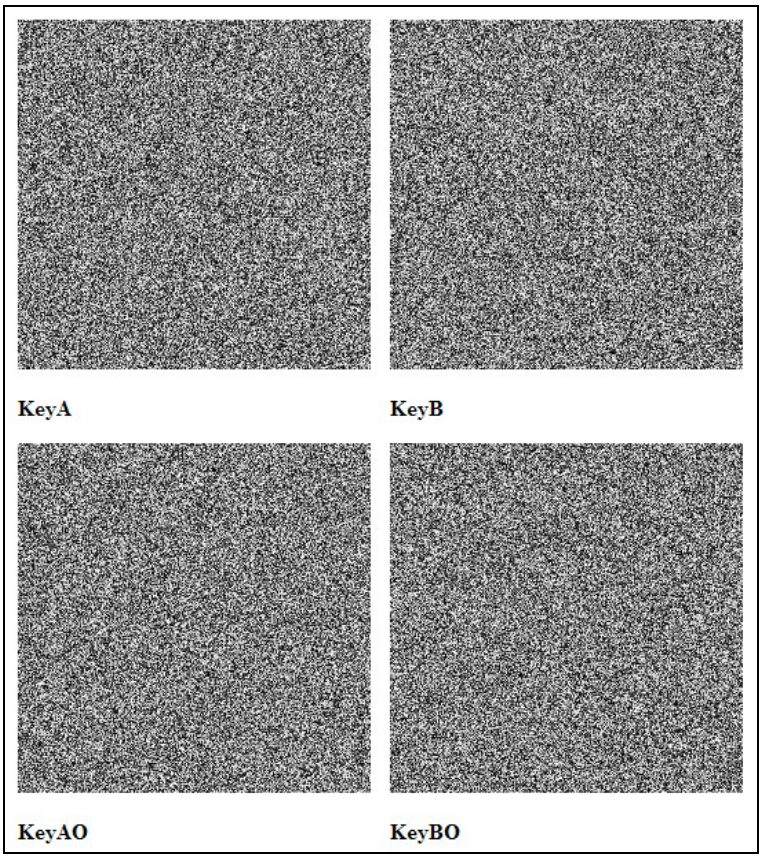

Рис. 4. Вигляд (2D) відомих генерованих МП: вгорі (пряма), внизу (зворотна) перестановки

На рис. 5-8 показані результати моделювання цих двох кроків протоколу узгодження секретного МК у Mathcad. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки у потрібну степінь (11 !) стороною ***x*** (Alisa) та модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки у потрібну степінь (17 !) стороною ***y*** (Bob) показані на рис.5, 6, а на рис. 7, 8 – аналогічні модулі для процедур ітераційних перестановок в отриманій від ***y*** (Bob) новій МП, ізоморфних піднесенню у потрібну степінь (11 !) стороною ***x*** (Alisa) та для процедур ітераційних перестановок в отриманій від ***x*** новій МП, ізоморфних піднесенню у потрібну степінь (17 !) стороною ***y*** (Bob). На рис. 9-10 показані вигляди отриманих проміжних та результативної секретної ГМП у ізоморфному представленні З. Сторони не знають степені іншої сторони, але отримані ними МП є ідентичними, що видно з рис. 10.

Таким чином піднесення МП (N*N бінарних, де $N=2^{16}$!) еквівалентно замінюється швидкими перестановками, які до того ж можуть бути ще більш прискореними при значних степенях за рахунок використання деякого базового набору фіксованих (фіксовані степені ГМП) та специфічної їх послідовності, що дає досягнення суттєвих переваг за рахунок прискорень обчислення степенів ГМП, простоти можливих реалізацій і зменшення витрат часу.

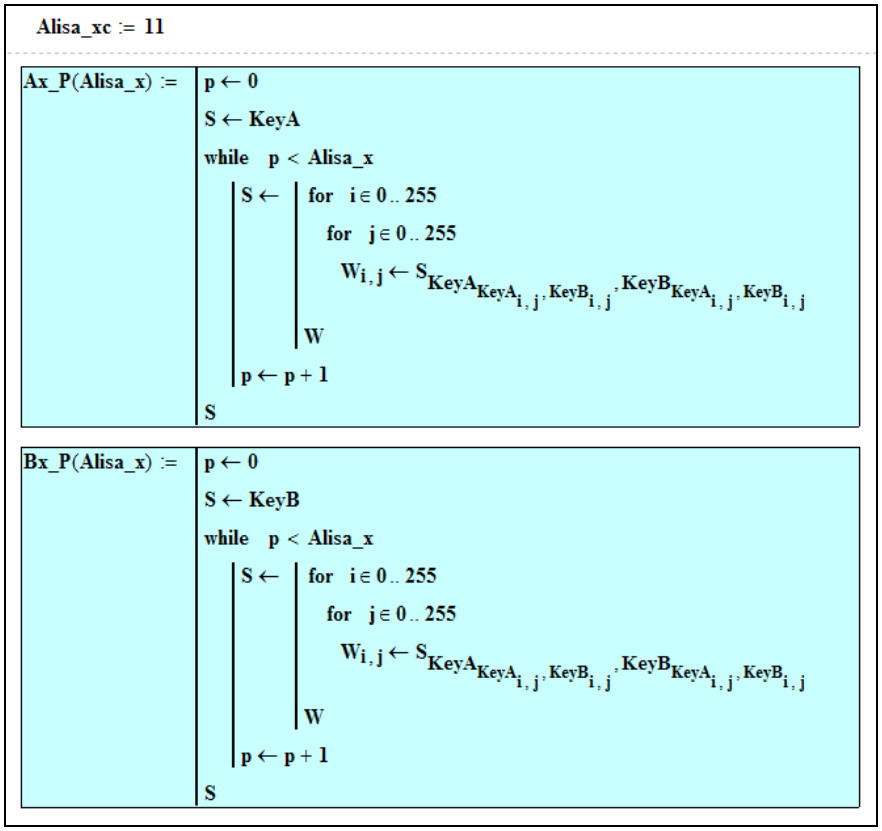

Рис. 5. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки у потрібну степінь (11 !) стороною *x* (Alisa)

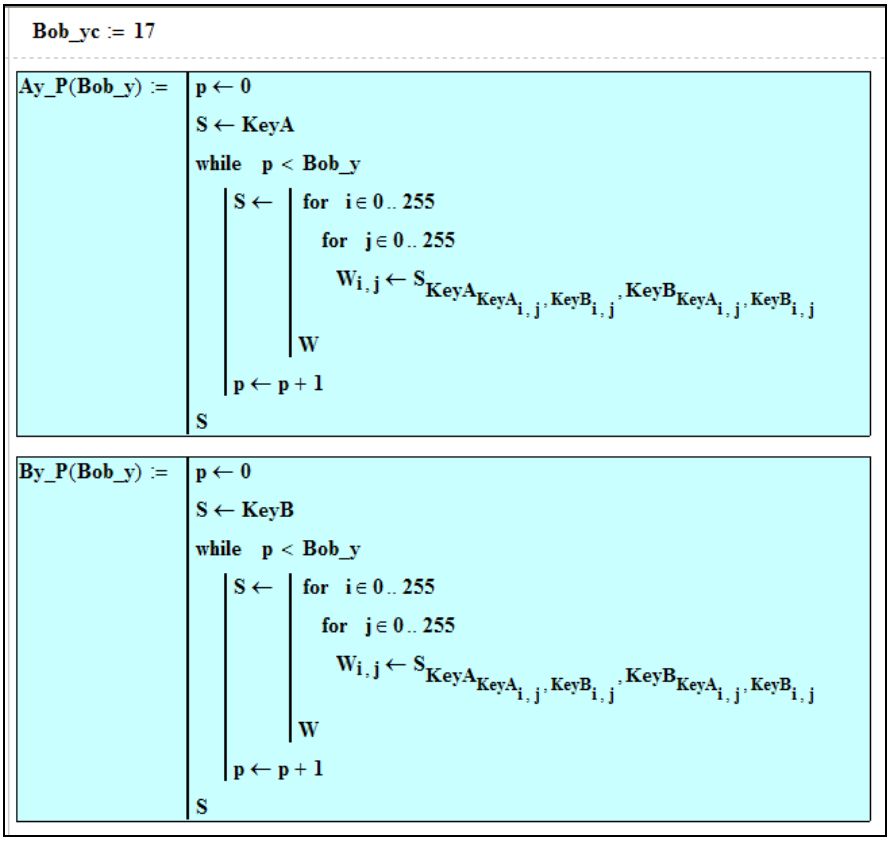

Рис. 6. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки у потрібну степінь (17 !) стороною *y* (Bob)

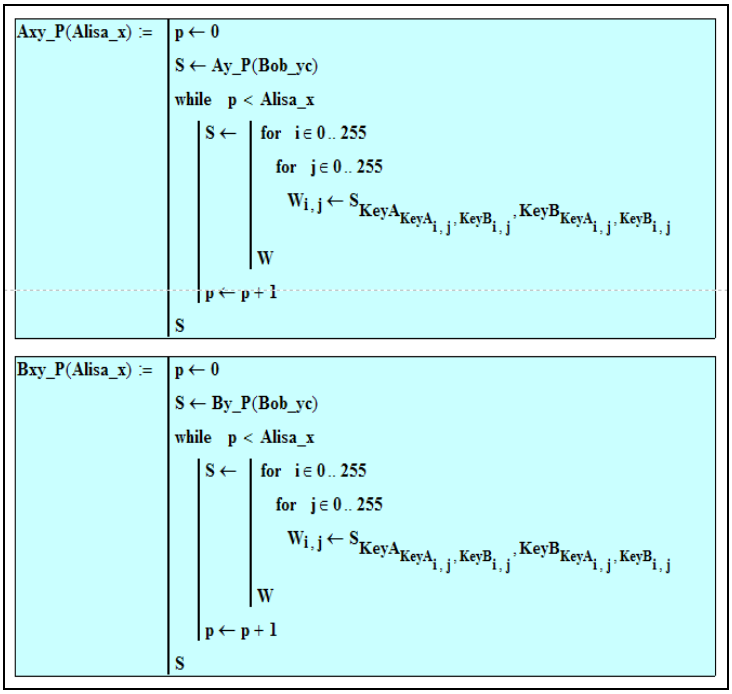

Рис. 7. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в отриманій від *y* новій МП, ізоморфних піднесенню у потрібну степінь (11 !) стороною *x* (Alisa)

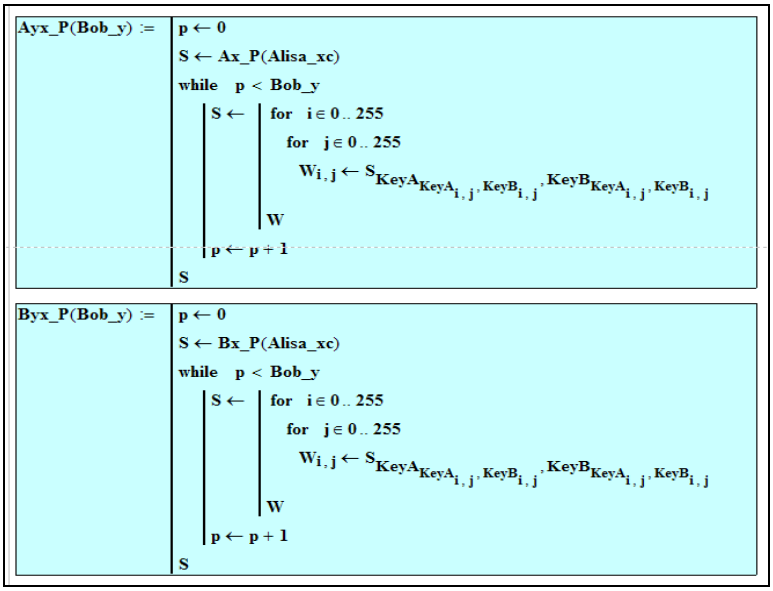

Рис. 8. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в отриманій від *x* новій МП, ізоморфних піднесенню у потрібну степінь (17 !) стороною *y* (Bob)

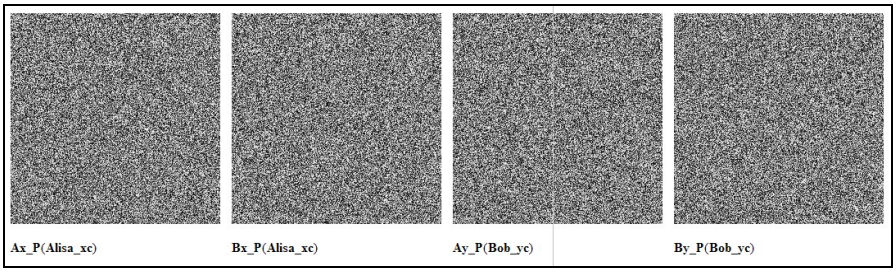

Рис. 9. Отримані сторонами нові МП (кожна у вигляді їх двох складових) після першого кроку протоколу, ті що пересилаються іншій стороні

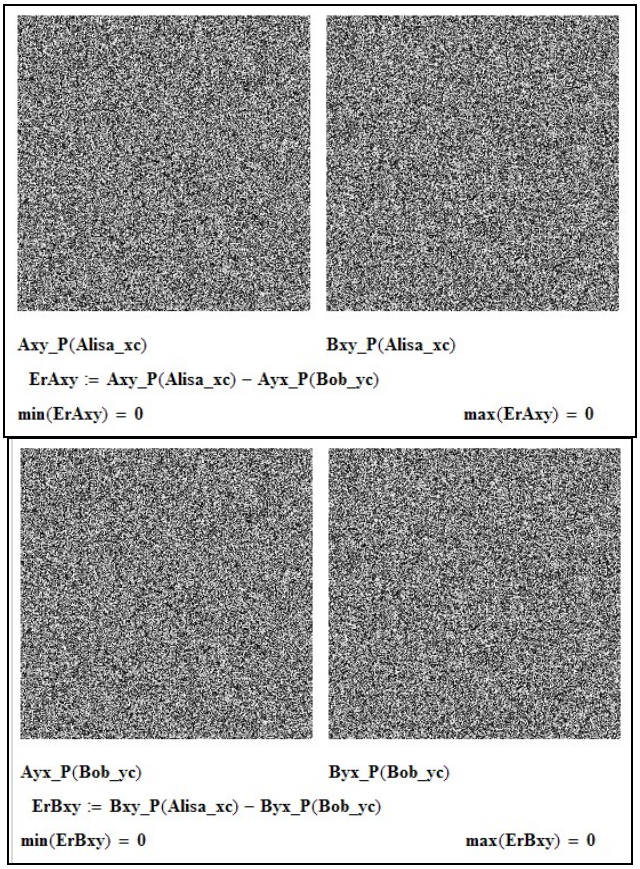

Рис. 10. Отримані сторонами ідентичні нові МП (кожна у вигляді їх двох складових) після другого кроку протоколу,тобто секретна МП

Оскільки степені, в які сторони підносять по суті ізоморфно представлені МП значних розмірностей, повинні бути досить значними для необхідної крипто-стійкості від перебірних атак, то нами виконано моделювання і для вище згаданих прискорених методів, наприклад, з наборами фіксованих МП, степені яких відповідають відповідним вагам розрядів двійкових чи інших кодових представлень вибраних випадкових чисел: ***xc*** (Alisa) та ***yc*** (Bob). Результати цих моделювань, відповідні формули, процедури, фрагменти ключів показані на рис.11-12. Порівняння елементів матриць на рис.12 засвічує їх рівність.

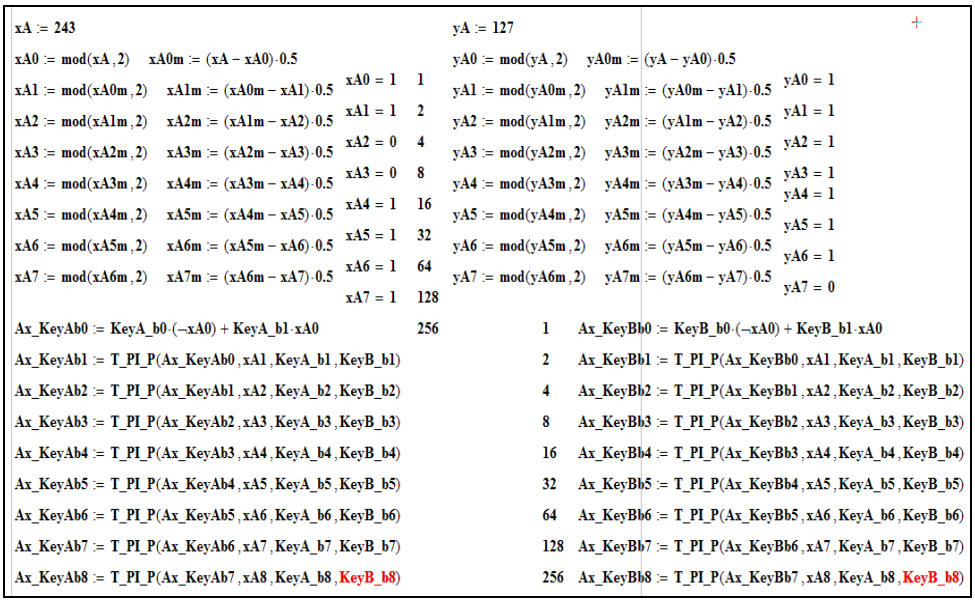

Рис. 11. Формули і процедури (копії з вікон Mathcad), що використовувались для моделювання прискорених процесів ізоморфного формування степенів матричних перестановок сторонами

Sxd = 7 **SdP = 262** **xA = 255**

Ax_P(SdP) =

	0	1	2	3	4	5	6	7	8	9
0	123	61	100	126	185	238	206	19	189	99
1	18	58	229	37	226	185	183	24	73	158
2	96	251	50	242	38	61	67	246	88	95
3	46	210	155	228	169	50	226	147	143	129
4	230	202	72	177	240	78	227	60	157	202
5	148	219	86	182	45	140	231	104	78	90
6	42	200	151	186	154	228	247	182	138	194
7	113	169	72	108	72	63	166	132	25	185
8	44	205	102	212	190	248	19	73	124	92
9	186	10	26	29	50	138	67	128	150	65
10	134	188	7	136	60	149	26	155	138	208
11	159	94	33	252	82	0	46	197	250	64
12	29	99	202	180	98	56	249	34	90	224
13	17	0	125	16	83	102	202	137	212	34
14	248	236	62	147	245	51	73	219	4	6
15	188	206	167	108	243	199	230	143	225	5

Ax_KeyAb7 =

	0	1	2	3	4	5	6	7	8	9
0	123	61	100	126	185	238	206	19	189	99
1	18	58	229	37	226	185	183	24	73	158
2	96	251	50	242	38	61	67	246	88	95
3	46	210	155	228	169	50	226	147	143	129
4	230	202	72	177	240	78	227	60	157	202
5	148	219	86	182	45	140	231	104	78	90
6	42	200	151	186	154	228	247	182	138	194
7	113	169	72	108	72	63	166	132	25	185
8	44	205	102	212	190	248	19	73	124	92
9	186	10	26	29	50	138	67	128	150	65
10	134	188	7	136	60	149	26	155	138	208
11	159	94	33	252	82	0	46	197	250	64
12	29	99	202	180	98	56	249	34	90	224
13	17	0	125	16	83	102	202	137	212	34
14	248	236	62	147	245	51	73	219	4	6
15	188	206	167	108	243	199	230	143	225	5

Bx_P(SdP) =

	0	1	2	3	4	5	6	7	8	9
0	130	208	190	17	36	35	172	99	141	194
1	126	217	150	102	238	91	88	215	194	129
2	172	64	195	24	174	67	179	204	89	211
3	24	41	230	149	136	126	46	34	47	65
4	196	100	161	59	84	215	208	190	58	199
5	64	226	43	161	163	4	65	239	75	233
6	32	116	252	124	14	210	105	91	9	205
7	58	195	143	102	11	157	248	92	23	201
8	191	181	190	18	159	160	190	75	168	148
9	83	181	168	166	205	61	20	162	118	102
10	206	92	186	45	27	89	9	108	85	51
11	26	209	75	65	122	69	38	42	15	139
12	235	212	38	48	217	167	152	225	177	28
13	7	186	3	10	67	237	79	146	98	254
14	228	34	46	152	72	137	65	147	73	237
15	84	78	166	74	248	85	116	105	230	149

Ax_KeyBb7 =

	0	1	2	3	4	5	6	7	8	9
0	130	208	190	17	36	35	172	99	141	194
1	126	217	150	102	238	91	88	215	194	129
2	172	64	195	24	174	67	179	204	89	211
3	24	41	230	149	136	126	46	34	47	65
4	196	100	161	59	84	215	208	190	58	199
5	64	226	43	161	163	4	65	239	75	233
6	32	116	252	124	14	210	105	91	9	205
7	58	195	143	102	11	157	248	92	23	201
8	191	181	190	18	159	160	190	75	168	148
9	83	181	168	166	205	61	20	162	118	102
10	206	92	186	45	27	89	9	108	85	51
11	26	209	75	65	122	69	38	42	15	139
12	235	212	38	48	217	167	152	225	177	28
13	7	186	3	10	67	237	79	146	98	254
14	228	34	46	152	72	137	65	147	73	237
15	84	78	166	74	248	85	116	105	230	149

Рис. 12. Фрагменти, утворених після другого кроку ключів, що свідчать про адекватність прискорених алгоритмів ізоморфного формування степенів матричних перестановок сторонами

Отримані моделюванням у Mathcad результати підтверджують правильність функціонування протоколу. Як було показано на рис. 1-3, за допомогою узгодженого цим пропонованим протоколом секретного ізоморфно представленого МК, процедури утворення якого описані вище, було виконано перевірку правильного до вимог їх синтезу та адекватності моделей шляхом прямого та зворотного КП З, використовуючи раніше розроблені та досліджені в [6-9] функціональні параметричні моделі КП зображень. Хоч початкова ГМП відома двом сторонам, протокол дозволяє без знання таємних степенів, що вибирають сторони, утворити секретний ключ, МП в аналогічному ізоморфному вигляді за час, пропорційний числу фіксованих перестановок. Крім того, аналіз стійкості з урахуванням потужності множини утворюваних цим протоколом відповідних МП значних розмірностей показав неможливість здійснення атак внаслідок величезної множини можливих МП, що оцінюється величиною $(2^{16})!$.

Висновки

Запропоновано протокол узгодження секретного ключа у вигляді ізоморфних представлень МП значних розмірностей, виконано модельні експерименти, що підтвердили адекватність функціонування моделей та пропонованих протоколу і методів генерування МП, перевірені алгоритми прискорених піднесень у значні степені матриць перестановок зі збереженням їх ізоморфних представлень, показали їх переваги. Моделі прості, зручні, адаптуються для різноформатних та кольорових зображень, реалізуються матричними процесорами, мають високі ефективність, значну крипто-стійкість, значну швидкодію.

Література

1. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісник НУ «Львів. політехніка». – 2009. – № 658. – С. 59-63.

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

3. Красиленко В. Г. Криптографічні перетворення зображень на основі матричних моделей перестановок з матрично-бітовозрізовою декомпозицією та їх моделювання / В. Г. Красиленко, В. М. Дубчак // Вісник Хмельницького національного університету. Технічні науки. - 2014. - № 1. - С. 74-79.

4. Красиленко В.Г. Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітово-зрізовою декомпозиціями / В.Г. Красиленко, Д.В. Нікітович // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2016. – № 23. – С. 31-36.

5. Красиленко В.Г. Моделювання та дослідження криптографічних перетворень зображень на основі їхньої матрично-бітовозрізової декомпозиції та матричних моделей перестановок з верифікацією цілісності / В.Г. Красиленко, Д.В. Нікітович // Електроніка та інформаційні технології. – Львів: ЛНУ імені Івана Франка, 2016. – Вип. 6. – С 111-127.

6. Красиленко В.Г. Моделі блокових матричних афінно-перестановочних шифрів (МАПШ) для криптографічних перетворень та їх дослідження / В.Г. Красиленко, Д.В. Нікітович // 72 НТК: матеріали конференції (13-15 грудня 2017 р.). – Одеса: ОНАЗ ім., 2017. – Ч. 1. – С.117-122.

7. Красиленко, В.Г. Моделювання матричних афінних алгоритмів для шифрування кольорових зображень / В. Г. Красиленко, К.В. Огородник, Ю.А.Флавицька // Комп'ютерні технології: наука і освіта: тези доповідей V Всеукр. НПК– К., 2010. – С.120-124.

8. Красиленко В.Г. Багатофункціональні параметричні матрично-алгебраїчні моделі (МАМ)

криптографічних перетворень (КП) з операціями за модулем та їх моделювання. / В.Г. Красиленко, Д.В. Нікітович. // 72 НПК: матеріали конференції (13-15 грудня 2017 року). – Одеса: ОНАЗ ім. О.С. Попова, 2017. – Частина 1. – С.123-128.

9. Красиленко В.Г. Моделювання сторінкових криптографічних перетворень масивів кольорових зображень на основі матричних моделей та перестановок / В.Г. Красиленко, Д.В. Нікітович // «Інформаційно-комп'ютерні технології – 2018»: Збірник тез доповідей IX Міжнародної НТК, 20-21 квітня 2018 року. – Житомир: Вид. О. О. Євенок, 2018. – С. 73-77.

10. Красиленко В.Г. Дослідження покращеного багатокрокового 2D RSA шифру та його гістограмно-ентропійних характеристик / В.Г. Красиленко, Д.В. Нікітович // «Інформаційна безпека та комп'ютерні технології»: Збірник тез доповідей III Міжнародної НПК, 19-20 квітня 2018 року. – Кропивницький: ЦНТУ, 2018. – С. 78-82.

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

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

13. Красиленко В.Г. Вдосконалення та моделювання електронних цифрових підписів матричного типу для текстографічних документів / В.Г. Красиленко, Д.В. Нікітович // Матеріали VI міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології» (ІУСТ-Одеса-2017), Одеський національний морський університет, 20-22 вересня 2017р. – Одеса: «ВидавІнформ НУ «ОМА», 2017. – С. 312 -318.

14. Красиленко В.Г. Моделювання покращених сліпих електронних цифрових підписів 2D типу / В.Г. Красиленко, Д.В. Нікітович // «Інформаційно-комп'ютерні технології – 2018»: Збірник тез доповідей IX Міжнародної науково-технічної конференції, 20-21 квітня 2018 року. – Житомир: Вид. О. О. Євенок, 2018. – С. 78-82.

15. Красиленко В.Г. Моделювання покращених багатокрокових 2D RSA алгоритмів для криптографічних перетворень та сліпого електронного цифрового підпису / В.Г. Красиленко, Д.В. Нікітович, Р.О. Яцковська, В.І. Яцковський // Системи обробки інформації: збірник наукових праць, 2019. – Вип. 1 (156). – С. 92-100.

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

17. Востриков А. А., Мишура О. В., Сергеев А. М., Чернышев С. А. О выборе матриц для процедур маскирования и демаскирования изображений // Фундаментальные исследования. 2015. № 2-24. С. 5335-5339.

18. Digital masking using Mersenne matrices and its special images / A. Vostricov, M. Sergeev, N. Balonin, S. Chernyshev // Procedia Computer Science. 2017. Vol. 112. P. 1151-1159.

19. Balonin N. Construction of Transformation Basis for Video and Image Masking Procedures / N. Balonin, M. Sergeev // Frontiers in Artificial Intelligence and Applications. 2014. Т. 262. С. 462-467.

20. Востриков А. А., Чернышев С. А. Об оценке устойчивости к искажениям изображений, маскированных М-матрицами // Научно-132 технический вестник информационных технологий, механики и оптики. 2013. № 5. С. 99-103.

21. Lee, M. H. Jacket Matrices: Constructions and Its Applications for Fast Cooperative Wireless Signal Processing / M. H. Lee / LAP LAMBERT Publishing, Germany, 2012.

22. M.A. Dabbah, W.L. Woo, S.S. Dlay, "SecureAuthentication for Face Recognition, "presented at Computational Intelligence in Image and Signal Processing, 2007. CIISP 2007. IEEE Symposium on, 2007.

23. Лужецький В. Методи шифрування на основі перестановки блоків змінної довжини / В. Лужецький, І. Горбенко //Захист інформації. – 2015. – Т. 17, № 2. – С. 169-175.

24. Білецький А.Я. Матричні аналоги протоколу Діффі-Хеллмана / А.Я. Білецький, А.А. Білецький, Р.Ю. Кандиба //Автоматика, вимірювання та керування: Вісник нац. ун-ту "Львівська політехніка". – 2012. – № 741. – С. 128-133.

25. Белецкий А.Я. Модифицированный матричный асимметричный криптографический алгоритм Диффи – Хэллма-на / А.Я. Белецкий, А.А. Белецкий, Д.А. Стеценко // Штучний інтелект. – 2010. – № 3. – С. 697-705.

26. Kutter M. Digital Signature Of Color Images Using Amplitude Modulation / M. Kutter, F. Jordan, F. Bossen // Proc. ofthe SPIE Storage and Retrieval for Image and Video Databases. – 1997. – Vol. 3022. – P. 518-526.

27. Квєтний Р.Н. Метод та алгоритм обміну ключами серед груп користувачів на основі асиметричних шифрів ЕССта RSA / Р.Н. Квєтний, Є.О. Титарчук, А.А. Гуржій // Інформаційні технології та комп'ютерна інженерія. – 2016. – № 3. – С. 38-43.

28. Красиленко В.Г. Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу / В.Г. Красиленко, Д.В. Нікітович // Системи

обробки інформації. – 2017. – Вип. 3 (149). – С. 151-157.

29. Красиленко В.Г. «Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів» / В.Г. Красиленко, Д.В. Нікітович // Комп`ютерно-інтегровані технології: освіта, наука, виробництво: науковий журнал.– Вип. 26. – С 111-120.

30. Красиленко В.Г. Моделювання процесів генерування матричних ключів / В.Г. Красиленко, Д.В. Нікітович // «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2018): Збірник тез доповідей IV Міжнародної науково-практичної конференції, 17-18 травня 2018 року. – Черкаси: ЧДТУ, 2018. – С. 32-35.

References

1. Krasilenko, V.H. and Flavyts'ka, Yu.A. (2009), “Modeliuvannia matrychnykh alhorytmiv kryptohrafichnoho zakhystu” [Modeling of matrix algorithms of cryptographic protection], Visnyk NU “L'viv. politekhnika”, No. 658. pp. 59-63.

2. Krasilenko, V.H. and Hrabovliak, S.K. (2012), “Matrychni afinno-perestanovochni alhorytmy dlia shyfruvannia ta deshyfruvannia zobrazhen'” [Matrix affine-permutation algorithms for encryption and decryption images], Information processing systems, No. 3(2). pp. 53-61.

3. Krasilenko V.H. and Dubchak, V.M. (2014), “Kryptohrafichni peretvorennia zobrazhen' na osnovi matrychnykh modelej perestanovok z matrychno-bitovozrizovoiu dekompozytsiieiu ta ikh modeliuvannia” [Transformations of images based on of matrix models of permutation with matrix bitplane decomposition and their modeling], Herald of Khmelnytskyi national university. Technical sciences, No. 1. pp. 74-79.

4. Krasilenko, V.H. and Nikitovych, D.V. (2016), “Modeliuvannia kryptohrafichnykh peretvoren' kol'orovykh zobrazhen' na osnovi matrychnykh modelej perestanovok zi spektral'noiu ta bitovo-zrizovoiu dekompozytsiiamy” [Simulation of cryptographic transformations of color images based on matrix models of permutations with spectral and bit-plane decompositions], Komp'iuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo : nauk. zhurn., No. 23. pp. 31-36.

5. Krasilenko, V.H. and Nikitovych, D.V. (2016), “Modeliuvannia ta doslidzhennia kryptohrafichnykh peretvoren' zobrazhen' na osnovi ikhn'oi matrychno-bitovozrizovoi dekompozytsii ta matrychnykh modelej perestanovok z veryfikatsiieiu tsilisnosti ” [Simulation and research of cryptographic transformations images based on of matrix bitplane decomposition and matrix models of permutation with verification integrity], Elektronika ta informatsijni tekhnolohii, No. 6. pp. 111-127.

6. Krasilenko, V.H. and Nikitovych, D.V. (2017), “Modeli blokovykh matrychnykh afinno-perestanovochnykh shyfriv (MAPSh) dlia kryptohrafichnykh peretvoren' ta ikh doslidzhennia” [Models of block matrix affine-permutation ciphers (MAPS) for cryptographic transformations and their research], 72 NTK: materialy konferentsii (13-15 hrudnia 2017 r.). Odesa: ONAZ im. O.S. Popova, Chastyna 1. pp.117-122.

7. Krasilenko, V.H., Ohorodnyk, K.V. and Flavyts'ka, Yu.A. (2010), Modeliuvannia matrychnykh afinnykh alhorytmiv dlia shyfruvannia kol'orovykh zobrazhen' [Simulation of matrix affine algorithms for encryption of color images], Komp'iuterni tekhnolohii: nauka i osvita: tezy dopovidej V Vseukr. *NPK* K., pp.120-124.

8. Krasilenko, V.H. and Nikitovych, D.V. (2017), “Bahatofunktsional'ni parametrychni matrychno-alhebraichni modeli (MAM) kryptohrafichnykh peretvoren' (KP) z operatsiiamy za modulem ta ikh modeliuvannia” [Multifunctional parametric matrix-algebraic models (MAM) of cryptographic transformations (CP) with modular operations and their modeling], *72 NPK:* materialy konferentsii (13-15 hrudnia 2017 roku). Odesa: ONAZ im. O.S. Popova, 2017. Chastyna 1. pp.123-128.

9. Krasilenko, V.H. and Nikitovych, D.V. (2018), “Modeliuvannia storinkovykh kryptohrafichnykh peretvoren' masyviv kol'orovykh zobrazhen' na osnovi matrychnykh modelej ta perestanovok ” [Modeling of page cryptographic transformations of arrays of color images on the basis of matrix models and permutations], «Informatsijno-komp'iuterni tekhnolohii – 2018»: Zbirnyk tez dopovidej IX Mizhnarodnoi NTK, 20-21 kvitnia 2018 roku. Zhytomyr: Vyd. O. O. Yevenok, 2018. pp. 73-77.

10. Krasilenko, V.H. and Nikitovych, D.V. (2018), “Doslidzhennia pokraschenoho bahatokrokovoho 2D RSA shyfru ta joho histohramno-entropijnykh kharakterystyk [Investigation of improved multi-step 2D RSA cipher and its histogram-entropy characteristics], «Informatsijna bezpeka ta komp'iuterni tekhnolohii»: Zbirnyk tez dopovidej III Mizhnarodnoi NPK, 19-20 kvitnia 2018 roku. Kropyvnyts'kyj: TsNTU, pp.78-82.

11. Krasilenko, V.H. and Hrabovliak, S.K. (2011), “Matrychni afinni shyfry dlia stvorennia tsyfrovykh slipykh pidpysiv na tekstohrafichni dokumenty” [Matrix affine ciphers for creation of digital blind signatures on textographic documents], Information processing systems, No. 7(97). pp. 60 – 63.

12. Krasilenko, V.H., Yatskovs'ka, R.O. and Trifonova, Yu.M. (2013), “Demonstratsiia protsesiv stvorennia slipykh elektronnykh tsyfrovykh pidpysiv na tekstohrafichnu dokumentatsiiu na osnovi modelej matrychnoho typu” [Demonstration of the processes of creating blind electronic digital signatures on textual documentation based on matrix-type models], Information processing systems, No. 3(110). T. 2. pp. 18 – 22.

13. Krasilenko, V.H. and Nikitovych, D.V. (2017), “Vdoskonalennia ta modeliuvannia elektronnykh tsyfrovykh pidpysiv matrychnoho typu dlia tekstohrafichnykh dokumentiv” [Improvement and modeling of electronic digital signatures of matrix type for textographic documents], Materialy VI mizhnarodnoi naukovo-praktychnoi konferentsii «Informatsijni upravliaiuchi systemy ta tekhnolohii» (IUST-Odesa-2017), Odes'kyj natsional'nyj mors'kyj universytet, 20-22 veresnia 2017r., Odesa: «VydavInform NU «OMA», pp. 312 -318.

14. Krasilenko, V.H. and Nikitovych, D.V. (2018), “Modeliuvannia pokraschenykh slipykh elektronnykh tsyfrovykh pidpysiv 2D typu [Modeling of improved blind electronic digital signatures of 2D type], «Informatsijno-komp'iuterni tekhnolohii – 2018»: Zbirnyk tez dopovidej IX Mizhnarodnoi naukovo-tekhnichnoi konferentsii, 20-21 kvitnia 2018 roku. Zhytomyr: Vyd. O. O. Yevenok, pp. 78-82.

15. Krasilenko, V.H., Nikitovych, D.V. Yatskovs'ka, R.O. and Yatskovs'kyj, V.I. (2019), “Modeliuvannia pokraschenykh bahatokrokovykh 2D RSA alhorytmiv dlia kryptohrafichnykh peretvoren' ta slipoho elektronnoho tsyfrovoho pidpysu” [Modeling of improved multi-stage 2D RSA algorithm for cryptographic transformations and blind electron digital signature], Information processing systems, No. 1 (156), pp. 92-100.

16. Vostrikov A., Sergeev M. Expansion of the Quasi-Orthogonal Basis to Mask Images // Intelligent Interactive Multimedia Systems and Services. Smart Innovations, Systems and Technologies 40. Springer, 2015. Pp. 161 – 168.

17. Vostrikov A. A., Mishura O. V., Sergeev A. M., Chernyishev S. A. O vyibore matrits dlya protsedur maskirovaniya i demaskirovaniya izobrazheniy // Fun-damentalnyie issledovaniya. 2015. № 2-24. pp. 5335-5339.

18. Digital masking using Mersenne matrices and its special images / A. Vostricov, M. Sergeev, N. Balonin, S. Chernyshev // Procedia Computer Science. 2017. Vol. 112. P. 1151-1159.

19. Balonin N. Construction of Transformation Basis for Video and Image Masking Procedures / N. Balonin, M. Sergeev // Frontiers in Artificial Intelligence and Applications. 2014. T. 262. pp. 462-467.

20. Vostrikov A.A., Chernyishev S.A. Ob otsenke ustoychivosti k iskazheniyam izobrazheniy, maskirovannyih M-matritsami // Nauchno-132 tehnicheskiy vestnik informatsionnyih tehnologiy, mehaniki i optiki. 2013. № 5. pp. 99-103.

21. Lee, M. H. Jacket Matrices: Constructions and Its Applications for Fast Cooperative Wireless Signal Processing / M. H. Lee / LAP LAMBERT Publishing, Germany, 2012.

22. M.A. Dabbah, W.L. Woo, S.S. Dlay, "Secure Authentication for Face Recognition, "presented at Computational Intelligence in Image and Signal Processing, 2007. CIISP 2007. IEEE Symposium on, 2007.

23. Luzhetskyi, V. and Horbenko, I. (2015), “Metody shyfruvannia na osnovi perestanovky blokiv zminnoi dovzhyny” [Encryption methods based on permutation of variable length blocks], Protection of information, Vol. 17, No. 2, pp. 169-175.

24. Biletskyi, A.Ia., Biletskyi, A.A. and Kandyba, R.Iu. (2012), “Matrychni analohy protokolu Diffi-Khellmana” [Matrixanalogues of the Diffie-Hellman protocol], Automation, Measurement and Control: Bulletin of the National University Lviv Pol-ytechnic University, No. 741, pp. 128-133.

25. Beletskyi, A.Ia., Beletskyi, A.A. and Stetsenko, D.A. (2010), “Modyfikovanyy asymetrychnyy kryptohrafichny yalhorytm Diffi-Khelmana” [Modified Diffie-Hellman Matrix Asymmetric Cryptographic Algorithm], Artificial Intelligence, No. 3, pp. 697-705.

26. Kutter, M., Jordan, F. and Bossen, F. (1997), Digital Signature Of Color Images Using Amplitude Modulation, Proc. ofthe SPIE Storage and Retrieval for Image and Video Databases, Vol. 3022, pp. 518-526.

27. Kvietnyi, R.N., Tytarchuk, Ye.O. and Hurzhii, A.A. (2016), “Metod ta alhorytm obminu kliuchamy sered hrupkorystuvachiv na osnovi asymetrychnykh shyfriv ECC ta RSA” [Method and algorithm for key exchange among user groups based on asymmetric ECC and RSA ciphers], Information Technology and Computer Engineering, No. 3, pp. 38-43.

28. Krasilenko, V.H. and Nikitovych, D.V. (2017), “Modeliuvannia protokoliv uzghodzhennia sekretnoho matrychnoho kliucha dlia kryptohrafichnykh peretvoren' ta system matrychnoho typu” [Modeling of coordination protocols of secret matrix key for cryptographic transformation and matrix type systems], Information processing systems, No. 3 (149). pp. 151-157.

29. Krasilenko, V.H. and Nikitovych, D.V. (2017), “Modeliuvannia bahatokrokovykh ta bahatostupenevykh protokoliv uzghodzhennia sekretnykh matrychnykh kliuchiv” [Modeling of multi-step and multi-protocol protocols for the harmonization of secret matrix keys], Komp’iuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo: naukovyi zhurnal, No. 26, LNTU, Lutsk, pp. 111-120.

30. Krasilenko, V.H. and Nikitovych, D.V. (2018), “Modeliuvannia protsesiv heneruvannia matrychnykh kliuchiv” [Modeling of matrix key generation processes], “Informatsijni tekhnolohii v osviti, nautsi i tekhnitsi ” (ITONT-2018): Zbirnyk tez dopovidej IV Mizhnarodnoi naukovo-praktychnoi konferentsii, 17-18 travnia 2018 roku. Cherkasy: ChDTU, pp. 32-35.

КРАСИЛЕНКО В. Г. ORCID ID: 0000-0001-6528-3150 krasvg@i.ua

ЮРЧУК Н. П. ORCID ID: 0000-0002-7987-9390

НІКІТОВИЧ Д. В. ORCID ID: 0000-0002-8907-1221 diananikitovych@gmail.com

Рецензія/Peer review : 15.03.2021 р. Надрукована/Printed :02.06.2021 р.