International Science Group

ISG-KONF.COM

X

INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE "PROBLEMS AND PROSPECTS OF MODERN SCIENCE AND EDUCATION"

Stockholm, Sweden

March 12 - 15, 2024

ISBN 979-8-89292-740-6

DOI 10.46299/ISG.2024.1.10

МЕТОДИ ГЕНЕРАЦІЇ ПОТОКУ ВЕЛИКОРОЗМІРНИХ ПЕРЕСТАНОВОК ПРИ ЇХ ІЗОМОРФНИХ ПРЕДСТАВЛЕННЯХ МАТРИЦЯМИ

Красиленко В. Г.,
Кандидат технічних наук, доцент
Вінницький національний аграрний університет

Нікітович Д. В.,
Аспірант
Вінницький національний технічний університет

Анотація: Розглядаються та моделюються методи та процеси генерації потоку матриць перестановок значної розмірності при їх нових ізоморфних поданнях. Обґрунтована необхідність та актуальність розробки методів формування потоку великорозмірних перестановок та особливості і переваги їх застосування для криптографічних перетворень, зашифрування зображень, маскування (приховування) відеофайлів, реалізації протоколів узгодження групою учасників головного секретного ключа-перестановки у криптосистемах матричного типу. Запропоновано три варіанти генерації потоку матриць перестановок. Показано, що прості по-елементні операції за модулем та зсуви, що виконуються у початкових ізоморфно представлених матрицями перестановках, та багатократні перестановки елементів у цих перестановках (еквівалентні піднесенням відповідних їм матриць перестановок у степені), дають можливість на основі цих базових операцій, процедур згенерувати у потоковому режимі потрібну низку спільних секретних матричних ключів-перестановок. Наведені результати моделювання методів та процесів генерації потоку великорозмірних матриць перестановок в цілому, їхніх алгоритмічних кроків, операцій. Отримані результати підтвердили адекватність та переваги пропонованих методів, що забезпечуються ізоморфними представленнями.

Ключові слова*:* метод генерації потоку великорозмірних матричних ключів, узгодження секретного ключа, матричні моделі**,** ізоморфні ключі-перестановки, криптограми, криптографічне перетворення.

Вступ. Останні три десятиріччя характеризуються масовим використанням електронних комунікацій, інформаційних технологій не тільки у виробничій, господарській, військовій та інших галузях, сферах народного господарства, а й у цивільних особистісних відносинах, суттєвим щорічним збільшенням обсягів інформаційних об’єктів (ІО) та їх потоків, їх значимості, загостренням проблем інформаційної безпеки, необхідністю забезпечення стійкості ІО до потенційних загроз, тощо. Поява значної кількості великого об’єму ІО та їх форматів, ріст частки зображень значної (мегабайтової) розмірності, включно з багато-спектральними, уніфікованих організаційно-розпорядчих, конструкторських та цілої низки інших специфічних текстографічних документів (ТГД) у вигляді

цифрових, табличних даних, малюнків, графіків, діаграм, підписів, резолюцій, віз, печаток, цифрових водяних знаків, тощо, які є по суті багатовимірними масивами чи зображеннями та часто містять інформацію з обмеженим чи закритим доступом, потребує відповідного таємного зберігання та передавання таких ІО. Для забезпечення необхідної стійкості інформаційно-комунікаційних систем, масивів ІО до потенційних загроз важливе місце серед великої кількості методів, технологій, засобів захисту інформації особливе місце займають криптографічні системи, які найбільш надійно здійснюють захист ІО.

Аналіз останніх досліджень і публікацій. **Обґрунтування.** Одним з ключових питань застосування інструментів криптографії, стеганографії, тощо є процеси (протоколи) узгодження електронним шляхом спільних секретних ключів чи низки похідних від них під-ключів. Проте, більшість протоколів, наприклад, традиційного Діффі-Хелмана, MTI, STS та інших, як і більшість методів криптографічних перетворень (КП) ІО, зорієнтовані на суто скалярні ключі та послідовну обробку блоків. Це викликано тим, що більшість використовуваних методів та засобів криптографічних перетворень (КП) інформаційних масивів, зображень, файлів, ТГД орієнтовані на послідовну скалярну обробку блоків, що попередньо перетворені у цифрові формати. Навіть для симетричних, широко використовуваних, алгоритмів (на основі діючого стандарту AES, IDEA, тощо) типові довжини блоків та ключів складають 256-1024 бітів, хоч для деяких виняткових шифрів FEAL, RC6 та інших новітніх модифікацій широкого спектру відомих шифрів ці довжини обмежуються 1К-2К бітами [1]. Як показує огляд тенденцій удосконалення крипто-алгоритмів, ускладнень їх математичних основ з метою усунення атак, огляд досягнень у крипто-аналізі, намітився стратегічний перехід від форматів даних скалярного типу у відомих системах до більш відповідних та природніх матрично-тензорних форматів, що у свою чергу інтенсифікувало пошук нових матрично-алгебраїчних моделей (МАМ) криптографічних перетворень (КП) ІО, 2D (тензорних) - масивів, зображень (З) різного формату та розмірів, пошук нових концепцій, що зручніше та краще реалізуються сучасними паралельними засобами, матричними спеціалізованими процесорами. Все це призвело та спонукає до збільшення довжин ключів (ДК) та їх нових різновидів, до створення моделей та криптосистем матричного типу (МТ) [2-5], до появи низки зорієнтованих на ці засоби модифікацій відомих алгоритмів КП та створення відповідних моделей, що були розглянуті в [6-11]. Переваги криптосистем на основі таких МАМ, продемонстровані в цих роботах, сприяли подальшим дослідженням МАМ та появі нових публікацій [6-10], якими було додатково підтверджено переваги і перспективність пропонованої концепції, нових удосконалень, модифікацій цих моделей та продемонстровано експериментально поліпшення їх характеристик та розширення областей їх ефективного застосування. Функціонування всіх таких МАМ підтверджено імітаційними моделюваннями, де показано переваги таких моделей, алгоритмів: розширені функціональні можливості, краще відображення при їх апаратних реалізаціях на матричні процесори. Так, наприклад, на основі нових просунутих модифікацій МАМ досліджувались

матричні афінні та афінно-перестановочні шифри (МАПШ), що пропонувались для криптографічних перетворень (КП) зображень, для створення на їх основі електронних цифрових підписів [11-15], для маскування при передачі відеофайлів [16-19], для генерування потоків секретних матричних ключів різного типу, що необхідні для вирішення таких завдань [20-21]. На основі узагальнених та модифікованих, з урахуванням поставлених завдань і цілей, МАМ були запропоновані та промодельовані блокові [7], багатофункціональні параметричні [9], багатосторінкові [10] шифри з їх підвищеною криптостійкістю [10] для КП як чорно-білих, так і кольорових зображень та можливістю виявлення перекручувань та цілісності криптограм [5, 6, 8]. Відмітимо, що процедури заміни, переставляння бітів, байтів чи їх груп є найбільш поширеними та обов'язковими для всіх відомих шифрів та їх алгоритмів, включно з новостворюваними [5-14]. Крім того, наведений тут короткий огляд та його акценти дозволяють зробити наступні висновки.

По-перше, для багатьох наведених вище шифрів, у тому числі узагальнених багатокрокових матричних афінно-перестановочних шифрів, однією з основних базових є матрична модель перестановок (ММ_П) [3, 5, 6], за допомогою якої після відповідних декомпозицій переставляються біти у бітових зрізах, байти у поточних блоках, чи блоки у зображеннях, файлах, масивах. При цьому для кожного поточного блоку, раундового чи ітераційного кроку чи відеокадру, поточної перестановки бажано її постійно змінювати, що також необхідно і для збільшення криптостійкості.

По-друге, якщо традиційні процеси (протоколи) узгодження електронним шляхом спільного секретного ключа скалярного типу майже вичерпно вивчені [22], а протоколи узгодження матричного ключа (деякого типу), адаптованого під новітні виклики [23-25] та під криптосистеми МТ, у достатній кількості запропоновані, описані та добре промодельовані [24, 26, 27], то робіт, що стосуються проблеми генерації потоку великорозмірних МК дуже мало [28].

По-третє, потреба та актуальність виконання КП над великорозмірними багатовимірними ІО, зображеннями (З) вимагає не лише спеціалізованих матрично-алгебраїчних моделей (МАМ) КП, що адаптовані під формати ІО, але і секретних матричних ключів (МК) [27, 28] великих розмірів, які б суттєво перевищували довжини використовуваних на сьогодні секретних ключів у відомих криптосистемах. Такі матричні ключі, наприклад, у вигляді матриць (зображень) своєю типовою структурою краще відповідають однорідній структурі багатовимірних сигналів, багато-спектральних зображень різних фізичних, аерокосмічних об'єктів, тощо, [28, 29], а гострота проблеми ємностей пам'яті для зберігання таких МК, навіть їх низки вже майже повністю анульована. Декілька аналогічних МК потрібні і для модифікованих ММ_П КП з верифікацією цілісності криптограм, розглянутих в [6]. Крім того, при виборі таких МК, їх типу, кількості, треба враховувати специфіку, розмір файлів, блоків та структуру форматів, розширень, які характерні для оброблюваних чорно-білих напівтонових, кольорових чи багато-спектральних зображень.

Постановка проблеми. Узагальнення протоколу Діффі-Хелмана на

матричний випадок і метод узгодження МК 1-ого типу у вигляді випадкового (шумового) З, який нами був позначений як МК_З (від «зображення»), були розглянуті в [26, 27], де експериментами Mathcad були підтверджені переваги таких протоколів узгодження секретного МК_З. Втім для багатьох МАПШ крім такого МК_З необхідно мати ще й набір бінарних матриць перестановок [3, 6, 26, 27], що ізоморфні просто перестановкам, тобто матричні ключі 2-го типу, які позначимо тут їх як МК_П. Питання щодо їх формувань і застосувань частково розглядались в [3, 6, 26], і лише в [28] запропоновано протокол узгодження двома сторонами МК вже типу МК_П. Проте в ній не розглядались протоколи для випадків узгодження МК_П, що був би спільний для всіх учасників групи, тобто ситуації, коли учасники бажають створити свій кооперативний груповий МК_П. Для змін гістограми та збільшення ентропії криптограми З при їх КП на основі ММ_П необхідні декомпозиція R,G,B складових і їх бітових зрізів та декілька матричних ключів (МК) і векторних (ВК) [4, 6, 8]. А для маскування відео-файлів чи потоку блоків необхідна низка псевдовипадкових МК, які повинні відповідати вимогам та швидко генеруватись. Тобто для МАМ є гостра необхідність формування цілої низки МК_П з головного МК типу МК_П, які б задовольняли ряду вимог. Відомо з [6, 8], що генерація низки поточних ключів (ПК) типу МК_П, що створюються з головного ключа (ГМК_П зі збільшеною на порядки розмірністю), дозволяє успішно вирішувати проблему стійкості. Оскільки в [26, 27] розглядались питання узгодження лиш головного МК загального виду, а не низки (потоку) МК_П, в [29] хоч і розглядались методи генерування потоку матричних ключів перестановок, але тільки для бітових МК_П розміром 256*256, а у [30] розглядався, так званий авторами, кооперативний протокол узгодження МК, але тільки стосовно МК_З, то **метою роботи** є спроба вдосконалити метод генерації низки МК_П, суттєво збільшивши розмір перестановок, покращити та адаптувати структуру, вид та опис ММ_П до формату З і до швидких апаратних рішень, передбачити подальше можливе розширення меж розмірності МК_П, промоделювати та дослідити процес формування потоку МК_П для МАМ КП у системах МТ, перевірити властивості генерованих МК_П та застосувати нові більш ефективні ізоморфні подання великорозмірних матриць-перестановок, як секретних ключів різних ієрархій.

Виклад основних результатів. Для ясності подальшого викладу матеріалу наведемо тут, дивись рис. 1, результати моделювання в Mathcad протоколу узгодження всього одного спільного секретного ключа-перестановки на основі вибраної нами для цього 1-го експерименту бітової квадратної матриці (PSAB) розміром 256*256 ел. Результати моделювання для випадку піднесення PSAB (типу МК_П) у випадкові, відомі лише кожній окремій з двох сторін обміну, степені та отримані проміжні та результатна МК_П показують, що у результаті таких піднесень початкової (основи) МК_П у степені формуються аналогічні їй матриці-перестановки. Відмітимо, що при значній потужності множини можливих перестановок, а вона для цього прикладу рівна N!=256!, де N - розмірність МК_П, навіть знання МК_П-основи не дає можливості без перехоплення обох створених сторонами проміжних МК_П взнати ключ. Але

для нас тут найважливішим моментом є той факт, що змінюючи послідовно степені, в які будемо підносити основу, і які відбираються у відповідності до рандомно згенерованої послідовності чисел, ми утворюємо послідовність потрібних матриць-перестановок. Якість такої низки, потоку перевірялась [31].

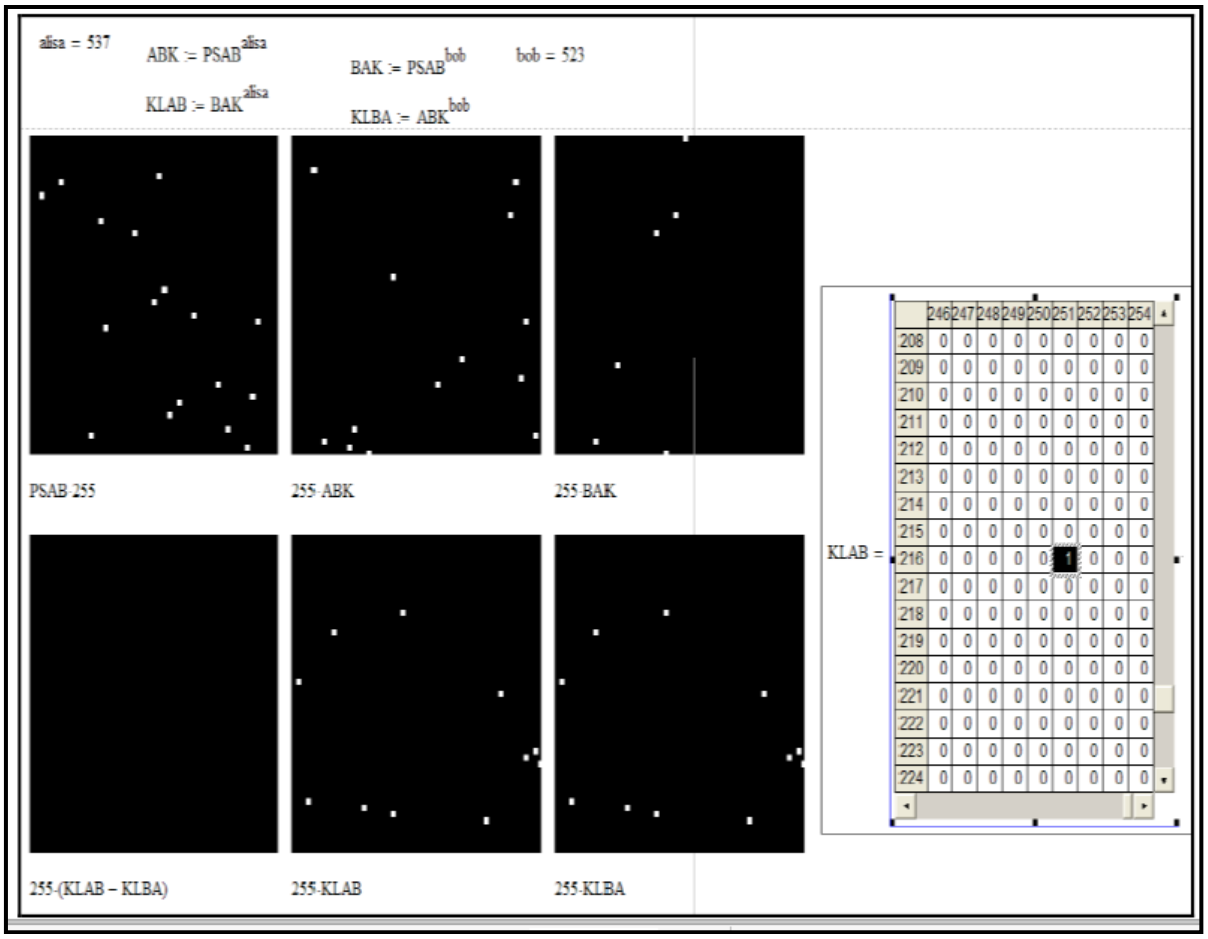


Рис. 1 Фрагмент вікна Mathcad з верифікацією модифікації протоколу Діффі-Хелмана для випадку піднесення у степені (537 та 523) МК_П, як основи. Вигляд основи (матриця PSAB 256*256), проміжних МК_П (ABK, BAK), що ними обмінюються сторони, та утворених ключів (KLAB, KLBA), які однакові

З вигляду матриць очевидно, що таке їх представлення є неефективним. Використовуючи підхід, описаний в [28, 29, 31], можна показати, що довільну перестановку довжиною 65536 (бітову матрицю 65536*65536 ел.) можна однозначно ізоморфно відобразити двома матрицями розміром 256*256, елементи яких приймають значення з діапазону 0-255. А тому в якості МК_П для 2-го експерименту було взято бітову квадратну матрицю з N*N елементами («0» чи «1»), де $N=2^{16}$, що збільшило потужність множини перестановок до значення (65536 !). Вікно Mathcad з програмним модулем для генерування базового (головного) МК (ГМК_П) та виглядом його складових KeyA та KeyB (двох напівтонових зображень) показано на рис.2, а модуль (копії з Mathcad), який реалізує процедуру ітераційних перестановок в МК_П, ізоморфних піднесенню цієї перестановки у потрібну степінь, показано на рис.3, 4. Такий і подібні йому використовувались для моделювання всіх покрокових процедур.

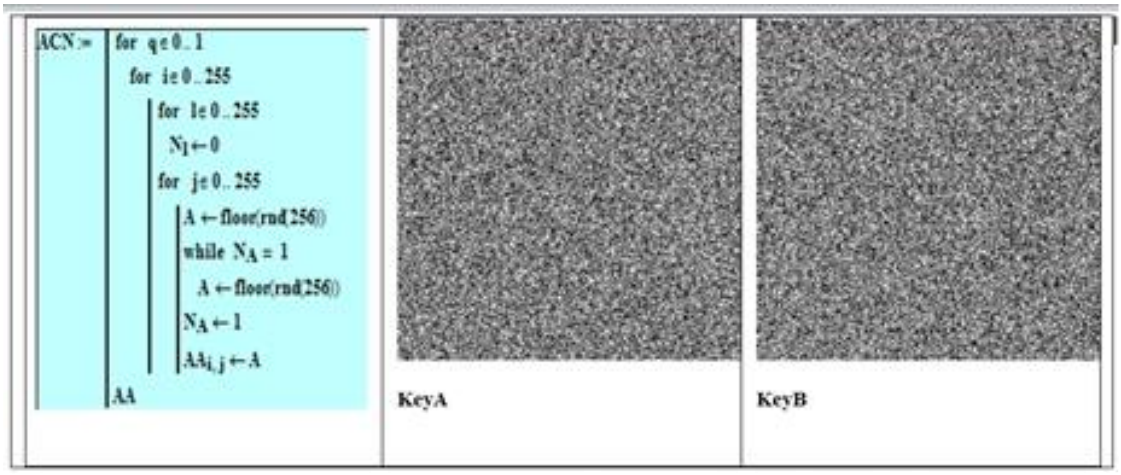
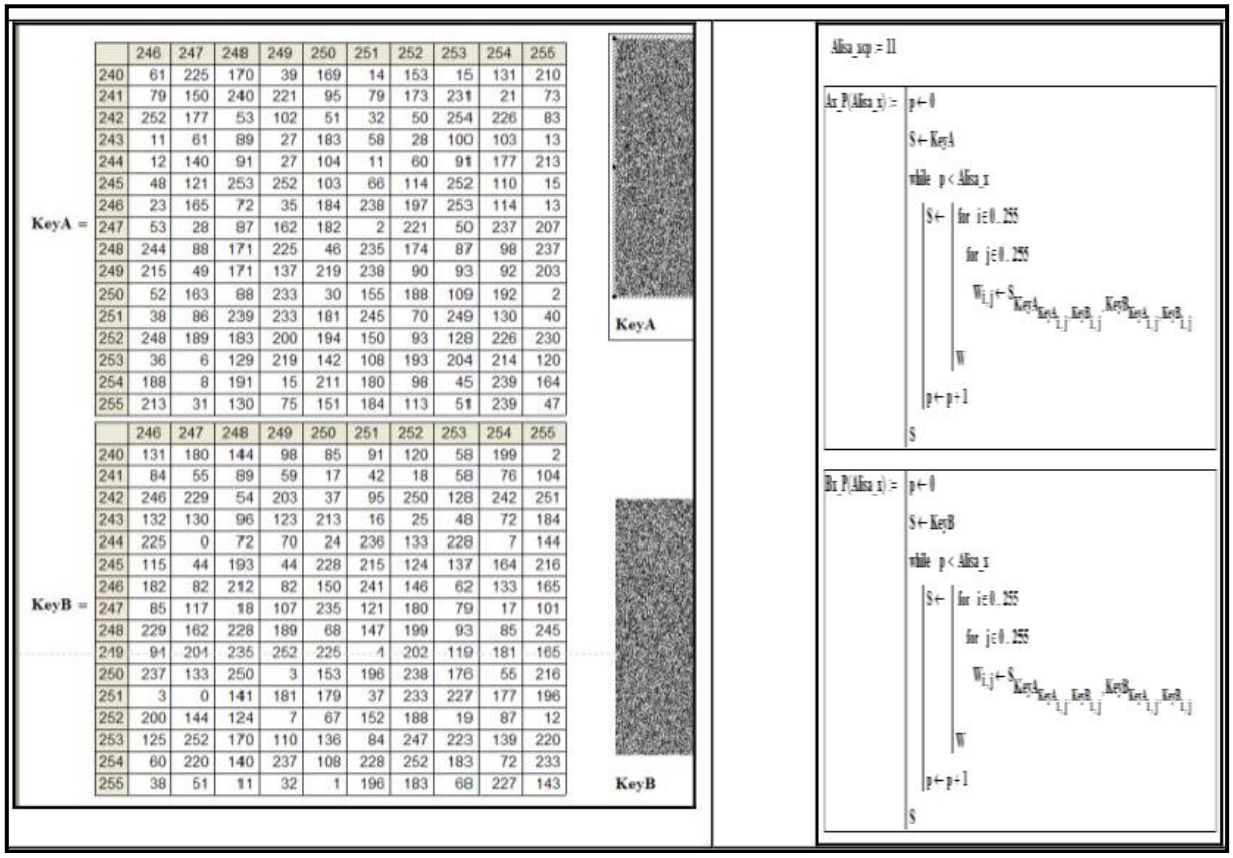


Рис. 2. Вікно Mathcad з модулем для генерування базового (головного) МК_П та вигляд його складових KeyA та KeyB у форматі двох чорно-білих зображень.



KeyA =

	246	247	248	249	250	251	252	253	254	255
240	61	225	170	39	169	14	153	15	131	210
241	79	150	240	221	95	79	173	231	21	73
242	252	177	53	102	51	32	50	254	226	83
243	11	61	89	27	183	58	28	100	103	13
244	12	140	91	27	104	11	60	91	177	213
245	48	121	253	252	103	66	114	252	110	15
246	23	165	72	35	184	238	197	253	114	13
247	53	28	87	162	182	2	221	50	237	207
248	244	88	171	225	46	235	174	87	98	237
249	215	49	171	137	219	238	90	93	92	203
250	52	163	88	233	30	155	188	109	192	2
251	38	86	239	233	181	245	70	249	130	40
252	248	189	183	200	194	150	93	128	226	230
253	36	6	129	219	142	108	193	204	214	120
254	188	8	191	15	211	180	98	45	239	164
255	213	31	130	75	151	184	113	51	239	47

KeyB =

	246	247	248	249	250	251	252	253	254	255
240	131	180	144	98	85	91	120	58	199	2
241	84	55	89	59	17	42	18	58	76	104
242	246	229	54	203	37	95	250	128	242	251
243	132	130	96	123	213	16	25	48	72	184
244	225	0	72	70	24	236	133	228	7	144
245	115	44	193	44	228	215	124	137	164	216
246	182	82	212	82	150	241	146	62	133	165
247	85	117	18	107	235	121	180	79	17	101
248	229	162	228	189	68	147	199	93	85	245
249	91	204	235	252	225	4	202	119	181	165
250	237	133	250	3	153	196	238	176	55	216
251	3	0	141	181	179	37	233	227	177	198
252	200	144	124	7	67	152	188	19	87	12
253	125	252	170	110	136	84	247	223	139	220
254	60	220	140	237	108	228	252	183	72	233
255	38	51	11	32	1	196	183	68	227	143

Рис. 3. Вікно Mathcad з вибраним великорозмірним МК_П, ізоморфно представленим двома складовими (KeyA, KeyB) у цифровому та візуальному виглядах, (ліворуч) та програмним модулем для багаторазових перестановок (праворуч).

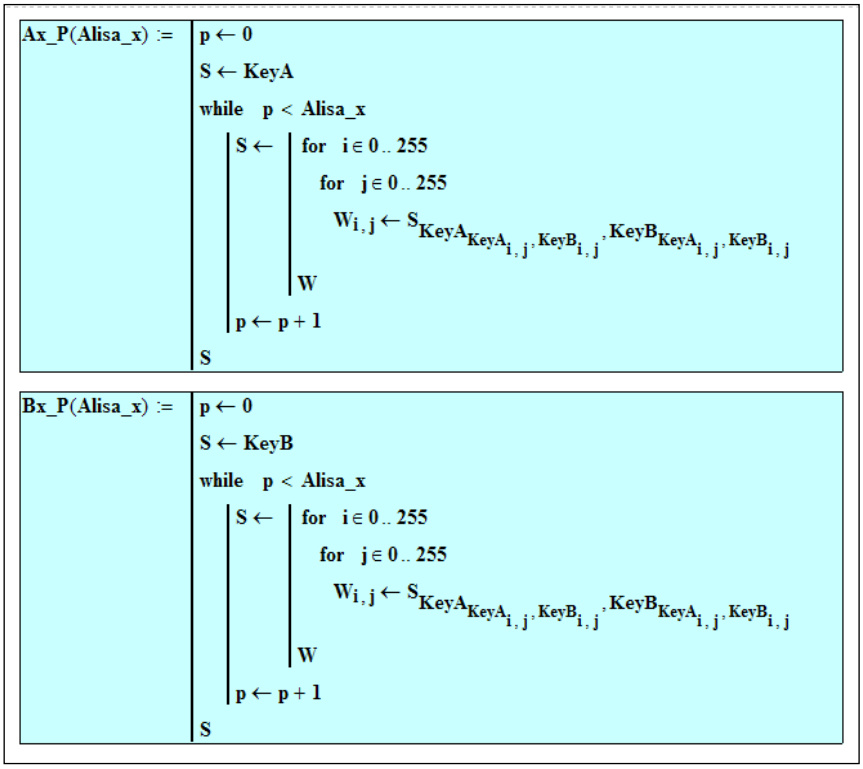


Рис. 4. Вікно з Mathcad з програмними модулями, що відображають процедуру ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки у потрібну степінь.

Отже, як було раніше показано та тут, ми можемо замінити піднесення у відповідні степені матриць-перестановок МК_П (N*N бінарних, де $N=2^{16}$) при їх ізоморфних поданнях ітераційними перестановками самих цих початкових перестановок. Крім того, час на виконання цих ніби вже спрощених ітераційних процедур необхідно ще зменшувати на порядки, бо значення степенів є досить великими для криптографічних застосувань. Але це можливо при використанні деякого базового набору фіксованих перестановок (фіксовані степені ГМП) та специфічної їх послідовності. Недоліком такого підходу є збільшені затрати, пов'язані з необхідністю у запам'ятовуванні цього набору. Для перевірки адекватності прискорених алгоритмів ізоморфного формування степенів матричних перестановок ми порівнювали піднесені у матричну степінь бітові матриці (після переведення їх у ізоморфний вигляд) з матрицями, отриманими швидкими перестановками у їх ізоморфних поданнях. встановлено їх рівність.

Ще одним з підходів, по аналогії з [29, 31], є використання деяких, узгоджених сторонами скалярів ***xa*** та ***xm*** (одного чи двох), як ключів для КП (зашифрування) ними складових KeyA та KeyB головної МП (ГМП) за допомогою афінного шифру з по-елементними операціями за модулем 257. Утворені з них криптограми, їх пара, будуть складовими нової МП, повністю будуть зберігати всі необхідні властивості ГМП, мати аналогічні гістограми та відповідати вимогам. При відкиданні значень «0» та «1» для ***xa*** та ***xm*** оцінки показують, що число різних таких пар скалярів може бути 254*254, а кількість можливих переставлять цих пар у їх псевдовипадковій послідовності-множині оцінюється величиною (254*254)!. Оскільки ця величина є досить значною, навіть у криптографічному сенсі, то можна гарантовано стверджувати про

можливість створення і таким методом потрібної низки-потоку МК_П значної розмірності. Для практичних застосувань навіть одного мультиплікативного афінного (лінійного) крипто-перетворення достатньо, щоб з множини 256-ти значень ***xm*** створювати, крім того, й без повторів, значну кількість (а саме **256!**) випадкових векторів довжиною 256 і більше, для формування цим узгодженим вектором послідовності необхідних МК_П у вигляді двох його складових виду зображень, тобто блоків байтів. Результати моделювання процесів генерування МК_П KeyM, як першої складової нової МК_П, зі складової KeyA початкової МК_П у Mathcad для описаної ситуації показані на рис. 5, де для ***xm*** **=** ***km*** = 17, наприклад, відображені програмні модулі-формули та відповідні матриці. Генерування другої складової МК_П KeyM виконується з тим же ***xm*** **=** ***km***=17, але від KeyB (не показано).

KeyM(km , KeyA) :=

for $i \in 0..255$

  for $j \in 0..255$

    $W_{i,j} \leftarrow \mathrm{mod}\left[\left(KeyA_{i,j}+1\right)\cdot km, 257\right]-1$

W

KeyAkm =

	0	1	2	3	4	5	6	7	8	9
0	201	128	218	79	195	71	175	159	86	115
1	6	170	118	190	169	16	246	216	48	46
2	26	205	35	29	173	141	90	34	240	183
3	10	69	46	150	45	28	48	172	191	43
4	73	65	139	94	230	105	84	59	87	162
5	124	19	204	43	5	220	142	78	57	45
6	21	96	223	232	31	233	158	91	41	40
7	223	22	66	90	129	151	118	181	4	126
8	206	232	1	175	98	199	19	200	228	238
9	141	194	244	154	146	155	82	44	90	76
10	224	216	152	80	169	213	99	88	39	107
11	179	121	68	238	123	45	141	33	141	218
12	194	86	82	163	198	8	36	38	136	46
13	56	176	185	31	85	95	84	182	173	87
14	202	207	35	119	6	218	43	172	30	111
15	104	81	62	0	56	196	27	5	171	15

KeyM(17 , KeyA) =

	0	1	2	3	4	5	6	7	8	9
0	201	128	218	79	195	71	175	159	86	115
1	6	170	118	190	169	16	246	216	48	46
2	26	205	35	29	173	141	90	34	240	183
3	10	69	46	150	45	28	48	172	191	43
4	73	65	139	94	230	105	84	59	87	162
5	124	19	204	43	5	220	142	78	57	45
6	21	96	223	232	31	233	158	91	41	40
7	223	22	66	90	129	151	118	181	4	126
8	206	232	1	175	98	199	19	200	228	238
9	141	194	244	154	146	155	82	44	90	76
10	224	216	152	80	169	213	99	88	39	107
11	179	121	68	238	123	45	141	33	141	218
12	194	86	82	163	198	8	36	38	136	46
13	56	176	185	31	85	95	84	182	173	87

Рис. 5. Формули та вигляд (2D) генерованого МК_П з ГМК_П простим лінійним КП та функціональним параметричним (вікно з Mathcad).

Гістограми всіх цих векторів з елементами, що не повторюються, також є горизонтальними лініями, як і обох складових всіх генерованих за їх допомогою перестановок, що відображаються у вигляді і-тих криптограм складових KeyA та KeyB ГМК_П та утворюються за допомогою афінного шифру, пари і-их компонентів векторів (адитивна і мультиплікативна складові) чи лише однієї і-тої компоненти з них. Пари цих криптограм і є по суті і-ими поточними матричними перестановками, що однозначно відображаються і у вигляді двох матриць розмірністю (256*256). Оскільки гістограми складових МК_П та випадкових векторів є горизонтальними лініями, а їх ентропія рівна 8 біт, то крипто-аналіз на їх основі унеможливлюється. Крім того, ГМК_П, два (може бути і один) узгоджені допоміжні псевдовипадкові векторні ключі є секретними, що дозволяє лише сторонам процесу КП створювати чи мати цю низку (потік) МК (МК_П типу). В принципі, секретною може бути лише ГМК_П, або узгодженими лише вищезгадані векторні ключі.

Розглянемо ще один з методів генерування поточних (на і-тому кроці) МК_П. Він полягає в наступному: однакові циклічні зсуви складових ГМК_П по ***x*** та ***y*** координатах на відповідні вибрані (узгоджені сторонами) значення з діапазону 1-254 теж дозволяють, як показують експерименти, отримувати у ізоморфному поданні з початкової перестановки нову перестановку, а для генерації всього потоку великорозмірних перестановок (МК_П) задіяти два (може бути і один) узгоджених сторонами допоміжних псевдовипадкових векторних ключів. З урахуванням обмежень, тут моделювання цього способу не наводяться, але отримані результати також підтверджують забезпечення тих же можливостей, якостей та вищенаведених оцінок, що і для першого методу. Оскільки ці зсуви є одним з часткових видів загальних можливих перестановок, але елементів самих складових ГМК_П, то відкривається можливість, здійснюючи самою ГМК_П одноразову (багаторазову) перестановку байтів її складових відображень, отримувати нові МП, що будуть повністю відповідати вимогам. Про цей метод та необхідний для реалізації та перевірки його функціонування інструментарій вже частково було сказано вище.

Результати формування цим методом потоку великорозмірних МК_П при його моделюванні у Mathcad показані на рис.6, 7 та підтверджують його адекватність, коректність, відповідність встановленим вимогам. Пропоновані методи, результати їх моделювання підтверджують досягнення суттєвих переваг за рахунок використання нових ізоморфних подань МК, що сприяли зменшенню часу обчислень при заміні операцій піднесення у степені послідовністю базових перестановок, зменшенню затрат та складності обчислювальних процедур, операцій та забезпечили простоту можливих варіантів реалізацій, які орієнтовані на матричні процесори та прискорювачі.

Використовуючи додатково розроблені та показані на рис.8 функціональні параметричні моделі КП на основі генерованих МК_П пропонованими методами, було виконано перевірку (правильного до вимог) їх синтезу та адекватності методів та їх моделей шляхом прямого та зворотного КП напівтонових та кольорових зображень лише за допомогою цих МК_П. Отримані

моделюванням у Mathcad результати КП одного з можливих зображень, його проміжні та кінцева криптограми, відновлені зображення, явні та різницеві показані на рис. 9.

P_s16A := T_PF(15, KeyA) P_s16B := T_PF(15, KeyB)

P_sAV := T_PF(75, KeyA) P_sBV := T_PF(34, KeyB)

P_sAV =

	0	1	2	3	4	5	6	7	8	9
0	170	88	242	27	94	166	117	16	11	185
1	250	225	13	106	20	140	2	86	154	137
2	29	87	171	78	55	9	92	104	115	106
3	212	203	173	73	26	111	255	37	96	236
4	88	178	205	155	190	58	138	32	204	194
5	230	134	215	101	149	88	220	48	4	223
6	113	27	166	121	25	255	31	169	221	199
7	111	96	249	42	171	187	24	212	101	64
8	210	202	91	25	187	26	203	63	197	227
9	8	61	213	143	171	250	89	85	17	29
10	109	103	219	127	66	35	237	225	158	114
11	4	208	105	200	205	123	245	227	43	112
12	74	13	136	83	73	241	62	160	17	156
13	132	54	201	99	126	185	121	69	157	184
14	113	10	134	112	203	64	151	18	53	239
15	178	88	50	129	176	119	134	213	87	216

P_sBV =

	0	1	2	3	4	5	6	7	8	9
0	247	171	226	116	214	113	85	115	6	152
1	87	21	32	230	178	45	170	139	77	43
2	38	10	45	29	226	245	181	81	36	62
3	84	249	31	194	157	214	30	137	61	148
4	179	252	250	228	145	142	105	221	56	133
5	8	252	221	48	192	254	192	29	3	22
6	27	108	100	54	136	117	195	121	133	202
7	174	208	151	14	96	83	239	190	180	168
8	154	115	120	75	234	28	193	129	161	117
9	60	77	212	58	110	201	221	45	76	79
10	29	186	49	0	14	32	57	155	184	185
11	221	224	55	137	113	172	145	181	109	206
12	208	64	248	88	37	216	241	141	128	239
13	171	90	214	10	56	244	218	154	62	129
14	198	134	154	204	130	111	194	48	251	152
15	100	202	82	220	93	228	229	252	42	165

P_SwVA := T_PFW(4, P_s16A, P_s8A, P_s8B) P_Sw84B := T_P

P_SwVB := T_PFW(1, P_s4B, P_s16A, P_s16B)

P_SwVA =

	0	1	2	3	4	5	6	7	8	9
0	170	88	242	27	94	166	117	16	11	185
1	250	225	13	106	20	140	2	86	154	137
2	29	87	171	78	55	9	92	104	115	106
3	212	203	173	73	26	111	255	37	96	236
4	88	178	205	155	190	58	138	32	204	194
5	230	134	215	101	149	88	220	48	4	223
6	113	27	166	121	25	255	31	169	221	199
7	111	96	249	42	171	187	24	212	101	64
8	210	202	91	25	187	26	203	63	197	227
9	8	61	213	143	171	250	89	85	17	29
10	109	103	219	127	66	35	237	225	158	114
11	4	208	105	200	205	123	245	227	43	112
12	74	13	136	83	73	241	62	160	17	156
13	132	54	201	99	126	185	121	69	157	184
14	113	10	134	112	203	64	151	18	53	239
15	178	88	50	129	176	119	134	213	87	216

P_SwVB =

	0	1	2	3	4	5	6	7	8	9
0	247	171	226	116	214	113	85	115	6	152
1	87	21	32	230	178	45	170	139	77	43
2	38	10	45	29	226	245	181	81	36	62
3	84	249	31	194	157	214	30	137	61	148
4	179	252	250	228	145	142	105	221	56	133
5	8	252	221	48	192	254	192	29	3	22
6	27	108	100	54	136	117	195	121	133	202
7	174	208	151	14	96	83	239	190	180	168
8	154	115	120	75	234	28	193	129	161	117
9	60	77	212	58	110	201	221	45	76	79
10	29	186	49	0	14	32	57	155	184	185
11	221	224	55	137	113	172	145	181	109	206
12	208	64	248	88	37	216	241	141	128	239
13	171	90	214	10	56	244	218	154	62	129
14	198	134	154	204	130	111	194	48	251	152
15	100	202	82	220	93	228	229	252	42	165

Рис. 6. Формули та частина цифрових масивів генерованого потоку МК_П з ГМК_П шляхом ітераційних чи послідовних фіксованих перестановок

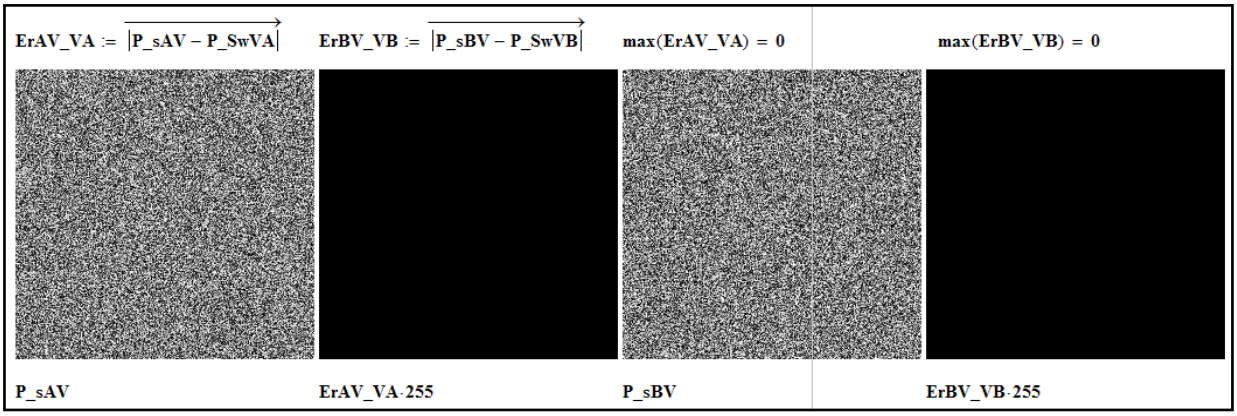


Рис. 7. Формули для порівняння та вигляд генерованих МК_П з ГМК_П та різницевих, що відображають похибку.

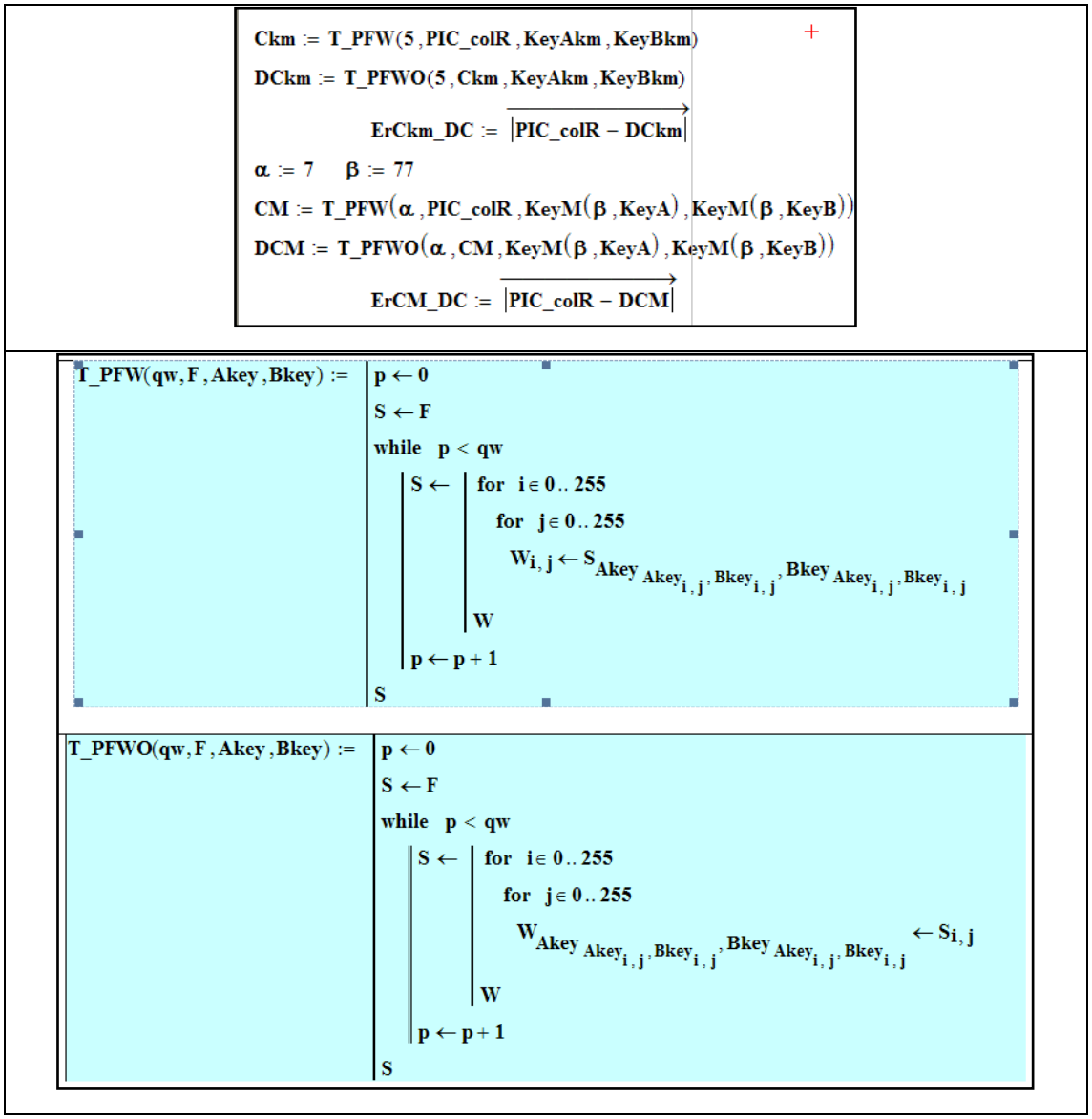


Рис. 8. Функціональні параметричні моделі КП на основі згенерованих МК_П

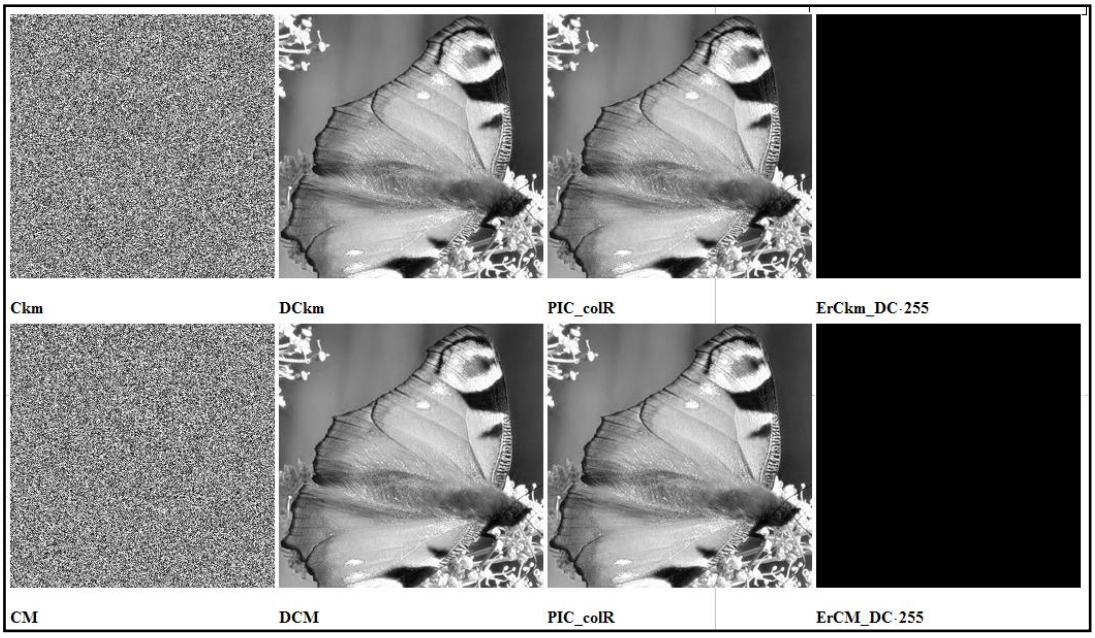


Рис. 9. Пряме та зворотне КП З на основі згенерованих МК_П

Висновки. Запропоновано та промодельовано три методи генерації потоку матриць перестановок значної розмірності при їх нових ізоморфних представленнях. Результати експериментів, оцінки стійкості підтвердили якість генерованих МК_П, адекватність роботи та функціонування методів, їх моделей, базових процедур, їх переваги, ефективність та перспективність.

Список літератури

1. S. Zeadallya, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," Internet of Things, 2019, doi: 10.1016/j.iot.2019.100075. Elsevier.

2. Моделювання матричних алгоритмів криптографічного захисту / В. Г. Красиленко, Ю. А. Флавицька // Вісн. Нац. ун-ту "Львів. політехніка". - 2009. - № 658. - С. 59-63.

3. 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. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2012_2_3_15.

4. 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. - Режим доступу: http://nbuv.gov.ua/UJRN/Vchnu_tekh_2014_1_16.

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

6. Красиленко В. Моделювання та дослідження криптографічних перетворень зображень на основі їхньої матрично-бітово-зрізової декомпозиції та матричних моделей перестановок з верифікацією цілісності / В. Красиленко, Д. Нікітович // Електроніка та інформаційні технології. - 2016. - Вип. 6. - С. 111-127. - Режим доступу: http://nbuv.gov.ua/UJRN/Telt_2016_6_14.

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

8. 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. - Режим доступу: http://nbuv.gov.ua/UJRN/Kitonv_2016_23_7.

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

10. Красиленко В.Г., Нікітович Д.В. Моделювання сторінкових криптографічних перетворень масивів кольорових зображень на основі матричних моделей та перестановок. «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.

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. - С. 60-63. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2011_7_17.

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., Нікітович Д.В. Вдосконалення та моделювання електронних цифрових підписів матричного типу для текстографічних документів. Матеріали VI МНПК «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 МНПК, 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. - 2019. - Вип. 1. - С. 92-100. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2019_1_14.

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. 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.

18. Krasilenko V. G., Kychak V. M., Nikolskyy A. I., Lazarev A. A., Nikitovych D. V. Simulation of algorithms for detection, localization and tracking of moving objects in video streams. Матеріали IX конференції «Сучасні проблеми інфокомунікацій, радіоелектроніки та наносистем (СПІРН-2023)», Вінниця, 15-17 листопада 2023 р. Вінниця, 2023. URL: https://conferences.vntu.edu.ua/index.php/spirn/spirn2023/paper/download/19349/16036 .

19. V.G. Krasilenko, A.A Lazarev, D.V Nikitovich, "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," Hershey, PA: IGI Global, pp. 170-214, 2020.

20. Krasilenko V. G., Pidlubnyi V. F., Nikitovich D. V. Research and simulation

of the method of generation of the flow of matrix keys of permutations and their characteristics for encryption-masking of video frames. Вісник Хмельницького національного університету. Технічні науки. 2023. №3 (321). С. 339-347.

21. Красиленко В. Г. Алгоритми формування двовимірних ключів для матричних алгоритмів криптографічних перетворень зображень та їх моделювання / В. Г. Красиленко, В. І. Яцковський, Р. О. Яцковська // Системи обробки інформації. - 2012. - Вип. 8. - С. 107-110. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2012_8_27.

22. W. Diffie, and M. E. Hellman, “New Directions in Cryptography”, IEEE Transactions on Information Theory, Vol. IT22, No. 6, Vol. 22, No. 6, pp. 644-654, 1976.

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

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

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

26. 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. - С. 151-157. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2017_3_32.

27. 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. - 2017. - № 26. - С. 111-120. - Режим доступу: http://nbuv.gov.ua/UJRN/Kitonv_2017_26_22.

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

29. 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. Режим доступу: https://chdtu.edu.ua/itont-2018/materiali-konferentsiji

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

31. Krasilenko V. G. Podlubnyi V. F., Nikitovych D. V. 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. 2nd International Conference on Innovative Solutions in Software Engineering, (ICISSE), Vasyl Stefanyk Precarpathian National University, 29-30 November 2023 p. Ivano-Frankivsk, 2023. Pp. 222-231. URL: https://doi.org/10.5281/zenodo.10397356