International Science Group

ISG-KONF.COM

VIII

INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE "PRIORITY AREAS OF RESEARCH IN THE SCIENTIFIC ACTIVITY OF TEACHERS"

Zagreb, Croatia

February 27 – March 01, 2024

ISBN 979-8-89292-749-9

DOI 10.46299/ISG.2024.1.8

МОДЕЛЮВАННЯ ПРОТОКОЛІВ УЗГОДЖЕННЯ ВЕЛИКОРОЗМІРНИХ СЕКРЕТНИХ КЛЮЧІВ-ПЕРЕСТАНОВОК ПРИ ЇХ ІЗОМОРФНИХ ВІДОБРАЖЕННЯХ

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

Нікітович Д. В.,
Аспірант
Вінницький національний технічний університет

Анотація: Запропоновано нові ізоморфні матричні представлення ключів-перестановок значної розмірності, їх особливості та переваги для моделювання протоколів узгодження сторонами головних секретних ключів-перестановок. Наведено результати моделювання процесів генерування матриць перестановок та їх степенів, як базових процедур пропонованих протоколів узгодження спільного секретного ключа-перестановки у ізоморфному їх представленні, у тому числі і запропонованих прискорених методів піднесення перестановок у значні степені. Для прискорення цих процедур використовуються набори (у їх ізоморфних форматах) фіксованих перестановок, степені яких відповідають відповідним вагам розрядів двійкових чи інших кодів, якими кодовані вибрані сторонами випадкові числа. Моделювання протоколів узгодження секретного ключа-перестановки в цілому, базового та кооперативного, продемонстрували адекватність та переваги ізоморфних представлень для опису та процесів функціонування моделей та запропонованого протоколу.

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

Вступ. Сучасний інформаційно-комунікаційний простір важко уявити без цілої низки зафіксованих камерами та подібними приладами реальних статичних та динамічних зображень, відеофайлів, що представлені в самих різноманітних форматах. Зі стрімким розширенням областей практичного використання зображень, методів та інструментів їх обробки, аналізу, розпізнавання, відстеження зросла і кількість різноманітного типу 2D (3D, 4D)-моделей об’єктів, що необхідні для цього та широко використовуються та досліджуються для вирішення багатьох задач, пов’язаних з представленням, візуалізацією та зберіганням даних. Згадаємо тут лише деякі приклади цих застосувань: інтерактивне моделювання, автоматизоване проектування, ігри, анімація, дизайн інтер’єру та архітектури, розпізнавання та сегментації об’єктів, геоінформаційні та інші системи спостереження, діагностики, моніторингу. Але широке застосування зображень, 2D-моделей об’єктів, з урахуванням їх специфічних особливостей, спричинило можливості втручань у ці інформаційні

масиви, порушення їх цілісності та конфіденційності, збільшення їх вразливості, що викликало занепокоєння щодо їхніх безпеки та контролю доступу. Несанкціонований доступ до таких моделей може призвести до значних порушень безпеки або збитків бізнесу. Саме тому зростав і продовжує зростати попит на алгоритми шифрування двовимірних, тривимірних об'єктів (зображень) з високим рівнем безпеки, цілісністю та стійкістю до атак. Численні алгоритми шифрування, що з'явилися ще з 1970-х років призвели до розробки низки досить відомих стандартів шифрування даних: DES, потрійного DES, розширеного стандарту шифрування (AES), асиметричного алгоритму шифрування RSA та інших. Незважаючи на те, що декілька шифрів 1D і 2D були розроблені спеціально для цифрових зображень, алгоритми шифрування 2D-об'єктів все ще досить обмежені.

Перехід від форматів даних скалярного типу у відомих системах до більш відповідних та природніх матрично-тензорних форматів інтенсифікував пошук нових матрично-алгебраїчних моделей (МАМ) криптографічних перетворень (КП) 2D (3D) - масивів, зображень (З). На основі МАМ появився новий клас криптосистем матричного типу (КМТ) [1-4]. Виявлені в цих роботах переваги таких криптосистем на основі МАМ, сприяли інтенсифікації досліджень КМТ, МАМ та появі публікацій [5-10], у яких було продемонстровано цілу низку нових їх покращень та запропоновано розширення областей їх ефективного застосування. Матричні афінні та афінно-перестановочні шифри (МАПШ) на основі нових просунутих МАМ, їх модифікації досліджувались та використовувались для криптографічних перетворень (КП) зображень, при створенні покращених цифрових підписів у [11-15]. Базовими процедурами КП у матричних моделях перестановок (ММ_П), є множення матриць та по-елементні операції за модулем над матрицями бітів чи байтів. Ці матриці байтів, утворених з конкатенованих рядків, колонок, векторів, що в унітарних чи інших кодах відображають символи, коди, байти, при використанні для КП таких ММ_П необхідно множити на матриці перестановок (МП). Пропоновані МАМ, в тому числі ММ_П, легше відображаються при їх апаратних реалізаціях на матричні процесори, мають розширені функціональні можливості, покращену крипто-стійкість, дозволяють перевіряти цілісність криптограм чорно-білих, кольорових зображень і наявність у них перекручувань [5,7]. Використання МАМ дозволяє створювати блокові [6], параметричні [8], багатосторінкові [9] моделі КП з їх підвищеною криптостійкістю [10]. Практично для всіх відомих алгоритмів та шифрів, включно з новостворюваними [16-23], 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]. З робіт [6, 8, 9] відомо, що при КП на основі МАПШ, векторних АПШ криптограми для деяких видів текстографічних документів (ТГД) і зображень, 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. Низка таких (поточних, покрокових, по-фреймових) псевдовипадкових МК, які б відповідали вимогам, швидко генерувались, потрібна і для маскування, криптографічних перетворень відео-файлів чи потоку блоків з файлів, зображень при їх значних розмірах [16-19].

Постановка проблеми. Таким чином, для покращених КП зображень, особливо послідовності відеокадрів, з використанням ММ_П або інших МАМ виникає гостра потреба у формуванні з головного МК набору (послідовності) різних МП, які б задовольняли ряду вимог. Методи генерування потоку МК-перестановок з головного МК (ГМК), але тільки для бітових МП невеликих розмірів (256*256), частково розглядались в [24]. Деякі аспекти питання узгодження головного матричного ключа (ГМК) загального виду розглядались в [25, 26]. Але вони не стосувались ситуацій, коли в якості головного чи сесійного матричного ключа використовується головна матриця перестановки (ГМП) та ще й значної розмірності. Крім того, необхідно передбачити, як було показано вище, можливість та зручність швидкого формування з такої ГМП потоку аналогічних МП. Тому **метою роботи** є спроба не тільки запропонувати, а й промоделювати, дослідити протокол узгодження секретного (головного) МК (МП значної розмірності), тобто ГМП для МАМ КП у криптосистемах МТ. Крім того, на основі застосування нових ізоморфних представлень МП та аналізу процедур здійснення протоколу, модифікувати, удосконалити та адаптувати вид, структуру великорозмірних ГМП до формату зображень і до швидких апаратних реалізацій протоколу.

Виклад основного матеріалу. Аналіз запронованих шифрів матричного типу, особливо багатофункціональних параметричних блочних [6-8], показав, що для їх опису та моделювання доцільно використовувати 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). У моделях КП бажано формувати та обробляти матриці перестановок (МП) чи їх необхідні степені теж у ізоморфних просторах, які є більш зручними та адекватними використовуваним засобам. 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. Відмітимо, що з урахуванням структури файлів самого різного типу та формату, тіло любого файлу чи й увесь файл є сукупністю (кортежом) байтів. Ніяким чином не зменшуючи загальності підходу, розглянемо ситуацію, коли файл даних чи великого розміру масив даних, що потрібно зашифрувати, розбивається на блоки довжиною у 256*256=65536 байтів, що еквівалентно значній довжині блоків. Кожен такий блок очевидно може бути представлений у вигляді матриці чорно-білого зображення розмірністю 256*256 елементів-пікселів, а інтенсивність (елемент матриці) відображається байтом. Можна показати, що при використанні різних шифрів, які б ми не робили криптографічні

перетворення над сукупністю байтів, кожен байт (код) явного тексту, файлу переходить лиш в один байт (нову кодову комбінацію), а множина цих комбінацій однозначна та обмежена. По суті всі відомі та нові шифри можна звести до двох простих процедурних кроків: 1) першого кроку заміни коду кожного байту у блоці на новий код байту, але для кожного байту існує своя специфічна заміна з усієї можливої множини таких замін та 2) другого кроку перестановок байтів у блоці. Нехай для другого кроку необхідно переставити всі байти блока у відповідності до матриці перестановок (МП). Для вибраного нами прикладу МП в загальноприйнятому вигляді повинна бути квадратною з N*N елементами («0» чи «1»), де $N=2^{\wedge 16}$. Кількість можливих таких МП для такого N, тобто потужність їх множини оцінюється, як N! , що вже для такого N дає колосальні значення (**65536** !). Дві координати (рядок і стовпчик) блоку з таким розміром теж представляються байтами. Тобто є можливість двома блоками байтів, по суті двома матрицями-зображеннями (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, можна любу МП однозначно ізоморфно відобразити двома матрицями розміром 256*256, елементи яких приймають значення з діапазону 0-255. На рис. 1 показано вікно Mathcad з модулем для генерування базового (головного) МК (МП), вигляд його складових KeyA та KeyB (двох напівтонових зображень) та їх гістограми у вигляді горизонтальних ліній, як і очікувалось. Зауважимо, що таке у вигляді двох зображень ізоморфне представлення МП дає нам додаткову 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. Деякі результати моделювання криптографічних перетворень зображення (Im) при використанні згенерованої МП та її складових, як ключів для МАПШ, показані на рис. 2 з матрицями явного зображення (Im), проміжних, його криптограм (Cmap) та перевірних зображень. А гістограми явного зображення, його криптограм після кожного перетворення афінними складовими МП показані у вікні Mathcad на рис.1. Вище згадані та ряд інших проведених модельних експериментів підтвердили, що криптографічні перетворення навіть дуже специфічних зображень, і довільних блоків байтів на основі МАПШ наявними 2-ма складовими з ізоморфного представлення 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.

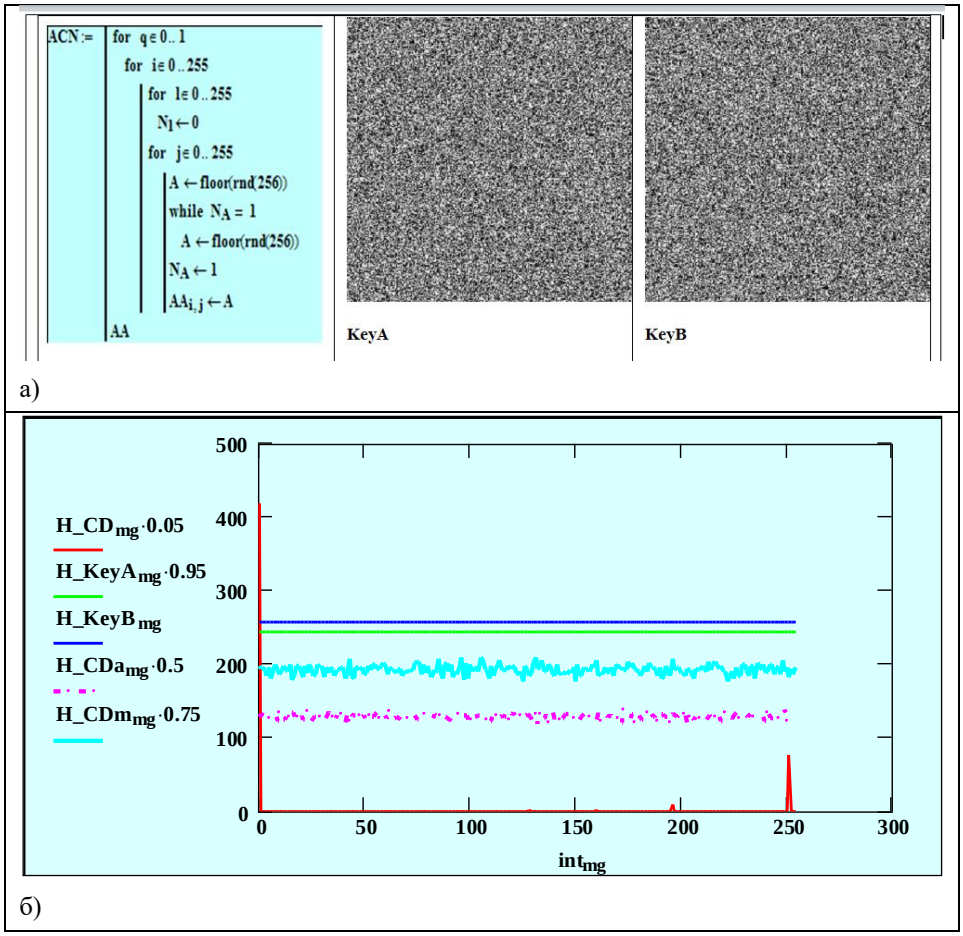

Рис. 1. а) Програмний модуль для генерування базового (головного) МК (МП) та вигляд складових KeyA та KeyB у форматі двох чорно-білих зображень (Вікно Mathcad). б) Гістограми H_KeyA та H_KeyB відповідних KeyA та KeyB МП, гістограма H_CD (співпадає з гістограмою явного З), відповідні гістограми H_CDa та H_CDm криптограм після адитивного та мультиплікативного афінних КП З за допомогою тих же KeyA та KeyB (Вікно Mathcad)

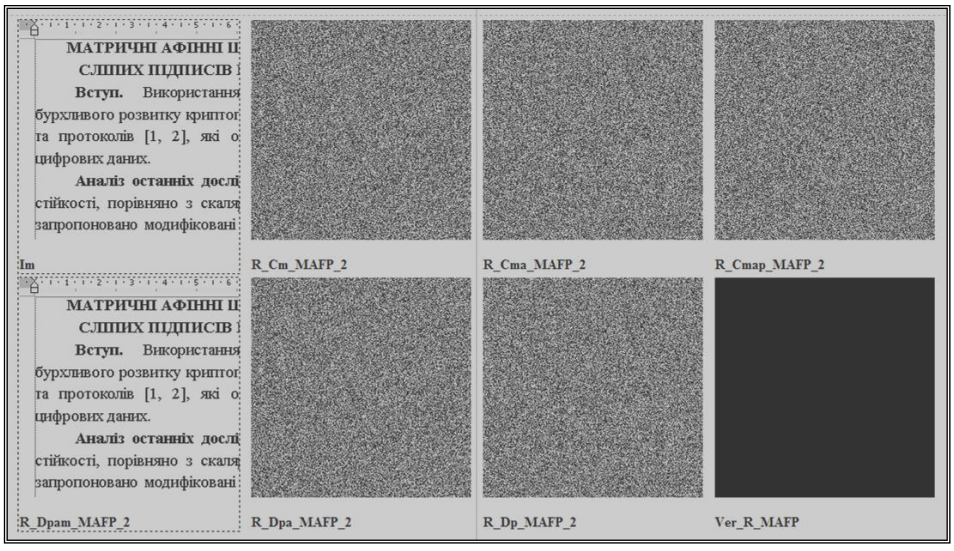

Рис. 2. Моделювання МАПШ на основі МП-складових, як адитивного та мультиплікативного МК. Верхній ряд, зліва направо: явне, після перетворень, криптограма; Нижній ряд: відновлене, проміжні та різницеве (праворуч) З ТГД

Результати моделювання МАПШ та багатокрокових МАПШ [2, 6-8], 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 високу якість криптографічних перетворень 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, 25], 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.

Для розгляду сутності протоколу узгодження ГМП сторонами допустимо, що є дві сторони: ***x*** (Alisa) та ***y*** (Bob) і їм відома якась одна МП з множини допустимих у її ізоморфному вигляді: складові KeyA та KeyB (два зображення), що було показано на рис. 1. Звідси випливає, що їм також відома і матриця зворотної перестановки (МЗП), яка теж подібно представлена у вигляді 2-х зображень 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. 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 з ізоморфно представленими МП, а не зі скалярами. Для наочності і спрощення демонстрації ми вибрали у першому експерименті ці степені для сторін, рівні 11 та 17, що частково буде видно на рис. 3-4, де показані результати моделювання цих двох кроків протоколу узгодження секретного МК у Mathcad.

Програмні модулі (копії вікон з Mathcad), що відображають процедуру ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки МП у потрібну степінь (11 !) стороною ***x*** (Alisa) показані на рис. 3. Аналогічні модулі (копії з Mathcad), що використовуються для процедури ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки у потрібну степінь (17 !) стороною ***y*** (Bob) тут не показані. Використовуючи 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), дивись рис. 4, сторони реалізують другий крок протоколу. Сторони не знають степені іншої сторони, але отримані ними МП є ідентичними, що видно з рис. 5, 6, де показані вигляди

проміжних і результативної секретної ГМП (у ізоморфному представленні З).

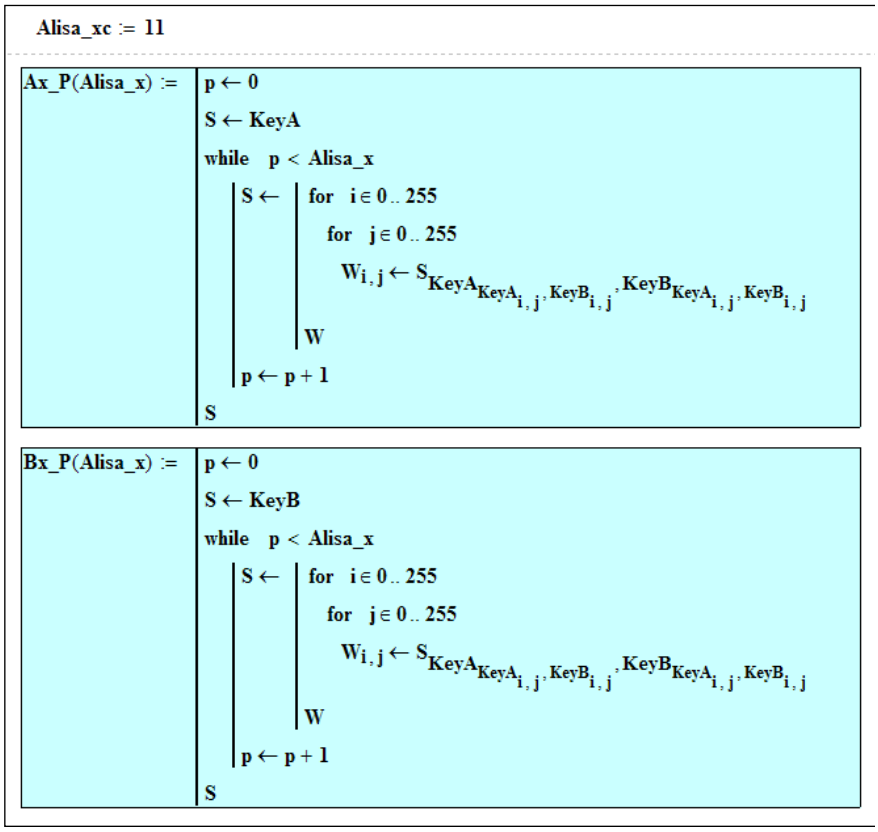

Рис. 3. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки у потрібну степінь (11 !) стороною *x* (Alisa)

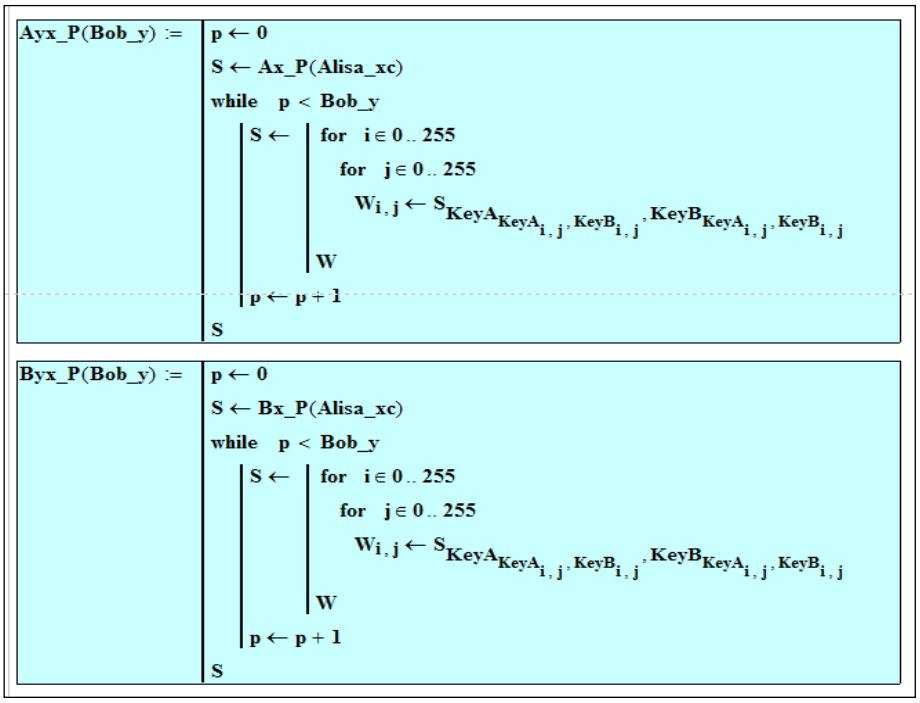

Рис. 4. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в отриманій від *x* новій МП, ізоморфних піднесенню у потрібну степінь (17 !) стороною *y* (Bob)

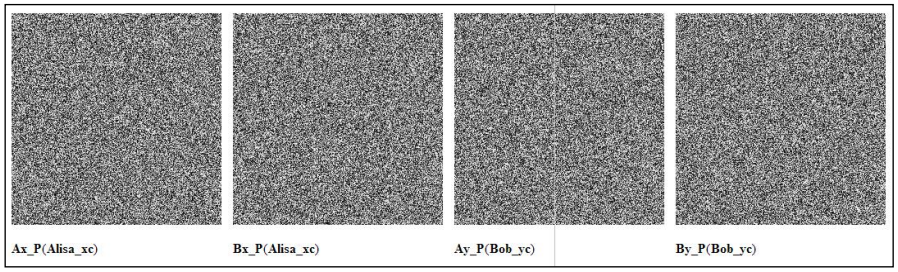

Рис. 5. Отримані сторонами нові МП (кожна у вигляді їх двох складових) після першого кроку протоколу, ті що пересилаються іншій стороні

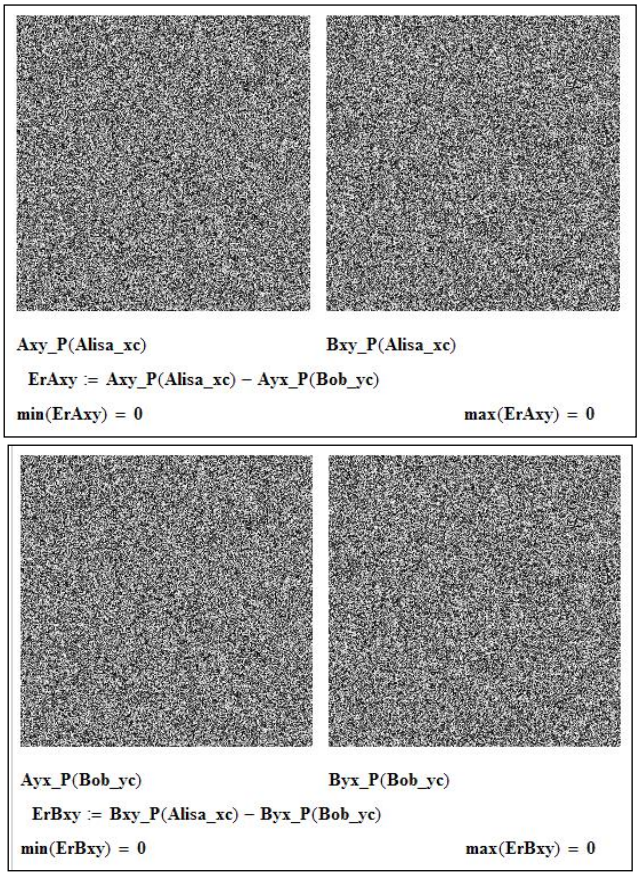

Рис. 6. Отримані сторонами ідентичні нові МП (кожна у вигляді їх двох складових) після другого кроку протоколу, тобто секретна МП

Отже піднесення матриць-перестановок МП (N*N бінарних, де $N=2^{16}$!) еквівалентно замінюється швидкими перестановками, які додатково можуть бути ще більш прискореними при значних степенях за рахунок використання деякого базового набору фіксованих (фіксовані степені ГМП) та специфічної їх послідовності. Такий підхід дає суттєві переваги за рахунок прискорень обчислення степенів ГМП, зменшення часу та простоти можливих реалізацій. Для необхідної крипто-стійкості від перебірних атак степені, в які сторони підносять по суті ізоморфно представлені МП значних розмірностей, повинні бути досить значними. Тому 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, фрагменти ключів, що показані на рис.7, засвічують їх рівність.

Sxd = 7 **SdP = 262**

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

xA = 255

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

Таким чином, протокол дозволяє з відомої ГМП без знання таємних степенів, що вибираються сторонами, створити для сторін секретний ключ, МП в ізоморфному вигляді за час, пропорційний числу фіксованих перестановок. Правильність функціонування протоколу підтверджена результатами моделювання у Mathcad. Вище було показано, що за допомогою узгодженого цим пропонованим протоколом секретного ізоморфно представленого МК, здійснена верифікація як його якості, так і адекватності раніше розроблених моделей [6-9] шляхом прямого та зворотного криптографічних перетворень ними зображень. Аналіз стійкості, з урахуванням потужності множини утворюваних цим протоколом відповідних великорозмірних МП, показав неможливість здійснення атак, так як вже для $N=2^{16}$ ця потужність оцінюється величиною $(2^{16})!$.

Висновки. Виконано моделювання протоколу узгодження секретного великорозмірного ключа-перестановки та підтверджено правильну його роботу, адекватність алгоритмічних кроків і методів формування проміжних, кінцевої МП. Перевірені алгоритми прискорених піднесень у значні степені матриць перестановок зі збереженням їх ізоморфних представлень, показані їх переваги.

Список літератури

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

2. Красиленко В. Г., Грабовляк С.К. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень. Системи обробки

інформації. – 2012. – Вип. 3(2). – С. 53-61.

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

4. 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.

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

6. 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.

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

8. 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.

9. 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.

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., Грабовляк С.К. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи.-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., 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: 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. 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. 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.

19. 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.

20. 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.

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

22. 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.

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

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

25. Красиленко В.Г., Нікітович Д.В. Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу.- Системи обробки інформації. – 2017. – Вип. 3 (149). – С. 151-

157.

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