УДК 004.056.55
Красиленко В.Г., к.т.н., с.н.с., доцент, професор; Нікітович Д.В., науковий співробітник
Вінницький інститут Університету "Україна"

МОДЕЛЮВАННЯ БАГАТОКРОКОВИХ ТА БАГАТОСТУПЕНЕВИХ ПРОТОКОЛІВ УЗГОДЖЕННЯ СЕКРЕТНИХ МАТРИЧНИХ КЛЮЧІВ.

Красиленко В.Г., Нікітович Д.В. Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів. Розглядаються протоколи узгодження секретного матричного ключа для криптографічних перетворень в системах і моделях матричного типу. Основою таких протоколів є узагальнення відомих протоколів Діффі-Хеллмана на матричний випадок і відповідні матричні процедури для формування двовимірних ключів. Обгрунтовані необхідність та переваги створення, узгодження та застосування матричних ключів для покращених криптографічних систем матричного типу і процедур зашифрування-розшифрування зображень. Запропоновані багатокрокові та багатоступеневі протоколи узгодження ключа з метою їх вдосконалення та підвищення стійкості до атак. Для підтвердження достовірності запропонованих удосконалень виконано ряд модельних експериментів у середовищі Mathcad Professional. Показані переваги багатокрокових протоколів узгодження ключа за рахунок використання в них багатоступеневих поелементно-матричних піднесень у степінь за модулем та конвеєрних процедур. Моделі та процедури враховують специфіку зображень і легко адаптуються до паралельних реалізацій та новітніх апаратних матричних процесорів. Наведено результати моделювання процесів створення секретних матричних ключів у вигляді зображень великої розмірності (320 * 240) на основі запропонованих протоколів.

Ключові слова: криптографічні перетворення зображень, матричний алгоритм Діффі-Хеллмана, узагальнені матричні моделі, секретний матричний ключ, багатокроковий протокол, розшифрування, протокол узгодження секретного спільного ключа, піднесення в ступінь по модулю.

Красиленко В.Г., Никитович Д.В. Моделирование многошаговых и многоступенчатых протоколов согласования секретных матричных ключей. Статья посвящена усовершенствованию и моделированию протоколов согласования секретного матричного ключа для криптографических преобразований в системах и моделях матричного типа. Основой таких протоколов является обобщение известных протоколов Диффи-Хеллмана на матричный случай и соответствующие математические процедуры для формирования двумерных ключей. Обоснована необходимость и преимущества создания, согласования и применения матричных ключей для улучшенных криптографических систем матричного типа и процедур зашифрования-расшифровки изображений. Предложены многоступенчатые и многошаговые матричные согласовательные протоколы с целью совершенствования их устойчивости к атакам. Для подтверждения достоверности предложенных протоколов выполнен ряд модельных экспериментов в программной среде Mathcad Professional. Показаны преимущества многоступенчатых поэлементно-матричных вознесений в степень по модулю и использования многошаговых конвейерных процедур. Вычислительные процедуры и матричные модели учитывают специфику изображений и легко адаптируются к параллельным реализациям и новейшим аппаратным матричным процессорам. Приведены результаты моделирования процессов создания секретных матричных ключей в виде изображений большой размерности (320*240) на основе предложенных модификаций протоколов.

Ключевые слова: криптографические преобразования изображений, матричный алгоритм Диффи-Хеллмана, обобщенные матричные модели, секретный матричный ключ, расшифровка, протокол согласования секретного совместного ключа, вознесение в степень по модулю.

Krasilenko V.G., Nikitovich D.V. Simulation of cryptographic transformations of color images based on matrix models of permutations with spectral and bit-plane decompositions. The article is devoted to the improvement and simulation of secret matrix key negotiation protocols for cryptographic transformations in matrix type systems and models. The basis of such protocols is the generalization of the known Diffie-Hellman and others protocols to the matrix case and the corresponding mathematical procedures for the formation of two-dimensional keys. The necessity and advantages of creation, matching and application of matrix keys for improved matrix-type cryptographic systems and image encryption-decryption procedures are substantiated. Multistage and multi step matrix reconciliation protocols are proposed with the aim of improving their resistance to attacks. To confirm the reliability of the proposed protocols a number of model experiments were performed in the software environment of Mathcad Professional. The advantages of multistage and multi step matrix reconciliation protocols are shown. Computational procedures and matrix models take into account the specificity of images and easily adapt to parallel implementations and the latest hardware matrix processors. The results of simulation the creation of secret matrix keys in the form of high-dimensional (320*240) images are presented on the basis of the proposed protocol modifications.

Keywords: Cryptographic image transformations, Diffie-Hellman matrix algorithm, generalized matrix models, secret matrix key, decryption, secret shared key negotiation protocol, modular exponentiation.

Вступ. Широке застосування інформаційних технологій при збільшенні обсягів та значимості інформаційних потоків в епоху електронних комунікацій потребує надійного та ефективного захисту цілісності інформаційних об'єктів (ІО) та стійкості різноманітних захищених систем управління до потенційних загроз. Зросла доля специфічних текстово-графічних документів (ТГД) у вигляді табличних даних, малюнків, діаграм, підписів, віз, резолюцій, тощо, які є зображеннями і

© Красиленко В.Г., Нікітович Д.В.

які необхідно опрацьовувати та передавати каналами з обмеженим чи закритим доступом, засвідчувати їх цифровими підписами. Особливе місце серед відомих методів захисту ІО віл несанкціонованого доступу займають криптографічні методи, що спираються на властивості самих ІО, а не носіїв ІО та пристроїв їх обробки та передачі, але якими б надійними не були б криптографічні системи, одним з ключових питань їх застосування на практиці є адміністрування ключами, включаючи процеси генерування ключів та їх узгодження електронним шляхом. Від надійності та стійкості до атак процесів створення спільних для обох сторін безпечних ключів залежить рівень безпеки. Перед обміном інформацією користувачам необхідно домовитись чи сформувати спільний безпечний ключ, з якого за необхідності створюються сесійний та низка похідних під-ключів. Відомі протоколи та алгоритми створення ключа при використанні навіть незахищених каналів зв'язку, наприклад алгоритми Діффі-Хелмана, MTI, STS та інші [1, 2]. Але більшість з них, як і більшість методів та засобів криптографічних перетворень (КП) ІО, зорієнтовані на системи з послідовною криптографічною обробкою сукупності виділених інформаційних блоків за допомогою одного ключа або його під-ключів, що є суто скалярами, незважаючи на їх довжину. Навіть для найкращих симетричних алгоритмів (на основі діючого стандарту AES, IDEA, тощо) довжини блоків та ключів не перевищують 256 бітів, за винятком хіба-що FEAL, RC6 та інших нових, де ці довжини можуть обмежуватись 1К-2К бітами [1]. Проте темпи розвитку методів криптоаналізу та комп'ютерних засобів спонукають до збільшення довжин ключів, вимірності скінченних полів і діапазонів чисел (модулів), які необхідно опрацьовувати, а це позначається на обчислювальній продуктивності, що в свою чергу призводить до пошуку нових операцій та методів їх прискорення, ускладнює процедури визначення, верифікації базових параметрів криптографічних систем (КС), генерування та зберігання ключів. Поява паралельних алгоритмів, а особливо матричних процесорів [2, 3]., потребує переорієнтації КП на ці засоби, та пошук і створення моделей матричного типу (МТ), засобів виконання КП ІО у вигляді ТГД (зображень), що краще відображаються на матричні процесори [4-11]. В останні роки збільшується доля задач, для яких КП необхідно виконувати над багатовимірними сигналами, багато-спектральними зображеннями різних фізичних, аерокосмічних об'єктів, а це потребує не лише матричних моделей (ММ) КП, але й однорідних до їх структури секретних матричних, тензорних ключів, наприклад у вигляді матриць-зображень [6-16].

Аналіз останніх досліджень і публікацій. Переваги КП матричними алгоритмами на основі більш узагальнених матричних афінних шифрів, в тому числі при створенні сліпих цифрових підписів на ТГД були продемонстровані в [4-7]. Ще більш узагальнені матричні афінно-перестановочні шифри були запропоновані та досліджені в [8], базовою операцією яких є матричні моделі перестановок (ММ_П), які мають наочну простоту. Зростання долі робіт, що присвячені КП, зашифруванню та розшифруванню різноманітних кольорових багато-спектральних зображень [6, 8-12, 17-20], теж підтверджує актуальність дослідження та удосконалення ММ КП та ставить, як показує аналіз цих робіт, на порядок денний гостру проблему створення для таких ММ і відповідних матричних ключів (МК). Для матрично-афінно-перестановочних алгоритмів [8] необхідно мати два види МК: набір бінарних матриць перестановок, позначимо тут їх як МК_П, що потрібні і для ММ_П [10-12, 17-20], та МК загального типу у вигляді чорно-білого чи кольорового (детермінованого, випадкового чи псевдо-випадкового) зображення, позначимо тут як МК_З (від «зображення»). Частково питання щодо формувань, застосувань МК_П розглядались в [8-10, 17-19, 21], добре досліджені в теорії груп та лінійній алгебрі, а тому тут ми їх розглядати не будемо, а специфіку їх застосування для протоколів узгодження секретного ключа розглянемо в іншій роботі. Стосовно МК_З відмітимо, що в роботі [14] була запропонована модифікація алгоритму Діффі-Хелмана на матричний випадок для створення 2-D ключа, а в [15] були розглянуті алгоритми формування двовимірних ключів для матричних алгоритмів криптографічних перетворень зображень, виконане їх часткове моделювання та запропонована ідея застосування і у матричному випадку покращених підходів та методів організації прискорених обчислень на основі матричної паралельної логіки. Але в цих роботах не проводились модельні експерименти зі збільшеною розмірністю МК_З та не були показані шляхи усунення відомих недоліків алгоритму Діффі-Хелмана.

© Красиленко В.Г., Нікітович Д.В.

Постановка наукової проблеми. Тому **метою** роботи є подальше вдосконалення протоколів узгодження секретного матричного ключа для ММ КП у системах та моделях матричного типу, покращення алгоритмів формування більш якісних та стійких до атак матричних ключів типу МК_З, їх моделювання та дослідження.

Виклад основного матеріалу та результатів дослідження.

Теоретична частина. Наведений у [15] протокол (базовий!) виконується так. Сторони узгоджують між собою чи й іншими користувачами мережею зв'язку матрицю-основу **К,** наприклад матрицю, що відповідає чорно-білому зображенню вибраного розміру. Бажано попередньо додаванням до неї матриці **R**, всі елементи якої дорівнюють «1» змістити її значення елементів у діапазон 1-256 або, як буде показано нижче, навіть у діапазон 2-256, щоб у результуючій матриці не було «0» та «1» елементів. Перша сторона, наприклад, абонент X (Alisa!), вибирає з множини зображень чи генерує відомим методом, засобом випадкове зображення матрицю **S_AS-R**, шляхом додавання до неї матриці **R** зміщує її значення елементів у діапазон 1-256, отримуючи скореговану матрицю **A** (у деяких експериментах позначена як S_AS) та обчислює 2-D масив (матрицю) **KSA** за формулою $\mathbf{KSA} \equiv \mathbf{K}^{\mathbf{A}} \bmod (m1 \cdot \mathbf{R})$, де матриці **A**, **K**, **R** та **KSA** мають однакові розміри $I \times J$, а операція піднесення у степінь за модулем m1 є по-елементною, тобто $\mathbf{KSA}_{i,j} \equiv \mathbf{K}_{i,j}^{\mathbf{Ai,j}} \bmod m1$. Цю матрицю шляхом віднімання від неї матриці **R** він коригує у стандартного формату зображення (**KSA-R)** та відправляє його другому абоненту Y (Bob!). Абонент Y взявши інше зображення **S_BS-R** та аналогічним чином коригуючи його у матрицю **B**, обчислює матрицю **KSB** за формулою $\mathbf{KSB} \equiv \mathbf{K}^{\mathbf{B}} \bmod (m1 \cdot \mathbf{R})$ та відправляє аналогічним чином скориговане відповідне йому зображення (**KSB-R)** першому абоненту X. Перший абонент X, отримавши це зображення коригує його у матрицю **KSB** (у подальшому пряме та обернене коригування матрицею **R** будемо опускати, розуміючи зв'язок між матрицями та зображеннями) та, використовуючи лише йому відому матрицю **A,** обчислює значення матричного ключа $\mathbf{KA} \equiv \mathbf{KSB}^{\mathbf{A}} \bmod (m1 \cdot \mathbf{R}) \equiv \mathbf{K}^{\mathbf{B*A}} \bmod (m1 \cdot \mathbf{R})$. Аналогічними діями абонент Y обчислює значення матричного ключа $\mathbf{KB} \equiv \mathbf{KSA}^{\mathbf{B}} \bmod (m1 \cdot \mathbf{R}) \equiv \mathbf{K}^{\mathbf{A*B}} \bmod (m1 \cdot \mathbf{R})$. Таким чином сторони отримують таємний ключ $\mathbf{KEY} \equiv \mathbf{K}^{\mathbf{A*B}} \bmod (m1 \cdot \mathbf{R})$, рівність якого забезпечена протоком для обох сторін. Вони можуть використовувати його як для зашифрування та розшифрування при передачі 2-D даних, зображень, особливо для ММ КП та у КС МТ [6-8,13,16,20], тощо, так і використати у якості матриці-основи для оновлень секретного ключа. Відомо, що не існує жодного ефективного алгоритму розв'язування задачі обчислення дискретного логарифма за модулем, а тому з урахуванням розширення та ускладнення задачі на матричний випадок, робить її розв'язування для зловмисника ще складнішим. Тому наведений протокол є взаємно безпечним. Якщо ж матриця **K** є невідомою для третьої сторони, як ми зазначали вище, то тоді цей протокол унеможливлює і так звану атаку «людина всередині». В загальному випадку діапазон значень елементів всіх використовуваних матриць у ММ такого протоколу може бути достатньо значним, що призводить до необхідності передавати по каналах зв'язку самі матриці, хоч і зменшує візуальне сприйняття. Вихід і у цих випадках можна знайти, якщо матриці представляти не одним а набором зображень, кожне з яких буде відповідати різним позиціям байтових багато-розрядних представлень значень елементів матриць. Якщо матриця **К** є публічною, то для підсилення стійкості протоколу сторони можуть лише відомим їм, наприклад, більш раннім ключем закривати її одним з вищевказаних шифрів [6-8, 20], що призводить фактично до чергового оновлення ключа. Крім того, можна закривати і матриці **A** та **B**, а в якості останніх чи в якості ключів закриття можуть бути використані характерні лише для кожної сторони зображення, що є по суті їх ідентифікаторами.

Сутність **багатокрокового протоколу** полягає у повторенні процедурних дій простого (одно-крокового) протоколу декілька разів по домовленості сторін. Використовуючи для наступних кроків в якості матриці-основи інші зображення, наприклад, отримані у попередніх кроках ключі чи результуючі степені за модулем, а у якості матриць-степенів обчислені їх попередні аналогічні степені чи деякі вибрані з певного набору зображення, сторони формують низку спільних ключів. Оскільки зловмиснику важче перехопити всі повідомлення, що

© Красиленко В.Г., Нікітович Д.В.

пересилаються сторонами та можуть містити закриті дані стосовно вибраних часу та інших ідентифікаторів сторін, вгадати час сеансів обміну, та необхідно розв'язати значно більшу кількість задач обчислення дискретного логарифма за модулем фактично для кожного елемента відповідних всіх 2-D масивів, то це підвищує стійкість багатокрокового протоколу у порівнянні з простим. Цьому сприяє і застосування конвеєрних багаторазових піднесень у степінь за модулем, і гнучкість вибору сторонами чергових матриць для процедур зі збільшеної по потужності їх множини. Розглянемо **теоретичні основи** та ММ одного з таких запропонованих варіантів удосконалення протоколу. Позначимо отриманий після першого кроку сторонами ключ як **КеуА1 (КеуВ1**), де букви відповідають стороні, а цифра – кроку. Тоді, взявши його як матрицю основу та виконавши необхідні аналогічні вищеописаним процедури протоколу, сторони після другого кроку отримають ключі: **КеуА2≡ КеуА1^{B*A}** mod (m1·**R**) **(КеуВ2≡ КеуВ1^{B*A}** mod (m1·**R**)), а оскільки ключі-основи **КеуА1** та **КеуВ1** рівні, то рівними є і ключі **КеуА2**, **КеуВ2**, тобто **КеуА2≡ КеуВ2**. А далі аналогічно: після 3-го кроку будуть обчислені ключі **КеуА3≡ КеуА2^{B*A}** mod (m1·**R**) **(КеуВ3≡ КеуВ2^{B*A}** mod (m1·**R**)) і т. д., при цьому буде забезпечена рівність покрокових ключів. Провівши деякі нескладні математичні перетворення, які тут не показані, можна встановити, що після виконання q кроків отримані ключі будуть виражені наступними виразами для обох сторін: **КеуАq≡ К$^{B\hat{}q*A\hat{}q}$** mod (m1·**R**) та **КеуВq≡ К$^{B\hat{}q*A\hat{}q}$** mod (m1·**R**), де кожен елемент відповідних матриць **А**^q **В**^q є q- а степінь (не за модулем!) кожного відповідного елемента матриць **А** та **В**. З цих виразів можна зробити цікаве припущення, яке потребує підтвердження і модельними експериментами, що замість взаємних передач проміжних повідомлень на кожному кроці можна виконати відповідні піднесення матриці **KSA ≡ К^{A}** стороною А у q- у степінь, а матриці **KSB ≡ К^{B}** стороною В у q- у степінь, а потім після обміну ними та піднесення їх сторонами у свої матриці степені **А** та **В** так само повторити піднесення останніх у q- у степінь. Іншими словами процедури піднесення у степінь можуть бути ієрархічними багатоступеневими, в тому числі і за модулем чи матрицею модулів, а багатоступеневість тісно пов'язана з повторенням кроків, тобто з багатокроковим аспектом запропонованих модифікацій протоколу.

Розглянемо деякі аспекти, які необхідно враховувати при використанні такого протоколу. По-перше, оскільки в якості основи можуть бути використані різні з відомої множини матриць чи з отриманої множини попередніх ключів, то виникає потреба в уточненні сторонами при колізіях цієї основи. Один з можливих варіантів полягає у застосуванні надійного та відомого для сторін ключа для шифрування ним та перевірки основи. Якщо до зображення цього надійного ключа інша сторона створить комплементарне зображення AD-R, так щоб їх сума дорівнювала m1·**R**, то на основі малої теореми Ферма, після за шифрування стороною Х матриці основи **К** піднесенням її у матрицю степінь **S_AS** та передачі результату **KSA-R** сторона Y підносить матрицю **К** у степінь **S_BS=AD** , отриману від сторони Х матрицю **KSA** множить по-елементно на обчислену **KSB** за модулем і отримує матрицю **F**, що повинна співпадати з основою **К**, дивись відповідні зображення на рис.1, отримані у результаті першого базового експерименту. Якщо зловмисник не знав **К**, то перехопивши **KSA** він ніяк не зможе знайти **S_AS** чи по аналогії з **KSB** знайти **S_BS.** Якщо ж він знає **К**, то згідно теорії розв'язування задачі обчислення дискретного логарифма за модулем є складним процесом, проте, як показав наш експеримент (рис.1), при невеликих значеннях чисел у матрицях (у наших зображеннях) у деяких окремих випадках, хоч і не повністю, вдається відновити зображення **S_AS** , зламавши брутальною атакою. По-друге, враховуючи перше та необхідність покращення стійкості протоколу до можливих атак, особливо для випадків, коли основа **К** є відомою, бажано ускладнити задачу зловмиснику. А це можна зробити, застосувавши вищерозглянуті ієрархічні піднесення у степінь за модулем, тим більше, що вони пов'язані з багатокроковими протокольними процедурами. Крам того, навіть і матриці **А** та **В** і всі проміжні матриці можна підносити за додатковими простими домовленостями у якісь скалярні чи навіть матричні степені, що дуже сильно за рахунок вкладених ієрархій ускладнює задачу зловмиснику.

Експериментальна частина. На рис. 1-9 зображені результати моделювання запропонованих багатокрокових багатоступеневих протоколів узгодження секретного ключа. Зображення, що були використані для моделювання варіантів реалізації таких протоколів та для сприятливого відображення всіх проміжних дій та кроків показані на рис. 2, там же частково і результатні ключі: КА_4-R, тощо. На рис.3 показані програмні модулі-формули, що використовувались, як один з можливих без прискорень варіант піднесення матриць у матричні степені за матрицею модулів та для імітації брутальної атаки зловмисником для обчислення степені з перехопленого повідомлення. Як видно з рис.4. для більш якісного, навіть на візуальному

© Красиленко В.Г., Нікітович Д.В.

рівні закриття зображень, їх перетворення різними багатоступеневими піднесеннями у степені за модулями кращим є перший варіант, а для майже всіх варіантів бажано, щоб у матрицях були відсутні елементи зі значеннями «0» та «1», оскільки вони при перетвореннях ну будуть змінюватись. Особливу увагу треба приділяти «0», оскільки після коригувань вони стають «1». Експерименти показали, що краще генерувати відомими у пакеті інструментами псевдо-випадкові зображеннями зразу у відповідності до встановлених меж діапазону значень, проте для відображення результатів і їх кращого аналізу тут ми наводимо саме такі вибрані нами для демонстрації правильних проміжних, кінцевих результатів.

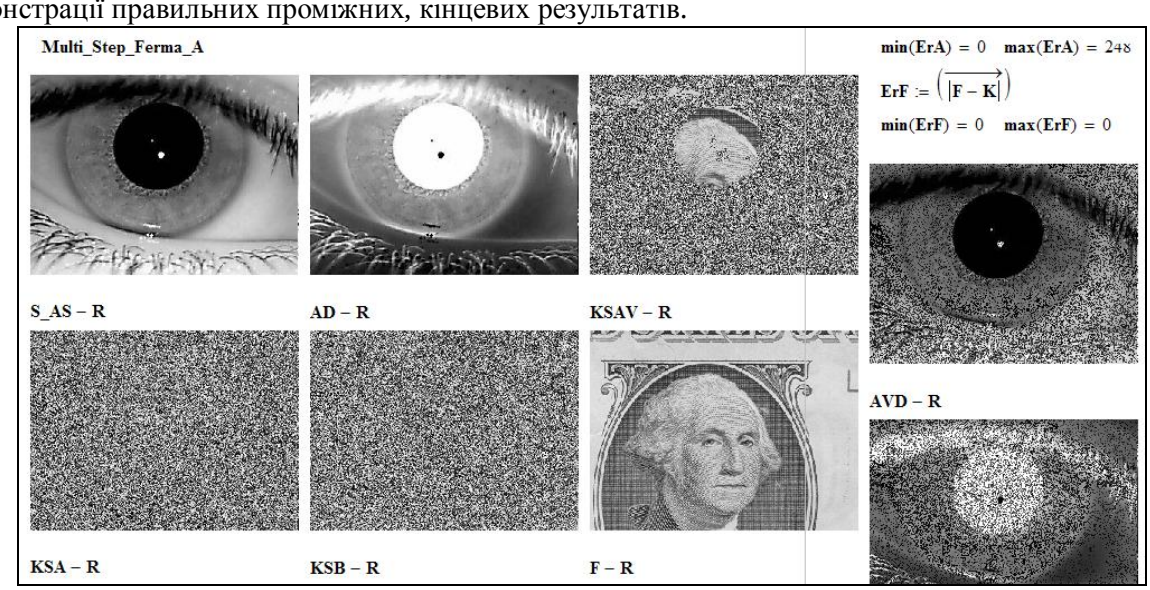
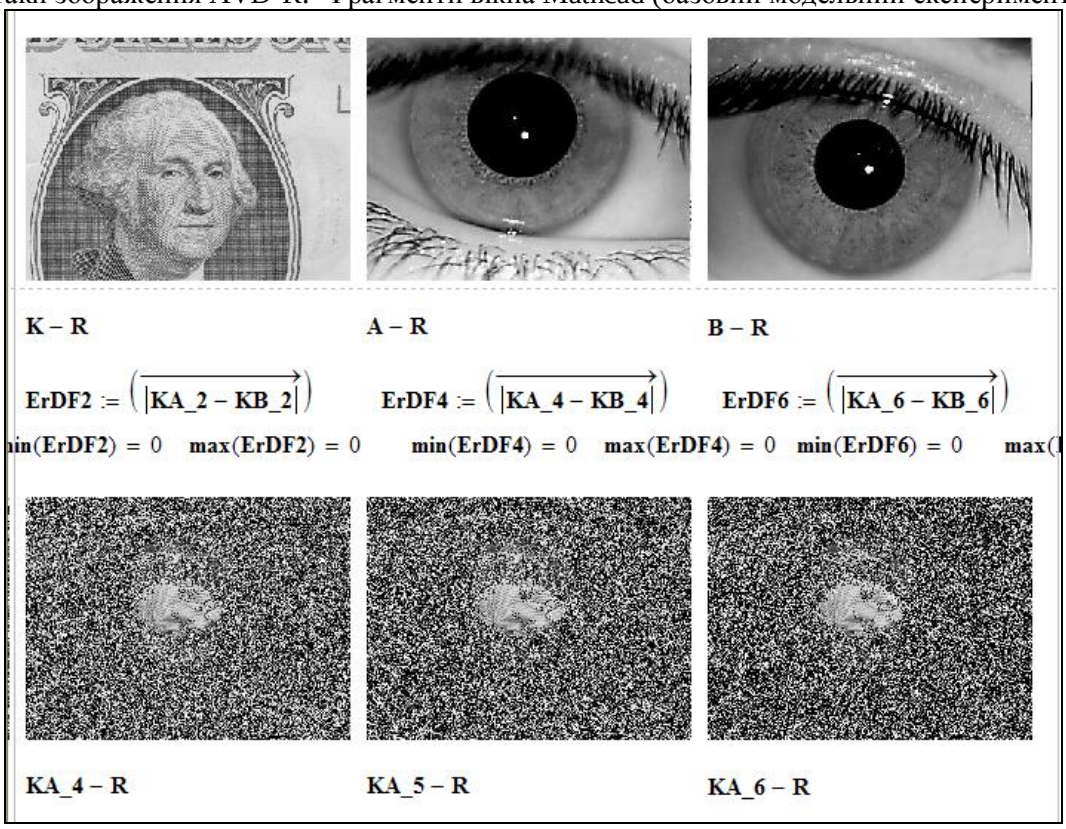


Рис.1. Вигляд вибраних для моделювання зображень S_AS-R з комплементарним до нього (негатив!) AD-R, зображень утворених шляхом матричного піднесення зображення-основи K-R у відповідні матриці-степені (S_AS-R та AD-R) матриць-зображень KSA-R та KSB-R, верифікаційного зображення F-R та розрахованого (на основі K і KSA-R) імітацією брутальної атаки зображення AVD-R. Фрагменти вікна Mathcad (базовий модельний експеримент).



© Красиленко В.Г., Нікітович Д.В.

Рис. 2. Фрагмент з Mathcad. Вигляд вибраних для моделювання багатокрокового протоколу зображень: зображення-основи K-R, довільних ідентифікаторів-зображень A-R та B-R відповідно сторони A та сторони B, утворених протоколом повідомлень та ключів (нижній ряд) у вигляді зображень та формули для перевірки рівності ключів після кожного кроку (1,2,3-го).

На рис.5 показані програмні модулі-формули з вікна Mathcad, що використовувались при моделюванні багатокрокового узагальненого протоколу узгодження секретного матричного ключа сторонами A (ліворуч) та B (праворуч) . Показані перший (1 та 2 дії обох сторін, згори вниз) та другий (3 та 4 дії обох сторін, згори вниз) кроки. Отриманими масивами KA та KB з непарними номерами сторони обмінюються, а відповідні масиви з парними номерами використовуються як основа для подальших кроків або як отриманий (отримані!) ключі. Вигляд утворених та отриманих сторонами зображень показані на рис.6. Вони свідчать про зміну ключів при переходах та різницю між переданими сторонами повідомленнями після непарних дій та рівності покрокових ключів (темні зображення!).

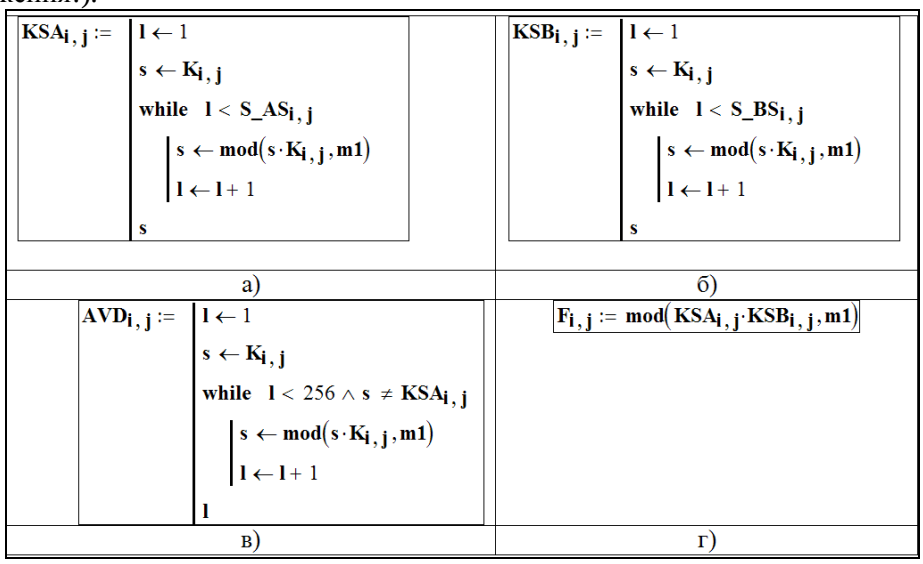


Рис. 3. Програмні модулі-формули з вікна Mathcad, що використовувались при моделюванні операцій поелементно-матричного піднесення у степінь за модулем (матриця K-основа, S_AS та S_BS – матриці-степені, m1- модуль), множення за модулем матриць та знаходження матриці-степені AVD на основі K та перехопленого повідомлення KSA.

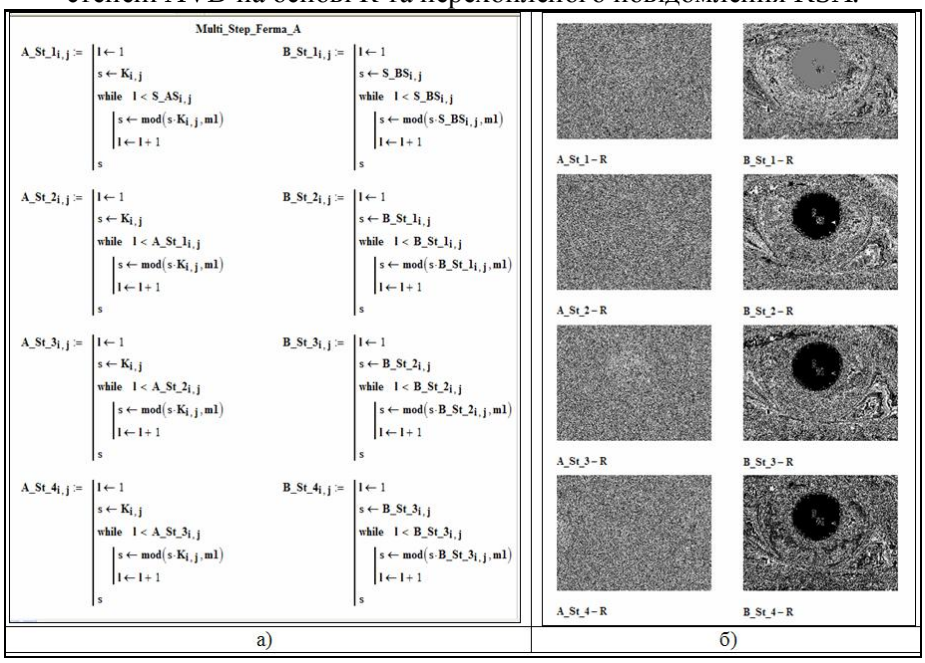


Рис.4. Програмні модулі-формули з вікна Mathcad, що використовувались при моделюванні багатокрокового поелементно-матричного піднесення у степінь за модулем: а) –варіант 1 піднесення матриці основи K у послідовно створені нові матричні степені за модулем (ліворуч!) та

© Красиленко В.Г., Нікітович Д.В.

варіант 2 піднесення степеня B_St_1(2,3,…) матриці S_BS у послідовно створені нові матричні степені за модулем (праворуч!); б)- зображення, отримані після таких піднесень (ліворуч для 1-го варіанту та праворуч для 2-го варіанту).

Отримані результати моделювання процесу узгодження секретного ключа багатокроковим протоколом свідчать, про коректність моделей та правильну роботу проколу та його модифікацій на різних кроках перетворень. Результати моделювання, що наведені на рис.7,та їх порівняння з результатами на рис.6 показують наскільки кращими є отримані ключі у випадку усунення небажаних темних («0» та «1») значень з матриць-зображень. Вони також засвічують правильність висловлених вище припущень та відповідність теоретичним положенням і правильну роботу протоколу.

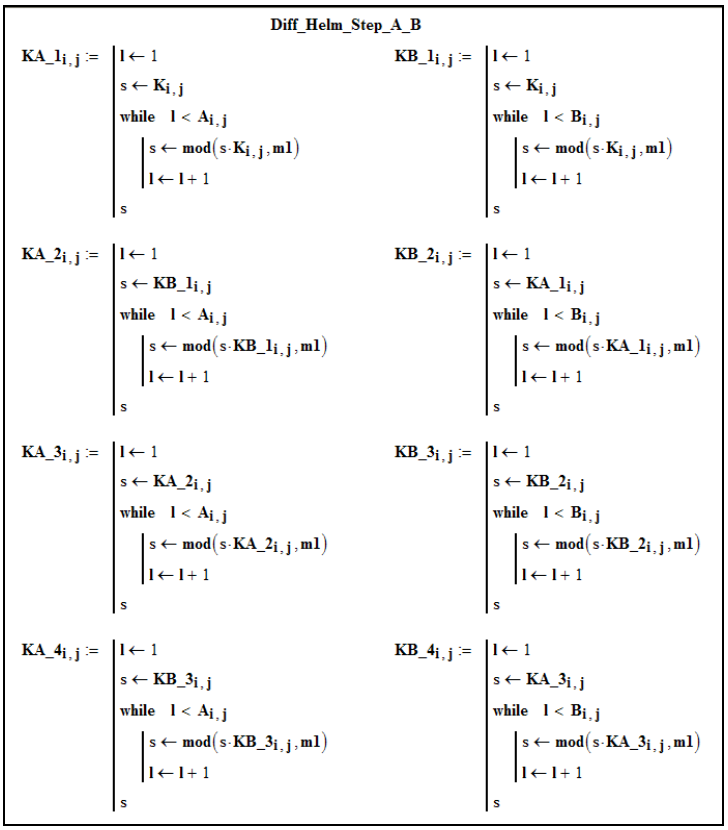


Рис.5. Програмні модулі-формули з вікна Mathcad, що використовувались при моделюванні багатокрокового узагальненого протоколу узгодження секретного матричного ключа сторонами A (ліворуч) та B (праворуч) . Показані перший (1 та 2 дії обох сторін, згори вниз) та другий (3 та 4 дії обох сторін, згори вниз) кроки. Отриманими масивами KA та KB з непарними номерами сторони обмінюються, а відповідні масиви з парними номерами використовуються як основа для подальших кроків або як отриманий (отримані!) ключі.

Програмні модулі-формули з вікна Mathcad, що використовувались при моделюванні для верифікації сторонами протокольного обміну проміжних повідомлень та створених матричних ключів на попередніх кроках багатокрокового протоколу узгодження секретного ключа для варіанту застосування попередніх, відомих сторонам, проміжних прийнятих повідомлень та ключів, показані на рис.8, а відповідні зображення-результати отримані за їх допомогою показані на рис.9. Розробленою нами раніше та наведеною у наших попередніх роботах програмою-модулем було проведено вимірювання ентропії секретних матричних ключів та проміжних матриць-зображень з метою встановлення суттєвості змін статистичних характеристик і гістограм них особливостей. Експериментами встановлено, що ентропія **K** була рівна 7,194, для A дорівнювала 7,373, для B – 7,128, а для всіх варіантів та видів степеневих перетворень ентропії проміжних та результуючих матриць-зображень мало змінювалась на всіх кроках та діях та знаходились завжди у межах від 7,73 до 7,83. Зауважимо, що протокол ніяким чином не змінюється при зміні розмірів матриць чи зображень, може бути повністю паралельним, і має підвищену стійкість за рахунок застосування ієрархічних багато-ступеневих піднесень тим паче у матричні і не лише однорідні а й неоднорідні масиви модулів. Довжина отриманих тут у експериментах ключів при переводі їх у скалярний вимір становить 320*240=76800 байтів !

© Красиленко В.Г., Нікітович Д.В.

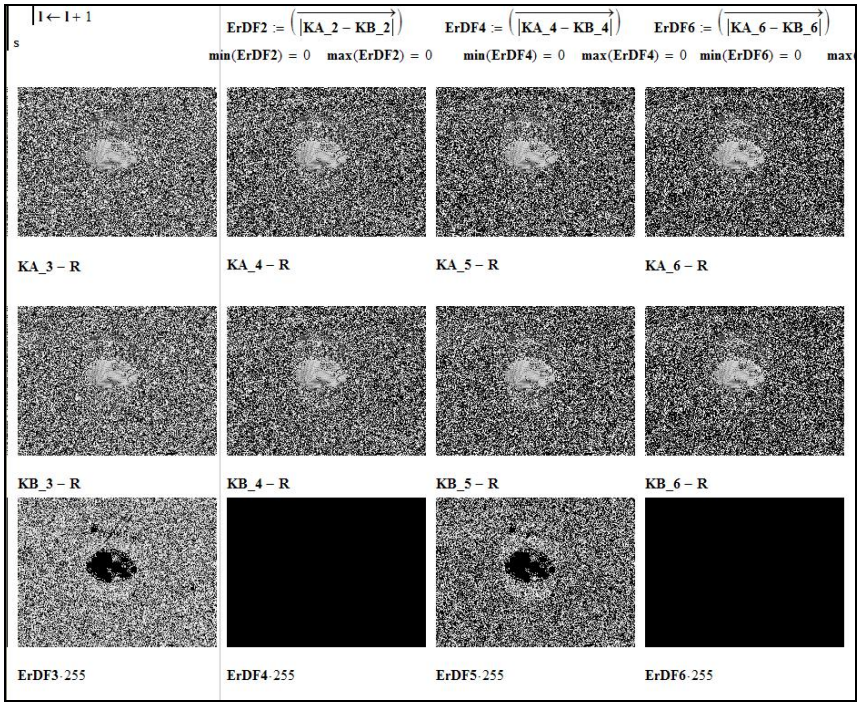


Рис.6. Вигляд утворених та отриманих сторонами зображень (переданих повідомлень KA_3M_R та KB_3M_R, KA_5M_R та KB_5M_R, відповідно після 3-ої, 5-ої дій), секретного ключа (KA_4M_R = KB_4M_R) на другому кроці (3 та 4 дії), ключа (KA_6M_R = KB_6M_R) на третьому кроці (після 5 та 6 дії) (перший та наступні після 3-ого кроки не показані!) та різницевих перевірочних зображень (нижній ряд), що свідчать про їх зміну при переходах та різницю між переданими сторонами повідомленнями після непарних дій та рівності покрокових ключів (темні зображення!). Фрагменти вікна Mathcad (модельний експеримент 1).

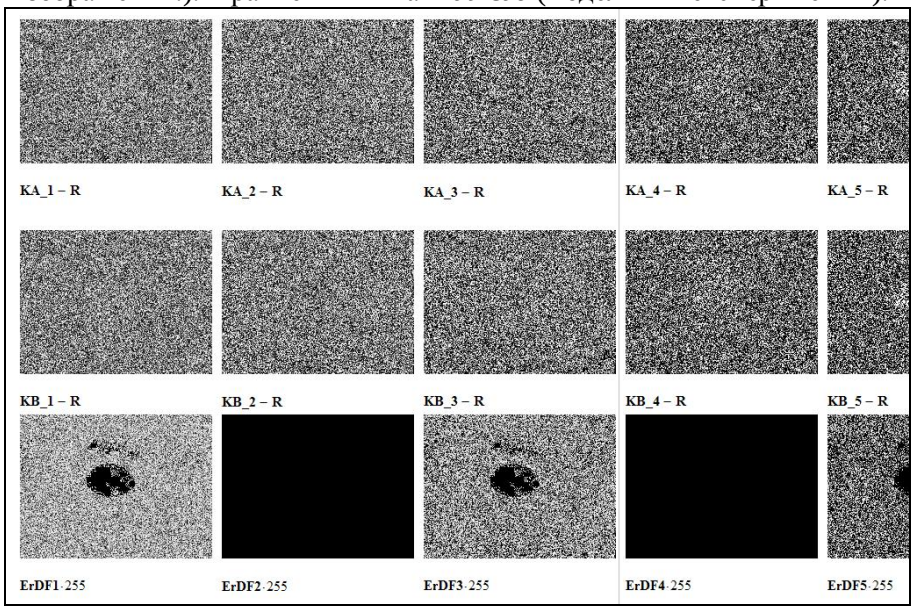


Рис.7. Вигляд утворених та отриманих сторонами зображень (переданих повідомлень KA_1M_R та KB_1M_R, KA_3M_R та KB_3M_R, KA_5M_R та KB_5M_R відповідно після 1-ої, 3-ої, 5-ої дій), секретного ключа (KA_2M_R = KB_2M_R) на першому кроці (1 та 2 дії), ключа (KA_4M_R = KB_4M_R) на другому кроці (після 3-го та наступних кроків не показані!) та різницевих перевірочних зображень (нижній ряд), що свідчать про їх зміну при переходах та різницю між переданими сторонами повідомленнями після непарних дій та рівності покрокових ключів (темні зображення!). Фрагменти вікна Mathcad (модельний експеримент 2).

© Красиленко В.Г., Нікітович Д.В.

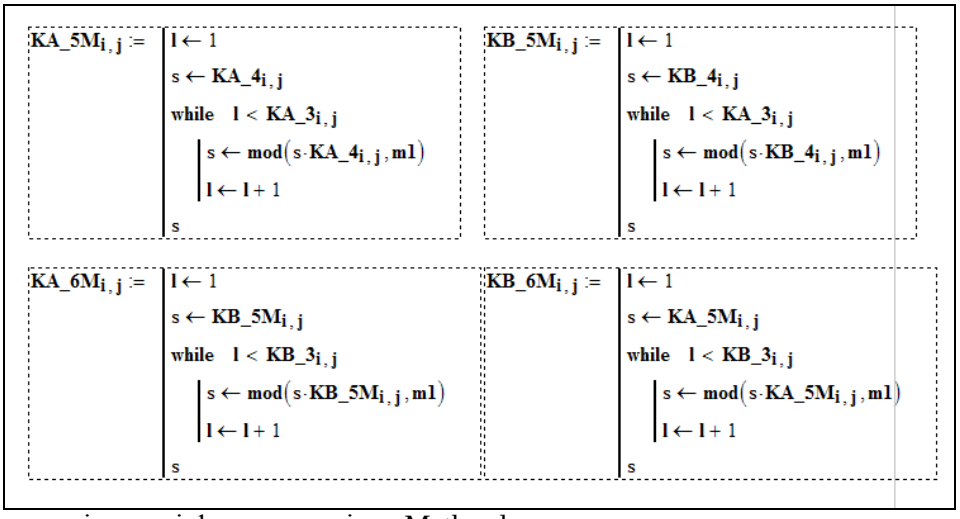


Рис.8. Програмні модулі-формули з вікна Mathcad, що використовувались при моделюванні для верифікації сторонами протокольного обміну проміжних повідомлень та створених матричних ключів на попередніх кроках багатокрокового протоколу узгодження секретного ключа. Показано режим верифікації після першої та другої дії на третьому кроці.

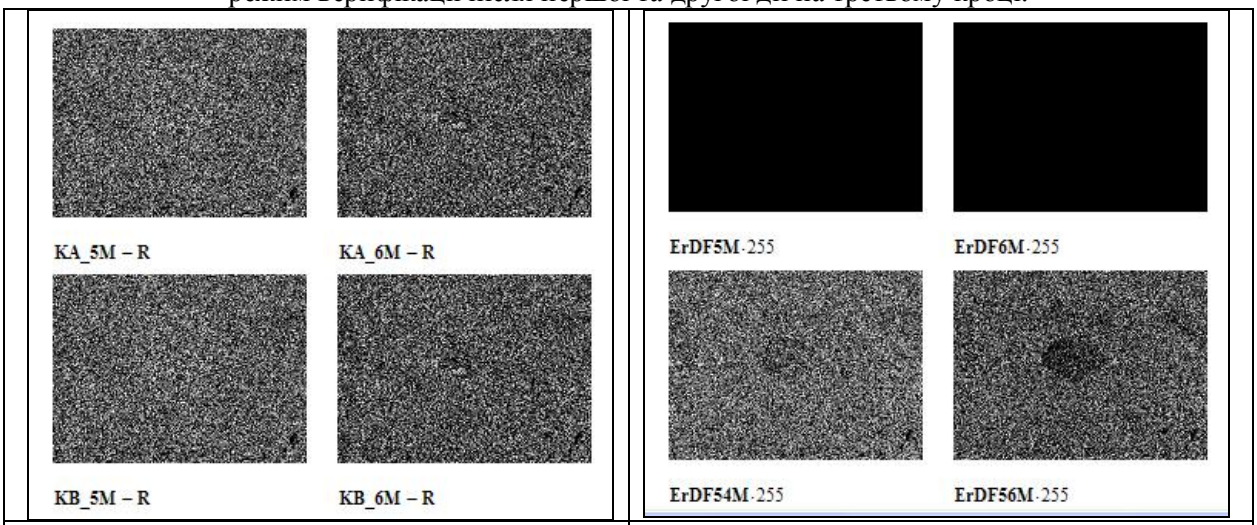


Рис.9. Вигляд утворених та отриманих сторонами зображень (верифікаційних KA_5M_R та KB_5M_R повідомлень), секретного ключа (KA_6M_R = KB_6M_R) на третьому кроці – а) та різницевих перевірочних зображень –б), що свідчать про їх зміну при переходах від 4-ої до 5-ої дії , від 5-ої до 6-ої дії (внизу праворуч) та про рівність зображень, утворених сторонами після 5-ої та 6-ої дій (вгорі праворуч).

Висновки Обґрунтовані необхідність та переваги створення, узгодження та застосування матричних ключів для покращених криптографічних систем матричного типу і процедур зашифрування-розшифрування зображень. Запропоновані багатокрокові та багатоступеневі протоколи узгодження ключа з метою їх вдосконалення та підвищення стійкості до атак. Для підтвердження достовірності запропонованих удосконалень виконано ряд модельних експериментів у середовищі Mathcad Professional. Показані переваги багатокрокових протоколів узгодження ключа за рахунок використання в них багатоступеневих поелементно-матричних піднесень у степінь за модулем та конвеєрних процедур. Моделі та процедури враховують специфіку зображень і легко адаптуються до паралельних реалізацій та новітніх апаратних матричних процесорів. Наведено результати моделювання процесів створення секретних матричних ключів у вигляді зображень великої розмірності (320 * 240) на основі запропонованих протоколів. Довжина отриманих тут у експериментах ключів при переводі їх у скалярний вимір становить 320*240=76800 байтів !

1. Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.

© Красиленко В.Г., Нікітович Д.В.

2. Коркішко Т. Алгоритми та процесори симетричного блокового шифрування / Т. Коркішко, А. Мельник, В. Мельник. – Львів: БаК, 2003. – 168 с.
3. Красиленко В.Г. Алгоритми та архітектури для високоточних матрично-матричних перемножувачів на основі оптичної чотирьохзначної знакозмінної арифметики / В.Г. Красиленко // Вимірювальна та обчислювальна техніка в технологічних процесах. - 2004. - №1.- С. 13-26.
4. Красиленко В.Г. Розробка методу криптографічного захисту інформації тексто-графічного типу / В.Г. Красиленко, С.А. Свіренюк // Наука і навчальний процес: науково-методичний збірник НПК. – Вінниця, 2006. – С. 73-74.
5. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісник НУ «Львівська політехніка» «Комп'ютерні системи та мережі». - № 658. – С. 59-63.
6. Красиленко В.Г. Моделювання матричних афінних алгоритмів для шифрування кольорових зображень / В.Г. Красиленко, К. Огородник, Ю. Флавицька // Комп'ютерні технології: наука і освіта. Тези доповідей V Всеукр. наук.–пр. конф. – Київ, 2010. – С. 120-124.
7. Красиленко В.Г., Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97**). –** С. 60 – 63.
8. Красиленко В.Г. Матричні афінно-перестановочні шифри для шифрування та дешифрування зображень / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. - Х.: ХУПС, 2012. – Вип. 3 (101).-т. 2. **–** С. 53-62.
9. Красиленко В.Г. Матричні моделі криптографічних перетворень зображень з матрично-бітово-зрізовою декомпозицією і перемішуванням та їх моделювання / В. Г. Красиленко, Д.В. Нікітович //Матеріали 68 НТК «Сучасні інформаційні системи і технології. Інформаційна безпека», ч. 3, секції 3-4. – Одеса, ОНАЗ ім.. О.С.Попова, 2013. – С.139-143.
10. 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.
11. Красиленко В.Г. Моделювання модифікованих матричних моделей криптографічних перетворень зображень з верифікацією цілісності криптограм / В.Г. Красиленко, Д.В. Нікітович // Матеріали II міжнародної науково-практичної Інтернет-конференції «Інформаційні технології: теорія, інновації, практика». – Полтава: ПолтНТУ, 2015. – С. 86-89.
12, Красиленко В.Г. Моделювання криптографічних перетворень зображень на основі їх матрично-бітовозрізової декомпозиції та матричних моделей перестановок з верифікацією цілісності / В.Г. Красиленко, Д.В. Нікітович // Всеукраїнська науково-практична конференція молодих вчених та студентів «Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем» (MEICS-2015). – Дніпропетровськ: Дніпропетровський національний університет ім. Олеся Гончара, 2015. - С. 32-34.
13. 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. наук.-пр. конф. – К., 2010. – С.120-124.
14. Красиленко В.Г. Моделювання модифікованого алгоритму створення 2-D ключа в криптографічних застосуваннях / В.Г. Красиленко, О.І. Нікольський, О.О. Лазарєв // Науково-методичний збірник НПК «Наука і навчальний процес». – Вінниця, 2008. – С. 107-109.
15. 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.
16. Красиленко В. Г. Модифікації системи RSA для створення на її основі матричних моделей та алгоритмів для зашифрування та розшифрування зображень / В. Г. Красиленко, С. К. Грабовляк // Системи обробки інформації. - Х.: ХУПС, 2012. - Вип. 8. - С. 102-106.
17. 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: збірник наукових праць. – Львів: Львівський національний університет імені Івана Франка, 2015. – Вип. 6. – С 111-127. – Режим доступу: http://elit.lnu.edu.ua/pdf/6_12.pdf
18. 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 : наук. журн. – Луцьк: Видавництво Луц. нац. техн. ун-т., - 2016. - № 23. - С. 31-36. – Режим доступу: http://ki.lutsk-ntu.com.ua/node/132/section/9
19. Красиленко В.Г. Моделювання криптографічних перетворень кольорових зображень з верифікацією цілісності криптограм на основі матричних моделей перестановок / В.Г. Красиленко, Д.В. Нікітович// Матеріали науково-практичної інтернет-конференції «Проблеми моделювання та розроблення інформаційних систем». – Дрогобич : ДДПУ ім. І. Франка, 2016. – С. 128-136. Режим доступу: http://ddpu.drohobych.net/wp-content/uploads/2016/04/material_konf.pdf37
20. Красиленко В.Г. / В.Г. Красиленко, Д.В. Нікітович Моделювання матричних афінних шифрів для криптографічних перетворень зображень // Інформатика та системні науки (ІСН-2017): матеріали VIII Всеукраїнської науково-практичної конференції за міжнародною участю, (м. Полтава, 16–18 березня 2017 року) / за ред. О.О.Ємця – Полтава: ПУЕТ, 2017. – Режим доступу: http://dspace.puet.edu.ua/handle/123456789/5558
21. Krasilenko V.G. A noise-immune cryptographic infor-mation protection method for facsimile information transmission and the realization algorithms [Text] / V.G. Krasilenko, V.F. Bardachenko, A.I. Nikolsky, et. al., // Proc.SPIE, 2006. - Vol. 6241. – P. 316-322.

© Красиленко В.Г., Нікітович Д.В.