УДК 004.3

В.Г. Красиленко, Д.В. Нікітович

Вінницький соціально-економічний інститут Університету «Україна», Вінниця

МОДЕЛЮВАННЯ ПРОТОКОЛІВ УЗГОДЖЕННЯ СЕКРЕТНОГО МАТРИЧНОГО КЛЮЧА ДЛЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ТА СИСТЕМ МАТРИЧНОГО ТИПУ

Стаття присвячена моделюванню протоколів узгодження секретного матричного ключа для криптографічних перетворень у системах та моделях матричного типу. Підґрунтям таких протоколів є узагальнення відомих протоколів Діффі-Хелмана та інших на матричний випадок і відповідні математичні процедури-алгоритми на основі матричних моделей для формування двовимірних ключів. Обґрунтована необхідність та переваги створення, узгодження та застосування матричних ключів для покращених криптографічних систем матричного типу та процедур зашифрування-розшифрування зображень. Запропоновано нові модифікації матричних узгоджувальних протоколів з метою вдосконалення їх стійкості до атак. Для підтвердження достовірності запропонованих протоколів і їх модифікацій та порівняння їх характеристик, складності обчислювальних процедур виконана низка модельних експериментів у програмному середовищі Mathcad Professional. Показані переваги швидких обчислень при поелементно-матричному піднесенні до степеня за модулем на основі матричних АЦ-перетворень та використання фіксованих вагових матричних степенів за модулем і бінарних розрядних матриць для керованого вибору зважених компонентів. Обчислювальні процедури і матричні моделі враховують специфіку зображень і легко адаптуються до паралельних реалізацій та найновітніших апаратних матричних процесорів. Наведені результати моделювання процесів створення секретних матричних ключів-зображень великої розмірності запропонованими модифікаціями протоколів.

Ключові слова: *криптографічні перетворення зображень, матричний алгоритм Діффі-Хелмана, матричні моделі, секретний матричний ключ, розшифрування, протокол узгодження спільного ключа.*

Вступ

Необхідність вирішення проблем інформаційної безпеки та захисту інформації державного, військового, комерційного, приватного та іншого конфіденційного змісту, особливо в епоху інформаційного суспільства та масових комунікацій, спричинили до бурхливого розвитку та появи великої кількості різних методів та засобів захисту інформації, серед яких важливе місце займають криптографічні та стеганографічні системи. Якими б складними та надійними не були б криптографічні системи, одним з ключових питань застосування криптографії на практиці є адміністрування ключами, включаючи процеси генерування ключів та їх узгодження електронним шляхом. Від надійності, криптостійкості процесів створення спільних для обох сторін безпечних ключів залежить рівень безпеки. В симетричних системах і в деяких асиметричних користувачам необхідно перед обміном інформацією формувати спільний безпечний ключ, так званий головний, з якого за необхідності створюються сесійний та низка похідних підключів, наприклад циклових, тощо. Відомі протоколи та алгоритми створення двома сторонами спільного безпечного таємного ключа при використанні навіть незахищених каналів зв'язку, наприклад алгоритми Діффі-Хелмана, MTI, STS та інші [1; 2]. Але більшість відомих криптосистем при великих об'ємах даних зорієнтовані на послідовну криптографічну обробку сукупності виділених інформаційних блоків за допомогою одного і того ж самого ключа або підключа, що є суто скаляром, незважаючи на його довжину. Це призводить до недоліків таких алгоритмів послідовної обробки, усунення яких вимагає збільшення довжин ключів і діапазонів чисел (модулів), які необхідно опрацьовувати, що позначається не лише на збільшенні вимірності скінченних полів а й негативно на обчислювальній продуктивності, що в свою чергу призводить до пошуку нових операцій та методів їх прискорення, ускладнює процедури визначення, верифікації базових параметрів криптосистем та генерування та зберігання ключів, наприклад, масиву строго закріплених за абонентами відкритих (таємних!) неповторних ключів у RSA системі. В той же час епоха електронних комунікацій характеризується суттєвим зростанням необхідності опрацьовувати та передавати специфічні текстово-графічні документи (ТГД) у вигляді цифрових, табличних даних, малюнків, графіків, діаграм, підписів, віз, резолюцій, тощо, і є по суті 2-D масивами (зображеннями) значної розмірності. Крім того, за останнє десятиріччя суттєво збільшується доля нових задач, в яких криптографічні перетворення (КП) необхідно виконувати над багатовимірними сигналами, серед яких особливе місце займають представлені в різних

форматах чорно-білі, кольорові, багато-спектральні зображення різних фізичних об'єктів, а це потребує створення для таких задач не лише відповідних матричних моделей, алгоритмів криптографічних перетворень, але й однорідних до їх структури секретних 2D (3D, 4D) вимірних ключів у вигляді по суті зображень чи матриць, тензорів [3–10].

Огляд публікацій. Поява паралельних алгоритмів та засобів, особливо спеціалізованих багатопроцесорних, багатоядерних, матричних лінійно-алгебраїчних та матричного (картинного типу) процесорів [4; 5] сприяла переорієнтації при дослідженні КП зображень на ці нові засоби та створенню і відповідних моделей матричного типу (МТ) [6–10]. Серед значної кількості робіт в області криптографії, які тут з урахуванням обмежень ми не наводимо, лише незначна їх частина присвячена саме методам та алгоритмам орієнтованим на матричні моделі (ММ) та матричні спеціалізовані алгоритми і засоби [6–18]. Результати цих досліджень показали, що матричні афінні [6; 7] та матричні афінно-перестановочні алгоритми [8] мають суттєві переваги у порівнянні з традиційними, по суті скалярними, афінними асиметричними шифрами та можуть бути застосовані для створення цифрових сліпих підписів [9]. Було показано, що для реалізації таких матричних, більш загальних, моделей та алгоритмів КП зображень необхідно мати один або декілька ключів, представлених також у вигляді 2-D масиву чи зображення. За декілька останніх років спостерігається суттєве зростання долі робіт, що присвячені шифруванню та розшифруванню різноманітних кольорових багато-спектральних зображень [3; 6–8, 13–18], що теж підтверджує актуальність не лише пошуку, дослідження та удосконалення ММ КП, існуючих матричних шифрів та засобів для їх реалізації, але й ставить, як показує аналіз цих робіт, на порядок денний гостру проблему створення для таких ММ і відповідних матричних ключів (МК). Відмітимо і той факт, що для вищезгаданих робіт, наприклад, для матрично-афінно-перестановочних алгоритмів [8] необхідно мати два види МК: набір бінарних матриць перестановок, позначимо тут їх як МК_П, 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 МК_П та їх формувань, застосувань для ММ КП розглядались в [8; 10; 15–17], 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. А стосовно МК_З відмітимо, що в роботі [11] була запропонована модифікація алгоритму Діффі-Хелмана на матричний випадок для створення 2-D ключа, а в [12] були розглянуті алгоритми формування двовимірних ключів для матричних алгоритмів криптографічних перетворень зображень та виконане їх часткове моделювання. Але в цих роботах не було проведено достатньої кількості модельних експериментів, не зроблено оцінок можливих характеристик складності та часу виконання обчислювальних процедур для МК_З зі збільшеною розмірністю, не досліджені гістограмно-ентропійні показники якості ключів, не показані шляхи усунення відомих недоліків алгоритму Діффі-Хелмана. Проте була висловлена та частково експериментально показана в [12] ідея узагальнення і на матричний випадок застосування одного з покращених підходів до організації обчислень на основі матричної паралельної логіки.

Постановка задачі. Тому метою даної роботи є подальше використання та удосконалення запропонованих протоколів узгодження секретного матричного ключа для криптографічних перетворень у системах та моделях матричного типу, алгоритмів формування двовимірних ключів типу МК_З для ММ криптографічних перетворень зображень, їх моделювання та експериментальні дослідження.

Основна частина

Теоретичні основи. Розглянемо алгоритм створення 2-D ключа на основі узагальнення та модифікації [12] на матричний випадок алгоритму Діффі-Хелмана. Нехай двом абонентам відоме число m1, наприклад, просте число 257, що є як відомо з наших попередніх робіт дуже зручним для роботи з байтами, і 2-D масив **OSN**, що являє собою довільно вибране зображення чи згенероване відомими методами та засобами випадкове зображення відповідної розмірності $I \times J$. Використовувати в якості 2-D масивів можна чорно-білі зображення такої ж розмірності, чи одну з основних кольорових складових R,G,B кольорового зображення. Така інформація може бути і часто є відкритою та відома користувачам. Проте зауважимо, що нами у процесі моделювань було встановлено можливість у деяких випадках розв'язання задачі обчислення дискретного логарифма за модулем при роботі з матрицями чисел невеликої розрядності. Тому ми пропонуємо масив **OSN**, що буде основою базових модульних операцій, тримати сторонам у секреті, як один з варіантів усунення цього недоліку. Один з низки попередньо використаних ключів МК_З чи його фрагмент по домовленості сторін перед початком сеансу виконання протоколу теж може бути використаний в якості **OSN,** незнання якого унеможливлює атаку третьої сторони. Бажано також усунути з цього масиву нульові компоненти та навіть і одиничні, що також усуває деякі колізії, шляхом його коригування довільним відомим способом [14] чи додаванням-відніманням до неї фіксованої матриці. В результаті

отримаємо скориговану матрицю **OB**. Протокол виконується наступним чином. Одна з сторін, наприклад абонент X (Alisa!), вибирає з набору множини зображень чи генерує випадкове зображення-матрицю Pic_Fp_1, шляхом додавання до неї матриці **R** зміщує її значення елементів у діапазон 1-256 отримуючи скореговану матрицю **A** та обчислює 2-D масив **KAR** за формулою $\mathbf{KAR} \equiv \mathbf{OB}^{\mathbf{A}} \bmod(m1 \cdot \mathbf{R})$, де **R –** матриця всі елементи якої дорівнюють одиниці, матриці **A**, **OB**, **R** та **KAR** мають одну розмірність $I \times J$, а операція піднесення в степінь за модулем m1 є по-елементною, тобто $\mathbf{KAR}_{i,j} \equiv \mathbf{OB}_{i,j}^{\mathbf{A}i,j} \bmod m1$. Цей масив-матрицю він шляхом віднімання від неї матриці **R** коригує у стандартного формату зображення-матрицю (**KAR-R)** та відправляє другому абоненту Y (Bob!). Другий абонент Y аналогічним чином бере інше зображення-матрицю Pic_Fp_2, коригує його у інший випадковий 2-D масив-матрицю **B**, обчислює значення масиву **KBR** за формулою $\mathbf{KBR} \equiv \mathbf{OB}^{\mathbf{B}} \bmod(m1 \cdot \mathbf{R})$ та відправляє аналогічним чином скориговане відповідне йому зображення (**KBR-R)** першому абоненту X. Перший абонент X, отримавши це зображення коригує його у матрицю **KBR** додаванням **R** та використовуючи знову ж таки лише йому відому матрицю **A,** обчислює значення матричного ключа $\mathbf{KXYA} \equiv \mathbf{KBR}^{\mathbf{A}} \bmod(m1 \cdot \mathbf{R})$. Аналогічними діями другий абонент Y - значення матричного ключа $\mathbf{KYXB} \equiv \mathbf{KAR}^{\mathbf{B}} \bmod(m1 \cdot \mathbf{R})$. Таким чином абоненти одержать таємний ключ $\mathbf{KEY} \equiv \mathbf{OB}^{\mathbf{B} \cdot \mathbf{A}} \bmod(m1 \cdot \mathbf{R})$, однаковий для обох сторін і використовувати який можуть для зашифрування та розшифрування при передачі 2-D даних, зображень, тощо. Такі ключі бажано використовувати для матричних моделей симетричних, асиметричних та симетрично-асиметричних криптосистем [6–9, 14–18]. У таких ММ протоколу всі матриці мають однаковий формат.

Наведений протокол взаємно безпечний, оскільки зловмисник для обчислення ключа повинен розв'язати задачу обчислення дискретного логарифма за модулем фактично для кожного елемента 2-D масиву. Відомо, що не існує жодного ефективного алгоритму її розв'язування, а розширення і ускладнення задачі на матричний випадок робить її розв'язування ще більш складнішим. Якщо ж матриця **OB** є невідомою для третьої сторони, як ми зазначали вище, то тоді цей протокол унеможливлює атаку «людина всередині». Запропонований алгоритм формування матричних ключів можна удосконалити у напрямі його стійкості до прямих атак, узагальнивши відомі протоколи STS чи MTI на матричний випадок. Ще одна наша нова пропозиція по удосконаленню цього протоколу полягає у зашифруванні відомим лише двом сторонам ключем матриці **OB**, якщо вона є публічною. Це призводить фактично до оновлення протоколом старого ключа, його заміна новим, бо всі вони мають ті ж розміри, формати, параметри. В якості ключа, яким можна закривати не лише матрицю-основу **OB**, але й матриці-степені **A** та **B**, можуть бути використані спеціальні характерні лише для кожної сторони зображення, що є по суті ідентифікаторами і сторін і часу здійснення протоколу.

На відміну від роботи [12], у якій всі формули для реалізації протоколу були скалярними для кожного i,j-го елемента матриць, тут ми використали і наводимо повністю з урахуванням наявних у Mathcad методів векторизації лише формули у матричному вигляді. Для прискореного піднесення у степінь за модулем у відповідності до вищенаведених базових формул, ми пропонуємо формувати з матриці-основи набір матриць компонентів, що є кратними степеням двійки фіксованими степенями за модулем, а для їх вибору та включення (виключення) у кінцеву операцію множення вибраних компонентів використовувати бітові матричні зрізи-розряди матриць, що будуть степенями. Таким чином матриці-степені **A** та **B** необхідно за допомогою ММ АЦП, а відповідні їм апаратні реалізації паралельних АЦП матричного типу відомі, перетворити у відповідні набори бітових матриць.

Експериментальна частина. Для такого варіанту організації обчислювальних процесів абоненти X та Y вибирають зображення, що показані на рис. 1, за допомогою розробленої програми автоматично виконуються згідно з наведеними на рис. 2–3 формулами формування з **OB** компонентів а з відповідних матриць **A**, **B** на першому кроці, чи **KAR**, **KBR** на другому, необхідних наборів бінарних бітових матриць, що показані на рис. 4.

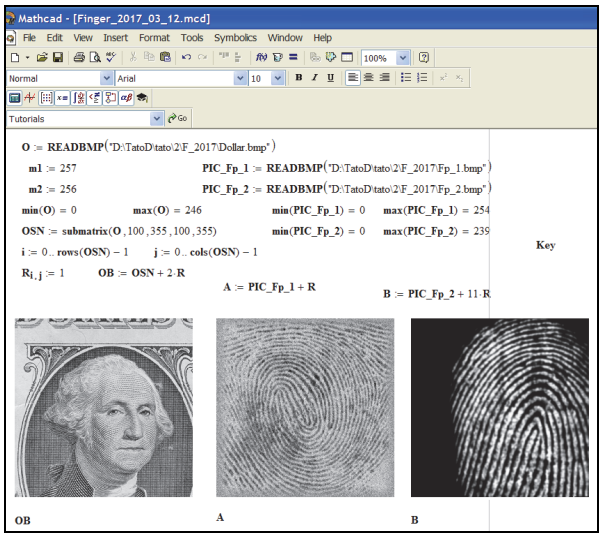

Рис. 1. Фрагмент вікна Mathcad з формулами введення та відображення трьох зображень (256*256), що були використані для моделювання

Використовуючи сукупність отриманих проміжних масивів-компонентів **OSN0-OSN7**, які відповідають піднесеним у степінь 1, 2, 4, 8 і т.п., маси-

вам **OB** за модулем m1, та бітові матриці BP0-BP7 абонент X обчислює значення **KAR** у відповідності до повністю матричних формул (рис. 5).

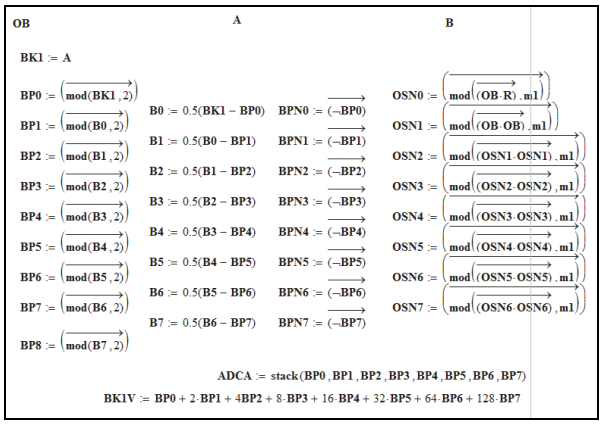

Рис. 2. Фрагмент вікна Mathcad з формулами для АЦ-перетворення зображення A (Alisa!) у набір ADCA з восьми бітових матриць-зрізів BP0-BP7 та формування вагових компонентів **OSN0-OSN7** за модулем основи **OB** при моделюванні

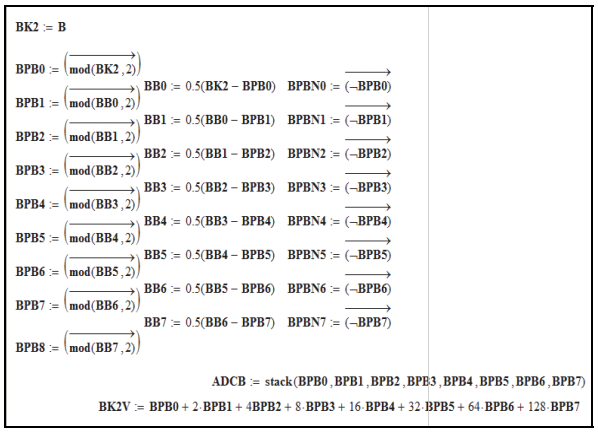

Рис. 3. Фрагмент вікна Mathcad з формулами, що були використані для АЦ-перетворення зображення **B** (Bob!) у набір ADCB з восьми бітових матриць-зрізів BPB0-BPB7 для моделювання

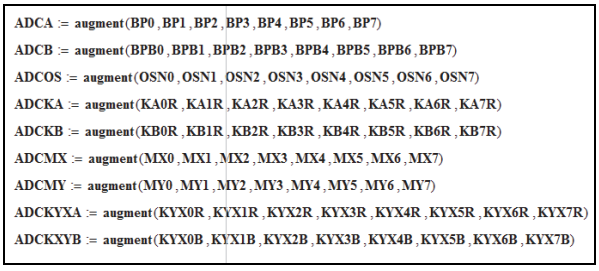

Рис. 4. Фрагмент вікна Mathcad з формулами, що були використані для формування відповідних наборів бітових матриць-зрізів після АЦ-перетворень та наборів чорно-білих компонентів-степенів для їх обробки та візуалізації

Якщо i,j-й елемент бітового зрізу дорівнює «1», то відповідний елемент чорно-білої компоненти-степеня включається, якщо ж він дорівнює «0», то відповідний елемент чорно-білої компоненти-степеня встановлюється рівним «1». Цей масив у скоригованому вигляді отримує Y.

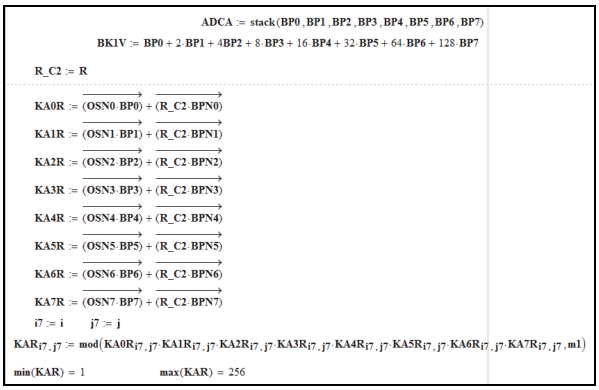

Рис. 5. Фрагмент вікна Mathcad з формулами, що були використані для формування компонент та результуючої матриці, що є піднесеною степінню за модулем (обчислення **KAR**)

Аналогічним чином, використовуючи проміжні масиви-компоненти **OSN0-OSN7** та відповідні бінарні матриці BPB0-BPB7 (бінарні зрізи матриці **B**), абонент Y обчислює значення матриці **KBR** у відповідності до формул, що на рис. 6 для відправки абоненту **X.**

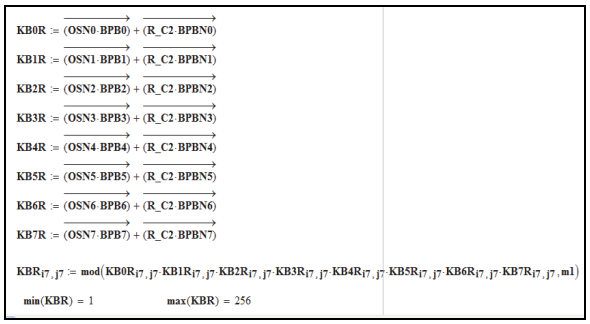

Рис. 6. Фрагмент вікна Mathcad (обчислення **KBR**)

Подальші дії сторін у протоколі можуть бути описані на основі використання аналогічних підходів і декомпозицій за допомогою використаних у Mathcad MM і наведених на рис. 7.

Результати моделювання розробленого алгоритму в програмному середовищі Mathcad на основі вищенаведених формул показані на рис. 8–10, де у кожному рядку об'єднано по 8 матриць зображень розмірністю 256×256 елементів. Ці всі проміжні результати підтверджують адекватність.

Після коригування отриманих матриць програмою, що є у кожної сторони, отримані ключі можуть бути збережені сторонами як зображення у тих же форматах, у яких були всі початкові зображення, а потім використані для сесійного криптографічного перетворення або для наступних аналогічних генерувань нових ключів. Отримані в результаті виконання протоколу та його моделювання ключі показані на рис. 11.

Для цього модельного експерименту ми спеціально вибирали деякі специфічні зображення, а не брали чи генерували як випадкові, для того, щоб краще продемонструвати всі деталі та аспекти процесів узгодження секретного спільного ключа і в той же час показати можливості протоколу працювати з індивідуальними ідентифікаторами.

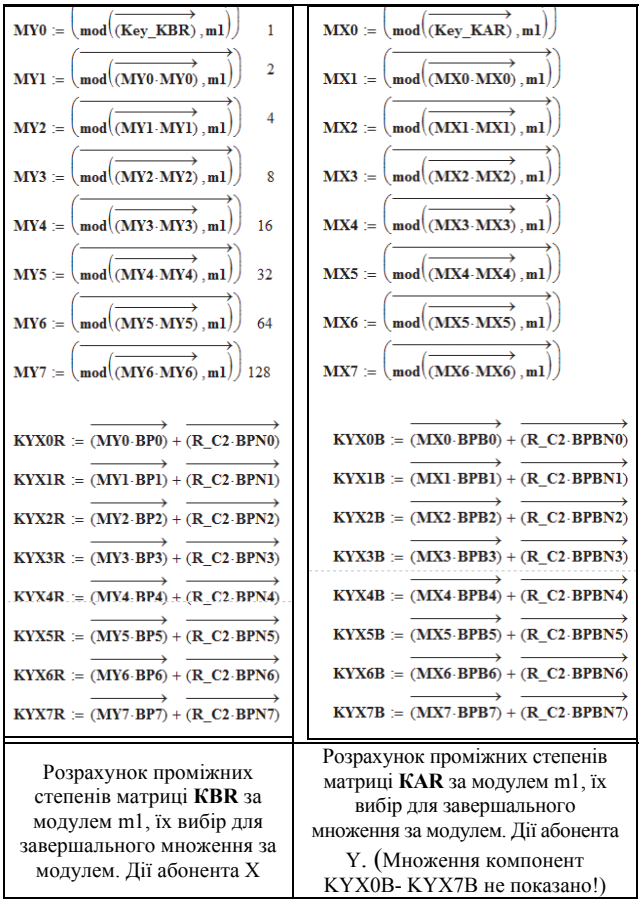

Рис. 7. Фрагмент вікна Mathcad (другий крок), процес формування ключа абонентом X з отриманого масиву **KBR** та формування ключа абонентом Y з отриманого масиву **KAR**

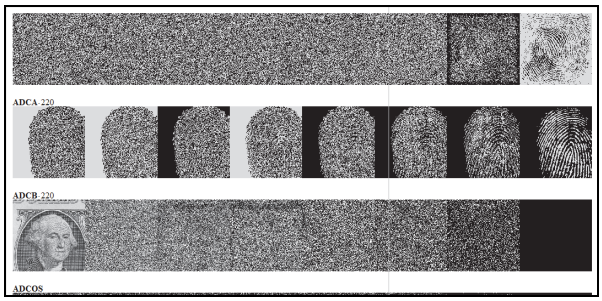

Рис. 8. Зображення сукупностей **ADCA**, **ADCB** (одно-бітові) бітових зрізів відповідно матриць **A**, **B**, та сукупності **ADCOS** проміжних степенів **OSN0-OSN7** (1-а, тобто **OB,** 2-а і т.д., чорно-білі!) за модулем m1 основи **OB**

Останні можуть бути легко зчитані камерами перед початком протоколу прямо з зовнішньої сцени, а ще краще, якщо у цій сцені будуть відображені час (з годинника, телевізора, тощо) чи інші ознаки.

Другий наш модельний експеримент, результати якого показані на рис. 12, підтвердив вище висловлену нами гіпотезу, про необхідність усунення чи коригування з основи чи степеневих зображень значень елементів з нульовими, одиничними значеннями, бо тоді і у результуючих ключах будуть видимими ці області, що є небажаним. Крім того, при використанні у цьому експерименті в якості основи матриці з рівними значеннями всіх елементів ми демонструємо переваги застосування як основ спеціально згенерованих псевдо-випадкових, (навіть цим самим нашим протоколом!), зображень, що мають якнайвищі значення ентропії.

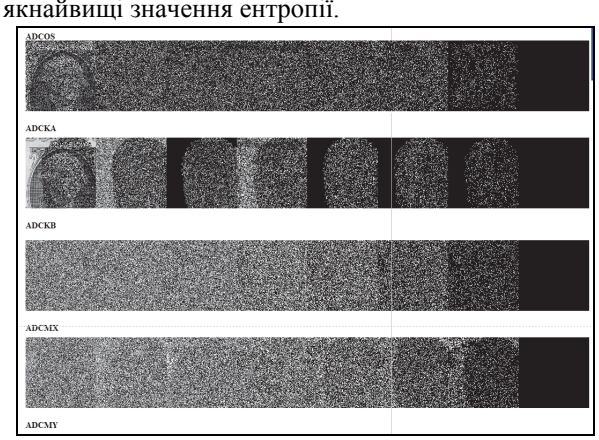

Рис. 9. Зображення сукупностей **ADCKA**, **ADCKB**, **ADCMX**, **ADCMY** (чорно-білі!) проміжних степенів **KA0R-KA7R** (1-а, 2-а і т.д., чорно-білі!) за модулем m1 для обчислення **KAR** (перший ряд), аналогічні для обчислення **KBR** (2-ий ряд), степенів MY0-MY7 матриці **KBR** для обчислення ключа стороною X (3-ій ряд) та степенів MX0-MX7 матриці **KAR** для обчислення ключа стороною Y (4-ий ряд)

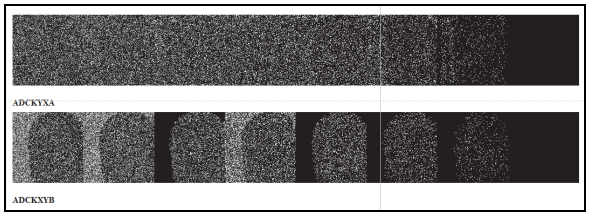

Рис. 10. Матриці ADCKYXA (X-Alisa) ADCKXYB (Y-Bob) як набори проміжних, вибраних біт-картами, матриць **KXY0R-KXY7R** та **KYX0B-KYX7B** (чорно-білі!), що були отримані та використовувались для кінцевого (шляхом їх множення за модулем) обчислення абонентами своїх (спільного!) ключів: Key_XY_A та Key_YX_B (після коригування матрицею **R**)

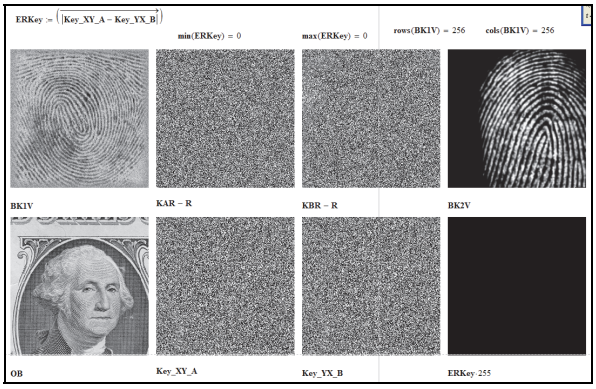

Рис. 11. Вікно Mathcad з показаними вхідними для сторін зображеннями (відбитки пальців), спільним зображенням основою **OB**, отриманими проміжними на першому кроці та результуючими для обох сторін зображеннями-ключами (друге та третє у нижньому ряду) та різницевим, що свідчить про однаковість ключів

Використовуючи програмно-математичний модуль нами було визначено та порівняно ентропії

отриманих ключів у першому (7,98 біт на елемент) та другому експериментах (на 15-25 % менше). Як показують ці та їм аналогічні дослідження з наших робіт [15–18], що були виконані на більш значних вибірках, ентропійні та гістограмні показники, отриманих запропонованими ММ та алгоритмами, ключів чи шифрограм є відповідними до вимог.

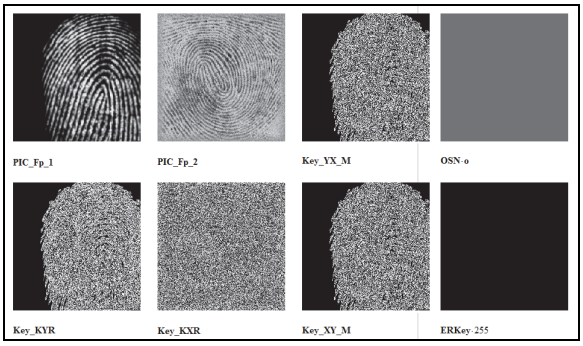

Рис. 12. Вікно з показаними вхідними зображеннями, спільним зображенням основою **OSN**, проміжними та результуючими для обох сторін зображеннями-ключами Key_XY_M та Key_YX_M та різницевим

Третя група наших модельних експериментів полягала у порівнянні часу роботи створених у Mathcad програмного модуля, що реалізував протокольні обчислення для прискореного метода піднесення у степінь за модулем без застосування векторизації [12] та розробленого і пропонованого тут модуля, що застосовував векторизацію на всіх етапах та повністю відповідав суто паралельним матричним моделям та базується на матричних багатозначних логіках і може бути на основі цих ММ апаратно побудований. Для коректності ми проводили порівняння цих модулів при їх запуску на одному і тому ж широковживаному ПЕОМ з продуктивністю середнього класу. Вони показали, що на загальну тривалість виконання необхідних процедур найбільше впливають розміри масивів, кількість необхідних операцій піднесення у степінь за модулем, спосіб запису програмних модулів при емулюванні моделей, і застосування векторних паралельних обчислень, що тривалість виконання протокольних процедур модулями у Mathcad для зображень з розмірністю 256×256 та 320×240 елементів не перевищує декількох секунд і при їх оптимізації може бути зменшена на порядок, що застосування векторних обчислень теж на порядок чи навіть два зменшує цю тривалість. Таким чином підтверджено, що наші з декомпозицією ММ узгодження секретного ключа є кращими, мають внутрішній паралелізм, легше відображаються на апаратні матричні засоби.

Висновки

Обґрунтована необхідність та переваги створення, узгодження та застосування матричних ключів для покращених процедур зашифрування-розшифрування зображень, систем матричного типу. Підґрунтям протоколів створення МК_З є узагальнення відомих протоколів Діффі-Хелмана та інших на матричний випадок і відповідні математичні процедури-алгоритми на основі матричних моделей. Запропоновано нові модифікації матричних узгоджувальних протоколів з метою вдосконалення їх стійкості до атак. Для підтвердження достовірності запропонованих протоколів і їх модифікацій та порівняння стосовно складності обчислювальних процедур виконана низка модельних експериментів у програмному середовищі Mathcad Professional. Результати моделювання протоколів узгодження секретного матричного ключа для систем та моделей КП матричного типу підтвердили їх відповідність теоретичним положенням і суттєві переваги швидких обчислень при поелементно-матричному піднесенні до степеня за модулем на основі матричних АЦ-перетворень та використання фіксованих вагових матричних степенів за модулем і бінарних розрядних матриць для керованого вибору зважених компонентів. Обчислювальні процедури і матричні моделі враховують специфіку зображень і легко адаптуються до паралельних реалізацій та найновітніших апаратних матричних процесорів. Наведені результати моделювання процесів створення секретних матричних ключів-зображень великої розмірності.

Список літератури

1. Хорошко В.О. Методи та засоби захисту інформації : навч. Посібник / В.О. Хорошко, А.О. Четков. – К.: Юніор, 2003. – 502 с.

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

3. 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.

4. Коркішко Т. Алгоритми та процесори симетричного блокового шифрування / Т. Коркішко, А. Мельник, В. Мельник. – Львів: БаК, 2003. – 168 с.

5. 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.

6. 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.

7. 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.

8. Красиленко В.Г. Матричні афінно-перестановочні шифри для шифрування та дешифрування зображень [Текст] / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х: ХУПС, 2012. – Вип. 3(101), т. 2. – С. 53-61.

9. 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.

10. 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.

11. 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.

12. 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. – Х.: ХУПС, 2012. – Вип. 8(106). – С. 107-110.

13. 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.

14. 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(106). – С. 102-106.

15. 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. – [Електронний ресурс]. – Режим доступу: http://elit.lnu.edu.ua/pdf/6_12.pdf.

16. Красиленко В.Г. Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітовозрізовою 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. – [Електронний ресурс]. – Режим доступу: http://ki.lutsk-ntu.com.ua/node/132/section/9.

17. 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. [Електронний ресурс]. – Режим доступу: http://ddpu.drohobych.net/wp-content/uploads/2016/04/material_konf.pdf37.

18. Красиленко В.Г. Моделювання матричних афінних шифрів для криптографічних перетворень зображень / В.Г. Красиленко, Д.В. Нікітович // 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. – [Електронний ресурс]. Режим доступу: .http://dspace.puet.edu.ua/handle/123456789/5558

Надійшла до редколегії 18.01.2017

Рецензент: д-р техн. наук проф. В.А. Лужецький, Вінницький національний технічний університет, Вінниця.

МОДЕЛИРОВАНИЕ ПРОТОКОЛОВ СОГЛАСОВАНИЯ СЕКРЕТНЫХ МАТРИЧНЫХ КЛЮЧЕЙ ДЛЯ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ И СИСТЕМ МАТРИЧНОГО ТИПА

В. Г. Красиленко, Д. В. Никитович

Статья посвящена моделированию протоколов согласования секретного матричного ключа для криптографических преобразований в системах и моделях матричного типа. Основой таких протоколов является обобщение известных протоколов Диффи-Хеллмана и других на матричный случай и соответствующие математические процедуры-алгоритмы на основе матричных моделей 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 новые модификации матричных согласовательных протоколов с целью совершенствования их устойчивости к атакам. Для подтверждения достоверности предложенных протоколов и их модификаций и сравнения их характеристик, сложности вычислительных процедур выполнен ряд модельных экспериментов в программной среде Mathcad Professional. Показаны преимущества быстрых вычислений при поэлементно-матричных вознесениях в степень по модулю на основе матричных АЦ-преобразований и использования фиксированных весовых матричных степеней по модулю и бинарных разрядных матриц для управляемого выбора взвешенных компонентов. 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 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.*

MODELING OF COORDINATION PROTOCOLS OF SECRET MATRIX KEY FOR CRYPTOGRAPHIC TRANSFORMATION AND MATRIX TYPE SYSTEMS

V. Krasilenko, D. Nikitovich

The article is devoted to the 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-algorithms based on matrix models 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. New modifications of matrix matching protocols are proposed with the aim of improving their resistance to attacks. To confirm the reliability of the proposed protocols and their modifications and compare their characteristics, the complexity of the computational procedures, a number of model experiments were performed in the software environment of Mathcad Professional. The advantages of fast computational calculations for element-by-element matrix modular exponentiation are shown on the basis of matrix AC transformations and using fixed weight matrix degrees modulo and binary bit matrices for controlled selection of weighted components. 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 modeling the creation of secret matrix keys in the form of high-dimensional 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.