УДК 004.3

В.Г. Красиленко[1], В.І. Яцковський[2], Р.О. Яцковська[3]

[1] *Вінницький соціально-економічний інститут університету «Україна», Вінниця*
[2] *Вінницький національний державний університет, Вінниця*

АЛГОРИТМИ ФОРМУВАННЯ ДВОВИМІРНИХ КЛЮЧІВ ДЛЯ МАТРИЧНИХ АЛГОРИТМІВ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ЗОБРАЖЕНЬ ТА ЇХ МОДЕЛЮВАННЯ.

У статті розглядаються узагальнення протоколу Діффі-Хелмана на матричний випадок, алгоритми формування двовимірних ключів та їх реалізація на основі. матричних моделей. Сформовані запропонованим алгоритмом ключі застосовуються для матричних моделей та алгоритмів криптоперетворень зображень. Запропоновано процедури швидких обчислень на основі порозрядно-зрізових бінарних матриць та фіксованих поелементно-матричних степенів за модулем, що враховують специфіку зображень і можуть бути адаптованими до апаратних паралельних реалізацій. Наведені результати моделювання процесів створення матричного ключа-зображення розмірністю 128×128 елементів у програмному середовищі Mathcad Professional.

Ключові слова: *криптографічні перетворення зображень, алгоритм Діффі-Хелмана,, матричні моделі, матричні ключі, розшифрування ,протокол формування спільного ключа.*

Вступ

В сучасному інформаційному суспільстві з кожним роком зростає необхідність вирішення проблеми інформаційної безпеки та захисту від несанкціонованого доступу інформації державного, військового, комерційного та приватного змісту. Існує велика кількість 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, вони використовують ключі, а тому від надійності, криптостійкості процесів створення спільних для обох сторін безпечних ключів залежить рівень безпеки. В симетричних системах і в деяких асиметричних двом користувачам перед обміном інформацією необхідно з початку сформувати спільний безпечний ключ. 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 орієнтовані на послідовну обробку скалярних даних, при великих об'ємах яких криптографічні перетворення виконуються за допомогою одного і того ж самого ключа або підключа над різними виділеними інформаційними блоками. Це призводить до нестійкості таких алгоритмів послідовної обробки і вимагає збільшення довжини ключа і діапазонів чисел (модулів) які використовуються для визначення розмірностей скінченних полів параметрів криптосистем та реалізації процедур генерування ключів. В той же час поява великої кількості задач, в яких необхідно виконувати криптографічні перетворення над багатовимірними сигналами, серед яких особливе місце займають представлені в різних форматах багатоградаційні та кольорові зображення, потребує створення для таких задач і відповідних матричних моделей та алгоритмів, а також ключів у вигляді двовимірних масивів тобто зображень [3].

Огляд публікацій. Для забезпечення більшої стійкості алгоритмів в порівнянні з послідовними скалярними перетвореннями у роботах [4 – 6] були запропоновані та промодельовані у середовищі MathCad матричні моделі та алгоритми криптоперетворень 2-D масивів і зображень. Результати цих досліджень показали, що матричні афінні [4, 5] та матричні афінно-перестановочні алгоритми [6] мають суттєві переваги у порівнянні з традиційними, по суті скалярними, афінними асиметричними шифрами та можуть бути застосовані для створення цифрових сліпих підписів [7]. Було показано, що для реалізації таких матричних, більш загальних, моделей та алгоритмів крипто перетворень зображень необхідно мати один або декілька ключів представлених також у вигляді 2-D масиву чи зображення. В роботі [8] була запропонована модифікація алгоритму Діффі-Хелмана на матричний випадок для створення 2-D ключа. Але в цій роботі недостатньо було проведено модельних експериментів.

Постановка задачі. Метою даної роботи є подальше використання запропонованого концептуального підходу, розробка на його основі алгоритмів формування двовимірних ключів для матричних алгоритмів криптографічних перетворень зображень та їх моделювання.

Основна частина

Розглянемо алгоритм створення 2-D ключа на основі узагальнення та модифікації [8] на матричний випадок алгоритму Діффі-Хелмана. Нехай двом

абонентам відоме число γ і 2-D масив **ON**, що являє собою довільно вибране зображення чи згенероване відомими методами та засобами випадкове зображення **ONG** відповідної розмірності $I \times J$. Така інформація є відкритою та відома користувачам. В якості 2-D масивів можна використовувати чорно-білі зображення такої ж розмірності, чи одну з основних кольорових складових R,G,B кольорового зображення. Одна з сторін, наприклад абонент X, вибирає з набору множини зображень чи генерує випадкове зображення **A=GA** та обчислює 2-D масив **KA** за формулою $\mathbf{KA} \equiv \mathbf{ON}^{\mathbf{A}} \bmod(\gamma \cdot \mathbf{R})$, де **R –** матриця всі елементи якої дорівнюють одиниці, матриці **A**, **ON**, **R** та **KA** мають одну розмірність $I \times J$, а операція піднесення в степінь за модулем γ виконується поелементно, тобто $\mathbf{KA}_{i,j} \equiv \mathbf{ON}_{i,j}^{\mathbf{Ai,j}} \bmod \gamma$. Це зображення – масив **KA** він відправляє другому абоненту Y. Другий абонент Y аналогічним чином бере інший випадковий 2-D масив **B=GB**, обчислює значення масиву **KB** за формулою $\mathbf{KB} \equiv \mathbf{ON}^{\mathbf{B}} \bmod(\gamma \cdot \mathbf{R})$ та відправляє це зображення – масив **KB** першому абоненту X. Перший абонент X отримавши масив **KB** обчислює значення матричного ключа $\mathbf{KLBA} \equiv \mathbf{KB}^{\mathbf{A}} \bmod(\gamma \cdot \mathbf{R})$, а другий абонент Y - значення матричного ключа $\mathbf{KLAB} \equiv \mathbf{KA}^{\mathbf{B}} \bmod(\gamma \cdot \mathbf{R})$. Таким чином абоненти одержать однаковий таємний ключ $\mathbf{KEY} \equiv \mathbf{ON}^{\mathbf{B} \cdot \mathbf{A}} \bmod(\gamma \cdot \mathbf{R})$, який можуть використовувати для зашифрування та розшифрування при передачі 2-D даних, зображень, тощо. Такі ключі бажано використовувати для матричних моделей та алгоритмів симетричних, асиметричних та симетрично-асиметричних криптосистем [4 – 7]. Наведений протокол є узагальненням скалярного протоколу Діффі-Хелмана на матричний випадок, не використовує ніякого шифрування, проте є взаємно безпечним, 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. Запропонований алгоритм формування матричних ключів можна удосконалити у напрямі його стійкості до прямих атак, узагальнивши відомі протоколи STS чи MTI на матричний випадок.

Для прискорення обчислень, пов'язаних з піднесенням у степінь за модулем у відповідності до вищенаведених формул, ми пропонуємо використовувати порозрядно-зрізову декомпозицію масивів, що відповідають значенням степені і представляти їх у вигляді матриць побітових зрізів, а самі ці бітові матриці формувати відповідним аналого-цифровим перетворювачем картинного типу. Для такого варіанту організації обчислювальних процесів абоненти X та Y виконують згідно з нижче наведеними формулами (1-3) формування таких бінарних бітових матриць **BA0** ÷ **BA7**, **BP0** ÷ **BP7, KA0** ÷ **KA7,** з відповідних матриць **A**, **B**, чи **KA**:

$$A := GA;$$

$$\begin{aligned}
BA0 &:= \bmod(A_{i,j}, 2); & A0 &:= 0.5(A - BA0);\\
BA1 &:= \bmod(A0_{i,j}, 2); & A1 &:= 0.5(A0 - BA1);\\
BA2 &:= \bmod(A1_{i,j}, 2); & A2 &:= 0.5(A1 - BA2);\\
BA3 &:= \bmod(A2_{i,j}, 2); & A3 &:= 0.5(A2 - BA3);\\
BA4 &:= \bmod(A3_{i,j}, 2); & A4 &:= 0.5(A3 - BA4);\\
BA5 &:= \bmod(A4_{i,j}, 2); & A5 &:= 0.5(A4 - BA5);\\
BA6 &:= \bmod(A5_{i,j}, 2); & A6 &:= 0.5(A0 - BA6);\\
BA7 &:= \bmod(A6_{i,j}, 2); & A7 &:= 0.5(A6 - BA7);
\end{aligned} \quad (1)$$

$$B := GB;$$

$$\begin{aligned}
BP0_{i,j} &:= \bmod(B_{i,j}, 2); & B0 &:= 0.5(B - BP0);\\
BP1_{i,j} &:= \bmod(B0_{i,j}, 2); & B1 &:= 0.5(B0 - BP1);\\
BP2_{i,j} &:= \bmod(B1_{i,j}, 2); & B2 &:= 0.5(B1 - BP2);\\
BP3_{i,j} &:= \bmod(B2_{i,j}, 2); & B3 &:= 0.5(B2 - BP3);\\
BP4_{i,j} &:= \bmod(B3_{i,j}, 2); & B4 &:= 0.5(B3 - BP4);\\
BP5_{i,j} &:= \bmod(B4_{i,j}, 2); & B5 &:= 0.5(B4 - BP5);\\
BP6_{i,j} &:= \bmod(B5_{i,j}, 2); & B6 &:= 0.5(B5 - BP6);\\
BP7_{i,j} &:= \bmod(B6_{i,j}, 2); & B7 &:= 0.5(B6 - BP7);
\end{aligned} \quad (2)$$

$$\begin{aligned}
KA0_{i,j} &:= \bmod(KA_{i,j}, 2);\\
KA1_{i,j} &:= \bmod(AK0_{i,j}, 2); & AK0 &:= 0.5(KA - KA0);\\
KA2_{i,j} &:= \bmod(AK1_{i,j}, 2); & AK1 &:= 0.5(KA0 - KA1);\\
KA3_{i,j} &:= \bmod(AK2_{i,j}, 2); & AK2 &:= 0.5(KA1 - KA2);\\
KA4_{i,j} &:= \bmod(AK3_{i,j}, 2); & AK3 &:= 0.5(KA2 - KA3);\\
KA5_{i,j} &:= \bmod(AK4_{i,j}, 2); & AK4 &:= 0.5(KA3 - KA4);\\
KA6_{i,j} &:= \bmod(AK5_{i,j}, 2); & AK5 &:= 0.5(KA4 - KA5);\\
KA7_{i,j} &:= \bmod(AK6_{i,j}, 2); & AK6 &:= 0.5(KA5 - KA6).
\end{aligned} \quad (3)$$

Використовуючи сукупність отриманих проміжних масивів **X0** ÷ **X7**, які відповідають піднесеним у степінь 1, 2, 4, 8 і т.п., масивам **ON** за модулем γ, та бітові матриці **BA0** ÷ **BA7** абонент X обчислює значення **KA** за допомогою нижченаведених формул:

$$\begin{aligned}
KA1_{i,j} &:= \bmod[(X0_{i,j})^{BA0_{i,j}} \cdot (X1_{i,j})^{BA1_{i,j}} \times\\
&\times (X2_{i,j})^{BA2_{i,j}} \cdot (X3_{i,j})^{BA3_{i,j}}, \gamma];\\
KA2_{i,j} &:= \bmod[(X4_{i,j})^{BA4_{i,j}} \cdot (X5_{i,j})^{BA15_{i,j}} \times\\
&\times (X6_{i,j})^{BA6_{i,j}} \cdot (X7_{i,j})^{BA7_{i,j}}, \gamma];\\
KA_{i,j} &:= \bmod(KA1_{i,j} \cdot KA2_{i,j}, \gamma).
\end{aligned} \quad (4)$$

Аналогічним чином, використовуючи проміжні масиви **X0** ÷ **X7** та відповідні бінарні матриці **BP0** ÷ **BP7** (бінарні зрізи матриці **B**), абонент Y обчислює проміжний масив **KB** для відправки абоненту **X** за формулами:

$$KBl_{i,j} := \mathrm{mod}[(X0_{i,j})^{BP0_{i,j}} \cdot (Xl_{i,j})^{BPl_{i,j}} \times$$
$$\times (X2_{i,j})^{BP2_{i,j}} \cdot (X3_{i,j})^{BP3_{i,j}}, \gamma];$$
$$KB2_{i,j} := \mathrm{mod}[(X4_{i,j})^{BP4_{i,j}} \cdot (X5_{i,j})^{BP5_{i,j}} \times \quad (5)$$
$$\times (X6_{i,j})^{BP6_{i,j}} \cdot (X7_{i,j})^{BP7_{i,j}}, \gamma];$$
$$KB_{i,j} := \mathrm{mod}[(KBl_{i,j} \cdot KB2_{i,j}, \gamma).$$

Подальші дії протоколу з урахуванням використання бінарно-зрізових декомпозицій можуть бути описані за допомогою таких моделей:

1. Розрахунок проміжних степенів за модулем γ матриці **КВ** абонентом X:

$$YK0_{i,j} := \mathrm{mod}(KB_{i,j}, \gamma);$$
$$YK1_{i,j} := \mathrm{mod}[(YK0_{i,j})^2, \gamma];$$
$$YK2_{i,j} := \mathrm{mod}[(YK1_{i,j})^2, \gamma];$$
$$YK3_{i,j} := \mathrm{mod}[(YK2_{i,j})^2, \gamma];$$
$$YK4_{i,j} := \mathrm{mod}[(YK3_{i,j})^2, \gamma];$$
$$YK5_{i,j} := \mathrm{mod}[(YK4_{i,j})^2, \gamma];$$
$$YK6_{i,j} := \mathrm{mod}[(YK5_{i,j})^2, \gamma];$$
$$YK7_{i,j} := \mathrm{mod}[(YK6_{i,j})^2, \gamma].$$

2. Розрахунок проміжних степенів за модулем γ матриці **КА** абонентом Y

$$XK0_{i,j} := \mathrm{mod}(KA_{i,j}, \gamma);$$
$$XK1_{i,j} := \mathrm{mod}[(XK0_{i,j})^2, \gamma];$$
$$XK2_{i,j} := \mathrm{mod}[(XK1_{i,j})^2, \gamma];$$
$$XK3_{i,j} := \mathrm{mod}[(XK2_{i,j})^2, \gamma];$$
$$XK4_{i,j} := \mathrm{mod}[(XK3_{i,j})^2, \gamma];$$
$$XK5_{i,j} := \mathrm{mod}[(XK4_{i,j})^2, \gamma];$$
$$XK6_{i,j} := \mathrm{mod}[(XK5_{i,j})^2, \gamma];$$
$$XK7_{i,j} := \mathrm{mod}[(XK6_{i,j})^2, \gamma].$$

3. Процес формування ключа абонентом X з отриманого масиву **КВ:**

$$KXBA1_{i,j} := \mathrm{mod}[(YK0_{i,j})^{BA0_{i,j}} \cdot (YK1_{i,j})^{BA1_{i,j}} \times$$
$$\times (YK2_{i,j})^{BA2_{i,j}} \cdot (YK3_{i,j})^{BA3i,j}, \gamma];$$
$$KXBA2_{i,j} := \mathrm{mod}[(YK4_{i,j})^{BA4_{i,j}} \cdot (YK5_{i,j})^{BA5_{i,j}} \times$$
$$\times (YK6_{i,j})^{BA6_{i,j}} \cdot (YK7_{i,j})^{BA7i,j}, \gamma];$$
$$KLBA_{i,j} := \mathrm{mod}(KXBA1_{i,j} \cdot KXBA2_{i,j}, \gamma).$$

4. Процес формування ключа абонентом Y з отриманого масиву **КА**

$$KXABl_{i,j} := \mathrm{mod}[(XK0_{i,j})^{BP0_{i,j}} \cdot (XK1_{i,j})^{BPl_{i,j}} \times$$
$$\times (XK2_{i,j})^{BP2_{i,j}} \cdot (XK3_{i,j})^{BP3i,j}, \gamma];$$
$$KXAB2_{i,j} := \mathrm{mod}[(XK4_{i,j})^{BP4_{i,j}} \cdot (XK5_{i,j})^{BP5_{i,j}} \times$$
$$\times (XK6_{i,j})^{BP6_{i,j}} \cdot (XK7_{i,j})^{BP7i,j}, \gamma];$$
$$KLAB_{i,j} := \mathrm{mod}(KXABl_{i,j} \cdot KXAB2_{i,j}, \gamma).$$

Результати моделювання розробленого алгоритму в програмному середовищі MathCad показані на рис. 1 – 5, де вибране спільне зображення **ON**, вибране абонентом X випадкове зображення **A**, вибране абонентом Y випадкове зображення **B** є матрицями зображеннями розмірністю 128×128 елементів.

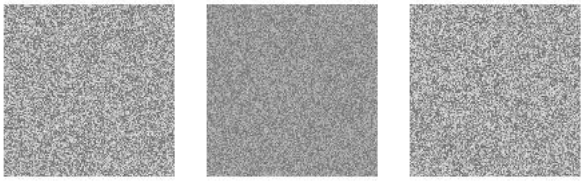

Рис. 1. Зображення, які використовувалися для моделювання.

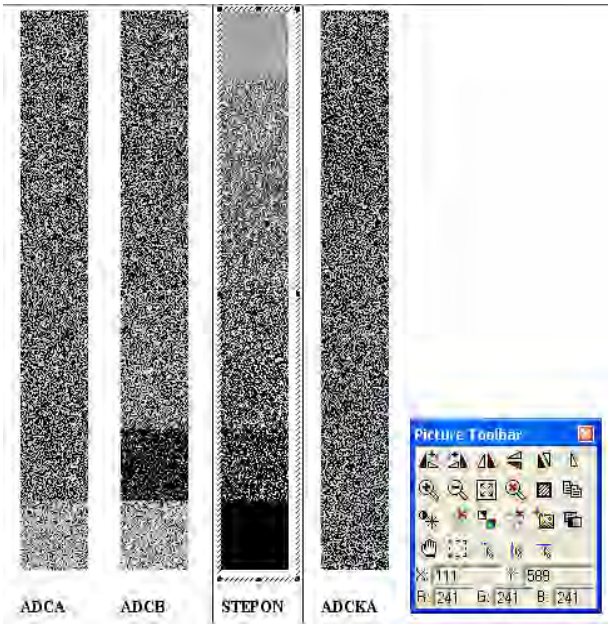

Рис. 2. Зображення сукупностей **ADCA**, **ADCB**, **ADCKA** бітових зрізів відповідно матриць **A**, **B**, **КА** та сукупності **STEPON** проміжних степенів **X0** ÷ **X7** за модулем γ основи **ON**

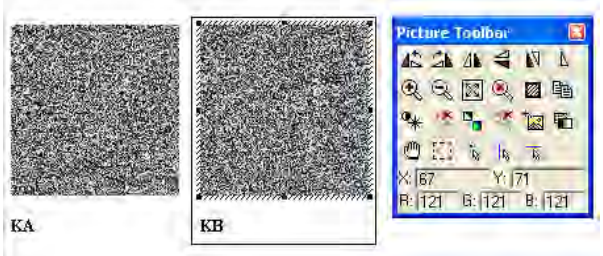

Рис. 3. Проміжні матриці – масиви **КА** та **КВ,** що передаються між абонентами по відкритому каналу зв'язку

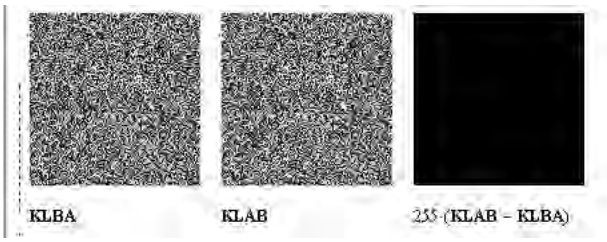

Рис. 4. Сформований ключ KLBA абонентом X та сформований ключ KLAB абонентом Y та різницеве зображення (матриця з нульовими елементами)

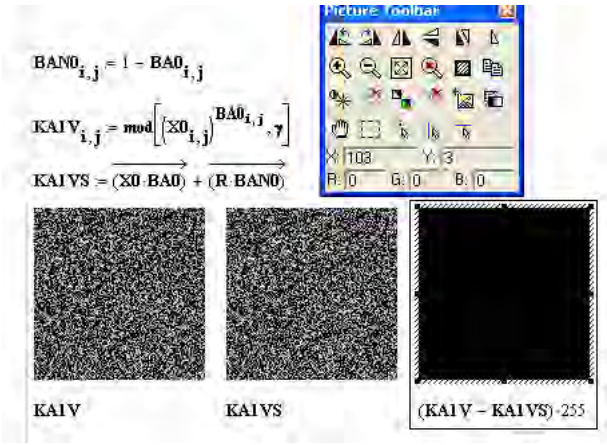

Рис. 5. Зображення, що показують один з можливих покращений підхід до організації обчислень на основі матричної паралельної логіки

Висновки

Результати моделювання алгоритму формування 2-D ключів на основі запропонованих матричних моделей та алгоритмів з використанням порозрядно-зрізової декомпозиції, матричної паралельної логічної обробки та аналого-цифрових перетворювачів картинного типу показали їх відповідність теоретичним положенням і суттєві переваги.

Список літератури

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

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

3. *M. A. Dabbah, W. L. Woo, and 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. *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.*

5. *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.*

6. *Красиленко В.Г. Матричні афінно – перестановочні шифри для шифрування та дешифрування зображень [Текст] / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – 2012 р. – №3 (101). – т. 2. – С. 53 – 61.*

7. *Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – 2011. – № 7 (97). – С. 60 – 63.*

8. *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 науково – практичної конференції «Наука і навчальний процес». – Вінниця, 2008. – С. 107 – 109.*

Надійшла до редколегії 5.10.2012

Рецензент: д-р техн. наук, проф. В.М. Лисогор, Вінницький національний аграрний університет, Вінниця.

АЛГОРИТМЫ ФОРМИРОВАНИЯ ДВУМЕРНЫХ МАТРИЧНЫХ КЛЮЧЕЙ ДЛЯ МАТРИЧНЫХ АЛГОРИТМОВ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ ИЗОБРАЖЕНИЙ И ИХ МОДЕЛИРОВАНИЕ

В.Г. Красиленко, В.И. Яцковский, Р.А. Яцковская

В статье рассматриваются обобщения протокола Диффи-Хеллмана на матричный случай, алгоритмы формирования двумерных ключей и их реализация на основе матричных моделей. Сформированные предложенным алгоритмом ключи применяются для матричных моделей и алгоритмов криптопреобразования изображений. Предложены процедуры быстрых вычислений на основе разрядно-срезовых бинарных матриц и фиксированных поэлементно-матричных степеней за модулем, учитывающие специфику изображений и которые могут быть адаптированы к аппаратным параллельным реализациям. Приведены результаты моделирования процессов создания матричного ключа-изображения размерностью 128 × 128 элементов в программной среде Mathcad Professional.

***Ключевые слова**: криптографические преобразования изображений, алгоритм Диффи-Хеллмана, матричные модели, матричные ключи, расшифровка, протокол формирования общего ключа.*

ALGORITHMS OF TWO-DIMENSIONAL MATRIX OF KEYS FOR CRYPTOGRAPHIC ALGORITHMS, MATRIX TRANSFORMATIONS OF IMAGES AND THEIR MODELLING

V.G Krasilenko, V.I Yatskovskiy, R.A Yatskovskiy

In this paper we consider the generalized Diffie-Hellman key to the matrix case, the formation of two-dimensional key algorithms and their implementation on the basis of matrix models. Generated by key algorithm used for matrix models and algorithms kriptopreobrazovaniya images. The procedures of quick calculations based on bit-slice design matrix and elementwise fixed-matrix power by module tailored to image and that can be adapted to the parallel hardware implementations. The results of the simulation of a matrix-key image dimensions of 128 × 128 elements in a software environment Mathcad Professional.

***Keywords**: cryptographic transformation of images, Diffie-Hellman, matrix models, matrix switches, decoding, protocol, forming a common key*