УДК 004.056.55 **doi: 10.26906/SUNZ.2018.1.141**

С.В. Сисоєнко

Черкаський державний технологічний університет, Черкаси

ОЦІНКА ШВИДКОСТІ РЕАЛІЗАЦІЇ ГРУПОВОГО МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

У статті розглянуто та теоретично обґрунтовано результати досліджень визначення відносної складності та збільшення відносної швидкості групового матричного криптографічного перетворення в залежності від розрядності матриць. Встановлена закономірність обчислення складності логічних визначників для узагальненої моделі групового матричного криптографічного перетворення. Побудовано залежність для обчислення відносної складності та відносного часу реалізації групового матричного криптоперетворення порівняно з швидкістю та складністю матричного криптоперетворення.

***Ключові слова**: складність логічних визначників, відносна складність, відносна швидкість, пряме та обернене криптографічне перетворення.*

Вступ

Постановка проблеми. Проблема захисту інформації на сьогоднішній день стає надзвичайно актуальною для користувачів глобальних інформаційних систем. Відомі на даний час засоби криптографічного захисту інформації забезпечують інформаційну безпеку та можуть значною мірою впливати на швидкість її обробки та передачі даних по захищених каналах і корпоративних мережах передачі даних. Зважаючи на те, що одним з найбільш ефективним засобом захисту інформації є використання крипто алгоритмів, в сьогоденні актуальною задачею можна назвати розробку та вдосконалення швидкодіючих алгоритмів криптографічного захисту. Основними характеристиками криптографічних систем є стійкість та швидкість виконання перетворення, які необхідно постійно підвищувати. Одним із шляхів вирішення даної проблеми є застосування матричних операцій криптографічного перетворення для розробки крипто алгоритмів. Захист даних за допомогою методів криптографічного захисту інформації – одне з можливих рішень проблеми безпеки інформації [1].

Аналіз останніх досліджень і публікацій. В роботах [1, 2] була проведення оцінка криптостійкості та швидкості реалізації криптографічного захисту інформації на основі операцій матричного та розширеного матричного криптографічного перетворення. Проте в даних дослідженнях не була здійснена оцінка відносної швидкості реалізації групового матричного криптографічного перетворення. Саме це й робить тему дослідження актуальною.

Ця робота продовжує почате в [2,3] дослідження Даний підхід забезпечує побудову результуючої послідовності, з покращеними характеристиками.

Метою роботи є побудова залежностей для оцінки підвищення швидкості та зменшення складності матричного групового криптографічного перетворення.

Основний матеріал

Для підвищення швидкості та зменшення складності групового матричного криптографічного перетворення у роботах [4, 5] була отримана узагальнена модель двохоперандного групового матричного криптографічного перетворення. Дана модель [4, 5] дозволяє зробити припущення про можливість побудови узагальненої моделі групового матричного криптографічного перетворення. Узагальнена модель буде представлена в такому вигляді:

якщо

$$G^k = \begin{bmatrix} a_{11}F_1^k(z_1) \oplus a_{12}F_2^k(z_2) \oplus ... \oplus a_{1n}F_n^k(z_n) \\ a_{21}F_1^k(z_1) \oplus a_{22}F_2^k(z_2) \oplus ... \oplus a_{2n}F_n^k(z_n) \\ ..... \\ a_{n1}F_1^k(z_1) \oplus a_{n2}F_2^k(z_2) \oplus ... \oplus a_{nn}F_n^k(z_n) \end{bmatrix}, \quad (1)$$

де $a_{ij} \in [0,1]$ – коефіцієнти матриці прямого групового криптографічного перетворення, F_i^k – операції негрупових криптографічних перетворень, $\oplus$ – операція «сума за mod 2». z_i – вхідні дані для прямого перетворення,

тоді

$$G^d = \begin{bmatrix} b_{11}F_1^d(w_1) \oplus b_{12}F_1^d(w_2) \oplus ... \oplus b_{1n}F_1^d(w_n) \\ b_{21}F_2^d(w_1) \oplus b_{22}F_2^d(w_2) \oplus ... \oplus b_{2n}F_2^d(w_n) \\ ..... \\ b_{n1}F_n^d(w_1) \oplus b_{n2}F_n^d(w_2) \oplus ... \oplus b_{nn}F_n^d(w_n) \end{bmatrix}, \quad (2)$$

де коефіцієнти матриці оберненого групового криптографічного перетворення – $b_{ij} \in [0,1]$, F_i^d – криптографічних перетворень, w_i – вхідні дані (результати прямого перетворення) для оберненого перетворення.

Оцінку швидкості реалізації групового матричного криптографічного перетворення запропонованої моделі [4, 5] оцінимо за складністю знаходження логічних визначників та їх відносною складністю

обчислення. Операції декодування інформації, можливо за допомогою логічних визначників [6]. Логічний визначник другого порядку є вираз:

$$\Delta_2 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} \oplus a_{12}a_{21}, \qquad (3)$$

де $a_{ij} \in K$, $K = \langle \{0,1\}, \oplus, \otimes \rangle$ двійкове поле над яким розглядаються, так звані, визначники і матриці, які називаються логічними [6].

При проведенні досліджень, під складністю логічного визначника будемо розуміти кількість логічних операцій множення та додавання за модулем два, які необхідно виконати для його розрахунку. Знайдемо складність обчислення визначника другого порядку позначивши його через $C_{кл2}$, визначивши кількість логічних операцій при обчисленні виразу (3), яка включає дві операції логічного множення $\otimes$ та одну операцію логічного додавання $\oplus$ за модулем 2 отримаємо $C_{кл2} = 3$. Складність обчислення визначника третього порядку $C_{кл3}$ визначимо кількістю логічних операцій при обчисленні виразу [6].

$$\Delta_3 = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} \oplus a_{13}a_{21}a_{32} \oplus \qquad (4)$$

$$\oplus a_{12}a_{23}a_{31} \oplus a_{13}a_{22}a_{31} \oplus a_{12}a_{21}a_{33} \oplus a_{11}a_{23}a_{32}.$$

Отже $C_{кл3} = 17$, яка включає 12 операцій логічного множення та 5 операції логічного додавання за модулем 2. Складність обчислення логічного визначника четвертого порядку (5) $C_{кл4}$ проаналізуємо на основі обчислення логічного визначника третього порядку, який дорівнює логічній сумі добутків елементів якого-небудь рядка (стовпця) [6] на їхні логічні доповнення. Логічним доповненням L_{ij} елемента a_{ij} логічного визначника називається логічний визначник, який утворюється з даного визначника в результаті викреслення i-го рядка та j-го стовпця [6].

Нехай задано логічний визначник 4 порядку

$$\Delta_4 = \begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{vmatrix} = \qquad . \qquad (5)$$

$$= a_{11}L_{11} \oplus a_{12}L_{12} \oplus a_{13}L_{13} \oplus a_{14}L_{14}.$$

Тоді

$$\Delta_4 = a_{11}\begin{vmatrix} a_{22} & a_{23} & a_{24} \\ a_{32} & a_{33} & a_{34} \\ a_{42} & a_{43} & a_{44} \end{vmatrix} \oplus a_{12}\begin{vmatrix} a_{21} & a_{23} & a_{24} \\ a_{31} & a_{33} & a_{34} \\ a_{41} & a_{43} & a_{44} \end{vmatrix} \oplus \qquad . \qquad (6)$$

$$\oplus a_{13}\begin{vmatrix} a_{21} & a_{22} & a_{24} \\ a_{31} & a_{32} & a_{34} \\ a_{41} & a_{42} & a_{44} \end{vmatrix} \oplus a_{14}\begin{vmatrix} a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ a_{41} & a_{42} & a_{43} \end{vmatrix}.$$

При виконанні відповідних логічних обчислень виразу (6) складність обчислення логічного визначника четвертого порядку $C_{кл4} = 95$. Аналогічно розрахункам складності обчислення логічного визначника четвертого порядку, проведемо розрахунок складності логічного визначника п‘ятого порядку $C_{кл5} = 599$. На основі розрахунку складності логічного визначника п‘ятого порядку знайдемо $C_{кл6} = 863$. При проведенні даних розрахунків була встановлена закономірність обчислення складності логічних визначників:

$$C_{клn} = \left[(17 + (n-3)\times 6)\times 4 + 3\right]n + (n-1), \qquad (7)$$

де n>4 – порядок логічного визначника.

Результати розрахунку складності логічного визначника в залежності від порядку наведені в табл. 1 (n – порядок логічного визначника, $C_{клn}$ – Складність обчислення логічного визначника).

Таблиця 1

Результати розрахунку складності логічного визначника

n	n=2	n=3	n=4	n=5	n=6	n=7	n=8
$C_{клn}$	3	17	95	599	863	1175	1538

Проведемо порівняльну оцінку зменшення кількості операцій для знаходження складності обчислень логічних визначників при застосуванні розробленої моделі [5] оберненого криптографічного перетворення зі складності обчислень логічних визначників при знаходженні A^{-1}.

Нехай $G^{k}_{(2\times 2)} = \begin{bmatrix} a_{11}F^{k}_{l(2\times 2)} \oplus a_{12}F^{k}_{2(2\times 2)} \\ a_{21}F^{k}_{l(2\times 2)} \oplus a_{22}F^{k}_{2(2\times 2)} \end{bmatrix}$, тоді відповідно до моделі [5]

$$G^{d}_{(2\times 2)} = \begin{bmatrix} b_{11}F^{d}_{l(2\times 2)} \oplus b_{12}F^{d}_{l(2\times 2)} \\ b_{21}F^{d}_{2(2\times 2)} \oplus b_{22}F^{d}_{2(2\times 2)} \end{bmatrix} \to A^{-1}_{(4\times 4)}. \qquad (8)$$

Для знаходження складності обчислення логічного визначника виразу (8) запропонованої моделі [5] необхідно знайти складність розрахунку матриць: $C_{кл}G^{d}_{(2\times 2)}$, $C_{кл}F^{d}_{l(2\times 2)}$ та $C_{кл}F^{d}_{2(2\times 2)}$. Тому складність розрахунку запропонованої моделі [5] для першого випадку позначимо

$$C^{скл1}_{\sum м(2\times 2)} = C_{кл}G^{d}_{(2\times 2)} \oplus C_{кл}F^{d}_{l(2\times 2)} \oplus C_{кл}F^{d}_{2(2\times 2)}.$$

Згідно даних табл. 1 для даного випадку $C^{скл1}_{\sum м(2\times 2)} = 9$. А складність $A^{-1}{}_{скл(4\times 4)} = C_{кл4} = 95$. Отже $C^{скл1}_{\sum м(2\times 2)} = 9 < A^{-1}{}_{скл(4\times 4)} = 95$. Для даного випадку проведемо оцінку швидкості реалізації групового матричного криптографічного перетворення на основі оцінки відносної складності обчислення логічних визначників: $C^{скл1}_{\sum м(2\times 2)}$, $A^{-1}{}_{скл(4\times 4)}$. Відносна складність обчислення логічних визначників

першого випадку $v_{скл1}$ позначимо через відношення обчислення складності логічних визначників матриці $A^{-1}_{скл(4\times4)}$ до складності розрахунку логічних визначників запропонованої моделі [5] для першого випадку $C^{скл1}_{\sum м(2\times2)}$.

$$v_{скл1} = A^{-1}_{скл(4\times4)} \Big/ C^{скл1}_{\sum м(2\times2)}. \quad (9)$$

Відносну швидкість можна розгляати як обернене значення відносної складності

$$v_{шв} = 1/v_{скл1} = C^{скл1}_{\sum м(2\times2)} \Big/ A^{-1}_{скл(4\times4)}. \quad (10)$$

Підставивши в (9) результати розрахунків, отримаємо відносну складність обчислення логічних визначників першого випадку $v_{скл1} = 10,5$раза. Аналогічно проведемо розрахунок для моделі [5]

$$G^{k}_{(2\times2)} = \begin{bmatrix} a_{11}F^{k}_{l(3\times3)} \oplus a_{12}F^{k}_{2(3\times3)} \\ a_{21}F^{k}_{l(3\times3)} \oplus a_{22}F^{k}_{2(3\times3)} \end{bmatrix}, \text{ тоді}$$

$$G^{d}_{(2\times2)} = \begin{bmatrix} b_{11}F^{d}_{l(3\times3)} \oplus b_{12}F^{d}_{l(3\times3)} \\ b_{21}F^{d}_{2(3\times3)} \oplus b_{22}F^{d}_{2(3\times3)} \end{bmatrix} \to A^{-1}_{(6\times6)}. \quad (11)$$

Для знаходження складності обчислення логічного визначника виразу (11) необхідно знайти складність розрахунку матриць: $C_{кл}G^{d}_{(2\times2)}$, $C_{кл}F^{d}_{l(3\times3)}$, $C_{кл}F^{d}_{2(3\times3)}$. Складність розрахунку запропонованої моделі [5] для другого випадку позначимо

$$C^{скл2}_{\sum м}(2\times2) = C_{кл}G^{d}_{(2\times2)} \oplus C_{кл}F^{d}_{l(3\times3)} \oplus C_{кл}F^{d}_{2(3\times3)}.$$

Згідно даних табл. 1 $C^{скл2}_{\sum м}(2\times2) = 37$ а складність обчислення логічного визначника матриці $A^{-1}_{скл(6\times6)} = C_{кл6} = 863$. Для даного випадку $C^{скл2}_{\sum м}(3\times3) = 37 < A^{-1}_{скл(6\times6)} = 863$. Відносна складність $v_{скл2} = 23,3$раза. Проведемо розрахунок при

$$G^{k}_{(2\times2)} = \begin{bmatrix} a_{11}F^{k}_{l(4\times4)} \oplus a_{12}F^{k}_{2(4\times4)} \\ a_{21}F^{k}_{l(4\times4)} \oplus a_{22}F^{k}_{2(4\times4)} \end{bmatrix}, \text{ тоді}$$

$$G^{d}_{(2\times2)} = \begin{bmatrix} b_{11}F^{d}_{l(4\times4)} \oplus b_{12}F^{d}_{l(4\times4)} \\ b_{21}F^{d}_{2(4\times4)} \oplus b_{22}F^{d}_{2(4\times4)} \end{bmatrix} \to A^{-1}_{(8\times8)}. \quad (12)$$

Складність розрахунку 3-го випадку (12)

$$C^{скл3}_{\sum м}(2\times2) = C_{кл}G^{d}_{(2\times2)} \oplus C_{кл}F^{d}_{l(4\times4)} \oplus C_{кл}F^{d}_{2(4\times4)}.$$

Згідно даних табл. 1 $C^{скл3}_{\sum м}(2\times2) = 193$ а складність обчислення логічного визначника матриці $A^{-1}_{скл(8\times8)} = C_{кл8} = 1538$. Для даного випадку $C^{скл3}_{\sum м}(2\times2) = 193 < A^{-1}_{скл(8\times8)} = 1538$. Відносна складність $v_{скл3} = 7,97$раза. Для знаходження складності обчислення логічного визначника виразу (13) запропонованої моделі (1,2) для четвертого випадку необхідно знайти складність розрахунку матриць: $C_{кл}G^{d}_{(3\times3)}$, $C_{кл}F^{d}_{l(2\times2)}$, $C_{кл}F^{d}_{2(2\times2)}$ та $C_{кл}F^{d}_{3(2\times2)}$.

Нехай

$$G^{k}_{(3\times3)} = \begin{bmatrix} a_{11}F^{k}_{l(2\times2)} \oplus a_{12}F^{k}_{2(2\times2)} \oplus a_{13}F^{k}_{3(2\times2)} \\ a_{21}F^{k}_{l(2\times2)} \oplus a_{22}F^{k}_{2(2\times2)} \oplus a_{23}F^{k}_{3(2\times2)} \\ a_{31}F^{k}_{l(2\times2)} \oplus a_{32}F^{k}_{2(2\times2)} \oplus a_{33}F^{k}_{3(2\times2)} \end{bmatrix}, \text{ тоді}$$

відповідно до моделі (1), (2)

$$G^{d}_{(3\times3)} = \begin{bmatrix} b_{11}F^{d}_{l(2\times2)} \oplus b_{12}F^{d}_{l(2\times2)} \oplus b_{13}F^{d}_{l(2\times2)} \\ b_{21}F^{d}_{2(2\times2)} \oplus b_{22}F^{d}_{2(2\times2)} \oplus b_{23}F^{d}_{2(2\times2)} \\ b_{31}F^{d}_{3(2\times2)} \oplus b_{32}F^{d}_{3(2\times2)} \oplus b_{33}F^{d}_{3(2\times2)} \end{bmatrix} \to A^{-1}_{(6\times6)}. \quad (13)$$

Позначимо $C^{скл4}_{\sum м}(3\times3) = C_{кл}G^{d}_{(3\times3)} \oplus C_{кл}F^{d}_{l(2\times2)} \oplus \oplus C_{кл}F^{d}_{2(2\times2)} \oplus C_{кл}F^{d}_{3(2\times2)}$. Для даного випадку $C^{скл4}_{\sum м}(3\times3) = 26$. Складність обчислення логічного визначника матриці $A^{-1}_{скл(6\times6)} = C_{кл6} = 863$. Отже $C^{скл4}_{\sum м}(3\times3) = 26 < A^{-1}_{скл(6\times6)} = 863$.

Відносна складність обчислення логічних визначників четвертого випадку проводиться згідно виразу (9) на основі даних розрахунків даного випадку $v_{скл4} = 33,2$раза. Аналогічно проведено наступні розрахунки складності матриць при наступних випадках 5-6 за умови: $C_{кл}G^{d}_{(3\times3)}$, $C_{кл}F^{d}_{l(3\times3)}$, $C_{кл}F^{d}_{2(3\times3)}$ та $C_{кл}F^{d}_{3(3\times3)}$. Позначимо $C^{скл5}_{\sum м}(3\times3) = = C_{кл}G^{d}_{(3\times3)} \oplus C_{кл}F^{d}_{l(3\times3)} \oplus C_{кл}F^{d}_{2(3\times3)} \oplus C_{кл}F^{d}_{3(3\times3)}$.

Для даного випадку $C^{скл5}_{\sum м}(3\times3) = 68$. Складність обчислення логічного визначника матриці знайдемо за (7) $A^{-1}_{скл(9\times9)} = C_{кл9} = 1079$. Отже $C^{скл5}_{\sum м}(3\times3) = 68 < < A^{-1}_{скл(9\times9)} = 1079$. Відносна складність $v_{скл5} = = 15,9$ раза. Позначимо $C^{скл6}_{\sum м}(3\times3) = C_{кл}G^{d}_{(3\times3)} \oplus \oplus C_{кл}F^{d}_{l(4\times4)} \oplus C_{кл}F^{d}_{2(4\times4)} \oplus C_{кл}F^{d}_{3(4\times4)}$. Для даного випадку $C^{скл6}_{\sum м}(3\times3) = 302$. Складність обчислення логічного визначника матриці знайдемо за (7) $A^{-1}_{скл(12\times12)} = C_{кл12} = 3455$. Отже $C^{скл6}_{\sum м}(3\times3) = 302 < < A^{-1}_{скл(12\times12)} = 3455$. Відносна складність $v_{скл6} = = 11,4$ раза. Для знаходження складності обчислення логічного визначника (14) знайдемо складність розрахунку матриць: $C_{кл}G^{d}_{(4\times4)}$, $C_{кл}F^{d}_{l(2\times2)}$, $C_{кл}F^{d}_{2(2\times2)}$, $C_{кл}F^{d}_{3(2\times2)}$, $C_{кл}F^{d}_{4(2\times2)}$.

Нехай

$$G^{k}_{(4\times4)} =$$

$$= \begin{bmatrix} a_{11}F^{k}_{1(2\times2)} \oplus a_{12}F^{k}_{2(2\times2)} \oplus a_{13}F^{k}_{3(2\times2)} \oplus a_{14}F^{k}_{4(2\times2)} \\ a_{21}F^{k}_{1(2\times2)} \oplus a_{22}F^{k}_{2(2\times2)} \oplus a_{23}F^{k}_{3(2\times2)} \oplus a_{24}F^{k}_{4(2\times2)} \\ a_{31}F^{k}_{1(2\times2)} \oplus a_{32}F^{k}_{2(2\times2)} \oplus a_{33}F^{k}_{3(2\times2)} \oplus a_{34}F^{k}_{4(2\times2)} \\ a_{41}F^{k}_{1(2\times2)} \oplus a_{42}F^{k}_{2(2\times2)} \oplus a_{43}F^{k}_{3(2\times2)} \oplus a_{44}F^{k}_{4(2\times2)} \end{bmatrix},$$

Тоді відповідно до моделі (1), (2)

$$G^{d}_{(4\times4)} =$$

$$= \begin{bmatrix} b_{11}F^{d}_{1(2\times2)} \oplus b_{12}F^{d}_{1(2\times2)} \oplus b_{13}F^{d}_{1(2\times2)} \oplus b_{14}F^{d}_{1(2\times2)} \\ b_{21}F^{d}_{2(2\times2)} \oplus b_{22}F^{d}_{2(2\times2)} \oplus b_{23}F^{d}_{2(2\times2)} \oplus b_{24}F^{d}_{2(2\times2)} \\ b_{31}F^{d}_{3(2\times2)} \oplus b_{32}F^{d}_{3(2\times2)} \oplus b_{33}F^{d}_{3(2\times2)} \oplus b_{34}F^{d}_{3(2\times2)} \\ b_{41}F^{d}_{4(2\times2)} \oplus b_{42}F^{d}_{4(2\times2)} \oplus b_{43}F^{d}_{4(2\times2)} \oplus b_{44}F^{d}_{4(2\times2)} \end{bmatrix} \rightarrow (14)$$

$$\rightarrow A^{-1}_{(8\times8)}.$$

Складність розрахунку для (14) позначимо $C^{скл7}_{\sum м\,(2\times2)} = C_{кл}G^{d}_{(4\times4)} \oplus C_{кл}F^{d}_{1(2\times2)} \oplus C_{кл}F^{d}_{2(2\times2)} \oplus \oplus C_{кл}F^{d}_{3(2\times2)} \oplus C_{кл}F^{d}_{4(2\times2)}$. Згідно даних табл. 1 $C^{скл7}_{\sum м\,(4\times4)} = 107$ а складність обчислення логічного визначника матриці $A^{-1}{}_{скл(8\times8)} = C_{кл8} = 1538$. Для даного випадку $C^{скл7}_{\sum м\,(4\times4)} = 107 < A^{-1}{}_{скл(8\times8)} = 1538$.

Відносна складність $v_{скл7} = 14,37$раза.

Аналогічно проведено наступні розрахунки складності матриць при випадках 8-9 за умови: $C_{кл}G^{d}_{(4\times4)}$, $C_{кл}F^{d}_{1(3\times3)}$, $C_{кл}F^{d}_{2(3\times3)}$, $C_{кл}F^{d}_{3(3\times3)}$ та $C_{кл}F^{d}_{4(3\times3)}$. Позначимо $C^{скл8}_{\sum м\,(4\times4)} = C_{кл}G^{d}_{(4\times4)} \oplus \oplus C_{кл}F^{d}_{1(3\times3)} \oplus C_{кл}F^{d}_{2(3\times3)} \oplus C_{кл}F^{d}_{3(3\times3)} \oplus C_{кл}F^{d}_{4(3\times3)}$.

Для даного випадку $C^{скл8}_{\sum м\,(4\times4)} = 163$. Складність обчислення логічного визначника матриці знайдемо за (7) $A^{-1}{}_{скл(12\times12)} = C_{кл12} = 3455$. Отже $C^{скл8}_{\sum м\,(4\times4)} = 163 < A^{-1}{}_{скл(12\times12)} = 3455$. Відносна складність $v_{скл8} = 21,2$раза.

Позначимо $C^{скл9}_{\sum м\,(4\times4)} = C_{кл}G^{d}_{(4\times4)} \oplus C_{кл}F^{d}_{1(4\times4)} \oplus \oplus C_{кл}F^{d}_{2(4\times4)} \oplus C_{кл}F^{d}_{3(4\times4)} \oplus C_{кл}F^{d}_{4(4\times4)}$. Для даного випадку $C^{скл9}_{\sum м\,(4\times4)} = 475$. Складність обчислення логічного визначника матриці знайдемо за (7) $A^{-1}{}_{скл(16\times16)} = C_{кл12} = 6143$. Отже $C^{скл9}_{\sum м\,(4\times4)} = 475 < < A^{-1}{}_{скл(16\times16)} = 6143$. Відносна складність $v_{скл9} = 12,9$раза

Дані розрахунків занесено в табл. .2 та відображено графічно на гістограмі рис. 1.

Аналіз представлених даних на рис. 1 та даних табл. 2 свідчить про те, що зменшення складності обчислень логічних визначників при запропонованих моделях дає виграш від 8 до 33 разів.

Висновки

Для спрощеної оцінки відносної складності запропоновано використати логічні визначники. Розрахунок складності обчислень логічних визначників забезпечить коректність розрахунків та достовірність результатів за рахунок використання операцій, які мають однаковий час виконання та складність технічної реалізації. На основі узагальнення дослідження було встановлено залежність для визначення відносної складності та збільшення відносної швидкості в залежності від розрядності групового та не групового матричного криптографічного перетворення.

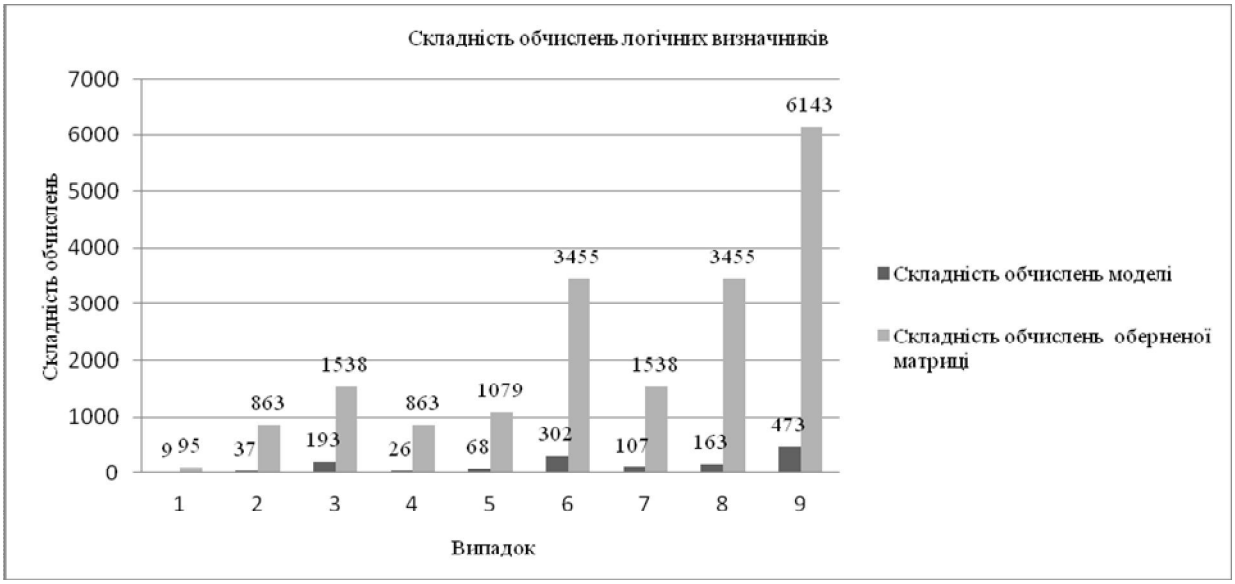

Рис. 1. Гістограма складності обчислень логічних визначників розробленої моделі (темний стовпчик) в порівнянні зі складністю обчислень логічних визначників матриць A^{-1} відповідних розмірностей

Таблиця 2

Результати складності обчислень логічних визначників
при застосуванні розроблених моделей та відповідних значень логічних визначників при знаходженні A^{-1}

№ випадку	Розмірність G^d	Розмірність F^d	Розмірність матриці A^{-1}	Складність запропонованої моделі $C_{\sum м}^{скл}$	Складність матриці A^{-1}	Відносна складність $v_{скл}$, *раза*
1	2×2	2×2	4×4	9	95	10,5
2	2×2	3×3	6×6	37	863	23,3
3	2×2	4×4	8×8	193	1538	7,97
4	3×3	2×2	6×6	26	863	33,2
5	3×3	3×3	9×9	68	1079	15,9
6	3×3	4×4	12×12	302	3455	11,4
7	4×4	2×2	8×8	107	1538	14,4
8	4×4	3×3	12×12	163	3455	21,2
9	4×4	4×4	16×16	473	6143	12,9

Результати досліджень підтверджують ефективність практичного застосування групових моделей матриць криптоперетворення за рахунок підвищення відносної швидкості та зменшення відносної складності при їх застосуванні в крипто алгоритмах та крипто примітивах.

Список літератури

1. Бабенко В.Г., Мельник Р.П., Гончар С.В. Оцінка ефективності використання операцій криптографічного перетворення. Вісник інженерної академії України. – Вип. 2. - Київ, 2014. - С. 39–41.

2. Рудницький В.М., Сисоєнко С.В., Мельник О.Г., Пустовіт М.О. Дослідження методу підвищення стійкості комп'ютерних криптографічних алгоритмів. Вісник Черкаського державного технологічного університету. Серія : Технічні науки : наук.-техн. журн. Черкас. держ. технол. ун-т. – Черкаси: ЧДТУ, 2017 – Вип. 3 – С.- 5-10.

3. Сисоєнко С.В., Мельник О.Г. Використання операцій та алгоритмів криптоперетворення двох блоків змінних в криптографії.. Матеріали міжнародної науково-практичної конференції (за підтримки представництва Торговельно-Промислової Палати України в Республіці Ірак та Iraqi-Ukrainian Business Council) «Інноваційні тенденції сьогодення в сфері природничих, гуманітарних та точних наук» 17 жовтня 2017 рік том 2 м. Івано-Франківськ 2017. - С. 47–49.

4. Сисоєнко С.В., Мельник О.Г. Дослідження операцій оберненого групового матричного криптографічного перетворення інформації. Міжнародна науково-практична конференція «Наука у контексті сучасних глобалізаційних процесів» 19 листопада 2017 рік том 10 м. Полтава 2017. - С. 44–46.

5. Сисоєнко С.В., Мельник О.Г., Пустовіт М.О.. Синтез операцій оберненого групового матричного криптографічного перетворення інформації. Вісник Черкаського державного технологічного університету. Серія : Технічні науки : наук.-техн. журн. Черкас. держ. технол. ун-т. – Черкаси: ЧДТУ, 2017 – Вип. 4 – С.- 118-125.

6. Бабенко В.Г., Стабецька Т.А.Операції матричного криптографічного декодування на основі логічних визначників. Тези доповідей четвертої міжн. НПК «Методи та засоби кодування, захисту й ущільнення інформації» 23-25 квітня 2013 рік м. Вінниця, - С. 135-137.

Надійшла до редколегії 27.12.2017

Рецензент: д-р техн. наук, проф. І.В. Шостак, Національний аерокосмічний університет імені М.Є. Жуковського «ХАІ», Харків.

ОЦЕНКА СКОРОСТИ РЕАЛИЗАЦИИ ГРУППОВОГО МАТРИЧНОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

С.В. Сысоенко

В статье рассмотрены и теоретически обоснованы результаты исследований определения относительной сложности и увеличение относительной скорости группового матричного криптографического преобразования в зависимости от разрядности матриц. Установлена закономерность вычисления сложности логических определителей для обобщенной модели группового матричного криптографического преобразования. Построено зависимость для вычисления относительной сложности и относительного времени реализации группового матричного криптопреобразования в сравнении со скоростью и сложностью матричного криптопреобразования.

Ключевые слова: *сложность логических определителей, относительная сложность, относительная скорость, прямое и обратное криптографическое преобразование.*

EVALUATION OF SPEEDITY OF IMPLEMENTATION OF GROUPS MATRIX CRYPTOGRAPHIC CONVERGENCE

S.V. Sysoienko

The article considers the results of studies of the definition of relative complexity and an increase in the relative speed of the matrix cryptographic group transformation as a function of the bit width of the matrices. Their theoretical substantiation is carried out. For the generalized model, a regularity is established for calculating the complexity of the logical determinants of a matrix cryptographic group transformation. A dependence is constructed to calculate the relative complexity and relative time of realization of group matrix crypto-transformation in comparison with the speed and complexity of matrix crypto-transformation.

Keywords: *complexity of logical determinants, relative complexity, relative velocity, direct and reverse cryptographic transformation.*