УДК 003.26:004.056.55

Н.В. Лада

Черкаський державний технологічний університет, Черкаси

АНАЛІЗ КОРЕКТНОСТІ ВЗАЄМОЗВ'ЯЗКІВ МІЖ ПРЯМИМИ ТА ОБЕРНЕНИМИ МАТРИЧНИМИ МОДЕЛЯМИ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

В статті здійснено аналіз результатів обчислювального експерименту по моделюванню прямих і обернених операцій криптоперетворення для використання в матричних алгоритмах. Проведено аналіз і дослідження взаємозв'язків між прямими та оберненими матричними моделями операцій криптографічного перетворення інформації. Доведено коректність використання синтезованих за результатами обчислювального експерименту моделей операцій в матричних алгоритмах.

Ключові слова: *аналіз, взаємозв'язок, матрична модель, матричний алгоритм, операція криптографічного перетворення, операція додавання за модулем два.*

Вступ

Постановка проблеми. Захист інформації криптографічними методами залишається одним із найважливіших напрямів діяльності у сфері забезпечення безпеки інформації. Для здійснення основних криптографічних цілей, зокрема забезпечення конфіденційності, цілісності та аутентифікації інформації, необхідно постійно підвищувати ефективність криптографічних методів та алгоритмів, що, в першу чергу, зумовлено збільшенням (об'ємів даних, що передаються) пропускної здатності каналів передачі даних.

Отже, актуальною задачею є створення та вдосконалення алгоритмів криптографічного захисту, що використовують в своїй структурі функції криптографічного перетворення здатні обробляти дані великої розмірності. Одним із способів реалізації зазначених функцій є синтез на їх базі матричних моделей операцій криптографічного перетворення. Найчастіше базовими операціями функцій криптоперетворення є перестановки та заміни, а саме криптоперетворення полягає в додаванні до даних, що захищаються, деякої таємної інформації (ключа).

Враховуючи вище зазначене, постає проблема пошуку та синтезу інших операцій перетворення, які можливо застосовувати в якості операції криптографічного додавання з метою розширення множини функцій криптоперетворення.

Аналіз останніх досліджень і публікацій. У [1] запропоновано метод синтезу базових операцій криптографічного перетворення на основі заміщення однієї або декількох основних елементарних операцій зі збереженням інформативності.

У [2] описаний спосіб побудови математичної моделі матриці декодування з відомої матриці кодування на основі операції суми за модулем два.

Синтез та аналіз групи операцій дворозрядного криптографічного додавання за модулем два та доведення, що дана група операцій є групою перестановок і може бути використана для збільшення кількості операцій, що застосовуються у блокових та потокових шифрах представлено в [3].

У роботах [4, 5] представлені результати дослідження щодо використання операцій додавання за модулем два та перестановки для реалізації матричних операцій криптоперетворення, а також виявлено, що взаємозв'язки між операціями, що застосовуються для криптографічного перетворення на основі матричних моделей, характеризуються циклічністю. Проте в даних роботах відсутнє підтвердження коректності отриманих результатів, а саме обгрунтування правильності виявлених взаємозв'язків між операціями в матричних моделях, що потребує доведення на основі побудови відповідних їм моделей обернених операцій.

Мета статті – провести аналіз взаємозв'язків між прямими та оберненими матричними моделями операцій криптографічного перетворення інформації та підтвердити коректність синтезованих моделей операцій за результатами обчислювального експерименту.

Основний матеріал

Систематизовані результати обчислювального експерименту по дослідженню можливості використання операцій додавання за модулем два з точністю до перестановки операндів в матричних операціях (алгоритмах) криптографічного перетворення інформації були проаналізовані та наведені у вигляді таблиці (табл. 1, $O_i^{\oplus}$ – двохоперандна операція додавання за модулем два з урахуванням перестановки, i – номер операції; M_j^k – двохрозрядна матрична модель операції криптографічного перетворення з номером j, відібрана для обчислювального експерименту; $O_i^{\oplus} M_j^k$ – матрична модель операції криптографічного перетворення з операцією $O_i^{\oplus}$) [5].

Таблиця 1

Результати обчислювального експерименту

	M_1^k	M_2^k	M_3^k	M_4^k	M_5^k	M_6^k
$O_1^{\oplus}$	$O_1^{\oplus}\ M_1^k$	$O_1^{\oplus}\ M_2^k$	$O_1^{\oplus}\ M_3^k$	$O_1^{\oplus}\ M_4^k$	$O_1^{\oplus}\ M_6^k$	$O_1^{\oplus}\ M_5^k$
$O_2^{\oplus}$	$O_1^{\oplus}\ M_1^k$	$O_2^{\oplus}\ M_2^k$	$O_4^{\oplus}\ M_3^k$	$O_2^{\oplus}\ M_4^k$	$O_3^{\oplus}\ M_6^k$	$O_4^{\oplus}\ M_5^k$
$O_3^{\oplus}$	$O_1^{\oplus}\ M_1^k$	$O_4^{\oplus}\ M_2^k$	$O_3^{\oplus}\ M_3^k$	$O_3^{\oplus}\ M_4^k$	$O_4^{\oplus}\ M_6^k$	$O_2^{\oplus}\ M_5^k$
$O_4^{\oplus}$	$O_1^{\oplus}\ M_1^k$	$O_3^{\oplus}\ M_2^k$	$O_2^{\oplus}\ M_3^k$	$O_4^{\oplus}\ M_4^k$	$O_2^{\oplus}\ M_6^k$	$O_3^{\oplus}\ M_5^k$
$O_5^{\oplus}$	$O_1^{\oplus}\ M_1^k$	---	---	$O_5^{\oplus}\ M_4^k$	---	---

Проаналізуємо результати проведеного за допомогою спеціально розробленого програмного забезпечення обчислювального експерименту, які представлені в табл. 1. В роботах [4, 5] на основі аналізу моделей операцій криптографічного перетворення отримано підтвердження результатів теоретичних досліджень по встановленню взаємозв'язків між матричними алгоритмами та матричними операціями при їх взаємному використанні в криптоперетворенні інформації. Проте, отримані результати можна вважати достовірними лише тоді, коли доведена коректність результатів обчислювального експерименту. Адже на результат обчислювального експерименту могли впливати не лише збої обчислювальної техніки, а й помилки при розробці програмного забезпечення. Для перевірки коректності і правильності одержаних результатів обчислювального експерименту необхідно перейти до опису матричних моделей криптографічного перетворення, які дозволяють знаходити операції оберненого матричного криптографічного перетворення.

Матричні моделі криптографічного перетворення відібрані для обчислювального експерименту можна представити таким чином:

$$M^k_{1(3,5)} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ x_4^* \end{pmatrix}; \quad (1)$$

$$M^k_{2(6,5)} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \\ x_3^* \\ x_4^* \end{pmatrix}; \quad (2)$$

$$M^k_{3(3,6)} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \end{pmatrix} = \begin{pmatrix} x_1^* \\ x_2^* \\ x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \end{pmatrix}; \quad (3)$$

$$M^k_{4(5,3)} = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}; \quad (4)$$

$$M^k_{5(5,6)} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \end{pmatrix} = \begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \end{pmatrix}; \quad (5)$$

$$M^k_{6(6,3)} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix} = \begin{pmatrix} x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}. \quad (6)$$

Для знаходження матричних моделей операцій оберненого криптографічного перетворення скористаємося методом, що описаний в [2]. Алгоритм знаходження операції оберненого криптографічного перетворення буде заданий рівнянням (7) [2], де $a_{ij}, b_i \in [0,1]$ – коефіцієнти матриці прямого та оберненого перетворення відповідно, $x_1 \ldots x_n$ – операнди-розряди відповідно; $\oplus$ – операція «сума за mod 2».

$$\vec{F}_d = \begin{pmatrix} b_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n) \oplus \\ \oplus b_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n) \oplus \ldots \oplus \\ \oplus b_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{n\,n}x_n) \\ b_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n) \oplus \\ \oplus b_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n) \oplus \ldots \oplus \\ \oplus b_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{n\,n}x_n) \\ \ldots \\ b_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n) \oplus \\ \oplus b_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n) \oplus \ldots \oplus \\ \oplus b_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{n\,n}x_n) \end{pmatrix} = \quad (7)$$

$$= \begin{pmatrix} a_{11}x_1 & & & \\ & a_{22}x_2 & & \\ & & \ldots & \\ & & & a_{n\,n}x_n \end{pmatrix}.$$

Скористаємося виразом (7) для знаходження матричних моделей операцій оберненого криптографічного перетворення, що задані виразами (1-6):

$$M^k_{1(3,5)} = \begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ x_4^* \end{pmatrix}, \quad \text{тоді } M^d_{1(3,5)} = \begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ x_4^* \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix};$$

$$M^k_{2(6,5)} = \begin{pmatrix} x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \\ x_3^* \\ x_4^* \end{pmatrix}, \text{ тоді } M^d_{2(6,5)} = \begin{pmatrix} x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \\ x_3^* \\ x_4^* \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix};$$

$$M^k_{3(3,6)} = \begin{pmatrix} x_1^* \\ x_2^* \\ x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \end{pmatrix}, \text{ тоді } M^d_{3(3,6)} = \begin{pmatrix} x_1^* \\ x_2^* \\ x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \end{pmatrix} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \end{pmatrix};$$

$$M^k_{4(5,3)}=\begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}, \qquad \text{тоді } M^d_{4(5,3)}=\begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}=\begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \\ x_{12} \end{pmatrix}=\begin{pmatrix} x_2 \\ x_1 \end{pmatrix};$$

$$M^k_{5(5,6)}=\begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \end{pmatrix}, \text{ тоді } M^d_{5(5,6)}=\begin{pmatrix} x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}=\begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix};$$

$$M^k_{6(6,3)}=\begin{pmatrix} x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}, \text{ тоді } M^d_{6(6,3)}=\begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \end{pmatrix}=\begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix},$$

що відповідає результатам експерименту.

Наведені результати знаходження обернених операцій показали коректність запропонованого підходу щодо перевірки виявлених взаємозв'язків між прямими та оберненими матричними моделями операцій криптографічного перетворення інформації.

Скористаємося даним підходом для перевірки результатів обчислювального експерименту. Для цього введемо аналогічні позначення для операцій $O_1^{\oplus}$ – $O_4^{\oplus}$:

$$O_1^{\oplus}=\begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}=\begin{vmatrix} x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \end{vmatrix}=\begin{vmatrix} x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \end{vmatrix}; \qquad (8)$$

$$O_2^{\oplus}=\begin{vmatrix} x_1 \oplus y_2 \\ x_2 \oplus y_1 \end{vmatrix}=\begin{vmatrix} x_{11} \oplus x_{22} \\ x_{12} \oplus x_{21} \end{vmatrix}=\begin{vmatrix} x_1^* \oplus x_4^* \\ x_2^* \oplus x_3^* \end{vmatrix}; \qquad (9)$$

$$O_3^{\oplus}=\begin{vmatrix} x_2 \oplus y_1 \\ x_1 \oplus y_2 \end{vmatrix}=\begin{vmatrix} x_{12} \oplus x_{21} \\ x_{11} \oplus x_{22} \end{vmatrix}=\begin{vmatrix} x_2^* \oplus x_3^* \\ x_1^* \oplus x_4^* \end{vmatrix}; \qquad (10)$$

$$O_4^{\oplus}=\begin{vmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{vmatrix}=\begin{vmatrix} x_{12} \oplus x_{22} \\ x_{11} \oplus x_{21} \end{vmatrix}=\begin{vmatrix} x_2^* \oplus x_4^* \\ x_1^* \oplus x_3^* \end{vmatrix}. \qquad (11)$$

Введемо позначення $M^k_x\left|O^{\oplus}_y\right|$ де x – номер матричного алгоритму, y – номер операції. Якщо в матричних алгоритмах $M^k_{1(3,5)}$ - $M^k_{6(6,3)}$ використана операція $O_1^{\oplus}$ (8), тоді операції оберненого перетворення будуть відповідно до виразу (7) мати такий опис моделей як в табл. 2.

Таблиця 2

Операції оберненого перетворення з використаною операцією $O_1^{\oplus}$

Матричні алгоритми на основі операції $O_1^{\oplus}$ (8)	Операції оберненого перетворення згідно виразу (7)
$M^k_{1(3,5)}\left\|O_1^{\oplus}\right\|=\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}=\begin{pmatrix} x_{11} \\ x_{12} \\ x_{21} \\ x_{22} \end{pmatrix}=\begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ x_4^* \end{pmatrix}$	$M^d_{1(3,5)}\left\|O_1^{\oplus}\right\|=\begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ x_4^* \end{pmatrix}=\begin{pmatrix} x_{11} \\ x_{12} \\ x_{21} \\ x_{22} \end{pmatrix}=\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$
$M^k_{2(6,5)}\left\|O_1^{\oplus}\right\|=\begin{pmatrix} x_1\left\|O_1^{\oplus}\right\|x_2 \\ x_2 \end{pmatrix}=\begin{pmatrix} x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \\ x_{21} \\ x_{22} \end{pmatrix}=\begin{pmatrix} x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \\ x_3^* \\ x_4^* \end{pmatrix}$	$M^d_{2(6,5)}\left\|O_1^{\oplus}\right\|=\begin{pmatrix} x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \\ x_3^* \\ x_4^* \end{pmatrix}=\begin{pmatrix} x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \\ x_{21} \\ x_{22} \end{pmatrix}=\begin{pmatrix} x_1\left\|O_1^{\oplus}\right\|x_2 \\ x_2 \end{pmatrix}$
$M^k_{3(3,6)}\left\|O_1^{\oplus}\right\|=\begin{pmatrix} x_1 \\ x_1\left\|O_1^{\oplus}\right\|x_2 \end{pmatrix}=\begin{pmatrix} x_{11} \\ x_{12} \\ x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \end{pmatrix}=\begin{pmatrix} x_1^* \\ x_2^* \\ x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \end{pmatrix}$	$M^d_{3(3,6)}\left\|O_1^{\oplus}\right\|=\begin{pmatrix} x_1^* \\ x_2^* \\ x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \end{pmatrix}=\begin{pmatrix} x_{11} \\ x_{12} \\ x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \end{pmatrix}=\begin{pmatrix} x_1 \\ x_1\left\|O_1^{\oplus}\right\|x_2 \end{pmatrix}$
$M^k_{4(5,3)}\left\|O_1^{\oplus}\right\|=\begin{pmatrix} x_2 \\ x_1 \end{pmatrix}=\begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \\ x_{12} \end{pmatrix}=\begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}$	$M^d_{4(5,3)}\left\|O_1^{\oplus}\right\|=\begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}=\begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \\ x_{12} \end{pmatrix}=\begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$
$M^k_{5(5,6)}\left\|O_1^{\oplus}\right\|=\begin{pmatrix} x_2 \\ x_1\left\|O_1^{\oplus}\right\|x_2 \end{pmatrix}=\begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \end{pmatrix}=\begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \end{pmatrix}$	$M^d_{5(5,6)}\left\|O_1^{\oplus}\right\|=\begin{pmatrix} x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}=\begin{pmatrix} x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \\ x_{11} \\ x_{12} \end{pmatrix}=\begin{pmatrix} x_1\left\|O_1^{\oplus}\right\|x_2 \\ x_1 \end{pmatrix}$
$M^k_{6(6,3)}\left\|O_1^{\oplus}\right\|=\begin{pmatrix} x_1\left\|O_1^{\oplus}\right\|x_2 \\ x_1 \end{pmatrix}=\begin{pmatrix} x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \\ x_{11} \\ x_{12} \end{pmatrix}=\begin{pmatrix} x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}$	$M^d_{6(6,3)}\left\|O_1^{\oplus}\right\|=\begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \oplus x_3^* \\ x_2^* \oplus x_4^* \end{pmatrix}=\begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \oplus x_{21} \\ x_{12} \oplus x_{22} \end{pmatrix}=\begin{pmatrix} x_2 \\ x_1\left\|O_1^{\oplus}\right\|x_2 \end{pmatrix}$

Якщо в матричних алгоритмах $M^k_{1(3,5)} - M^k_{6(6,3)}$ використана операція $O_2^{\oplus}$ (9), тоді операції оберненого перетворення згідно виразу (7) представлені відповідно моделями (табл. 3).

Якщо в матричнних алгоритмах $M^k_{1(3,5)} - M^k_{6(6,3)}$ використана операція $O_3^{\oplus}$ (10), тоді операції оберненого перетворення будуть відповідно до виразу (7) представлені моделями (табл. 4).

Таблиця 3

Операції оберненого перетворення з використаною операцією $O_2^{\oplus}$

Матричні алгоритми на основі операції $O_2^{\oplus}$ (9)	Операції оберненого перетворення згідно виразу (7)
$M^k_{1(3,5)}\left\|O_2^{\oplus}\right\| = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ x_4^* \end{pmatrix}$	$M^d_{1(3,5)}\left\|O_2^{\oplus}\right\| = \begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ x_4^* \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$
$M^k_{2(6,5)}\left\|O_2^{\oplus}\right\| = \begin{pmatrix} x_1\left\|O_2^{\oplus}\right\|x_2 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_{11} \oplus x_{22} \\ x_{12} \oplus x_{21} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1^* \oplus x_4^* \\ x_2^* \oplus x_3^* \\ x_3^* \\ x_4^* \end{pmatrix}$	$M^d_{2(6,5)}\left\|O_2^{\oplus}\right\| = \begin{pmatrix} x_1^* \oplus x_4^* \\ x_2^* \oplus x_3^* \\ x_3^* \\ x_4^* \end{pmatrix} = \begin{pmatrix} x_{11} \oplus x_{22} \\ x_{12} \oplus x_{21} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1\left\|O_2^{\oplus}\right\|x_2 \\ x_2 \end{pmatrix}$
$M^k_{3(3,6)}\left\|O_2^{\oplus}\right\| = \begin{pmatrix} x_1 \\ x_1\left\|O_2^{\oplus}\right\|x_2 \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{11} \oplus x_{22} \\ x_{12} \oplus x_{21} \end{pmatrix} = \begin{pmatrix} x_1^* \\ x_2^* \\ x_1^* \oplus x_4^* \\ x_2^* \oplus x_3^* \end{pmatrix}$	$M^d_{3(3,6)}\left\|O_2^{\oplus}\right\| = \begin{pmatrix} x_1^* \\ x_2^* \\ x_1^* \oplus x_4^* \\ x_2^* \oplus x_3^* \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{11} \oplus x_{22} \\ x_{12} \oplus x_{21} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_1\left\|O_2^{\oplus}\right\|x_2 \end{pmatrix}$
$M^k_{4(5,3)}\left\|O_2^{\oplus}\right\| = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}$	$M^d_{4(5,3)}\left\|O_2^{\oplus}\right\| = \begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \\ x_2^* \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$
$M^k_{5(5,6)}\left\|O_2^{\oplus}\right\| = \begin{pmatrix} x_2 \\ x_1\left\|O_2^{\oplus}\right\|x_2 \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \oplus x_{22} \\ x_{12} \oplus x_{21} \end{pmatrix} = \begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \oplus x_4^* \\ x_2^* \oplus x_3^* \end{pmatrix}$	$M^d_{5(5,6)}\left\|O_2^{\oplus}\right\| = \begin{pmatrix} x_1^* \oplus x_4^* \\ x_2^* \oplus x_3^* \\ x_1^* \\ x_2^* \end{pmatrix} = \begin{pmatrix} x_{11} \oplus x_{22} \\ x_{12} \oplus x_{21} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_1\left\|O_2^{\oplus}\right\|x_2 \\ x_1 \end{pmatrix}$
$M^k_{6(6,3)}\left\|O_2^{\oplus}\right\| = \begin{pmatrix} x_1\left\|O_2^{\oplus}\right\|x_2 \\ x_1 \end{pmatrix} = \begin{pmatrix} x_{11} \oplus x_{22} \\ x_{12} \oplus x_{21} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_1^* \oplus x_4^* \\ x_2^* \oplus x_3^* \\ x_1^* \\ x_2^* \end{pmatrix}$	$M^d_{6(6,3)}\left\|O_2^{\oplus}\right\| = \begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \oplus x_4^* \\ x_2^* \oplus x_3^* \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \oplus x_{22} \\ x_{12} \oplus x_{21} \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1\left\|O_2^{\oplus}\right\|x_2 \end{pmatrix}$

Таблиця 4

Операції оберненого перетворення з використаною операцією $O_3^{\oplus}$

Матричні алгоритми на основі операції $O_3^{\oplus}$ (10)	Операції оберненого перетворення згідно виразу (7)
$M^k_{1(3,5)}\left\|O_3^{\oplus}\right\| = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ x_4^* \end{pmatrix}$	$M^d_{1(3,5)}\left\|O_3^{\oplus}\right\| = \begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ x_4^* \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$
$M^k_{2(6,5)}\left\|O_3^{\oplus}\right\| = \begin{pmatrix} x_1\left\|O_3^{\oplus}\right\|x_2 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_{12} \oplus x_{21} \\ x_{11} \oplus x_{22} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_2^* \oplus x_3^* \\ x_1^* \oplus x_4^* \\ x_3^* \\ x_4^* \end{pmatrix}$	$M^d_{2(6,5)}\left\|O_3^{\oplus}\right\| = \begin{pmatrix} x_2^* \oplus x_3^* \\ x_1^* \oplus x_4^* \\ x_3^* \\ x_4^* \end{pmatrix} = \begin{pmatrix} x_{12} \oplus x_{21} \\ x_{11} \oplus x_{22} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1\left\|O_3^{\oplus}\right\|x_2 \\ x_2 \end{pmatrix}$

Закінчення табл. 4

Матричні алгоритми на основі операції $O_3^{\oplus}$ (10)	Операції оберненого перетворення згідно виразу (7)
$M^k_{3(3,6)}\left\|O_3^{\oplus}\right\| = \begin{pmatrix} x_1 \\ x_1\left\|O_3^{\oplus}\right\|x_2 \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{12}\oplus x_{21} \\ x_{11}\oplus x_{22} \end{pmatrix} = \begin{pmatrix} x_1^* \\ x_2^* \\ x_2^*\oplus x_3^* \\ x_1^*\oplus x_4^* \end{pmatrix}$	$M^d_{3(3,6)}\left\|O_3^{\oplus}\right\| = \begin{pmatrix} x_1^* \\ x_2^* \\ x_2^*\oplus x_3^* \\ x_1^*\oplus x_4^* \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{12}\oplus x_{21} \\ x_{11}\oplus x_{22} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_1\left\|O_3^{\oplus}\right\|x_2 \end{pmatrix}$
$M^k_{4(5,3)}\left\|O_3^{\oplus}\right\| = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}$	$M^d_{4(5,3)}\left\|O_3^{\oplus}\right\| = \begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \\ x_2^* \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$
$M^k_{5(5,6)}\left\|O_3^{\oplus}\right\| = \begin{pmatrix} x_2 \\ x_1\left\|O_3^{\oplus}\right\|x_2 \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{12}\oplus x_{21} \\ x_{11}\oplus x_{22} \end{pmatrix} = \begin{pmatrix} x_3^* \\ x_4^* \\ x_2^*\oplus x_3^* \\ x_1^*\oplus x_4^* \end{pmatrix}$	$M^d_{5(5,6)}\left\|O_3^{\oplus}\right\| = \begin{pmatrix} x_2^*\oplus x_3^* \\ x_1^*\oplus x_4^* \\ x_1^* \\ x_2^* \end{pmatrix} = \begin{pmatrix} x_{12}\oplus x_{21} \\ x_{11}\oplus x_{22} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_1\left\|O_3^{\oplus}\right\|x_2 \\ x_1 \end{pmatrix}$
$M^k_{6(6,3)}\left\|O_3^{\oplus}\right\| = \begin{pmatrix} x_1\left\|O_3^{\oplus}\right\|x_2 \\ x_1 \end{pmatrix} = \begin{pmatrix} x_{12}\oplus x_{21} \\ x_{11}\oplus x_{22} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_2^*\oplus x_3^* \\ x_1^*\oplus x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}$	$M^d_{6(6,3)}\left\|O_3^{\oplus}\right\| = \begin{pmatrix} x_3^* \\ x_4^* \\ x_2^*\oplus x_3^* \\ x_1^*\oplus x_4^* \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{12}\oplus x_{21} \\ x_{11}\oplus x_{22} \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1\left\|O_3^{\oplus}\right\|x_2 \end{pmatrix}$

Якщо в матричнних алгоритмах $M^k_{1(3,5)} - M^k_{6(6,3)}$ використана операція $O_4^{\oplus}$ (11), тоді операції оберненого перетворення будуть відповідно до виразу (7) представлені моделями, котрі описані в табл. 5.

Таблиця 5

Операції оберненого перетворення з використаною операцією $O_4^{\oplus}$

Матричні алгоритми на основі операції $O_4^{\oplus}$ (11)	Операції оберненого перетворення відповідно до виразу (7)
$M^k_{1(3,5)}\left\|O_4^{\oplus}\right\| = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ x_4^* \end{pmatrix}$	$M^d_{1(3,5)}\left\|O_4^{\oplus}\right\| = \begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ x_4^* \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$
$M^k_{2(6,5)}\left\|O_4^{\oplus}\right\| = \begin{pmatrix} x_1\left\|O_4^{\oplus}\right\|x_2 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_{12}\oplus x_{22} \\ x_{11}\oplus x_{21} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_2^*\oplus x_4^* \\ x_1^*\oplus x_3^* \\ x_3^* \\ x_4^* \end{pmatrix}$	$M^d_{2(6,5)}\left\|O_4^{\oplus}\right\| = \begin{pmatrix} x_2^*\oplus x_4^* \\ x_1^*\oplus x_3^* \\ x_3^* \\ x_4^* \end{pmatrix} = \begin{pmatrix} x_{12}\oplus x_{22} \\ x_{11}\oplus x_{21} \\ x_{21} \\ x_{22} \end{pmatrix} = \begin{pmatrix} x_1\left\|O_4^{\oplus}\right\|x_2 \\ x_2 \end{pmatrix}$
$M^k_{3(3,6)}\left\|O_4^{\oplus}\right\| = \begin{pmatrix} x_1 \\ x_1\left\|O_4^{\oplus}\right\|x_2 \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{12}\oplus x_{22} \\ x_{11}\oplus x_{21} \end{pmatrix} = \begin{pmatrix} x_1^* \\ x_2^* \\ x_2^*\oplus x_4^* \\ x_1^*\oplus x_3^* \end{pmatrix}$	$M^d_{3(3,6)}\left\|O_4^{\oplus}\right\| = \begin{pmatrix} x_1^* \\ x_2^* \\ x_2^*\oplus x_4^* \\ x_1^*\oplus x_3^* \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{12}\oplus x_{22} \\ x_{11}\oplus x_{21} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_1\left\|O_4^{\oplus}\right\|x_2 \end{pmatrix}$
$M^k_{4(5,3)}\left\|O_4^{\oplus}\right\| = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \\ x_2^* \end{pmatrix}$	$M^d_{4(5,3)}\left\|O_4^{\oplus}\right\| = \begin{pmatrix} x_3^* \\ x_4^* \\ x_1^* \\ x_2^* \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$
$M^k_{5(5,6)}\left\|O_4^{\oplus}\right\| = \begin{pmatrix} x_2 \\ x_1\left\|O_4^{\oplus}\right\|x_2 \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{12}\oplus x_{22} \\ x_{11}\oplus x_{21} \end{pmatrix} = \begin{pmatrix} x_3^* \\ x_4^* \\ x_2^*\oplus x_4^* \\ x_1^*\oplus x_3^* \end{pmatrix}$	$M^d_{5(5,6)}\left\|O_4^{\oplus}\right\| = \begin{pmatrix} x_2^*\oplus x_4^* \\ x_1^*\oplus x_3^* \\ x_1^* \\ x_2^* \end{pmatrix} = \begin{pmatrix} x_{12}\oplus x_{22} \\ x_{11}\oplus x_{21} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_1\left\|O_4^{\oplus}\right\|x_2 \\ x_1 \end{pmatrix}$

Закінчення табл. 5

Матричні алгоритми на основі операції $O_4^{\oplus}$ (11)	Операції оберненого перетворення відповідно до виразу (7)
$M^{k}_{6(6,3)}\left\|O_4^{\oplus}\right\| = \begin{pmatrix} x_1 \left\| O_4^{\oplus} \right\| x_2 \\ x_1 \end{pmatrix} = \begin{pmatrix} x_{12} \oplus x_{22} \\ x_{11} \oplus x_{21} \\ x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_2^* \oplus x_4^* \\ x_1^* \oplus x_3^* \\ x_1^* \\ x_2^* \end{pmatrix}$	$M^{d}_{6(6,3)}\left\|O_4^{\oplus}\right\| = \begin{pmatrix} x_3^* \\ x_4^* \\ x_2^* \oplus x_4^* \\ x_1^* \oplus x_3^* \end{pmatrix} = \begin{pmatrix} x_{21} \\ x_{22} \\ x_{12} \oplus x_{22} \\ x_{11} \oplus x_{21} \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \left\| O_4^{\oplus} \right\| x_2 \end{pmatrix}$

Наведені перетворення доводять коректність отриманих результатів обчислювального експерименту, а також підтверджують результати теоретичних досліджень по встановленню взаємозв'язків між матричними алгоритмами та матричними операціями при їх взаємному використанні в криптоперетворенні інформації.

Висновки

В статті здійснено аналіз результатів використання операцій додавання за модулем два з точністю до перестановки операндів в матричних операціях криптографічного перетворення інформації, що підтвердило коректність виявлених взаємозв'язків між операціями.

На основі методу синтезу операцій оберненого матричного криптографічного перетворення доведено збіжність теоретичних та експериментальних результатів досліджень, що отримані при виявлені взаємозв'язків між матричними алгоритмами та матричними операціями в моделях операцій криптографічного перетворення.

Список літератури

1. Голуб С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два / С. В. Голуб, В. Г. Бабенко, С. В. Рудницький // Системи обробки інформації : зб. наук. праць. – Вип. 3 (101), т. 1. – Х. : ХУПС ім. І. Кожедуба, 2012. – С. 119–122.

2. Рудницький В.М. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації / В.М. Рудницький, В.Г. Бабенко, С.В. Рудницький // Збірник наукових праць Харківського університету Повітряних Сил – Х.: ХУПС ім. І. Кожедуба, 2012. – Випуск 4(33). – С. 198-200.

3. Бабенко В.Г. Синтез і аналіз операцій криптографічного додавання за модулем два / В.Г. Бабенко, Н.В. Лада // Системи обробки інформації: зб. наук. пр. – Харків: ХУПС ім. І. Кожедуба. – 2014. – Вип. 2(118) – С. 116-118.

4. Бабенко В.Г. Аналіз множини операцій синтезованих на основі додавання за модулем два / В.Г. Бабенко, Н.В. Лада, С.В. Лада // Методи та засоби кодування, захисту й ущільнення інформації: тези доп. П'ятої міжнародної науково-практичної конференції, 19-21 квітня 2016 року. – Вінниця: ВНТУ, 2016. – С. 54-57.

5. Бабенко В.Г. Дослідження взаємозв'язків між операціями в матричних моделях криптографічного перетворення / В.Г. Бабенко, Н.В. Лада, С.В. Лада // Вісник ЧДТУ, 2016. – №1. – С. 5-11.

Надійшла до редколегії 16.09.2015

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

АНАЛИЗ КОРРЕКТНОСТИ ВЗАИМОСВЯЗЕЙ МЕЖДУ ПРЯМЫМИ И ОБРАТНЫМИ МАТРИЧНЫМИ МОДЕЛЯМИ ОПЕРАЦИЙ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ

Н.В. Лада

В статье осуществлен анализ результатов вычислительного эксперимента по моделированию прямых и обратных операций криптопреобразования для использования в матричных алгоритмах. Проведен анализ и исследование взаимосвязей между прямыми и обратными матричными моделями операций криптографического преобразования информации. Доказано корректность использования синтезированных по результатам вычислительного эксперимента моделей операций в матричных алгоритмах.

Ключевые слова: *анализ, взаимосвязь, матричная модель, матричный алгоритм, операция криптографического преобразования, операция сложения по модулю два.*

ANALYSIS OF CORRECTNESS OF RELATIONSHIP BETWEEN DIRECT AND INVERSE MATRIX MODELS OF CRYPTOGRAPHIC INFORMATION TRANSFORMATION OPERATIONS

N.V. Lada

The article analyzes the results of a computational experiment on modeling direct and inverse operations of cryptographic transformation for use in matrix algorithms. The analysis and investigation of the relationship between direct and inverse matrix models of cryptographic information transformation operations. It proved the correctness of the use of synthesized according to the results of computational experiment models of operations of matrix algorithms.

Keywords: *analysis, relationship, matrix model, the matrix algorithm, operations of cryptographic transformation, the operation of addition modulo two.*