УДК 003.26:004.056.55

В. Г. Бабенко[1], *к.т.н., доцент,*
доцент кафедри інформаційної безпеки та комп'ютерної інженерії
e-mail: zolot_verba@rambler.ru
Н. В. Лада[1], *аспірант*,
e-mail: LadaHatali256@gmail.com
С. В. Лада[2], *аспірант*
e-mail: raphaello1986@gmail.com
[1]Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
[2]Черкаський національний університет ім. Б. Хмельницького
б-р Шевченка, 81, м. Черкаси, Україна

ДОСЛІДЖЕННЯ ВЗАЄМОЗВ'ЯЗКІВ МІЖ ОПЕРАЦІЯМИ В МАТРИЧНИХ МОДЕЛЯХ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

У статті представлено результати дослідження з використання операцій додавання за модулем два та перестановки для реалізації матричних операцій криптоперетворення. За результатами проведеного обчислювального експерименту здійснено поділ матричних моделей криптоперетворення на три групи за наявністю та типом перестановки в них. У ході аналізу одержаних результатів експерименту виявлено, що взаємозв'язки між операціями, що застосовуються для криптографічного перетворення на основі матричних моделей, характеризуються циклічністю. Отримані цикли послідовності застосування операцій дозволяють будувати операції прямого та оберненого криптоперетворення в групі дворозрядних матричних операцій при використанні запропонованих двоопераднних операцій.

Ключові слова: *криптографічне перетворення, операція, матрична модель, взаємозв'язки, пряме та обернене перетворення, перестановка, група, цикл, симетричне та несиметричне перетворення, шифрування, розшифрування, базова матриця, ліва та права підстановка.*

Постановка проблеми. Криптографічне шифрування інформації проводиться на основі виконання послідовності операцій криптографічного перетворення. З метою розшифрування зашифрованої інформації необхідно знати послідовність виконання операцій для розшифрування інформації. Необхідно відзначити, що при симетричному криптоперетворенні послідовності шифрування і розшифрування збігаються, а при несиметричному криптоперетворенні послідовності шифрування і розшифрування не збігаються. При розшифруванні зашифрованої інформації зловмисник повинен побудувати послідовність операцій для розшифрування зашифрованої інформації. Складність цієї задачі напряму залежить від довжини послідовності та кількості операцій криптографічного перетворення, які в ній використовуються.

Виходячи з цього, можна стверджувати, що збільшення кількості операцій, придатних для криптографічного перетворення інформації, дозволить будувати алгоритми захисту інформації з кращими криптографічними властивостями.

Аналіз останніх досліджень. Особливу увагу у сучасних друкованих виданнях приділено застосовуванню матричних операцій криптографічного перетворення та криптопримітивів, побудованих на їх основі, для алгоритмів захисту інформаційних ресурсів [1–4].

Серед останніх досліджень і публікацій варто виділити дослідження матричних операцій криптографічного перетворення, синтезованих на основі операції додавання за модулем [1, 2], синтез і аналіз операцій двоопераднього криптографічного додавання за модулем два та чотири [1, 4], які можна використовувати для здійснення криптографічного перетворення [3]. Зокрема, в [4] синтезовано групу операцій додавання за модулем два та доведено, що вона є групою перестановок, показано її придатність для використання в алгоритмах криптографічного перетворення.

Проте в цих дослідженнях не було проведено аналізу зв'язків операцій в матричних

операціях криптографічного перетворення для реалізації кодування та розкодування інформації. Отже, дослідження взаємозв'язків між операціями, що використовуються в матричних операціях криптоперетворення, є, безперечно, актуальною темою дослідження.

Метою цього дослідження є виявлення взаємозв'язків між операціями в матричних моделях прямого та оберненого криптографічного перетворення.

Виклад основного матеріалу. Дослідимо можливість використання п'яти моделей операцій додавання за модулем два (операції 1–5, табл. 1) для реалізації матричних операцій криптоперетворення на прикладі групи з шести дворозрядних операцій матричного криптографічного перетворення (операції 1–6, табл. 2) [1].

При проведенні обчислювального експерименту обмежимося лише поєднанням операцій базової групи та операцій перестановки.

Будемо розглядати ці операції як матричні моделі (матриці) криптографічного перетворення із застосуванням у них відібраних п'яти операцій додавання за модулем два.

Таблиця 1

Основні операції

Модель операції				
$O_1^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$	$O_2^{\oplus} = \begin{vmatrix} x_1 \oplus y_2 \\ x_2 \oplus y_1 \end{vmatrix}$	$O_3^{\oplus} = \begin{vmatrix} x_2 \oplus y_1 \\ x_1 \oplus y_2 \end{vmatrix}$	$O_4^{\oplus} = \begin{vmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{vmatrix}$	$O_5^{\oplus} = \begin{vmatrix} x_1 \oplus x_2 \\ y_1 \oplus y_2 \end{vmatrix}$

Таблиця 2

Матричні моделі криптографічного перетворення, відібрані для обчислювального експерименту

Номер матриці для перетворення	Кодування	Розкодування
1	$M_1^k = F_{3,5}^d = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$	$M_1^d = F_{3,5}^d = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$
2	$M_2^k = F_{6,5}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix}$	$M_2^d = F_{6,5}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix}$
3	$M_3^k = F_{3,6}^k = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \end{pmatrix}$	$M_3^d = F_{3,6}^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \end{pmatrix}$
4	$M_4^k = F_{5,3}^k = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$	$M_4^d = F_{5,3}^d = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$
5	$M_5^k = F_{5,6}^k = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix}$	$M_5^d = F_{5,6}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix}$
6	$M_6^k = F_{6,3}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix}$	$M_6^d \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix}$

Систематизовані результати обчислювального експерименту наведені в табл. 3, де використані такі позначення: $O_i^{\oplus}$ – двоопераднa операція додавання за модулем два з урахуванням перестановки, i – номер операції (згідно з табл. 1); M_j^k – дворозрядна матрична модель операції криптографічного перетворення, j – номер моделі (згідно з табл. 2); $O_i^{\oplus} M_j^k$ – матрична модель операції криптографічного перетворення, в якій використана операція $O_i^{\oplus}$.

Таблиця 3

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 наведені в табл. 3. Можемо відзначити, що деякі з матриць для перетворення належать до повного симетричного криптоперетворення (M_1^k, M_4^k): послідовності шифрування і розшифрування збігаються для всієї групи операцій, а деякі – до частково несиметричного криптоперетворення: послідовності шифрування і розшифрування не збігаються. А саме, симетричними криптоперетворення M_2^k будуть для операцій $O_1^{\oplus}$, $O_2^{\oplus}$; M_3^k – для операцій $O_1^{\oplus}$, $O_3^{\oplus}$. Оскільки для M_5^k та M_6^k послідовності шифрування і розшифрування збігаються лише для операції $O_1^{\oplus}$, що є базовою операцією, то ці матриці можемо умовно віднести до групи матриць для перетворення, що належать до повного несиметричного криптоперетворення. Крім того, при шифруванні M_5^k та M_6^k для їх розшифрування на операціях $O_2^{\oplus}$, $O_3^{\oplus}$, $O_4^{\oplus}$, окрім зміни операції, змінюється і матриця розшифрування.

Припустимо, що це ділення на три групи пов'язане з поділом даних матриць для перетворення за наявністю і типом перестановки в них.

Усі дані матриці належать до множини $Mn(R)$ усіх квадратних дійсних матриць порядку n із бінарними діями додавання, множення, унарними – взяття протилежної матриці, транспонування і 0-арними – виділеними нульовою матрицею 0 та одиничною матрицею E, де $n = 2$ [5].

Розглянемо групу матриць для перетворення, що належать до повного симетричного криптоперетворення (M_1^k, M_4^k). Матриці для перетворення складаються з множини M, із заданим на ній певним набором алгебраїчних дій (ωi), $i \in$ I (можливо, різної арності), а набір {арн $\omega i \mid i \in$I} – її типом. Зазвичай позначається M; $(\omega i) i \in$ I [5].

Припустимо, M_1^k є базовою матрицею, тоді дана матриця є матрицею з 0-арними діями (0-арна дія – це просто виділення певного елемента, наприклад, 0 або 1 у полі, в нашому випадку x_1 та x_2):

$$M_1^k = F_{3,5}^k = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \{x_1, x_2\}.$$

Тоді матриця M_4^k буде матрицею з діями арності 1, унарною матрицею – взяття протилежної матриці, оскільки в даній матриці реалізована базова перестановка – взяття протилежної матриці:

$$\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \rightarrow \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}\right).$$

Дії арності 1 (їх ще називають унарними) трапляються досить часто, наприклад, взяття протилежного або оберненого елемента, взяття цілої або дробової частини числа, перехід до транспонованої матриці чи до спряженого числа. Дії арності ≥ 3 трапляються рідко [5].

Розглянемо групу матриць для перетворення, що належать до частково несиметричного криптоперетворення (M_2^k, M_3^k). В основі даних матриць є базова матриця з 0-арними діями. Оскільки $x_1 + x_2 = x_2 + x_1$, то додавання до базової матриці x_1 назвемо лівою підстановкою, а додавання до базової матриці x_2 – правою підстановкою. Звідси легко бачити, що

матриця M_2^k буде базовою матрицею з правою підстановкою, а M_3^k, відповідно, – базовою матрицею з лівою підстановкою.

Розглянемо групу матриць для перетворення, що належать до повного несиметричного криптоперетворення (M_5^k, M_6^k). В основі даних матриць є унарна матриця. За аналогією до групи матриць для перетворення, що належать до частково несиметричного криптоперетворення, матриця M_5^k буде унарною матрицею з правою підстановкою, а M_6^k, відповідно, – унарною базовою матрицею з лівою підстановкою.

Більш детально зупинимося на операціях, що використовуються в матричних моделях операцій криптографічного перетворення. Нехай операція криптоперетворення $O_1^{\oplus}$ буде операцією з базовим розміщенням елементів x_i, y_i, $i \in \{1,2\}$, оскільки розміщення x_i збігається з розміщенням у базовій матриці для перетворення. Тоді $O_2^{\oplus}$ буде операцією з базовим розміщенням x_i і перестановкою y_i, $O_3^{\oplus}$ – буде операцією з перестановкою x_i і базовим розміщенням y_i, а $O_4^{\oplus}$ – операцією з перестановкою як x_i, так і y_i.

Враховуючи вищенаведене, побудуємо цикли для здійснення криптоперетворення на базі матричних моделей операцій криптографічного перетворення $O_i^{\oplus} M_j^k$.

Для M_2^k операція криптоперетворення $O_3^{\oplus}$, операція з перестановкою x_i, розкодовується операцією $O_4^{\oplus}$, а операція криптоперетворення $O_4^{\oplus}$, навпаки, розкодовується операцією $O_3^{\oplus}$, тобто для M_2^k маємо подвійний цикл криптоперетворення (рис. 1):

$$M_2^k\ O_3^{\oplus} \rightarrow M_2^k\ O_4^{\oplus} \rightarrow M_2^k\ O_3^{\oplus}.$$

Аналогічно для M_3^k операція криптоперетворення $O_2^{\oplus}$, операція з перестановкою y_i, розкодовується операцією $O_4^{\oplus}$, а операція криптоперетворення $O_4^{\oplus}$, навпаки, розкодовується операцією $O_2^{\oplus}$, тобто для M_3^k маємо подвійний цикл криптоперетворення (рис. 2).

$$M_3^k\ O_2^{\oplus} \rightarrow M_3^k\ O_4^{\oplus} \rightarrow M_3^k\ O_2^{\oplus}.$$

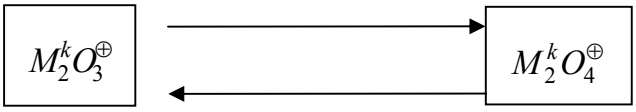

Рис. 1. Подвійний цикл криптоперетворення для матриці M_2^k

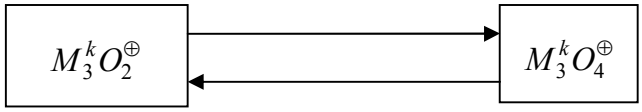

Рис. 2. Подвійний цикл криптоперетворення для матриці M_3^k

Можемо відзначити, що для обох матриць даної групи спільною частиною циклу також буде операція $O_4^{\oplus}$, операція з перестановкою як x_i, так і y_i.

Для M_5^k операція криптоперетворення $O_2^{\oplus}$, операція з перестановкою y_i, розкодовується операцією $O_3^{\oplus}$, операцією з перестановкою x_i, а операція криптоперетворення $O_3^{\oplus}$ розкодовується операцією $O_4^{\oplus}$, яка, в свою чергу, розкодовується операцією $O_2^{\oplus}$, тобто для M_5^k маємо, на відміну від подвійного циклу, в групі з матриць для перетворення, що належать до частково несиметричного криптоперетворення, потрійний цикл криптоперетворення (рис. 3):

$$M_5^k\ O_2^{\oplus} \to M_5^k\ O_3^{\oplus} \to M_5^k\ O_4^{\oplus} \to M_5^k\ O_2^{\oplus}.$$

Аналогічно, для M_6^k операція криптоперетворення $O_2^{\oplus}$, операція з перестановкою y_i, розкодовується операцією $O_4^{\oplus}$, а операція криптоперетворення $O_4^{\oplus}$ розкодовується операцією $O_3^{\oplus}$, операцією з перестановкою x_i, яка, в свою чергу, розкодовується операцією $O_2^{\oplus}$, тобто для M_6^k також маємо аналогічно до M_5^k потрійний цикл криптоперетворення (рис. 4):

$$M_6^k\ O_2^{\oplus} \to M_6^k\ O_4^{\oplus} \to M_6^k\ O_3^{\oplus} \to M_6^k\ O_2^{\oplus}.$$

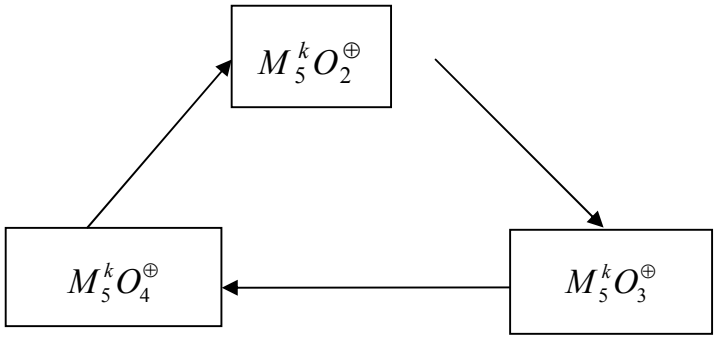

Рис. 3. Потрійний цикл криптоперетворення для матриці M_5^k

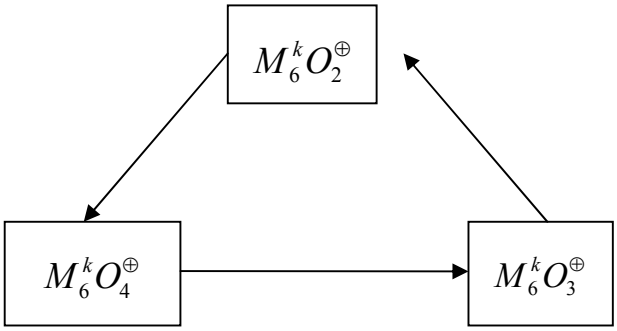

Рис. 4. Потрійний цикл криптоперетворення для матриці M_6^k

Крім того, цикл криптоперетворень для M_6^k буде оберненим до циклу криптоперетворень для M_5^k. Це пояснюється тим, що і для розшифрування криптоперетворення матриці M_5^k буде матриця M_6^k, і для розшифрування криптоперетворення матриці M_6^k – матриця M_5^k, тому що $M_5^d = M_6^k$, а $M_6^d = M_5^k$.

Наведені цикли дозволяють будувати операції прямого та оберненого криптоперетворення в групі дворозрядних матричних операцій з використанням запропонованих двоопераднних операцій.

Висновки. За результатами проведеного обчислювального експерименту здійснено поділ матричних моделей криптоперетворення на три групи за наявністю та типом перестановки в них.

У ході аналізу одержаних результатів експерименту виявлено, що взаємозв'язки між операціями, що застосовуються для криптографічного перетворення на основі матричних моделей, характеризуються циклічністю.

Отримані цикли послідовності застосування операцій дозволяють будувати операції прямого та оберненого криптоперетворення в групі дворозрядних матричних операцій з використанням запропонованих двоопераднних операцій.

Список літератури

1. Бабенко В. Г. Синтез і аналіз операцій криптографічного додавання за модулем два / В. Г. Бабенко, Н. В. Лада // Системи обробки інформації : зб. наук. праць. – Вип. 2 (118). – Х. : ХУПС ім. І. Кожедуба, 2014. –С. 116–118.
2. Бабенко В. Г. Дослідження матричних операцій криптографічного перетворення на основі арифметичних операцій за модулем / В. Г. Бабенко // Системи управління, навігації та зв'язку : зб. наук. праць. – Вип. 4 (24). – К., 2012. – С. 85–88.
3. 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.
4. Криптографическое кодирование : [кол. монография] / под ред. В. Н. Рудницкого, В. Я. Мильчевича. – Х. : Щедрая усадьба плюс, 2014. – 240 с.
5. Ганюшкін О. Г. Теорія груп : навч. посіб. для студ. мех.-мат. факультету / О. Г. Ганюшкін, О. О. Безущак. – К. : Вид.-поліграф. центр «Київський університет», 2005. – 123 с.

References

1. Babenko, V. G. and Lada, N. V. (2014). Synthesis and analysis of cryptographic addition operations modulo two. *Systemy obrobky informaciyi*, 2 (118), pp. 116–118 [in Ukrainian].
2. Babenko, V. G. (2012). The research of matrix operations of cryptographic transformation based on arithmetic modulo. *Systemy upravlinnya, navigatsiyi ta zvyazku*, 4 (24), pp. 85–88 [in Ukrainian].
3. Golub, S. V., Babenko, V. G. and Rudnytsky, S. V. (2012). The method of synthesis of cryptographic transformation operations based on addition modulo two. *Systemy obrobky informaciyi*, 3 (101), vol. 1, pp. 119–122 [in Ukrainian].
4. Rudnicki, V. N. and Milchevich, V. Ya (eds.) (2014) The cryptographic coding: collective monograph. Kharkov : Schedraya usadba plus, 240 p. [in Russian].
5. Ganyushkin, O. G. and Bezuschak, O. O. (2005) Groups theory: manual for students of mechanics and mathematics faculty. Kyiv: Vydav.-poligraf. tsentr "Kyivskyy universytet", 123 p. [in Ukrainian].

V. G. Babenko[1], *Ph.D., associate professor,*
associate professor of information security and computer engineering chair
e-mail: zolot_verba@rambler.ru
N. V. Lada[1], *postgraduate student,*
e-mail: LadaHatali256@gmail.com
S. V. Lada[2], *postgraduate student*
e-mail: raphaello1986@gmail.com
[1]Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine
[2]Bohdan Khmelnytsky National University of Cherkasy
Shevchenko blvd, 81, Cherkasy, Ukraine

RESEARCH OF THE RELATIONSHIPS BETWEEN THE OPERATIONS IN MATRIX MODELS OF CRYPTOGRAPHIC TRANSFORMATION

Introduction. *Data encryption is based on the sequence of cryptographic transformation operations. To decrypt the encrypted data it is necessary to know the sequence of operations for information decrypting. Therefore, an increase in the number of operations suitable for cryptographic transformation of information would allow to build data protection algorithms with better cryptographic properties.*

The purpose of scientific work. *The objective of this research is to identify the relationships between operations in matrix models of direct and reverse cryptographic transformation.*

Formulation of the problem. *In modern printed editions special attention is given to the use of matrix operations of cryptographic transformation and cryptographic primitives, based on them, for the algorithms of information resources protection. However, in these studies, the analysis of the relationships in matrix operations of cryptographic transformation has not been done to implement the encoding and decoding of information.*

The main material. *The article presents the results of the research on the use of the operations of addition modulo two and permutations to implement matrix operations of cryptographic transformation. According to the results of computational experiment the division of matrix models of cryptographic transformation into three groups according to the presence and type of permutation in them: full symmetric cryptographic transformation, the sequences of encryption and decryption operations in which are the same for the whole group; partially asymmetric cryptographic transformation, where the sequences of encryption and decryption operations are not the same; conditional full asymmetric cryptographic transformation, in some models, apart from changing the operation, changing matrix decryption, is carried out.*

During the analysis of the results of the experiment it is revealed that the relationships between the operations, which are used for cryptographic transformation based on matrix models, are characterized by cycles.

Conclusions. *The received cycles of the sequences of operations allow to build direct and reverse cryptographic transformation in a group of two-digit matrix operations using the proposed two-operand operations.*

Keywords: *cryptographic transformation, operation, matrix model, relationships, direct and reverse transformation, permutation, group, cycle, symmetric and asymmetric transformation, encryption, decryption, basic matrix, left and right substitution.*

Рецензенти: С. В. Голуб, д.т.н., професор,
В. М. Рудницький, д.т.н., професор