УДК 004. 056.55:004.312.2 **doi: 10.26906/SUNZ.2020.1.093**

Н. В. Лада[1], С. В. Рудницький[1], В. М.Зажома[2], Ю. В. Рудницька[1]

[1] Черкаський державний технологічний університет, Черкаси, Україна
[2] Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля, Черкаси, Україна

# ДОСЛІДЖЕННЯ І СИНТЕЗ ГРУПИ СИМЕТРИЧНИХ МОДИФІКОВАНИХ ОПЕРАЦІЙ ПРАВОСТОРОННЬОГО ДОДАВАННЯ ЗА МОДУЛЕМ ЧОТИРИ

**Анотація.** В статті представлено основні результати дослідження і синтезу групи двохоперандних двохрозрядних симетричних операцій правостороннього додавання за модулем чотири шляхом використання групи двохрозрядних одноопераднних операцій крипто перетворення. Синтез групи операцій на основі операції правостороннього додавання за модулем чотири, раніше не досліджувався. Встановлено, що побудована група операцій криптографічних перетворень відрізняється від груп криптоопераций побудованих на основі додавання за модулем два та класичним лівостороннім додаванням за модулем чотири. Використання нової синтезованої групи дає змогу підвищити якість потокового шифрування за рахунок збільшення варіативності криптографічних перетворень. Встановлено, що за рахунок симетричних синтезованих операцій в системах потокового шифрування буде використовуватися додатково до двадцяти чотирьох таблиць підстановки.

**Ключові слова**: криптографічна операція, модифікації операцій, математична група операцій, додавання за модулем, моделі операції, потокове шифрування.

## Вступ

**Постановка проблеми.** На сьогоднішній день ні у кого не викликає сумнівів, що інформація посідає провідне місце в життєдіяльності людства. В свою чергу надійний захист інформаційних ресурсів є запорукою інформаційної безпеки як кожної людини так і держав в цілому. Тенденція постійного збільшення обсягів інформації, що обробляється, зберігається та передається в інформаційних системах вимагає вирішення проблеми підвищення швидкодії систем захисту інформації [1, 2]. Одним з основних напрямків захисту інформації були і залишаються криптографічні методи її захисту [3, 4]. Особливо актуальними в наш час стають дослідження спрямовані на збільшення швидкодії та надійності засобів криптографічних обчислень, придатних до застосування в постквантовій криптографії.

Однією з тенденцій покращення якості алгоритмів сучасної комп'ютерної криптографії стає збільшення варіативності криптографічних операцій, придатних до практичного застосування [5-7]. І хоча даному напряму приділяється все більше уваги, питання побудови нових логічних операцій криптографічного перетворення інформації, дослідженням їх побудови або використанням арифметичних операцій з різними модулями все ще потребують більш детального дослідження. Розвиток даного напрямку є досить різновекторним, вимагає систематизації та комплексного підходу.

**Аналіз останніх досліджень і публікацій.** Провівши аналіз останніх досліджень та публікацій, в яких проведено дослідження спрямовані на розширення спектра нових криптографічних операцій замість криптографічного додавання за модулем, варто виділити наступні роботи. В роботі [8] запропоновано вирішення даної проблеми за рахунок застосування багаторозрядних операцій криптографічного кодування під управлінням криптосистем. В роботах [8, 9] доведено, що застосування матричних операцій криптографічного перетворення підвищує швидкодію обробки даних в криптосистемах за рахунок паралельного процесу виконання операції криптоперетворення, а складність виконання матричних операцій криптоперетворення інформації напряму залежить від кількості операндів.

В роботі [10] представлено результати дослідження взаємозв'язків між операціями в матричних моделях криптографічного перетворення. Послідовність кроків переходу від результатів комп'ютерного моделювання до придатної в інженерній практиці формалізованої операції крипто перетворення інформації наведена в [11]. Синтезу нових операцій потокового шифрування на основі модифікації операцій додавання по модулю з точністю до перестановки також присвячена робота [12]. Особливої уваги заслуговують дослідження груп симетричних модифікованих операцій додавання за модулем два та модулем чотири [13-18]. Синтезовані модифікації двохрозрядної двохоперандної операції додавання за модулем чотири, наведені в табл. 1 [18].

**Метою роботи** є дослідження і синтез груп двохоперандних двохрозрядних симетричних модифікованих операцій додавання за модулем чотири на основі використання лівостороннього та правостороннього розповсюдження переносів для підвищення варіативності алгоритмів комп'ютерної криптографії.

## Основний матеріал

При побудові модифікованих операцій додавання за модулем чотири було встановлено що синтез проводиться за умови:

$$\begin{cases} y_1 = x_2 \cdot k_2 \oplus k_1, \\ y_2 = k_2. \end{cases} \quad (1)$$

Операція додавання за модулем два описується як

$$O_1^{\text{mod}\,2} = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix}. \quad (2)$$

*Таблиця 1* – **Результати дослідження синтезу модифікацій двохрозрядної двохоперандної операції лівостороннього додавання за модулем чотири**

| Класифікатор операцій | Операції інверсії | | | |
|---|---|---|---|---|
| | $\begin{bmatrix}0\\0\end{bmatrix}$ | $\begin{bmatrix}0\\1\end{bmatrix}$ | $\begin{bmatrix}1\\0\end{bmatrix}$ | $\begin{bmatrix}1\\1\end{bmatrix}$ |
| **Базові операції** | $O_1=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\end{bmatrix}$ | $O_2=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}$ | $O_3=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\end{bmatrix}$ | $O_4=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}$ |
| | $O_5=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}$ | $O_6=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\oplus 1\end{bmatrix}$ | $O_7=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}$ | $O_8=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}$ |
| | $O_9=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$ | $O_{10}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$ | $O_{11}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$ | $O_{12}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$ |
| **Операції перестановок** | $O_{13}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$ | $O_{14}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$ | $O_{15}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$ | $O_{16}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$ |
| | $O_{17}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$ | $O_{18}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$ | $O_{19}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$ | $O_{20}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$ |
| | $O_{21}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$ | $O_{22}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$ | $O_{23}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$ | $O_{24}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$ |

Операція додавання за модулем чотири описується виразом

$$O_1^{\text{mod }4}=\begin{bmatrix}x_1\oplus k_1\oplus x_2\cdot k_2\\ x_2\oplus k_2\end{bmatrix}. \quad (3)$$

Якщо $x_2, k_2$ - молодші розряди операндів, а $x_1, k_1$ - старші розряди операндів, то умову (1) можна розглядати як правила формування переносу з молодшого розряду в старший. Даний алгоритм криптографічного додавання за модулем чотири назвемо лівостороннім двохрозрядним додавання за модулем чотири, тому що традиційно переноси формувалися в сторону старших розрядів, тобто вліво. Дану модифікацію операції позначимо як $O_1^{\text{mod }4\leftarrow}$.

Якщо в операціях криптографічного додавання за модулем чотири виділено лівостороннє додавання, то повинно існувати і правостороннє додавання, яке повинно описуватися виразом:

$$O_1^{\text{mod }4\rightarrow}=\begin{bmatrix}x_1\oplus k_1\\ x_2\oplus k_2\oplus x_1\cdot k_1\end{bmatrix}. \quad (4)$$

Виходячи з виразу (4) наведемо умову для синтезу модифікованих операцій правостороннього криптографічного додавання за модулем чотири:

$$\begin{bmatrix}y_1=k_1,\\ y_2=k_2\oplus x_1\cdot k_1\end{bmatrix}. \quad (5)$$

Перевіримо коректність припущення, що на основі умови (5) можливо синтезувати групу синтезу модифікованих операцій правостороннього криптографічного додавання за модулем чотири. Синтезуємо три базові операції для побудови групи модифікованих операцій правостороннього криптографічного додавання за модулем чотири.

Так як перша базова операція лівостороннього додавання за модулем чотири була отримана як [18] :

$$O_1^{\text{mod }4\leftarrow}=\begin{bmatrix}x_1\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\end{bmatrix}, \quad (6)$$

то і операція правостороннього додавання за модулем буде синтезована таким чином:

$$O_1^{\text{mod }4\rightarrow}=\begin{bmatrix}x_1\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_2\oplus k_2\oplus x_1\cdot k_1\end{bmatrix}. \quad (7)$$

Друга базова операція лівостороннього [18] та правостороннього додавання за модулем чотири представлені відповідними виразами:

$$O_5^{\text{mod }4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus \\ \oplus\begin{bmatrix}x_2\cdot k_2\oplus k_1\oplus k_2\\ k_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \quad (8)$$

$$O_5^{\text{mod }4\rightarrow}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\end{bmatrix}= \\ =\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\cdot k_1\oplus x_2\oplus k_2\end{bmatrix}. \quad (9)$$

Так як синтез третьої базової операції лівостороннього додавання за модулем чотири представлений виразом [18]:

$$O_9^{\text{mod }4\leftarrow}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_1\oplus y_2\end{bmatrix}=$$

$$= \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix}, \quad (10)$$

то і третя базова операція правостороннього додавання за модулем буде синтезована таким чином:

$$O_9^{\text{mod}\,4\rightarrow} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \overrightarrow{\oplus} \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix}. \quad (11)$$

Розглянемо синтез інших модифікацій операції правостороннього криптографічного додавання за модулем чотири. На основі моделей модифікації базової операції групи модифікованих операцій лівостороннього криптографічного додавання за модулем чотири, що описуються виразами (12-14) [18] синтезуємо відповідні їм операції (15-17)

$$O_2^{\text{mod}\,4\leftarrow} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}; \quad (12)$$

$$O_3^{\text{mod}\,4\leftarrow} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix}; \quad (13)$$

$$O_4^{\text{mod}\,4\leftarrow} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}; \quad (14)$$

$$O_2^{\text{mod}\,4\rightarrow} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \end{bmatrix}; \quad (15)$$

$$O_3^{\text{mod}\,4\rightarrow} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \end{bmatrix}; \quad (16)$$

$$O_4^{\text{mod}\,4\rightarrow} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \end{bmatrix}; \quad (17)$$

По аналогії було синтезовано інші модифікації двохрозрядної двохоперандної операції правостороннього додавання за модулем чотири.

Зведені результати дослідження синтезу модифікації двохрозрядної двохоперандної операції правостороннього додавання за модулем чотири наведемо в табл. 2.

*Таблиця 2* – **Результати дослідження синтезу модифікацій двохрозрядної двохоперандної операції правостороннього додавання за модулем чотири**

| Класифікатор операцій | Операції інверсії | | | |
|---|---|---|---|---|
| | $\begin{bmatrix}0\\0\end{bmatrix}$ | $\begin{bmatrix}0\\1\end{bmatrix}$ | $\begin{bmatrix}1\\0\end{bmatrix}$ | $\begin{bmatrix}1\\1\end{bmatrix}$ |
| Базові операції | $O_1^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \end{bmatrix}$ | $O_2^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \end{bmatrix}$ | $O_3^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \end{bmatrix}$ | $O_4^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \end{bmatrix}$ |
| | $O_5^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \end{bmatrix}$ | $O_6^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \end{bmatrix}$ | $O_7^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \end{bmatrix}$ | $O_8^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \end{bmatrix}$ |
| | $O_9^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix}$ | $O_{10}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}$ | $O_{11}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix}$ | $O_{12}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}$ |
| Операції перестановок | $O_{13}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \\ x_1 \oplus k_1 \end{bmatrix}$ | $O_{14}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix}$ | $O_{15}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \end{bmatrix}$ | $O_{16}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix}$ |
| | $O_{17}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix}$ | $O_{18}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}$ | $O_{19}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix}$ | $O_{20}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}$ |
| | $O_{21}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_1 \oplus k_1 \end{bmatrix}$ | $O_{22}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix}$ | $O_{23}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \end{bmatrix}$ | $O_{24}^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix}$ |

За результатами порівняння синтезованої групи операцій з групами операцій додавання за модулем два [17] та лівостороннього криптографічного додавання за модулем чотири, представленого в роботі [18] встановлено: синтезовані моделі нових операцій відрізняються від відомих операцій; таблиці істинності синтезованих операцій та результати їх виконання також відрізняються.

Операція криптоперетворення буде симетричною, якщо повторне її використання приведе до розшифрування інформації.

Якщо $O_i^{\text{mod}\,4\rightarrow}(x) = y$,

то $O_i^{\text{mod}\,4\rightarrow}(O_i^{\text{mod}\,4\rightarrow}(x)) = x$,

де $x$ і $y$ - вхідні дані і результат виконання $i$-ої операції криптоперетворення відповідно.

Перевірка синтезованих операцій на симетричність проводилась на основі обчислювального експерименту. Результати експерименту підтвердили, що всі модифікації операції правостороннього додавання за модулем чотири відповідають вимогам симетричності операцій.

Так як практичне застосування групи операцій лівостороннього криптографічного додавання за модулем чотири забезпечило підвищення варіативності потокового шифрування, то можна стверджувати що збільшення кількості операцій за рахунок використання нової синтезованої групи також підвищить варіативність потокового шифрування.

## Висновки

1. Синтезована група двохоперандних двохрозрядних симетричних операцій правостороннього додавання за модулем чотири. Встановлено, що побудована група операцій криптографічних перетворень відрізняється від груп криптоопераций побудованих на основі додавання за модулем два та класичним лівостороннім додаванням за модулем чотири.

2. Встановлено, що всі синтезовані операції забезпечують як пряме так і обернене криптоперетворення, що значно спрощує їх використання в потокових шифрах Невелика складність наведених моделей операцій забезпечує простоту їх реалізації як на апаратному так і програмному рівнях.

СПИСОК ЛІТЕРАТУРИ


1. Рудницький В.М. Криптографічне кодування: обробка та захист інформації: колективна монографія. Харків: ТОВ «ДІСА ПЛЮС», 2018. 139 с.
2. Мао Венбо. Современная криптография: теория и практика. пер. с англ. Изд. дом «Вильямс», 2005. 768 с.: ил. Парал. тит. англ. ISBN 5-8459-0847-7 (рус.)
3. Хорошко В.А. Чекатков А. А. Методи й засоби захисту інформації. К.: Юніор, 2003. 504 с.
4. Richard A. Mollin, «Codes: the guide to secrecy from ancient to modern times», Chapman & Hall/CRC, 2005. С.142.
5. Бабенко В. Г. Дослідження матричних операцій криптографічного перетворення на основі арифметичних операцій за модулем. Системи управління, навігації та зв'язку: зб. наук. праць. К., 2012. Вип. 4 (24). С. 85–88.
6. Рудницький В. М., Бердибаєв Р. Ш., Бреус Р. В., Лада Н. В., Пустовіт М. О. Синтез обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда (eng.) Сучасні інформаційні системи. Харків, 2019. Т. 3, № 4, С. 109-114. - DOI: https://doi.org/10.20998/2522-9052.2019.4.16
7. Бабенко В.Г., Лада Н.В. Синтез і аналіз операцій криптографічного додавання за модулем два. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2014. Вип. 2 (118). С. 116–118.
8. Рудницький В.М. Алгебраїчна структура множини логічних операцій кодування / В.М. Рудницький, В.Г. Бабенко, Д.А. Жиляєв // Наука і техніка Повітряних Сил Збройних Сил України: наук.-техн. журн. – Х.: ХУПС ім. І. Кожедуба. – 2011. – № 2 (6). – С. 112-114.
9. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2014. Вип. 2 (118). С. 116–118.
10. Бабенко В. Г., Лада Н. В., Лада С. В. Дослідження взаємозв'язків між операціями в матричних моделях криптографічного перетворення. Вісник Черкаського державного технологічного університету. 2016. № 1. С. 5–11
11. Рудницький В. М., Лада Н. В., Козловська С. Г. Технологія побудови двохоперандних операцій криптографічного перетворення інформації за результатами моделювання. Сучасні інформаційні системи, Т. 2, № 4, С. 26-30, 2018.
12. В.М.Рудницький, Н.В. Лада, В.Г. Бабенко. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія. Харків: ТОВ «ДІСА ПЛЮС», 2018. 184 с.
13. Mozhaev O. Multiservise network security metric / O. Mozhaev, H. Kuchuk, N. Kuchuk, M. Mozhaev, M. Lohvynenco // IEEE Advanced information and communication technologies-2017. Proc. of the 2th Int. Conf. – Lviv, 2017. – P. 133-136. – DOI: https://doi.org/10.1109/AIACT.2017.8020083
14. Kuchuk N. Method for calculating of R-learning traffic peakedness / N. Kuchuk; O. Mozhaiev, M. Mozhaiev; H. Kuchuk // 2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2017. – 2017. – P. 359 – 362. URL : http://dx.doi.org/10.1109/INFOCOMMST.2017.8246416
15. Svyrydov, A., Kuchuk, H., Tsiapa, O. (2018), "Improving efficienty of image recognition process: Approach and case study", Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018, pp. 593-597, DOI: http://dx.doi.org/10.1109/DESSERT.2018.8409201
16. Коваленко А.А. Использование временных шкал при аппроксимации длины очередей компьютерных сетей / А.А. Коваленко, Г.А. Кучук, И.В. Рубан // Сучасний стан наукових досліджень та технологій в промисловості. – 2018. – № 2 (4). – С. 12–18. – DOI: http://doi.org/10.30837/2522-9818.2018.4.012
17. Лада Н. В., Козловська С. Г., Рудницький С. В. Побудова математичної групи симетричних операцій на основі додавання за модулем два. Сучасна спеціальна техніка: науково-практичний журнал. Київ, 2019. № 4 (59). С. 33-41.
18. Лада Н. В., Козловська С. Г., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій додавання за модулем чотири. Центральноукраїнський науковий вісник. Технічні науки. Збірник наукових праць. Кропивницький: КНТУ, 2019. Вип. 2 (33). С. 181–189.


Received (Надійшла) 11.12.2019
Accepted for publication (Прийнята до друку) 29.01.2020

**Research and synthesis of a group of symmetric modified operations of right-handed addition by module four**

N. Lada, S. Rudnitsky, V. Zazhoma, Y. Rudnytska

**Abstract.** The main results of research and synthesis of a group of two-operand two-bit symmetric operations of right-handed addition by module four by using a group of two-bit single-operand cryptocurrency operations are presented in the article. Synthesis of a group of operations on the basis of operation of right-handed addition by module four has not previously been investigated. It is established that the constructed group of operations of cryptographic transformations differs from cryptocurrency groups built on the basis of addition by module two and classic left-handed addition by module four. The use of a new synthesized group allows to improve the quality of streaming encryption by increasing the variability of cryptographic transformations. It is revealed that up to twenty-four substitution tables will be used due to symmetrical synthesized operations in streaming encryption systems.

**Keywords:** cryptographic operation, operations modifications, mathematical group of operations, addition by module, operation models, streaming encryption.