УДК 004.056.55:004.312.2 DOI: https://doi.org/10.32515/2664-262X.2019.2(33).181-189

Н.В. Лада, канд. техн. наук, докторант**, Ю.В. Рудницька,** асп.
Черкаський державний технологічний університет, м.Черкаси, Україна
С.Г. Козловська, доц.,канд. техн. наук
Східноєвропейського університету економіки і менеджменту, м.Черкаси, Україна
e-mail: Ladanatali256@gmail.com, kozlovskifamili@ukr.net, Y.V.Rudnitskaya@gmail.com

Дослідження і синтез групи симетричних модифікованих операцій додавання за модулем чотири

В статті наведено основні результати дослідження синтезу групи двохоперандних двохрозрядних симетричних модифікованих операцій додавання за модулем чотири на основі використання групи двохрозрядних одноопераднних операцій криптоперетворення, для підвищення варіативності алгоритмів комп'ютерної криптографії. На основі чотирьох модифікацій моделей операції додавання за модулем два з врахуванням моделі розповсюдження переносу побудовано аналогічні модифікації моделей операції додавання за модулем чотири. Було встановлено, що побудувати всі модифікації двохрозрядної двохоперандної операції додавання за модулем чотири, можна на основі групи двохрозрядних двохоперандних операції операцій криптографічного перетворення інформації. Синтез моделей двохоперандної симетричної операції проводився поєднанням довільної двохрозрядної операції для перетворення другого операнда з базовою для даної операції операцією перетворення першого операнда шляхом додавання за модулем два. Коректність отриманих результатів підтверджено результатами обчислювального експерименту. У подальшому потрібно продовжити дослідження направлені на вдосконалення алгоритмів потокового шифрування на основі синтезованої групи нових криптографічних операцій.

криптографічна операція, модифікації операцій, математична група операцій, додавання за модулем, моделі операції, потокове

Н.В. Лада, канд. техн. наук, докторант, **Ю.В. Рудницкая,** асп.
Черкасский государственный технологический университет, г.Черкассы, Украина
С.Г. Козловская, доц., канд. техн. наук
Восточноевропейский университет экономики и менеджмента, г.Черкассы, Украина

Исследование и синтез группы симметричных модифицированных операций сложения по модулю четыре

В статье приведены основные результаты исследования синтеза группы двухоперандных двухразрядных симметричных модифицированных операций сложения по модулю четыре на основе использования группы двухразрядных одноопераднних операций криптопреобразования, для повышения вариативности алгоритмов компьютерной криптографии. На основе четырех модификаций моделей операции сложения по модулю два с учетом модели распространения переноса построено аналогичные модификации моделей операции сложения по модулю четыре. Было установлено, что построить все модификации двухразрядных двухоперандных операций сложения по модулю четыре, можно на основе группы двухразрядных двухоперандных операции операций криптографического преобразования информации. Синтез моделей двухоперандной симметричной операции проводился сочетанием произвольной двухразрядной операции для преобразования второго операнда с базовой для данной операции операцией преобразования первого операнда путем сложения по модулю два. Корректность полученных результатов подтверждается результатами вычислительного эксперимента. В дальнейшем необходимо продолжить исследования направлены на совершенствование алгоритмов потокового шифрования на основе синтезированной группы новых криптографических операций.

Постановка проблеми. Всесвітня тенденція до щорічного збільшення кібератак характеризується як зростанням їх кількості так і розширенням переліку автоматизованих та інформаційних системи, що піддалися нападу. Особливо важливо забезпечити ефективну протидію криптоатакам, адже саме вони направлені на заволодіння конфіденційною інформацією, розголошення якої приводить до негативних наслідків та фінансових збитків. Все це в сукупності робить проблему підвищення ефективності систем комп'ютерного криптографічного захисту інформації особливо актуальною. Вирішення даної проблеми полягає у вдосконаленні вже існуючих та побудові нових криптоалгоритмів та криптосистем, в тому числі на основі застосування нових, раніше невідомих підходів. Одним з нових шляхів розвитку сучасної та постквантової криптографії полягає в розробці криптопримітивів основаних на застосуванні нових багатоопераднних операцій криптографічного перетворення інформації.

Аналіз останніх досліджень і публікацій. Операції криптографічного перетворення інформації забезпечують збільшення стійкості криптоперетворень [1-3]. Крім того аналіз даних операцій дозволяє виокремити нові підходи для побудови систем комп'ютерної криптографії [4, 5]. В алгоритмах комп'ютерної криптографії особливе місце займають операції додавання за модулем а також модифікації даних операцій з точністю до перестановки [6-8]. Збільшення кількості операцій додавання за модулем дозволяє збільшити варіативність алгоритмів, стійкість результатів шифрування та надійність криптосистем [9].

В роботах [10-11] наведено результати обчислювального експерименту на основі якого отримано 96 симетричних двохрозрядних двохоперандних симетричних операцій представлених поєднанням одноопераднних операцій та їх таблицями підстановки. В основу експерименту було взято групу одноопераднних операцій криптоперетворення наведених в табл. 1 [12].

Таблиця 1– Класифікація одноопераднних двохрозрядних операцій криптографічного перетворення інформації

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	$F_1=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	$F_2=\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}$	$F_3=\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}$	$F_4=\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}$
	$F_5=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	$F_6=\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}$	$F_7=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}$	$F_8=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}$
	$F_9=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	$F_{10}=\begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}$	$F_{11}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}$	$F_{12}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
Операції перестановок	$F_{13}=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	$F_{14}=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}$	$F_{15}=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}$	$F_{16}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$
	$F_{17}=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	$F_{18}=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}$	$F_{19}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}$	$F_{20}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
	$F_{21}=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	$F_{22}=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}$	$F_{23}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\end{bmatrix}$	$F_{24}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$

Джерело: розроблено авторами

Експериментально отримані операції було поділено на 4 математичних групи по 24 операції в кожній, що дає змогу досліджувати кожну групу окремо.

В роботі [13] досліджена можливість побудова повної групи двохоперандних операцій криптоперетворення, на основі відомої, за рахунок встановлення і застосування перестановочних взаємозв'язків між таблицями істинності. Встановлено, що застосування повної групи перестановочних схем забезпечить побудову повної групи наборів модифікованих двохоперандних операцій криптоперетворення невідомої групи, на основі однієї відомої операції. Отримані результати співпали з результатами обчислювального експерименту.

Робота [14] присвячена розробці технології побудови двохоперандних операцій криптографічного перетворення інформації, за результатами моделювання, придатних для практичного застосування в комп'ютерній криптографії.

Основним недоліком даної технології полягає в необхідності виконання громіздких математичних перетворень, що значно ускладнює ефективність досліджень.

Постановка завдання. Метою роботи є дослідження і синтез групи двохоперандних двохрозрядних симетричних модифікованих операцій додавання за модулем чотири на основі використання групи двохрозрядних одноопераднних операцій криптоперетворення для підвищення варіативності алгоритмів комп'ютерної криптографії.

Виклад основного матеріалу. В основу проведення дослідження було взято чотири математичні моделі двохоперандних двохрозрядних симетричних модифікованих операцій додавання за модулем два [9]. Дослідимо можливість побудови аналогічних модифікованих операцій на основі додавання за модулем чотири.

Так як операція двохрозрядного додавання за модулем два включає в себе операцію додавання за модулем два першого та другого розрядів, то вона буде задана моделлю:

$$O_1^{\mathrm{mod}\,2} = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix}, \tag{1}$$

де x_i, k_i – значення i-тих розрядів першого та другого операндів відповідно.

Операція двохрозрядного додавання за модулем чотири, відрізняється від двохрозрядного додавання за модулем два наявність переносу з молодшого в старший розряд. Виходячи з цього модель операції двохрозрядного додавання за модулем чотири можна представити як:

$$O_1^{\mathrm{mod}\,4} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix}, \tag{2}$$

Якщо ввести позначення, по аналогії з табл.1 $F_j^1 = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, $F_j^2 = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ та представити їх як j-ту операцію відображення в результатах додавання по модулю першого та другого операнда відповідно, тоді:

$$O_1^{\mathrm{mod}\,2} = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = F_1^1 \oplus F_1^2, \tag{3}$$

за умови що, $y_1 = k_1$, $y_2 = k_2$.

По аналогії модель операція двохрозрядного додавання за модулем чотири можна представити:

$$O_1^{\text{mod}\,4} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = F_1^1 \oplus F_1^2, \tag{4}$$

за умови що, $y_1 = x_2 \cdot k_2 \oplus k_1,\ y_2 = k_2$.

Розглянемо модифіковані операція додавання за модулем два [6] та по аналогії з виразами (3-4) побудуємо аналогічні модифіковані операція додавання за модулем чотири:

$$O_2^{\text{mod}\,2} = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = F_2^1 \oplus F_1^2, \tag{5}$$

за умови що, $y_1 = k_1,\ y_2 = k_2$;

$$O_2^{\text{mod}\,4} = F_2^1 \oplus F_1^2 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} \tag{6}$$

за умови що, $y_1 = x_2 \cdot k_2 \oplus k_1,\ y_2 = k_2$;

$$O_3^{\text{mod}\,2} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = F_3^1 \oplus F_1^2, \tag{7}$$

за умови що, $y_1 = k_1,\ y_2 = k_2$;

$$O_3^{\text{mod}\,4} = F_3^1 \oplus F_1^2 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix} \tag{8}$$

за умови що, $y_1 = x_2 \cdot k_2 \oplus k_1,\ y_2 = k_2$;

$$O_4^{\text{mod}\,2} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = F_4^1 \oplus F_1^2, \tag{9}$$

за умови що, $y_1 = k_1,\ y_2 = k_2$;

$$O_4^{\text{mod}\,4} = F_4^1 \oplus F_1^2 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}, \tag{10}$$

умови що, $y_1 = x_2 \cdot k_2 \oplus k_1,\ y_2 = k_2$.

Коректність наведених моделей двохоперандних двохрозрядних симетричних модифікованих операцій додавання за модулем два підтверджена застосуванням технології побудови двохоперандних операцій криптоперетворення, а також результатами обчислювального експерименту.

На основі аналізу отриманих модифікацій двохрозрядної операції додавання за модулем чотири, в тому числі, наведені в (3-10), можна зробити висновок, що їх можна отримати на основі одноопераднних операцій обробки першого операнда, шляхом додавання операції додавання за модулем два базової для них операції перетворення другого операнда, за умови врахування моделі переносу в старший розряд.

Перевіримо коректність даного висновку шляхом застосування інших одноопераднних операцій криптоперетворення, наведених в табл.1. При побудові модифікованих операцій додавання за модулем чотири буде виконуватися умова: $y_1 = x_2 \cdot k_2 \oplus k_1,\ y_2 = k_2$.

Так як для одноопераднної операції F_5 базовою одноопераднною операцією також є F_5 тоді:

$$O_5^{\text{mod}4} = F_5^1 \oplus F_5^2 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \\ = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix}, \quad (11)$$

Для одноопераднної операції F_6 базовою одноопераднною операцією також є F_5, виходячи з цього отримаємо:

$$O_6^{\text{mod}4} = F_5^1 \oplus F_6^2 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \\ = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}, \quad (12)$$

$$O_{12}^{\text{mod}4} = F_9^1 \oplus F_{12}^2 = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \\ = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}, \quad (13)$$

$$O_{14}^{\text{mod}4} = F_{13}^1 \oplus F_{14}^2 = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ y_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \oplus x_2 \cdot k_2 \end{bmatrix} = \\ = \begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix}, \quad (14)$$

$$O_{19}^{\text{mod}4} = F_{17}^1 \oplus F_{19}^2 = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \\ = \begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix}, \quad (15)$$

$$O_{24}^{\text{mod}4} = F_{21}^{1} \oplus F_{24}^{2} = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \cdot k_2 \oplus k_1 \end{bmatrix} =$$
$$= \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix}, \quad (16)$$

Результати дослідження синтезу модифікації двохрозрядної двохоперандної операції додавання за модулем чотири наведено в табл.2.

Таблиця 2 – Результати дослідження синтезу модифікацій двохрозрядної двохоперандної операції 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	$O_{13} = \begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix}$	$O_{14} = \begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix}$	$O_{15} = \begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \end{bmatrix}$	$O_{16} = \begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}$
	$O_{17} = \begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \end{bmatrix}$	$O_{18} = \begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}$	$O_{19} = \begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix}$	$O_{20} = \begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix}$
	$O_{21} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix}$	$O_{22} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix}$	$O_{23} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix}$	$O_{24} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix}$

Джерело: розроблено авторами

В процесі дослідження було встановлено, що побудувати всі модифікації двохрозрядної двохоперандної операції додавання за модулем чотири, можна на основі групи двохрозрядних двохоперандних операції операцій криптографічного перетворення інформації. При проведенні дослідження були отримані моделі симетричних операцій, кожна з яких забезпечує як пряме так і обернене криптоперетворення. Синтез моделі двохоперандної симетричної операції проводився шляхом поєднання довільної одноопераднодної двохрозрядної операції для перетворення другого операнда з базовою для даної операції операцією перетворення першого операнда. Поєднання одноопераднодних двохрозрядних операцій реалізовано на основі додавання за модулем два.

Отримані теоретичні результати повністю співпали з результатами обчислювального експерименту по моделюванню симетричних операцій криптоперетворення [9].

Висновки. В процесі дослідження отримано наступні результати:

На основі чотирьох модифікацій моделей операції додавання за модулем два з врахуванням моделі розповсюдження переносу побудовано аналогічні модифікації моделей операції додавання за модулем чотири.

Було встановлено, що побудувати всі модифікації двохрозрядної двохоперандної операції додавання за модулем чотири, можна на основі групи двохрозрядних двохоперандних операції операцій криптографічного перетворення інформації.

Синтез моделей двохоперандної симетричної операції проводився поєднанням довільної двох розрядної операції для перетворення другого операнда з базовою для даної операції операцією перетворення першого операнда шляхом додавання за модулем два. Коректність отриманих результатів підтверджено результатами обчислювального експерименту.

У подальшому потрібно продовжити дослідження направлені на вдосконалення алгоритмів потокового шифрування на основі синтезованої групи нових криптографічних операцій.

Список літератури

1. Бабенко В.Г. Складності та особливості побудови ефективних криптоалгоритмів. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2014. Вип. №3. С.87–91.
2. Фауре Е.В., Сисоєнко С.В., Миронюк Т.В. Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення. *Системи управління, навігації та зв'язку: зб. наук.* праць. Полтава: Полтавський нац. техн. ун-т ім. Юрія Кондратюка, 2015. Вип. 4 (36). С. 85–87.
3. Фауре Е.В.,Сисоєнко С.В. Метод підвищення стійкості псевдовипадкових послідовностей до лінійного криптоаналізу. *The scientific potential of the present: proceedings of the International Scientific Conference* (St. Andrews, Scotland, UK, December 1, 2016) / ed. N. P. Kazmyna. NGO «European Scientific Platform». Vinnytsia: PE Rogalska I. O., 2016. P. 119–122.
4. Миронець І.В., Миронюк Т.В., Сисоєнко С.В. Апаратна реалізація базової групи операцій перестановок, керованих інформацією. *Актуальні задачі та досягнення у галузі кібербезпеки: матеріали Всеукр. наук.-практ. конф.* (м. Кропивницький, 23–25 листоп. 2016 р.). Кропивницький: КНТУ, 2016. С. 141–142.
5. Стабецька Т.А. Математичне обґрунтування узагальненого методу синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення. *Наукові праці*: *наук.-метод. журнал*. Миколаїв: ЧДУ ім. Петра Могили, 2014. Вип.238(250). Комп'ютерні технології. С.110-114.
6. Лада Н.В., Козловська С.Г. Застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах. Системи управління, навігації та зв'язку: зб. наук. праць. Полтава: ПНТУ, 2018. Т. 1 (47). С. 127-130.
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. 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.
9. Рудницький В.М., Лада Н.В., Бабенко В.Г. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія. Харків: ТОВ «ДІСА ПЛЮС», 2018. 184 с.
10. Рудницкий В.Н., Пивнева С.В., Бабенко В.Г., Миронец И.В. и др Криптографическое кодирование: методы и средства реализации: монографія. Тольят. гос. ун-т. Тольятти, 2013. 196 с.
11. Голуб С.В., Бабенко В.Г., Рудницький С.В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два. *Системи обробки інформації*: зб. наук. праць. Х.: ХУПС ім. І. Кожедуба, 2012. Вип. 3 (101), Т. 1. С. 119–122.
12. Рудницький В.М., Бабенко В.Г., Жиляєв Д.А. Алгебраїчна структура множини логічних операцій кодування. *Наука і техніка Повітряних Сил Збройних Сил України*: наук.-техн. журн. 2011. Вип. 2 (6). С. 112–114.
13. Козловська С.Г. Синтез груп двохоперандних операцій криптоперетворення на основі перестановлюваних схем. *Сучасна спеціальна техніка*: науково-практичний журнал. Київ, 2018. № 4 (55). С. 47-56.

14. Рудницький В.М., Лада Н.В., Козловська С.Г. Технологія побудови двохоперандних операцій криптографічного перетворення інформації за результатами моделювання. *Сучасні інформаційні системи: щоквартальний науково-технічний журнал.* Харків, 2018. Т. 2. № 4. С. 26-30.

References

1. Babenko, V.G. (2014). Skladnosti ta osoblyvosti pobudovy efektyvnykh kryptoalhorytmiv [Complexities and specificities for constructing of effective cryptographic algorithms]. *Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu. Seriia: Tekhnichni nauky, 3*, 87–91 [in Ukrainian].
2. Faure, E.V., Sysoienko, S.V. & Mironiuk, T.V. (2015), "Syntez i analiz psevdovypadkovykh poslidovnostei na osnovi operatsii kryptohrafichnoho peretvorennia" [Synthesis and analysis of pseudorandom sequences based on cryptographic transformation operations], *Systemy upravlinnia, navihatsii ta zviazku. Zbirnyk naukovykh prats PNTU im. Yuriia Kondratiuka, No. 4 (36)*, 85–87 [in Ukrainian].
3. Faure, E.V. and Sysoienko, S.V. (2016), Metod pidvyshchennia stiikosti psevdovypadkovykh poslidovnostei do liniinoho kryptoanalizu. *The scientific potential of the present: proceedings of the International Scientific Conference*. (St. Andrews, Scotland, UK, December 1, 2016) / ed. N. P. Kazmyna. NGO «European Scientific Platform». Vinnytsia: PE Rogalska I. O., pp. 119–122 [in Ukrainian].
4. Myronets, I.V., Mironiuk, T.V. and Sysoienko, S.V. (2016), Aparatna realizatsiia bazovoi hrupy operatsii perestanovok, kerovanykh informatsiieiu. Aktualni zadachi ta dosiahnennia u haluzi kiberbezpeky: *materialy Vseukrainskoi naukovo-praktychnoi konferentsii* (m. Kropyvnytskyi, 23–25 lystop. 2016 r.). Kropyvnytskyi: KNTU, 141–142 [in Ukrainian].
5. Stabetskaya, T.A. (2014), "Matematychne obgruntuvannia uzahalnenoho metodu syntezu obernenykh operatsii neliniinoho rozshyrenoho matrychnoho kryptohrafichnoho peretvorennia" [Mathematical justification of generalized method of synthesis of feedback nonlinear operations of expanded matrix cryptographic transformations]. *Naukovi pratsi: naukovo-metodychnyi zhurnal. ChDU im. Petra Mohyly, Kompiuterni tekhnolohii, No. 238 (250)*, 110-114 [in Ukrainian].
6. Lada, N.V. & Kozlovska, S.H. (2018). Zastosuvannia operatsii kryptohrafichnoho dodavannia za modulem dva z tochnistiu do perestanovki v potokovykh shyfrakh [Applying cryptographic addition operations by module two with accuracy of permutation in stream ciphers*]. Systemy upravlinnia, navihatsii ta zviazku. Zbirnyk naukovykh prats PNTU, No. 1 (47)*, 127-130 [in Ukrainian].
7. Babenko, V.H. & Lada, N.V. (2014). "Syntez i analiz operatsii kryptohrafichnoho dodavannia za modulem dva" [Synthesis and analysis of operations of cryptographic addition modulo two], *Systemy obrobky informatsii: zbirnyk naukovykh prats KHUPS im. I. Kozheduba, No. 2 (118)*, 116–118 [in Ukrainian].
8. Babenko, V.G. (2012). "Doslidzhennia matrychnykh operatsii kryptohrafichnoho peretvorennia na osnovi aryfmetychnykh operatsii za modulem" [The research of matrix operations of cryptographic transformation based on arithmetic modulo]. *Systemy upravlinnya, navigatsiyi ta zvyazku. Zbirnyk naukovykh prats, No. 4 (24)*, 85-88 [in Ukrainian].
9. Rudnitskyi, V.M., Lada, N.V. & Babenko, V.H. (2018). *Kryptohrafichne koduvannia: syntez operatsii potokovoho shyfruvannia z tochnistiu do perestanovki: monohrafiia [Cryptographic encoding: Synthesis for streaming encryption operations within the accuracy of permutation: monograph]*, TOV «DISA PLIUS», Kharkiv [in Ukrainian].
10. Rudnitskyi, V.M., Pyvneva, S.V., Babenko, V.G. & et al. (2018). Kryptohrafichne koduvannia: metody i zasoby realizatsii: monohrafiia [Cryptographic encoding: methods and means of implementation: monograph], Toliatinskoho hosudarstvennii universytet [in Russian].
11. Golub, S.V., Babenko, V.G. & Rudnitskyi, S.V. (2012). "Metod syntezu operatsii kryptohrafichnoho peretvorennia na osnovi dodavannia za modulem dva" [The method of synthesis of the operations of cryptographic transformations on the basis of addition modulo two]. *Systemy obrobky informatsii: zbirnyk naukovykh prats KHUPS im. I. Kozheduba, No. 3 (101), Vol. 1*, 119–122 [in Ukrainian].
12. Rudnitskyi, V.M., Babenko, V.G. & Zhylyaev, D.A. (2011), "Alhebraichna struktura mnozhyny lohichnykh operatsii koduvannia" [Construction of reverse functions for the systems of protection to information]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy: naukovo-tekhnichnyi zhurnal, No. 2 (6)*, 112–114 [in Ukrainian].
13. Kozlovska, S.H. (2018). Syntez hrup dvokhoperandnykh operatsii kryptoperetvorennia na osnovi perestanovliuvanykh skhem [Synthesis of groups two-operand operations of criptoconversion on the basis of permutation schemes]. *Suchasna spetsialna tekhnika, No. 4 (55)*, 47-56 [in Ukrainian].
14. Rudnitskyi, V.M., Lada, N.V. & Kozlovska, S.H. (2018). Tekhnolohiia pobudovy dvokhoperandnykh operatsii kryptohrafichnoho peretvorennia informatsii za rezultatamy modeliuvannia [Technology of two

operand operations construction of information cryptographic transformation by modeling results]. *Suchasni informatsiini systemy, Vol.2, No. 4,* 26-30 [in Ukrainian].

Nataliia Lada, PhD tech. sci., Doctoral student, **Yulia Rudnitskaya,** post-graduate
Cherkasy State Technological University, Cherkasy, Ukraine
Svetlana Kozlovska, Assoc. Prof., PhD tech. sci.
East European University of Economics and Management, Cherkasy, Ukraine

Researching and Synthesizing a Group of Symmetric Modified Modulo-4 Addition Operations

The main research results of synthesizing a group of two-operand two-bit symmetric modified modulo-4 addition operations, based on using the group of two-bit one-operand cryptographic transformation operations for increasing the variability of computer cryptography algorithms are presented in the article.

In order to achieve this goal, based on four modulo-2 addition operation's models modifications, similar modifications' models of the modulo-4 addition operation's models were constructed in the article. For the construction of these models, the main difference between the operations of two-bit addition modulo-4 was used from the two-digit addition modulo-2, which consists in the transfer from junior to senior. The sequences of mathematical transformations given in the article provide the construction of a group of models of operations on the basis of a given, for example, the operation of adding modulo-4. The correctness of given models of two-operand two-bit symmetric modified modulo-2 addition operations is confirmed by the application of the two-operand cryptographic transformation operations construction technology, as well as by the computational experiment's results. The assumption on all two-bit two-operand modulo-4 addition operation modifications building possibility based on using the group of two-bit one-operand operations of information cryptographic transformation was proved in the article. During the study, the symmetric operations' models were obtained, each of which provides both direct and inverse cryptographic transformation. The established relationships between operations allowed to synthesize a models' group of two-bit two-operand symmetric modified modulo-4 addition operations, based on combining the random two-bit operation to transform the second operand, with the first operand's transforming operation, which is basic for this operation, through the modulo-2 addition.

The obtained theoretical results completely coincide with the computational experiment's results on simulating the symmetric operations of cryptographic transformation.

cryptographic operation, modifications of operations, mathematical group of operations, module addition, operation models, streaming encryption

Одержано (Received) 21.11.2019 *Прорецензовано (Reviewed) 10.12.2019*
Прийнято до друку (Approved) 23.12.2019