ISSN 2411-3816 (Print)
СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА
MODERN SPECIAL TECHNICS
DOI (Issue): https: //doi.org/
Issue 4(59) 2019

УДК 004.056.55:004.312.2

Лада Наталія Володимирівна,
кандидат технічних наук, старший викладач кафедри
інформаційної безпеки та комп'ютерної інженерії
Черкаського державного технологічного університету, м. Черкаси, Україна
ORCID ID 0000-0002-7682-2970
Козловська Світлана Григоріївна,
старший викладач кафедри менеджменту організацій
Східноєвропейського університету економіки і менеджменту,
м. Черкаси, Україна
ORCID ID 0000-0002-1754-1220
Рудницький Сергій Володимирович,
кандидат технічних наук, старший викладач кафедри
інформаційних технологій проектування
Черкаського державного технологічного університету, м. Черкаси, Україна
ORCID ID 0000-0003-4389-1088

ПОБУДОВА МАТЕМАТИЧНОЇ ГРУПИ СИМЕТРИЧНИХ ОПЕРАЦІЙ НА ОСНОВІ ДОДАВАННЯ ЗА МОДУЛЕМ ДВА

Стаття присвячена підвищенню якості систем потокового шифрування конфіденційної інформації за рахунок збільшення варіативності криптографічних перетворень шляхом використання нової групи двоопераднних дворозрядних операцій, синтезованої на основі додавання за модулем два.

Для досягнення цієї мети розроблено метод синтезу групи операцій додавання за модулем два для потокового шифрування на основі операції додавання за модулем два. Сутність цього методу полягає в синтезі дворозрядних двоопераднних операцій базової групи на основі поєднання однакових базових операцій перетворення першого та другого операнда шляхом додавання за модулем два. Побудова повної математичної групи даних операцій здійснюється на основі додаткового застосування криптографічних операцій перестановки та інверсії операндів операцій базової групи.

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

Статья посвящена повышению качества систем потокового шифрования конфиденциальной информации за счет увеличения вариативности криптографических преобразований путем использования новой группы двухоперандных двухразрядных операций, синтезированной на основе сложения по модулю два.

Для достижения такой цели разработан метод синтеза группы операций сложения по модулю два для потокового шифрования на основе операции сложения по модулю два. Сущность этого метода заключается в синтезе двухраз-

рядных двухоперандных операций базовой группы на основе сочетания одинаковых базовых операций преобразования первого и второго операнда путем сложения по модулю два. Построение полной математической группы данных операций производится на основе дополнительного применения криптографических операций перестановки и инверсии операндов операции базовой группы.

Ключевые слова: *криптографическая операция, модификации операций, математическая группа операций, сложение по модулю, модели операции, потоковое шифрование.*

Постановка проблеми.

В останні роки спостерігається швидкий розвиток криптографічних засобів захисту інформації і відповідно вдосконалюються методи криптоаналізу. Характерними ознаками сучасних криптосистем є потреба у використанні нових методів не лише для блокового шифрування (більшість наукових досліджень припадає саме на нього), а й для потокового шифрування. Однією з головних переваг потокового шифрування є висока швидкість обробки інформації і відповідно підвищення надійності цього шифрування за рахунок впровадження нових методів та засобів не повинно суттєво погіршувати цю характеристику. Одним із перспективних шляхів вирішення цієї проблеми є виявлення, аналіз і відповідно синтез додаткових операцій, що можуть застосовуватися для криптоперетворення даних. Збільшення кількості придатних для криптографічного перетворення операцій дозволяє підвищувати надійність та стійкість шифрування, але не є максимально ефективним без дослідження в розрізі математичних груп, адже саме використання операцій у межах математичної групи дозволяє покращити показник швидкості криптоперетворення, що є надзвичайно актуальним у наш час. Проте слід зазначити, що питанням побудови математичних груп операцій криптоперетворення на сьогоднішній день приділяється недостатньо уваги.

Аналіз останніх досліджень і публікацій

У роботах [1–2] розглянуті модифікації операцій додавання за модулем на основі перестановок операндів і результатів виконання операцій. У роботі [3] опубліковані результати обчислювального експерименту по моделюванню двоопераднних операцій криптографічного перетворення на основі дворозрядних операцій криптоперетворення. Подальші дослідження були присвячені моделюванню двоопераднних операцій криптоперетворення на основі одноопераднних [4–5]. Поєднання одноопераднних операцій криптоперетворення в двоопераднні забезпечує зменшення складності алгоритмів шифрування та збільшення варіативності самих алгоритмів [6]. Синтез груп двоопераднних операцій криптоперетворення досліджувався на основі застосування перестановлюваних схем у роботі [7]. Наявні результати досліджень мають досить розрізнений характер і не дозволяють забезпечити побудову математичної групи моделей симетричних операцій криптоперетворення на основі додавання за модулем два, придатних для практичного застосування в потокових шифрах.

Метою роботи є підвищення якості систем потокового шифрування конфіденційної інформації за рахунок збільшення варіативності криптографічних

перетворень шляхом використання нової групи двоопераднних дворозрядних операцій, синтезованої на основі додавання за модулем два.

Основний матеріал

У роботі [9] було отримано математичні моделі чотирьох операцій математичної групи симетричних операцій на основі додавання за модулем два, а саме:

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix}; \quad (1)$$

$$O_2 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}; \quad (2)$$

$$O_3 = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix}; \quad (3)$$

$$O_4 = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}. \quad (4)$$

Дані двоопераднді операції криптографічного перетворення інформації відомі і вже достатньо досліджені [2].

Результати дослідження дворозрядних одноопераднних операцій показали, що одноопераднді операції криптографічного перетворення інформації діляться на базові операції, операції перестановок, які накладаються на базові операції та операції інверсії, та операції перестановок [2]. Класифікація одноопераднних дворозрядних операцій криптографічного перетворення інформації наведена в табл. 1. Наведена група операцій включає 24 операції, тому що існує лише 24 таблиці підстановки для відображення результатів перетворення двох біт інформації.

Зважаючи на зазначене вище, можна допустити, що:

– двоопераднних операцій в математичній групі також повинно бути 24, тому що результат їх виконання також буде дворозрядним;

– двоопераднді операції також можуть бути класифіковані по аналогії з одноопераднними операціями.

Дослідимо можливість розширення кількості математичних моделей двоопераднних дворозрядних операції криптографічного перетворення інформації, побудованих на основі додавання за модулем два, та їх класифікації.

Таблиця 1

Класифікація одноопераднних дворозрядних 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	$F_{13}=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	$F_{14}=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}$	$F_{15}=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}$	$F_{16}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$
	$F_{17}=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	$F_{18}=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}$	$F_{19}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}$	$F_{20}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
	$F_{21}=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	$F_{22}=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}$	$F_{23}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\end{bmatrix}$	$F_{24}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$

Для цього порівняємо двоопераднді операції $O_1 - O_4$ з одноопераднними $F_1 - F_4$. Порівняльний аналіз показує (як видно з табл. 2), що в операції $O_1 - O_4$ дублюються змінні першого операнда змінними другого операнда.

Доведемо відзначені взаємозв'язки.

Для викладення результатів проведеного дослідження введемо наступні позначення: $F_1^1=\begin{bmatrix}x_1\\x_2\end{bmatrix}$ – операція перетворення першого операнда; $F_1^2=\begin{bmatrix}k_1\\k_2\end{bmatrix}$ – операція перетворення другого операнда.

Таблиця 2

Взаємозв'язки між одноопераднними і двоопераднними операціями криптографічного перетворення інформації

$F_1=\begin{bmatrix}x_1\\x_2\end{bmatrix}\to O_1=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}$	$F_2=\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}\to O_2=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}$
$F_3=\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}\to O_3=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\end{bmatrix}$	$F_4=\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}\to O_4=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\oplus 1\end{bmatrix}$

Проаналізуємо операцію (1–4):

$$O_1=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\k_2\end{bmatrix}=F_1^1\oplus F_1^2;$$

$$O_2 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = F_2^1 \oplus F_1^2;$$

$$O_3 = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = F_3^1 \oplus F_1^2;$$

$$O_4 = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = F_4^1 \oplus F_1^2.$$

На основі аналізу можна зробити висновок, що перших чотири операції можна отримати на основі перших чотирьох одноопераднних операцій обробки першого операнда, шляхом додавання операції додавання за модулем два базової для них операції перетворення другого операнда. Базові операції знаходяться в першому стовпчику табл. 1.

Допустимо, що на основі додавання за модулем два базової операції обробки другого операнда можна отримати інші двоопераднді операції з підгруп операцій інверсії.

Перевіримо це на прикладах.

Побудуємо операцію O_6. $O_6 = F_6^1 \oplus F_5^2 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}$.

Побудуємо операцію O_{11}. $O_{11} = F_{11}^1 \oplus F_9^2 = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix}$.

Побудуємо операцію O_{18}.

$$O_{18} = F_{18}^1 \oplus F_{17}^2 = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}.$$

Побудуємо операцію O_{24}.

$$O_{24} = F_{24}^1 \oplus F_{19}^2 = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_1 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}.$$

Результати побудови всіх 24 двоопераднних операцій наведено в табл. 3. Крім того, табл. 3 візуалізує результати класифікації першої симетричної групи двоопераднних дворозрядних операції криптографічного перетворення інформації.

Таблиця 3

Класифікація групи двоопераднних дворозрядних симетричних операцій криптоперетворення на основі додавання за модулем два

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	$O_1=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}$	$O_2=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}$	$O_3=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\end{bmatrix}$	$O_4=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\oplus 1\end{bmatrix}$
	$O_5=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_2\oplus k_2\end{bmatrix}$	$O_6=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_2\oplus k_2\oplus 1\end{bmatrix}$	$O_7=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_2\oplus k_2\end{bmatrix}$	$O_8=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_2\oplus k_2\oplus 1\end{bmatrix}$
	$O_9=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{10}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$	$O_{11}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{12}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
Операції перестановок	$O_{13}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix}$	$O_{14}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}$	$O_{15}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus k_1\end{bmatrix}$	$O_{16}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus k_1\oplus 1\end{bmatrix}$
	$O_{17}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{18}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$	$O_{19}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{20}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
	$O_{21}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_1\oplus k_1\end{bmatrix}$	$O_{22}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}$	$O_{23}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\oplus k_1\end{bmatrix}$	$O_{24}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\oplus k_1\oplus 1\end{bmatrix}$

Зважаючи, що перша класифікована базова операція є дворозрядною операцією додавання по модулю два, то дану математичну групу операцій, будемо називати групою дворозрядних двоопераднних симетричних операцій на основі додавання за модулем два.

Розробимо метод синтезу групи дворозрядних двоопераднних симетричних операцій додавання за модулем два на основі відомих одноопераднних дворозрядних операцій, та вже відомих методів їх синтезу [2]. Для розробки цього методу синтезу було проведено порівняльне дослідження табл. 1 і табл. 3.

У результаті проведеного дослідження встановлено, що група дворозрядних операцій додавання за модулем два включає в себе базову групу дворозрядних операцій додавання за модулем два, групу операцій перестановок та групу операцій інверсії. Виходячи з цього, узагальнимо результати дослідження:

– синтез двоопераднних дворозрядних операцій базової групи на основі поєднання по модулю два двох однакових одноопераднних операцій базової групи для обробки двох різних операндів:

– розширення двоопераднних дворозрядних операцій базової групи на основі перестановок до групи базових операцій і операцій перестановок;

– розширення групи двоопераднних дворозрядних операцій базової групи і операцій перестановок на основі операцій інверсії до групи дворозрядних операцій додавання за модулем два.

Отримані узагальнені результати дозволили розробити метод синтезу груп дворозрядних двоопераднних операцій для симетричного потокового шифрування, що полягає в наступному:

– синтез двоопераднних операцій базової групи на основі додавання за модулем два одноопераднних операцій обробки кожного операнда. Виконується перетворення на основі моделі $F = \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$. Зважаючи на це, перетворення операцій базової групи будуть представлені:

$$O_1 = F_1^1 \oplus F_1^2 = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix}$$

$$O_5 = F_5^1 \oplus F_5^2 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix}$$

$$O_9 = F_9^1 \oplus F_9^2 = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix}$$

– виконання над операціями базової групи операцій перестановок;

– виконання над операціями базової групи в поєднанні з операціями перестановок операцій інверсії.

Висновки

Розроблено метод синтезу групи операцій додавання за модулем два для потокового шифрування на основі операції додавання за модулем два.

Сутність розробленого методу полягає в синтезі дворозрядних двоопераднних базових операцій на основі поєднання однакових базових операцій для перетворення першого та другого операнда на основі додавання за модулем два. Побудова повної математичної групи даних операцій провадиться на основі додаткового застосування операцій перестановки та інверсії операндів двоопераднних базових операцій.

Застосування цього методу дозволяє синтезувати всі дворозрядні операції додавання за модулем два на основі застосування трьох базових одноопераднних дворозрядних операцій, дворозрядних операцій додавання за модулем два.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Рудницький В.М.* Криптографічне кодування: обробка та захист інформації: колективна монографія. Харків: ТОВ “ДІСА ПЛЮС”, 2018. 139 с.

2. *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.

3. *Бабенко В.Г., Лада Н.В.* Технологія дослідження операцій додавання за модулем. “Smart and Young”: щомісячний наук. журн. 2016. № 11–12. Ч. 1. С. 49–54.

4. *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.

5. *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.

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. *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.

8. *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.

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

REFERENCES

1. *Rudnitskyi V.M.* (2018). Kryptohrafichne koduvannia: obrobka ta zakhyst informatsii: kolektyvna monohrafiia. "Cryptographic encoding: processing and protection of information: a collective monograph", TOV "DISA PLIUS", Kharkiv, 139 p. [in Ukrainian].

2. *Rudnitskyi V.M., Lada N.V. and 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, 184 p. [in Ukrainian].

3. *Babenko V.H. and Lada N.V.* (2016). Tekhnolohiia doslidzhennia operatsii dodavannia za modulem. "Technology of research operations of addition modulo", Smart and Young: shchomisiachnyi naukovyi zhurnal, No. 11–12(118), Vol. 1., P. 49–54 [in Ukrainian].

4. *Babenko V.H.* (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, Kyiv, No. 4(24), P. 85–88 [in Ukrainian].

5. *Holub S. V., Babenko V.H. and Rudnytskyi S.V.* (2012). Metod syntezu operatsii kryptohrafichnoho peretvorennia na osnovi dodavannia za modulem dva. "The method of synthesis of cryptographic transformation operations based on addition modulo two". Systemy obrobky informaciyi. Zbirnyk naukovykh prats KHUPS im. I. Kozheduba, Kharkiv, Vol. 1, No. 3(101), P. 119–122 [in Ukrainian].

6. *Lada N.V. and 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, Poltava, No. 1(47), P. 127–130 [in Ukrainian].

7. *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, Kyiv, No. 4(55), P. 47–56 [in Ukrainian].

8. *Rudnitskyi V.M., Lada N.V. and 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, Kharkiv, Vol. 2, No. 4, P. 26–30 [in Ukrainian].

9. *Babenko V.H. and 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, Kharkiv, No. 2(118), P. 116–118 [in Ukrainian].

UDC 004.056.55:004.312.2

Lada Nataliia,
Candidate of Technical Sciences, Senior Lecturer,
Cherkasy State Technological University, Cherkasy, Ukraine,
ORCID ID 0000-0002-7682-2970
Kozlovska Svitlana,
Senior Lecturer, East European University of Economics
and Management, Cherkasy, Ukraine,
ORCID ID 0000-0002-1754-1220
Rudnytskyi Serhii,
Candidate of Technical Sciences, Senior Lecturer,
Cherkasy State Technological University, Cherkasy, Ukraine,
ORCID ID 0000-0003-4389-1088

THE SYMMETRIC OPERATIONS' MATHEMATICAL GROUP CONSTRUCTING BASED ON MODULO-2 ADDITION

The article is devoted to improving the quality of the stream ciphering systems for confidential information encryption through increasing the variability of cryptographic transformations by using a new group of two-operand two-bit operations synthesized basing on modulo-2 addition.

For achieving the aim, a comparative analysis of two-operand operations with one-operand operations was performed, which showed that the first four operations can be obtained basing on the first four one-operand operations of the first operand processing, by adding the modulo-2 addition operation of their base operation of transforming the second operand, and by modulo-2 adding the basic operation of processing the second operand it can be obtained the other two-operand operations from inversion operations' subgroups. The results of classifying a group of two-operand two-bit symmetric operations of information's cryptographic transformation were visualized, which made it possible to establish relationships between groups of one-and two-operand operations.

Basing on the obtained results, a method for synthesizing the operations' group of modulo-2 addition is developed for stream ciphering based on the modulo-2 addition operation. The method's crux is in the base group's two-bit two-operand operations synthesis, based on combining the same basic operations of converting the first and second operands by modulo-2 addition. Constructing a complete mathematical group of these operations is carried out by the additional use of permutation operations and operands' inversion of the base group operations.

The application of the method allows synthesizing all the twenty-four modifications of two-bit symmetric modulo-2 addition operations based on applying the three basic one-operand two-bit operations of information cryptographic conversion.

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

Отримано 16.10.2019