ТЕХНОЛОГІЯ ДОСЛІДЖЕННЯ ОПЕРАЦІЙ ДОДАВАННЯ ЗА МОДУЛЕМ

Бабенко В.Г.,
кандидат технічних наук, доцент
Черкаський державний технологічний університет,
Черкаси, Україна

Лада Н.В.,
асистент
Черкаський державний технологічний університет,
Черкаси, Україна

TECHNOLOGY OF RESEARCH OPERATIONS OF ADDITION MODULO

Babenko V.G.,
Ph.D., Cherkasy State Technological University,
Cherkasy, Ukraine

Lada N.V.,
teaching assistant
Cherkasy State Technological University,
Cherkasy, Ukraine

Анотація.

В статті запропоновано підхід щодо модифікації операції додавання за модулем два на основі перестановок результатів їх виконання та технологію їх дослідження.

Об'єкт дослідження – операції додавання за модулем два придатні для використання при криптографічному перетворенні.

Метою даної роботи є розробка технології дослідження модифікації операції додавання за модулем два з точністю до перестановки операндів та результатів її виконання.

Метод дослідження – моделювання операцій прямого і оберненого криптоперетворення інформації на основі повного перебору з послідуючим формальним описом для встановлення взаємозв'язків за рахунок використання теорії графів.

В даній статті досліджено чотири модифікації операції додавання за модулем два з точністю до перестановки операндів. Запропоновано спосіб отримання чотирьох модифікацій операції з точністю до перестановки результатів її виконання на основі кожної з модифікації операції додавання за модулем два з точністю до перестановки операндів.

Встановлено, що повну множину модифікацій операцій з точністю до перестановки результатів виконання операції можна побудувати на основі будь-якої модифікації операції з точністю до перестановки операндів за допомогою використання трьох попарних перестановок.

Ключові слова: *технологія, дослідження, операція додавання за модулем два, перестановка, криптографічне перетворення, модифікована операція.*

Abstract

This paper proposes an approach to the modification of the operation of addition modulo two based on permutations of the results of their execution and their research technology.

The object of study – the operation of addition modulo two are suitable for use in cryptographic transformation.

The method of research – modeling of direct and reverse operation of cryptographic transformation of information based on exhaustive search, followed by a formal description o determine relationships through the use of graph theory.

In this paper investigated four modifications of operation of addition modulo two up to a permutation of the operands. A method of producing four modifications of the operation up to a permutation of the results of its execution on the basis of each of the modification of the operation of addition modulo two up to a permutation of the operands.

It was found that the total number of modifications of operations up to a permutation of the operation results can be constructed on the basis of any modification of the operation up to a permutation of the operands by using three pairs of permutations.

***Keywords**: technology, research, operation of addition modulo two, permutation, cryptographic transformation, a modified operation.*

Постановка проблеми. Застосування перестановки як однієї з базових операцій перетворення інформації характерне при вирішенні багатьох прикладних задач, наприклад, для захисту інформації при розробці алгоритмів блокового та потокового шифрування, для підвищення ефективності алгоритмів стиснення інформації при використанні перестановки в алгоритмах перетворення інформації з метою приведення даних до виду більш зручному для стиснення, для реалізації алгоритмів кодування даних та багатьох інших. Найпоширенішими базовими для симетричних криптографічних алгоритмів є такі типи перестановок: проста перестановка, одинарна перестановка по ключу, подвійна перестановка, перестановка «магічний квадрат», циклічна перестановка та комбінаційні перестановки.

Для криптографічного перетворення перестановки поєднують із додаванням за модулем, так як дані операції доповнюють одна одну і в сукупності з іншими операціями забезпечують якість криптоперетворення. Виходячи з цього, було б доцільно поєднати в одній операції властивості як додавання за модулем так і перестановок. Слід відмітити, що збільшення кількості операцій придатних для реалізації криптографічних перетворень, з однієї сторони, розширює можливості розробників криптоалгоритмів, а, з іншої, ускладнює роботу крипто аналітиків.

Аналіз публікацій і досліджень. В [1, 2] на основі синтезу та аналізу операцій двохоперандного додавання за модулем два та чотири здійснено моделювання двохоперандних двохрозрядних матричних операцій, які володіють властивостями необхідними для криптоперетворення, а в [3] проведено синтез та дослідження множини операцій двохрозрядного криптографічного додавання за модулем два з точністю до перестановки та обґрунтована можливість застосування виявленої групи операцій в якості операції криптографічного додавання за модулем два. Роботи [4, 5] присвячені дослідженню груп операцій синтезованих на основі додавання за модулем два з точністю до перестановки з метою встановлення взаємозв'язків між групами та операндами. В [4] на основі визначених особливостей операцій групи виявлені взаємозв'язки між операціями, що дозволило використовувати синтезовані операції для прямого та оберненого перетворення інформації. В статті [5] представлені 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.

Проте дослідженню можливості використання в криптоперетвореннях груп операцій додавання за модулем з точністю до перестановок не приділялось достатньої уваги.

Метою даної роботи є розробка підходу щодо дослідження модифікації операції додавання за модулем два з точністю до перестановки операндів та результатів її виконання.

Виклад основного матеріалу. В роботі [2] були синтезовані операції додавання за модулем два з точністю до перестановки операндів:

$$O_1^{\oplus} = \begin{vmatrix} x_1 & \oplus y_1 \\ x_2 & \oplus y_2 \end{vmatrix}, \; O_2^{\oplus} = \begin{vmatrix} x_1 & \oplus y_2 \\ x_2 & \oplus y_1 \end{vmatrix},$$

$$O_3^{\oplus} = \begin{vmatrix} x_2 & \oplus y_1 \\ x_1 & \oplus y_2 \end{vmatrix}, \; O_4^{\oplus} = \begin{vmatrix} x_2 & \oplus y_2 \\ x_1 & \oplus y_1 \end{vmatrix},$$

де використані наступні позначення: $\oplus O_i$ – і-та операція криптографічного додавання за модулем два, x_1 і x_2 – перший та другий розряди першого операнда, y_1 і y_2 – перший та другий розряди другого операнда.

Розглянемо технологію дослідження даних операцій на прикладі операції $O_1^{\oplus}$. Для цього розглянемо результати перестановок результатів операції криптографічного перетворення інформації двох змінних $O_1^{\oplus} = \begin{vmatrix} x_1 & \oplus y_1 \\ x_2 & \oplus y_2 \end{vmatrix}$. Таблична форма представлення даної операції наведена в табл.1.

Таблиця 1

Таблична форма представлення операції $O_1^{\oplus}$

$O_1^{\oplus} = \begin{vmatrix} x_1 & \oplus y_1 \\ x_2 & \oplus y_2 \end{vmatrix}$

	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Над операндами даної операції можуть бути виконані 24 варіанти перестановки результатів виконання операції криптографічного перетворення інформації двох змінних (табл. 2).

Таблиця 2

Нумерація перестановок результатів виконання операції $O_1^{\oplus}$

Перестановка		Перестановка		Перестановка		Перестановка	
1	0 1 2 3	7	1 0 2 3	13	2 1 0 3	19	3 1 2 0
2	0 1 3 2	8	1 0 3 2	14	2 1 3 0	20	3 1 0 2
3	0 2 3 1	9	1 2 3 0	15	2 0 3 1	21	3 2 0 1
4	0 2 1 3	10	1 2 0 3	16	2 0 1 3	22	3 2 1 0
5	0 3 1 2	11	1 3 0 2	17	2 3 1 0	23	3 0 1 2
6	0 3 2 1	12	1 3 2 0	18	2 3 0 1	24	3 0 2 1

Застосувавши будь-яку з вищезазначених перестановок (табл. 2) результатів виконання операції, ми отримаємо модифіковану операцію $O_1^{\oplus}$.

В результаті проведення обчислювального експерименту по моделюванню прямого і оберненого перетворення інформації з використанням модифікованої операції $O_1^{\oplus}$ з точністю до перестановки результатів її виконання було встановлено, що лише 4 модифіковані операції з 24 можуть бути використані в криптографічному перетворенні.

Результати обчислювального експерименту для операції $O_1^{\oplus}$ наведені в табл. 3, де сірим кольором позначені перестановки, що можуть бути використані в криптографічному перетворенні.

Таблиця 3

Результати коректного використання операції $O_1^{\oplus}$ з точністю до перестановки результатів її виконання

	Перестановка		Перестановка		Перестановка		Перестановка	
$O_1^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$	1	0 1 2 3	7	1 0 2 3	13	2 1 0 3	19	3 1 2 0
	2	0 1 3 2	8	1 0 3 2	14	2 1 3 0	20	3 1 0 2
	3	0 2 3 1	9	1 2 3 0	15	2 0 3 1	21	3 2 0 1
	4	0 2 1 3	10	1 2 0 3	16	2 0 1 3	22	3 2 1 0
	5	0 3 1 2	11	1 3 0 2	17	2 3 1 0	23	3 0 1 2
	6	0 3 2 1	12	1 3 2 0	18	2 3 0 1	24	3 0 2 1

Для формалізації отриманих результатів досліджень введемо наступні позначення:

– $P^{op}_{(0123)}$ – перестановка операндів операції де 0, 1, 2, 3 – варіант перестановки операндів операції 0, 1, 2, 3;

– $P^{ro}_{(1023)}$ – перестановка результатів операції (реалізується перестановкою результатів в табличному представленні операції), де 1, 0, 2, 3 – варіант перестановки результатів операції 0, 1, 2, 3;

– $P^{op}_{(0123)}(O_1^{\oplus})$ – перестановка операндів операції $O_1^{\oplus}$, де $O_1^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$;

– $P^{ro}_{(1023)}(O_4^{\oplus})$ – перестановка результатів операції $O_4^{\oplus}$, де $O_4^{\oplus} = \begin{vmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{vmatrix}$.

Як видно з табл. 3. лише чотири варіанти перестановок операції $O_1^{\oplus}$ можуть бути використані для реалізації операцій криптоперетворення інформації, це перестановки $P^{op}_{(0123)}(O_1^{\oplus})$, $P^{op}_{(1032)}(O_1^{\oplus})$, $P^{op}_{(2301)}(O_1^{\oplus})$, $P^{op}_{(3210)}(O_1^{\oplus})$.

Таблиця 4

Таблична форма операцій на основі $O_1^{\oplus}$ з точністю до перестановки результатів її виконання придатних для криптоперетворення

$P^{op}_{(0123)}(O_1^{\oplus})$		0	1	2	3
	0	0	1	2	3
	1	1	0	3	2
	2	2	3	0	1
	3	3	2	1	0
$P^{op}_{(1032)}(O_1^{\oplus})$		0	1	2	3
	0	1	0	3	2
	1	0	1	2	3
	2	3	2	1	0
	3	2	3	0	1
$P^{op}_{(2301)}(O_1^{\oplus})$		0	1	2	3
	0	2	3	0	1
	1	3	2	1	0
	2	0	1	2	3
	3	1	0	3	2
$P^{op}_{(3210)}(O_1^{\oplus})$		0	1	2	3
	0	3	2	1	0
	1	2	3	0	1
	2	1	0	3	2
	3	0	1	2	3

Для встановлення взаємозв'язків між перестановками результатів виконання операції в модифікованих операціях на основі операції $O_1^{\oplus}$ розглянемо операції наведені в табл. 4 більш детально.

Дослідження процесу перестановок результатів виконання операції в модифікованих операціях можливе лише тоді, коли буде вибрана модифікована операція, відносно якої буде проводитися дослідження. Нехай вибрану для проведення дослідження модифіковану операцію будемо називати базовою. Для проведення дослідження представимо послідовність результатів виконання операції в порядку збільшення значень аргументів операцій.

На основі базової операції $P^{op}_{(0123)}(O_1^{\oplus})$ можуть бути побудовані три модифіковані операції $P^{op}_{(1032)}(O_1^{\oplus})$, $P^{op}_{(2301)}(O_1^{\oplus})$, $P^{op}_{(3210)}(O_1^{\oplus})$.

В результатах виконання операції $P^{op}_{(1032)}(O_1^{\oplus})$ відносно базової операції $P^{op}_{(0123)}(O_1^{\oplus})$ відбулася попарна перестановка результатів виконання операції: перестановка результатів виконання операції відносно значень аргументів 0 і 1, а також перестановка результатів виконання операції відносно значень аргументів 2 і 3.

При проведенні досліджень будемо визначати перестановки відносно значень аргументів, тому що вони не змінюються при виборі будь якої базової операції, що забезпечить однозначність результатів дослідження.

В результатах виконання операції $P^{op}_{(2301)}(O_1^{\oplus})$ відносно базової операції $P^{op}_{(0123)}(O_1^{\oplus})$ відбулася попарна перестановка результатів виконання операції: перестановка результатів виконання операції відносно значень аргументів 0 і 2, а також перестановка результатів виконання операції відносно значень аргументів 1 і 3.

В результатах виконання операції $P^{op}_{(3210)}(O_1^{\oplus})$ відносно базової операції $P^{op}_{(0123)}(O_1^{\oplus})$ відбулася попарна перестановка результатів виконання операції: перестановка результатів виконання операції відносно значень аргументів 0 і 3, а також перестановка результатів виконання операції відносно значень аргументів 1 і 2.

На основі базової операції $P^{op}_{(1032)}(O_1^{\oplus})$ можуть бути побудовані три модифіковані операції

$P^{op}_{(0123)}(O_1^{\oplus})$, $P^{op}_{(2301)}(O_1^{\oplus})$, $P^{op}_{(3210)}(O_1^{\oplus})$.

В результатах виконання операції $P^{op}_{(0123)}(O_1^{\oplus})$ відносно базової операції $P^{op}_{(1032)}(O_1^{\oplus})$ відбулася попарна перестановка результатів виконання операції: перестановка результатів виконання операції відносно значень аргументів 0 і 1, а також перестановка результатів виконання операції відносно значень аргументів 2 і 3. Дана попарна перестановка дозволяє на основі операції $P^{op}_{(0123)}(O_1^{\oplus})$ отримати операцію $P^{op}_{(1032)}(O_1^{\oplus})$ і навпаки, на основі операції $P^{op}_{(1032)}(O_1^{\oplus})$ отримати операцію $P^{op}_{(0123)}(O_1^{\oplus})$.

В результатах виконання операції $P^{op}_{(2301)}(O_1^{\oplus})$ відносно базової операції $P^{op}_{(1032)}(O_1^{\oplus})$ відбулася попарна перестановка результатів виконання операції: перестановка результатів виконання операції відносно значень аргументів 0 і 3, а також перестановка результатів виконання операції відносно значень аргументів 1 і 2. Дана попарна перестановка дозволяє на основі операції $P^{op}_{(2301)}(O_1^{\oplus})$ отримати операцію $P^{op}_{(1032)}(O_1^{\oplus})$ і навпаки, на основі операції $P^{op}_{(1032)}(O_1^{\oplus})$ отримати операцію $P^{op}_{(2301)}(O_1^{\oplus})$.

В результатах виконання операції $P^{op}_{(3210)}(O_1^{\oplus})$ відносно базової операції $P^{op}_{(1032)}(O_1^{\oplus})$ відбулася попарна перестановка результатів виконання операції: перестановка результатів виконання операції відносно значень аргументів 0 і 2, а також перестановка результатів виконання операції відносно значень аргументів 1 і 3.

На основі базової операції $P^{op}_{(2301)}(O_1^{\oplus})$ можуть бути побудовані три модифіковані операції $P^{op}_{(0123)}(O_1^{\oplus})$, $P^{op}_{(1032)}(O_1^{\oplus})$, $P^{op}_{(2301)}(O_1^{\oplus})$.

В результатах виконання операції $P^{op}_{(0123)}(O_1^{\oplus})$ відносно базової операції $P^{op}_{(2301)}(O_1^{\oplus})$ відбулася попарна перестановка результатів виконання операції: перестановка результатів виконання операції відносно значень аргументів 0 і 2, а також перестановка результатів виконання операції відносно значень аргументі 1 і 3.

В результатах виконання операції $P^{op}_{(1032)}(O_1^{\oplus})$ відносно базової операції $P^{op}_{(2301)}(O_1^{\oplus})$ відбулася попарна перестановка результатів виконання операції: перестановка результатів виконання операції відносно значень аргументів 0 і 3, а також перестановка результатів виконання операції відносно значень аргументів 1 і 2.

В результатах виконання операції $P^{op}_{(3210)}(O_1^{\oplus})$ відносно базової операції $P^{op}_{(2301)}(O_1^{\oplus})$ відбулася попарна перестановка результатів виконання операції: перестановка результатів виконання операції відносно значень аргументів 0 і 1, а також перестановка результатів виконання операції відносно значень аргументів 2 і 3.

На основі базової операції $P^{op}_{(3210)}(O_1^{\oplus})$ можуть бути побудовані три модифіковані операції $P^{op}_{(0123)}(O_1^{\oplus})$, $P^{op}_{(1032)}(O_1^{\oplus})$, $P^{op}_{(2301)}(O_1^{\oplus})$.

В результатах виконання операції $P^{op}_{(0123)}(O_1^{\oplus})$ відносно базової операції $P^{op}_{(3210)}(O_1^{\oplus})$ відбулася попарна перестановка результатів виконання операції: перестановка результатів виконання операції відносно значень аргументів 0 і 3, а також перестановка результатів виконання операції відносно значень аргументів 1 і 2.

В результатах виконання операції $P^{op}_{(1032)}(O_1^{\oplus})$ відносно базової операції $P^{op}_{(3210)}(O_1^{\oplus})$ відбулася попарна перестановка результатів виконання операції: перестановка результатів виконання операції відносно значень аргументів 0 і 2, а також перестановка результатів виконання операції відносно значень аргументі 1 і 3.

В результатах виконання операції результатів виконання операції: перестановка ре-

зультатів виконання операції відносно значень аргументів 0 і 1, а також перестановка результатів виконання операції відносно значень аргументів 2 і 3.

Як бачимо, всі операції з точністю до перестановки взаємопов'язані і будь-яку операцію з цієї групи можна отримати за допомогою трьох попарних перестановок.

В результаті дослідження було встановлено, що повну множину операцій з точністю до перестановки результатів можна побудувати на основі будь-якої з них за допомогою використання трьох варіантів попарних перестановок, а саме: 0 і 1 та 2 і 3; 0 і 2 та 1 і 3; 0 і 3 та 1 і 2.

Висновки. В даній статті досліджено чотири модифікації операції додавання за модулем два з точністю до перестановки операндів.

В результаті проведеного дослідження було встановлено, що на основі кожної з модифікації операції додавання за модулем два з точністю до перестановки операндів, можна отримати чотири модифікації даної операції з точністю до перестановки результатів її виконання.

Дослідження показало, що модифікації операцій з точністю до перестановки результатів можуть бути отримані за допомогою трьох попарних перестановок результатів їх виконання. Було встановлено, що повну множину модифікацій операцій з точністю до перестановки результатів виконання операції можна побудувати на основі будь-якої модифікації операції з точністю до перестановки операндів за допомогою використання трьох попарних перестановок.

Перелік посилань

1. Бабенко В.Г. Синтез і аналіз мікрооперацій для криптографічного перетворення / В.Г. Бабенко, Н.В. Лада, С.В. Лада // Проблеми інформатизації: Матер. другої міжнародн. наук.-техн. конф. тези доп., Черкаси-Тольятті, 25-26 листопада 2014 року. – Черкаси: ЧДТУ; Тольятті: ТДУ; 2014. – С. 9-10.

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

3. Бабенко В.Г. Дослідження множини операцій криптографічного додавання / В.Г. Бабенко, Н.В. Лада // «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2014): Тези доп. ІІ міжнародн. наук.-практ. конф., Черкаси, 24-26 квітня 2014 року. – Черкаси: ЧДТУ, 2014. – Т.1. – С. 135-136.

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

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

References

1. Babenko V.G., Lada N.V., Lada S.V. (2014). Synthesis and analysis micro-operations for cryptographic transformation. Proceedings of the Second International abstracts of scientific and technical conference "Problems of informatization". Cherkassy, Tolyatti. 25-26 November 2014. P. 9-10. (Ukr)

2. Babenko V.G., Lada N.V. (2014). Synthesis and analysis of cryptographic operations addition modulo two. Information processing systems. No. (2(118)). P. 116-118. (Ukr)

3. Babenko V.G., Lada N.V. (2014). Research set addition cryptographic operations. Proceedings of the Second International abstracts of scientific-practical conference "Information Technology in Education, Science and Technology". Cherkassy. 24-26 April 2014. Vol. 1. P. 135-136. (Ukr)

4. Babenko V.G., Lada N.V., Lada S.V. (2014). Analysis of set of operations synthesized on the basis of the addition modulo two. Proceedings of the Fifth International abstracts of scientific-practical conference "Methods and means of coding, compression and protection information". 19-21 April 2016. Vinnytsia. P. 54-57. (Ukr)

5. Babenko V.G., Lada N.V., Lada S.V. (2016). Research the relationship between the operations in matrix models of cryptographic transformation. Vysnyk ChDTU. No. 1. P. 5-11. (Ukr)