https://www.sworldjournal.com/index.php/swj/article/view/swj06-06-125
DOI: 10.30888/2663-5712.2020-06-06-125

УДК 004.056.55:004.312.2

REALIZATION OF GROUP TWO-OPERAND OPERATIONS STRONG STABLE CRYPTOGRAPHIC ENCODING

РЕАЛІЗАЦІЯ ГРУПИ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ СТРОГОГО СТІЙКОГО КРИПТОГРАФІЧНОГО КОДУВАННЯ

Pustovit M.O. / Пустовіт М.О.
ORCID: 0000-0001-5313-1459
Cherkasy Institute of Fire Safety named after Chornobyl Heroes,
Cherkasy, Onoprienko str 8, 18034
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України, Черкаси, Онопрієнка, 8, 18034

Анотація. *В роботі розглянуто застосування групи двохоперандних операцій строгого стійкого криптографічного кодування. Для узагальнення і класифікації операцій криптографічного перетворення інформації синтезовану групу операцій зведено до таблиці операцій кодування-декодування. В результаті математичних перетворень спрощених моделей операцій криптоперетворення та моделей обробки сигналів інверсії отримано узагальнену модель групи двохоперандних двохрозрядних операцій строгого стійкого криптографічного кодування. Встановлено, що для задання будь якої двохоперандної двохрозрядної операцій строгого стійкого криптографічного кодування достатньо задати лише два символи - перший визначає вираз для розрахунку значень без врахування інверсії, другий визначає наявність інверсії. Наведено варіанти кодування синтезованих двохоперандних двохрозрядних операцій строгого стійкого криптографічного кодування для спрощення реалізації на апаратному та програмному рівнях.*

Ключові слова: *криптографічне кодування, криптоперетворення, перестановки, надійність шифрування, строге стійке криптографічне кодування, синтез операцій.*

Вступ

Створення сучасних та надійних швидкодіючих методів криптоперетворення на основі логічних функцій від великої кількості змінних є важливим для розвитку криптографії в цілому. Серед напрямів її розвитку актуальним також є синтез і аналіз операцій криптографічного кодування інформації, що забезпечує теоретико-інструментальну базу для побудови нових та вдосконалення існуючих [1]. Синтез подібних операцій базується на використанні логічних функцій та об’єднує як системи захисту інформації, так і комп’ютерну інженерію. За своєю сутністю дані операції є нічим іншим як формалізованими багатоваріантними моделями підстановок, при реалізації яких за допомогою засобів обчислювальної техніки забезпечується висока ефективність захисту інформації [2-4].

Поруч з тим, удосконалення методів строгого стійкого криптографічного кодування як одного з напрямків криптоперетворення на основі логічних функцій є необхідним, адже приводить до невизначеності значення кожного біта незакодованого повідомлення при спробах його декодування [5].

Синтез прямих і обернених двохоперандних операцій строгого стійкого криптографічного кодування показано та досліджено в [5, 6]. Отримані в процесі дослідження операції криптографічного перетворення інформації вимагають додаткового дослідження направленого на їх узагальнення і

класифікацію.

Метою роботи є встановлення шляхів реалізації групи двохоперандних операцій строгого стійкого криптографічного кодування на апаратному та програмному рівнях.

Основний матеріал

Для практичної реалізації двохоперандних двохрозрядних операцій строгого стійкого криптографічного кодування необхідно:

- узагальнити побудовані моделі операцій криптоперетворення;
- встановити закономірності узагальненої моделі операцій необхідні для розробки алгоритму синтезу групи операцій на програмному та апаратному рівні;
- встановити взаємозв'язки між прямими і оберненими операціями для побудови потокових шифрів.

Отримані в процесі дослідження операції криптографічного перетворення інформації вимагають додаткового дослідження направленого на їх узагальнення і класифікацію. Для цього зведемо синтезовану групу операцій до таблиці операцій кодування-декодування. При побудові таблиці операцій скористаємося представленням моделі операції як поєднанням спрощеної моделі операцій, без врахування інверсій, та моделі обробки сигналів інверсії. Результати класифікації двохоперандних двохрозрядних операцій строгого стійкого криптографічного кодування наведені в табл. 1.

В табл. 1 наведені 24 двохоперандні двохрозрядні операції строгого стійкого криптографічного кодування. Дані операції поділено по 12 операцій в кожній з двох колонок, при цьому в одному рядку операції з першої колонки відповідає обернена операція з другої колонки і навпаки операції з другої колонки відповідає обернена до неї операція з першої колонки. З таблиці видно, що пари операції прямого і оберненого перетворення не перетинаються.

Дане представлення прямих і обернених операцій забезпечує спрощення програмної реалізації групи операцій так як забезпечує необхідність реалізації лише 12 прямих операцій і 12 обернених операцій а не 24 прямих і відповідних їм 24 обернених операцій.

Двомірний табличний запис адрес процедур виконання операцій криптоперетворення забезпечує реалізацію всієї групи операцій на основі додавання за модулем два, при нумерації стовпців таблиці як «0» і «1».

В табл. 1. відтінками сірого виділено групи операцій по чотири операції. Виділені операції мають однакові спрощені моделі. Наведемо виділені спрощені моделі:

$$O_3^{k*} = \begin{bmatrix} x_1 \cdot (\overline{y_1 \oplus y_2}) \oplus x_2 \cdot (y_1 \oplus y_2) \\ x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot (\overline{y_1 \oplus y_2}) \end{bmatrix} \quad (1)$$

$$O_{16}^{k*} = \begin{bmatrix} x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot (\overline{y_1 \oplus y_2}) \\ x_1 \cdot (\overline{y_1 \oplus y_2}) \oplus x_2 \cdot (y_1 \oplus y_2) \end{bmatrix} \quad (2)$$

$$O_1^{k*} = \begin{bmatrix} x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \\ x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \end{bmatrix} \quad (3)$$

$$O_{18}^{k*} = \begin{bmatrix} x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \\ x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \end{bmatrix} \quad (4)$$

$$O_{4}^{k*} = \begin{bmatrix} x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \end{bmatrix} \quad (5)$$

$$O_{14}^{k*} = \begin{bmatrix} x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \end{bmatrix} \quad (6)$$

Таблиця 1

Класифікація двохоперандних двохрозрядних операцій строгого стійкого криптографічного кодування

$O_3^k = O_6^d = \begin{bmatrix} x_1 \cdot (\overline{y_1 \oplus y_2}) \oplus x_2 \cdot (y_1 \oplus y_2) \\ x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot (\overline{y_1 \oplus y_2}) \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ \bar{y}_1 \end{bmatrix}$	$O_6^k = O_3^d = \begin{bmatrix} x_1 \cdot (\overline{y_1 \oplus y_2}) \oplus x_2 \cdot (y_1 \oplus y_2) \\ x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot (\overline{y_1 \oplus y_2}) \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix}$
$O_{12}^k = O_9^d = \begin{bmatrix} x_1 \cdot (\overline{y_1 \oplus y_2}) \oplus x_2 \cdot (y_1 \oplus y_2) \\ x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot (\overline{y_1 \oplus y_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_1 \\ y_1 \end{bmatrix}$	$O_9^k = O_{12}^d = \begin{bmatrix} x_1 \cdot (\overline{y_1 \oplus y_2}) \oplus x_2 \cdot (y_1 \oplus y_2) \\ x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot (\overline{y_1 \oplus y_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_2 \\ y_2 \end{bmatrix}$
$O_{16}^k = O_{23}^d = \begin{bmatrix} x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot (\overline{y_1 \oplus y_2}) \\ x_1 \cdot (\overline{y_1 \oplus y_2}) \oplus x_2 \cdot (y_1 \oplus y_2) \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ \bar{y}_1 \end{bmatrix}$	$O_{23}^k = O_{16}^d = \begin{bmatrix} x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot (\overline{y_1 \oplus y_2}) \\ x_1 \cdot (\overline{y_1 \oplus y_2}) \oplus x_2 \cdot (y_1 \oplus y_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_2 \\ y_2 \end{bmatrix}$
$O_{20}^k = O_{13}^d = \begin{bmatrix} x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot (\overline{y_1 \oplus y_2}) \\ x_1 \cdot (\overline{y_1 \oplus y_2}) \oplus x_2 \cdot (y_1 \oplus y_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_1 \\ y_1 \end{bmatrix}$	$O_{13}^k = O_{20}^d = \begin{bmatrix} x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot (\overline{y_1 \oplus y_2}) \\ x_1 \cdot (\overline{y_1 \oplus y_2}) \oplus x_2 \cdot (y_1 \oplus y_2) \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix}$
$O_1^k = O_2^d = \begin{bmatrix} x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \\ x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix}$	$O_2^k = O_1^d = \begin{bmatrix} x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \\ x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ \overline{y_1 \oplus y_2} \end{bmatrix}$
$O_8^k = O_7^d = \begin{bmatrix} x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \\ x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_2 \\ y_2 \end{bmatrix}$	$O_7^k = O_8^d = \begin{bmatrix} x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \\ x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{y_1 \oplus y_2} \\ y_1 \oplus y_2 \end{bmatrix}$
$O_{18}^k = O_{21}^d = \begin{bmatrix} x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \\ x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix}$	$O_{21}^k = O_{18}^d = \begin{bmatrix} x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \\ x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{y_1 \oplus y_2} \\ y_1 \oplus y_2 \end{bmatrix}$
$O_{22}^k = O_{17}^d = \begin{bmatrix} x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \\ x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_2 \\ y_2 \end{bmatrix}$	$O_{17}^k = O_{22}^d = \begin{bmatrix} x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \\ x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ \overline{\bar{y}_1 \oplus y_2} \end{bmatrix}$
$O_4^k = O_5^d = \begin{bmatrix} x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ \bar{y}_1 \end{bmatrix}$	$O_5^k = O_4^d = \begin{bmatrix} x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ \overline{y_1 \oplus y_2} \end{bmatrix}$
$O_{15}^k = O_{24}^d = \begin{bmatrix} x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \\ x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ \bar{y}_1 \end{bmatrix}$	$O_{24}^k = O_{15}^d = \begin{bmatrix} x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \\ x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \end{bmatrix} = \begin{bmatrix} \overline{y_1 \oplus y_2} \\ y_1 \oplus y_2 \end{bmatrix}$
$O_{14}^k = O_{19}^d = \begin{bmatrix} x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix}$	$O_{19}^k = O_{14}^d = \begin{bmatrix} x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ \bar{y}_1 \end{bmatrix}$
$O_{10}^k = O_{11}^d = \begin{bmatrix} x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_2 \\ y_2 \end{bmatrix}$	$O_{11}^k = O_{10}^d = \begin{bmatrix} x_1 \cdot \bar{y}_2 \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \bar{y}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_1 \\ y_1 \end{bmatrix}$

Авторська розробка

Узагальнивши спрощені моделі (1 - 6) отримаємо:

$$O_i^{k*} = \begin{bmatrix} a_{11} \cdot x_1 \oplus a_{12} \cdot x_2 \\ a_{21} \cdot x_1 \oplus a_{22} \cdot x_2 \end{bmatrix} \quad (7)$$

де $a_{11}=a_{22}$; $a_{12}=a_{21}$; $a_{11}=\bar{a}_{12}$; $a_{11}=\bar{a}_{21}$; $a_{lj}\in\{y_1, \bar{y}_1, y_2, \bar{y}_2, y_1\oplus y_2, \overline{y_1\oplus y_2}\}$

По аналогії розглянемо моделі обробки сигналів інверсії. Було виділено також шість груп моделей:

$$\overline{O}_3^k=\begin{bmatrix} y_1 \\ \bar{y}_1 \end{bmatrix} \quad (8)$$

$$\overline{O}_{11}^k=\begin{bmatrix} \bar{y}_1 \\ y_1 \end{bmatrix} \quad (9)$$

$$\overline{O}_1^k=\begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix} \quad (10)$$

$$\overline{O}_8^k=\begin{bmatrix} \bar{y}_2 \\ y_2 \end{bmatrix} \quad (11)$$

$$\overline{O}_2^k=\begin{bmatrix} y_1\oplus y_2 \\ \overline{y_1\oplus y_2} \end{bmatrix} \quad (12)$$

$$\overline{O}_7^k=\begin{bmatrix} \overline{y_1\oplus y_2} \\ y_1\oplus y_2 \end{bmatrix} \quad (13)$$

Узагальнивши моделі обробки сигналів інверсії (8 - 13) отримаємо:

$$\overline{O}_i^k=\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \quad (14)$$

де $b_1=\bar{b}_2$; $b_1\in\{y_1, \bar{y}_1, y_2, \bar{y}_2, y_1\oplus y_2, \overline{y_1\oplus y_2}\}$.

Об'єднавши вирази (4.7) і (4.14) отримаємо узагальнену модель групи двохоперандних двохрозрядних операцій строгого стійкого криптографічного кодування:

$$O_i^k=O_i^{k*}\oplus\overline{O}_i^k=\begin{bmatrix} a_{11}\cdot x_1\oplus a_{12}\cdot x_2 \\ a_{21}\cdot x_1\oplus a_{22}\cdot x_2 \end{bmatrix}\oplus\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \quad (14)$$

де $a_{11}=a_{22}$; $a_{12}=a_{21}$; $a_{11}=\bar{a}_{12}$; $a_{11}=\bar{a}_{21}$; $a_{lj}\in\{y_1, \bar{y}_1, y_2, \bar{y}_2, y_1\oplus y_2, \overline{y_1\oplus y_2}\}$;
$b_1=\bar{b}_2$; $b_1\in\{y_1, \bar{y}_1, y_2, \bar{y}_2, y_1\oplus y_2, \overline{y_1\oplus y_2}\}$.

На основі узагальненої моделі (14) можна стверджувати, що для задання будь якої двохоперандної двохрозрядної операцій строгого стійкого криптографічного кодування достатньо задати лише a_{11} і b_1.

Розглянемо один із варіантів задання a_{11}.

Так як $a_{11}\in\{y_1, \bar{y}_1, y_2, \bar{y}_2, y_1\oplus y_2, \overline{y_1\oplus y_2}\}$, то можна множину виразів для розрахунку значень, які приймає параметр, упорядкувати, виокремивши вирази для його розрахунку які не мають інверсії, і вирази які мають інверсію тоді $a_{11}\in\{y_1, y_2, y_1\oplus y_2, \bar{y}_1, \bar{y}_2, \overline{y_1\oplus y_2}\}$. Для кодування даної впорядкованої множини достатньо двох символів: перший символ визначає вираз для розрахунку значень без врахування інверсії, другий визначає наявність інверсії: $10\rightarrow y_1$; $20\rightarrow y_2$; $30\rightarrow y_1\oplus y_2$; $11\rightarrow \bar{y}_1$; $21\rightarrow \bar{y}_2$; $31\rightarrow \overline{y_1\oplus y_2}$.

Так як параметр b_1 має множину виразів для розрахунку значень, аналогічно a_{11} то реалізуємо його кодування також аналогічно.

Пронумеруємо і закодуємо двохоперандні двохрозрядні операції строгого стійкого криптографічного кодування відповідно до табл. 1.

Таблиця 2

Варіант кодування синтезованих двохоперандних двохрозрядних операцій строгого стійкого криптографічного кодування

№п/п	операція			№п/п	операція		
1.1	$O_3^k = O_6^d$	3011	110011	1.2	$O_6^k = O_3^d$	3021	110101
2.1	$O_{12}^k = O_9^d$	3010	110010	2.2	$O_9^k = O_{12}^d$	3020	110100
3.1	$O_{16}^k = O_{23}^d$	3111	111011	3.2	$O_{23}^k = O_{16}^d$	3120	111100
4.1	$O_{20}^k = O_{13}^d$	3110	111010	4.2	$O_{13}^k = O_{20}^d$	3121	111101
5.1	$O_1^k = O_2^d$	1021	010101	5.2	$O_2^k = O_1^d$	1031	010111
6.1	$O_8^k = O_7^d$	1020	010100	6.2	$O_7^k = O_8^d$	1030	010110
7.1	$O_{18}^k = O_{21}^d$	1121	011101	7.2	$O_{21}^k = O_{18}^d$	1130	011110
8.1	$O_{22}^k = O_{17}^d$	1120	011100	8.2	$O_{17}^k = O_{22}^d$	1131	011111
9.1	$O_4^k = O_5^d$	2011	100011	9.2	$O_5^k = O_4^d$	2031	100111
10.1	$O_{15}^k = O_{24}^d$	2111	101011	10.2	$O_{24}^k = O_{15}^d$	2130	101110
11.1	$O_{14}^k = O_{19}^d$	2021	100101	11.2	$O_{19}^k = O_{14}^d$	2011	100011
12.1	$O_{10}^k = O_{11}^d$	2020	100100	12.2	$O_{11}^k = O_{10}^d$	2010	100010

Авторська розробка

В табл. 2. наведено результати кодування операцій в десятковій і двійковій системі числення. Кодування в десятковій системі числення спрощує програмну реалізацію операцій прямого і оберненого криптоперетворення, а в двійковій системі числення апаратну реалізацію. По своїй сутності табл. 2, визначає алгоритм потокового шифрування побудований на основі застосування двох псевдовипадкових послідовностей [7, 8]. З цих двох послідовностей, одна являється послідовністю значень другого операнда, який визначає порядок перетворення першого операнда. Друга послідовність визначає операцію яка буде виконуватися для перетворення першого операнда під керівництвом другого.

Заключення та висновки

Застосування вищенаведених операцій може бути реалізовано двома шляхами:

- збільшення кількості операцій, які реалізують даний метод – що забезпечить додаткове збільшення варіативності алгоритмів потокового шифрування, і, як наслідок, збільшиться криптостійкість;
- застосування синтезованої групи операцій замість дванадцяти операцій додавання по модулю два з точністю до перестановки, що в свою чергу забезпечить збільшення варіативності алгоритму, а також призведе до максимальної невизначеності результатів шифрування, оскільки кожен біт вхідної інформації буде змінено з ймовірністю одна друга.

На основі проведеного дослідження розглянуто застосування групи двохоперандних операцій операцій строгого стійкого криптографічного

кодування. Встановлено, що для задання будь якої двохоперандної двохрозрядної операцій строгого стійкого криптографічного кодування достатньо задати лише два символи - перший визначає вираз для розрахунку значень без врахування інверсії, другий визначає наявність інверсії. Наведено варіанти кодування синтезованих двохоперандних двохрозрядних операцій строгого стійкого криптографічного кодування для спрощення реалізації на апаратному та програмному рівнях.

Застосування групи операцій для вдосконалення методу підвищення стійкості та надійності потокових шифрів забезпечить збільшення варіативності алгоритму та максимальну невизначеність результатів шифрування.

Література:

1. В. Бабенко, С. Рудницький, "Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення" // Системи обробки інформації: зб. наук. праць, № 9 (107), С. 130- 139, 2012.

2. В. Рудницький, І. Миронець, В. Бабенко, "Систематизація повної множини логічних функцій для криптографічного перетворення інформації" // Системи обробки інформації: зб. наук. праць, 2011, Вип. 8 (98), С. 184-188.

3. В. Рудницький, В. Бабенко, Д. Жиляєв, "Алгебраїчна структура множини логічних операцій кодування"// Наука і техніка Повітряних Сил Збройних Сил України, 2011, Вип. 2 (6), С. 112-114,

4. В. Рудницький, Л. Шувалова, О. Нестеренко, "Метод синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування" // Вісник Черкаського державного технологічного університету, 2017, Вип. 1, С. 5-10.

5. Рудницький В. М., Лада Н. В., Федотова-Півень І. М., Пустовіт М. О., Нестеренко О. Б. Побудова двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування // Системи управління, навігації та зв'язку, 2018, випуск 6(52) – с. 113-116.

6. В. М. Рудницький, Р. Ш. Бердибаєв, Р. В. Бреус, Н. В. Лада, М. О. Синтез обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда // Сучасні інформаційні системи», том 3, №4. – Харків, 2019 – с. 109-114.

7. Бабенко В. Г., Козловська С. Г. Особливості використання матричних операцій криптографічного перетворення інформації // Системи обробки інформації. 2015, № 3 (128). С. 84-87.

8. 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. Збірник наукових праць. – Полтава: ПНТУ, 2018. – Т. 1 (47). – С. 127-130.

Abstract. *Particular attention deserve the operations that in the process of information transformation on the basis of the subdued sequence provide the achievement of strong cryptographic encoding, which means the maximum uncertainty of the cryptographic transformation results. However, it was paid not enough attention to the synthesis of these operations nowadays, and the processes of constructing the inverse operations of strong*

cryptographic coding were not studied at all

The aim of the work is to establish implementation ways group of two-operand operations of strong stable cryptographic coding at the hardware and software levels.

In this paper considered the application of a group of two-operand operations of strong stable cryptographic encoding. To generalize and classify operations of cryptographic information transformation, the synthesized group of operations is reduced to a table of encoding-decoding operations. As a result of mathematical transformations simplified models of cryptographic transformations and models of signal processing inversion, obtained generalized model of a group two-operand two-bit operations strong stable cryptographic encoding. Proved that for specify any two-operand two-bit operations of strong stable cryptographic encoding it is enough to specify only two symbols - the first defines the expression for calculating values without inversion, the second determines inversion presence. Listed coding options synthesized two-operand two-bit operations of strong stable cryptographic encoding for simplification to implement at the hardware and software levels.

Key words: *cryptographic encryption, cryptographic transformations, permutations, reliability of encryption, strong cryptographic encoding, synthesis of operations.*

Науковий керівник: д.т.н., доц. Опірський І.Р.