УДК 004. 056.55:004.312.2 **doi: 10.26906/SUNZ.2019.4.095**

І. М. Федотова-Півень[1], Н. В. Лада[1], Г. В. Канашевич[1], М. О. Пустовіт[2]

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

ТЕХНОЛОГІЯ ПОБУДОВИ ДВОХОПЕРАНДНОЇ ЧОТИРЬОХРОЗРЯДНОЇ ОПЕРАЦІЇ МІНІМАЛЬНОЇ СКЛАДНОСТІ ДЛЯ СТРОГОГО СТІЙКОГО КРИПТОГРАФІЧНОГО КОДУВАННЯ

Розвиток методів строгого стійкого криптографічного кодування як одного з напрямків криптографічного кодування і декодування на основі логічних функцій є важливим, тому що приводить до значної невизначеності значення кожного біта незакодованого повідомлення при спробах декодування повідомлення. В статті для захисту інформаційних ресурсів застосовано логічні функції в операції матричного криптографічного перетворення інформації на основі додавання за модулем два. Розроблено технологію побудови двохоперандної чотирьохрозрядної операції мінімальної складності з властивістю строгого стійкого криптографічного кодування. Таке строге стійке криптографічне кодування призводить до значної невизначеності значення кожного біта незакодованого повідомлення при спробах декодування закодованого повідомлення. Технологія перевірена шляхом створення однієї з двохоперандних чотирьохрозрядних операцій для потокового шифрування.

Ключові слова: криптографічне перетворення, логічні функції, додавання за модулем два, строге стійке криптографічне кодування.

Вступ

Постановка проблеми. Розробка нових швидкодіючих методів криптографічного кодування і декодування на основі логічних функцій над великою кількістю змінних і впровадження цих методів в цифрових пристроях важлива для криптографічної науки і практики криптографії. Розвиток методів строгого стійкого криптографічного кодування як одного з напрямків криптографічного кодування і декодування на основі логічних функцій є важливим, тому що приводить до значної невизначеності значення кожного біта незакодованого повідомлення при спробах декодування повідомлення [1-8].

Аналіз останніх досліджень і публікацій. В [1, 9-11] створені та частково досліджені одноопераднді чотирьохрозрядні операції мінімальної складності з властивістю строгого стійкого криптографічного кодування. Проте, залишається не вирішеною актуальна задача розробки методів створення двохоперандних чотирьохрозрядних операцій мінімальної складності для строгого стійкого криптографічного кодування.

Метою статті є розробка технології побудови двохоперандних чотирьохрозрядних операцій мінімальної складності для строгого стійкого криптографічного кодування.

Основний зміст

Як відомо, *транспозицією* є перестановка, яка міняє місцями два елемента, а всі інші лишає нерухомими. Повний набір одноопераднді чотирьохрозрядних операцій мінімальної складності містить 42 операції в залежності від числа транспозицій [1]. Ці операції створено шляхом інверсії двох розрядів і транспозицій [1].

Виберемо 16 операцій з 42 для створення чотирьохрозрядної двохоперандної операції строгого стійкого криптографічного кодування з урахуванням таких вимог: 1) для 4-х розрядів операція з одним інвертованим переставленим розрядом і одним інвертованим не переставленим іншим розрядом має властивість строгого стійкого криптографічного кодування; 2) інверсія не переставленого розряду приводить до однозначного визначення біта, який інвертується не залежно від значення цього біта; 3) інверсія переставленого розряду робить невизначеним біт, який інвертується [1]; 4) збільшення кількості транспозицій елементів приводить до зменшення залежності результату шифрування від гамуючої послідовності і до збільшення складності реалізації алгоритму.

Вимогам 1-4 задовольняють операції, які можливо отримати з базового набору операцій $F_1^4 - F_6^4$ [1] шляхом однієї транспозиції елементів, наприклад $F_7^4 - F_{22}^4$ з табл. 2 (верхній індекс для F означає розрядність операції, а нижній – порядковий номер операції). Так, кожна результуюча операція (Р) з табл. 1 (П – початкова операція, Р – результуюча операція) отримана з відповідної початкової (базової) операції з допомогою вказаної транспозиції елементів з урахуванням вимог 1-4.

Таблиця 1 – **Отримання операцій строгого стійкого криптографічного кодування з однією транспозицією елементів**

Р	Т	П	Р	Т	П
F_3^4	$x_2, x_4 \oplus 1$	F_7^4	F_2^4	$x_2, x_3 \oplus 1$	F_{15}^4
F_1^4	$x_4, x_2 \oplus 1$	F_8^4	F_1^4	$x_2 \oplus 1, x_3$	F_{16}^4
F_6^4	$x_2, x_4 \oplus 1$	F_9^4	F_6^4	$x_2, x_3 \oplus 1$	F_{17}^4
F_4^4	$x_4, x_2 \oplus 1$	F_{10}^4	F_5^4	$x_2 \oplus 1, x_3$	F_{18}^4
F_3^4	$x_3, x_4 \oplus 1$	F_{11}^4	F_4^4	$x_1, x_2 \oplus 1$	F_{19}^4
F_2^4	$x_3 \oplus 1, x_4$	F_{12}^4	F_5^4	$x_1, x_2 \oplus 1$	F_{20}^4
F_5^4	$x_3, x_4 \oplus 1$	F_{13}^4	F_2^4	$x_1 \oplus 1, x_2$	F_{21}^4
F_4^4	$x_3 \oplus 1, x_4$	F_{14}^4	F_3^4	$x_1 \oplus 1, x_2$	F_{22}^4

Застосуванням двох транспозицій до кожної операції з базового набору $F_1^4 - F_6^4$ з урахуванням вимог 1-4 можливо отримати операції $F_{31}^4 - F_{42}^4$ (табл. 2).

Таблиця 2 – **Чотирьохрозрядні одноопераднді операції строгого стійкого криптографічного кодування**

Без транспозицій		
$F_1^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \\ x_3 \\ x_4 \end{bmatrix}$	$F_2^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix}$	$F_3^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix}$
$F_4^4 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix}$	$F_5^4 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix}$	$F_6^4 = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}$

Одна транспозиція в наборі з чотирьох елементів			
$F_7^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_4 \oplus 1 \\ x_3 \\ x_2 \end{bmatrix}$	$F_8^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_4 \\ x_3 \\ x_2 \oplus 1 \end{bmatrix}$	$F_9^4 = \begin{bmatrix} x_1 \\ x_4 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{10}^4 = \begin{bmatrix} x_1 \\ x_4 \\ x_3 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
$F_{11}^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix}$	$F_{12}^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix}$	$F_{13}^4 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix}$	$F_{14}^4 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix}$
$F_{15}^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \\ x_4 \end{bmatrix}$	$F_{16}^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_3 \\ x_2 \oplus 1 \\ x_4 \end{bmatrix}$	$F_{17}^4 = \begin{bmatrix} x_1 \\ x_3 \oplus 1 \\ x_2 \\ x_4 \oplus 1 \end{bmatrix}$	$F_{18}^4 = \begin{bmatrix} x_1 \\ x_3 \\ x_2 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}$
$F_{19}^4 = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix}$	$F_{20}^4 = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix}$	$F_{21}^4 = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix}$	$F_{22}^4 = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix}$
$F_{23}^4 = \begin{bmatrix} x_3 \oplus 1 \\ x_2 \oplus 1 \\ x_1 \\ x_4 \end{bmatrix}$	$F_{24}^4 = \begin{bmatrix} x_3 \oplus 1 \\ x_2 \\ x_1 \\ x_4 \oplus 1 \end{bmatrix}$	$F_{25}^4 = \begin{bmatrix} x_3 \\ x_2 \oplus 1 \\ x_1 \oplus 1 \\ x_4 \end{bmatrix}$	$F_{26}^4 = \begin{bmatrix} x_3 \\ x_2 \\ x_1 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix}$
$F_{27}^4 = \begin{bmatrix} x_4 \oplus 1 \\ x_2 \oplus 1 \\ x_3 \\ x_1 \end{bmatrix}$	$F_{28}^4 = \begin{bmatrix} x_4 \oplus 1 \\ x_2 \\ x_3 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{29}^4 = \begin{bmatrix} x_4 \\ x_2 \oplus 1 \\ x_3 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{30}^4 = \begin{bmatrix} x_4 \\ x_2 \\ x_3 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
Дві транспозиції в наборі з чотирьох елементів			
$F_{31}^4 = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix}$	$F_{32}^4 = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix}$	$F_{33}^4 = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix}$	$F_{34}^4 = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix}$
$F_{35}^4 = \begin{bmatrix} x_3 \oplus 1 \\ x_4 \oplus 1 \\ x_1 \\ x_2 \end{bmatrix}$	$F_{36}^4 = \begin{bmatrix} x_3 \oplus 1 \\ x_4 \\ x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{37}^4 = \begin{bmatrix} x_3 \\ x_4 \oplus 1 \\ x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{38}^4 = \begin{bmatrix} x_3 \\ x_4 \\ x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
$F_{39}^4 = \begin{bmatrix} x_4 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \\ x_1 \end{bmatrix}$	$F_{40}^4 = \begin{bmatrix} x_4 \oplus 1 \\ x_3 \\ x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{41}^4 = \begin{bmatrix} x_4 \\ x_3 \oplus 1 \\ x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{42}^4 = \begin{bmatrix} x_4 \\ x_3 \\ x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$

По аналогії з моделлю двохрозрядного двохопераднього додавання за модулем два [12] використаємо операції О для всіх можливих наборів (k_1–k_4) значень чотирьох розрядів ($k_i \in \{0;1\}, i = \overline{1,4}$) як керуючих сигналів для побудови двохопераднді 4-хрозрядної операції додавання за модулем 2, яка має властивість строгого стійкого криптографічного кодування:

$$O = \begin{cases} F_7^4, & для\ k_1 = 0;\ k_2 = 0,\ k_3 = 0;\ k_4 = 0; \\ F_8^4, & для\ k_1 = 0;\ k_2 = 0,\ k_3 = 0;\ k_4 = 1; \\ F_9^4, & для\ k_1 = 0;\ k_2 = 0,\ k_3 = 1;\ k_4 = 0; \\ F_{10}^4, & для\ k_1 = 0;\ k_2 = 0,\ k_3 = 1;\ k_4 = 1; \\ F_{11}^4, & для\ k_1 = 0;\ k_2 = 1,\ k_3 = 0;\ k_4 = 0; \\ F_{12}^4, & для\ k_1 = 0;\ k_2 = 1,\ k_3 = 0;\ k_4 = 1; \\ F_{13}^4, & для\ k_1 = 0;\ k_2 = 1,\ k_3 = 1;\ k_4 = 0; \\ F_{14}^4, & для\ k_1 = 0;\ k_2 = 1,\ k_3 = 1;\ k_4 = 1; \\ F_{15}^4, & для\ k_1 = 1;\ k_2 = 0,\ k_3 = 0;\ k_4 = 0; \\ F_{16}^4, & для\ k_1 = 1;\ k_2 = 0,\ k_3 = 0;\ k_4 = 1; \\ F_{17}^4, & для\ k_1 = 1;\ k_2 = 0,\ k_3 = 1;\ k_4 = 0; \\ F_{18}^4, & для\ k_1 = 1;\ k_2 = 0,\ k_3 = 1;\ k_4 = 1; \\ F_{19}^4, & для\ k_1 = 1;\ k_2 = 1,\ k_3 = 0;\ k_4 = 0; \\ F_{20}^4, & для\ k_1 = 1;\ k_2 = 1,\ k_3 = 0;\ k_4 = 1; \\ F_{21}^4, & для\ k_1 = 1;\ k_2 = 1,\ k_3 = 1;\ k_4 = 0; \\ F_{22}^4, & для\ k_1 = 1;\ k_2 = 1,\ k_3 = 1;\ k_4 = 1 \end{cases} \quad (1)$$

Створимо двохопераднді чотирьохрозрядні операції строгого стійкого криптографічного кодування на основі одноопераднди операцій з їх почерговим додаванням за модулем два таким чином:

$$O^k = O^{k*} \oplus \overline{O}^k, \quad (2)$$

де O^k – модель чотирьохрозрядної двохопераднді операції строгого стійкого криптографічного кодування, O^{k*} – модель спрощеної операції, без врахування інверсій функцій, $\overline{O}^k$ – модель обробки сигналів інверсії функцій даної операції.

Для створення O^{k*} побудуємо таблиці істинності моделі даної спрощеної операції. Для цього використаємо матричне представлення операцій без врахування сигналів інверсії, в поєднанні з додаванням за модулем два до матриці інверсій (табл. 3).

В результаті отримаємо таблицю істинності (табл. 4) враховуючи те, що кожній елементарній функції одноопераднді операції відповідає змінна в моделі спрощеної операції, а узагальнена модель одноопераднді операції визначається також відповідним набором команд керування. Після мінімізації отримуємо наступні функції для спрощеної моделі:

Для побудови $f_1(x, y)$ отримуємо:

$$f_1(x_1, y) = x_1 \cdot (\overline{y}_1 \vee \overline{y}_2);\ \ f_1(x_3, y) = 0;$$
$$f_1(x_2, y) = x_2 \cdot (y_1 \cdot y_2);\ \ f_1(x_4, y) = 0.$$

В результаті об'єднання цих функцій з допомогою додавання за модулем два маємо $f_1(x, y)$:

$$f_1(x, y) = x_1 \cdot (\overline{y}_1 \vee \overline{y}_2) \oplus x_2 \cdot (y_1 \cdot y_2) = \\ = x_1 \cdot \overline{(y_1 \cdot y_2)} \oplus x_2 \cdot (y_1 \cdot y_2) \quad (3)$$

або $f_1(x, y) = x_1 \cdot \overline{(y_1 \cdot y_2)} \vee x_2 \cdot (y_1 \cdot y_2)$.

Таблиця 3 – **Матричне представлення вибраних однооперандних операцій**

$F_7^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_4 \oplus 1 \\ x_3 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0001 \\ 0010 \\ 0100 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$	$F_8^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_4 \\ x_3 \\ x_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0001 \\ 0010 \\ 0100 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$	$F_9^4 = \begin{bmatrix} x_1 \\ x_4 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0001 \\ 0010 \\ 0100 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$	$F_{10}^4 = \begin{bmatrix} x_1 \\ x_4 \\ x_3 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0001 \\ 0010 \\ 0100 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$
$F_{11}^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$	$F_{12}^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$	$F_{13}^4 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_4 \oplus 1 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$	$F_{14}^4 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$
$F_{15}^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_3 \oplus 1 \\ x_2 \\ x_4 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0010 \\ 0100 \\ 0001 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$	$F_{16}^4 = \begin{bmatrix} x_1 \oplus 1 \\ x_3 \\ x_2 \oplus 1 \\ x_4 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0010 \\ 0100 \\ 0001 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$	$F_{17}^4 = \begin{bmatrix} x_1 \\ x_3 \oplus 1 \\ x_2 \\ x_4 \oplus 1 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0010 \\ 0100 \\ 0001 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$	$F_{18}^4 = \begin{bmatrix} x_1 \\ x_3 \\ x_2 \oplus 1 \\ x_4 \oplus 1 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0010 \\ 0100 \\ 0001 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$
$F_{19}^4 = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0100 \\ 1000 \\ 0010 \\ 0001 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$	$F_{20}^4 = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix} = \begin{bmatrix} 0100 \\ 1000 \\ 0010 \\ 0001 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$	$F_{21}^4 = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_3 \oplus 1 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0100 \\ 1000 \\ 0010 \\ 0001 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$	$F_{22}^4 = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \\ x_3 \\ x_4 \oplus 1 \end{bmatrix} = \begin{bmatrix} 0100 \\ 1000 \\ 0010 \\ 0001 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$

Таблиця 4 – **Таблиця істинності для моделі спрощеної операції**

Операція	Команди (аргумент y)				Параметри елементів спрощеної моделі															
					$f_1(x,y)$				$f_2(x,y)$				$f_3(x,y)$				$f_4(x,y)$			
	y_1	y_2	y_3	y_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4
F_7^4	0	0	0	0	**1**	0	0	0	0	0	0	**1**	0	0	**1**	0	0	**1**	0	0
F_8^4	0	0	0	1	**1**	0	0	0	0	0	0	**1**	0	0	**1**	0	0	**1**	0	0
F_9^4	0	0	1	0	**1**	0	0	0	0	0	0	**1**	0	0	**1**	0	0	**1**	0	0
F_{10}^4	0	0	1	1	**1**	0	0	0	0	0	0	**1**	0	0	**1**	0	0	**1**	0	0
F_{11}^4	0	1	0	0	**1**	0	0	0	0	**1**	0	0	0	0	0	**1**	0	0	**1**	0
F_{12}^4	0	1	0	1	**1**	0	0	0	0	**1**	0	0	0	0	0	**1**	0	0	**1**	0
F_{13}^4	0	1	1	0	**1**	0	0	0	0	**1**	0	0	0	0	0	**1**	0	0	**1**	0
F_{14}^4	0	1	1	1	**1**	0	0	0	0	**1**	0	0	0	0	0	**1**	0	0	**1**	0
F_{15}^4	1	0	0	0	**1**	0	0	0	0	0	**1**	0	0	**1**	0	0	0	0	0	**1**
F_{16}^4	1	0	0	1	**1**	0	0	0	0	0	**1**	0	0	**1**	0	0	0	0	0	**1**
F_{17}^4	1	0	1	0	**1**	0	0	0	0	0	**1**	0	0	**1**	0	0	0	0	0	**1**
F_{18}^4	1	0	1	1	**1**	0	0	0	0	0	**1**	0	0	**1**	0	0	0	0	0	**1**
F_{19}^4	1	1	0	0	0	**1**	0	0	**1**	0	0	0	0	0	**1**	0	0	0	0	**1**
F_{20}^4	1	1	0	1	0	**1**	0	0	**1**	0	0	0	0	0	**1**	0	0	0	0	**1**
F_{21}^4	1	1	1	0	0	**1**	0	0	**1**	0	0	0	0	0	**1**	0	0	0	0	**1**
F_{22}^4	1	1	1	1	0	**1**	0	0	**1**	0	0	0	0	0	**1**	0	0	0	0	**1**

Побудуємо $f_2(x,y)$:

$f_2(x_1,y) = x_1 \cdot (y_1 \cdot y_2)$; $f_2(x_3,y) = x_3 \cdot (y_1 \cdot \overline{y}_2)$;

$f_2(x_2,y) = x_2 \cdot (\overline{y}_1 \cdot y_2)$; $f_2(x_4,y) = x_4 \cdot (\overline{y}_1 \cdot \overline{y}_2)$.

В результаті об'єднання цих функцій з допомогою додавання за модулем два маємо $f_2(x,y)$:

$$f_2(x,y) = x_1 \cdot (y_1 \cdot y_2) \oplus x_2 \cdot (\overline{y}_1 \cdot y_2) \oplus \oplus x_3 \cdot (y_1 \cdot \overline{y}_2) \oplus x_4 \cdot (\overline{y}_1 \cdot \overline{y}_2), \quad (4)$$

або

$$f_2(x,y) = x_1 \cdot (y_1 \cdot y_2) \vee x_2 \cdot (\overline{y}_1 \cdot y_2) \vee x_3 \cdot (y_1 \cdot \overline{y}_2) \vee x_4 \cdot (\overline{y}_1 \cdot \overline{y}_2).$$

Побудуємо $f_3(x,y)$:

$f_3(x_1,y) = 0$; $f_3(x_2,y) = x_2 \cdot (y_1 \cdot \overline{y}_2)$;

$f_3(x_3,y) = x_3 \cdot (y_1 \oplus y_2 \oplus 1)$; $f_3(x_4,y) = x_4 \cdot (\overline{y}_1 \cdot y_2)$.

В результаті об'єднання цих функцій з допомогою додавання за модулем два отримуємо $f_3(x,y)$:

$$f_3(x,y) = x_2 \cdot (y_1 \cdot \overline{y}_2) \oplus x_3 \cdot (y_1 \oplus y_2 \oplus 1) \oplus x_4 \cdot (\overline{y}_1 \cdot y_2) \quad (5)$$

або

$$f_3(x,y) = x_2 \cdot (y_1 \cdot \overline{y}_2) \vee x_3 \cdot (y_1 \oplus y_2 \oplus 1) \vee x_4 \cdot (\overline{y}_1 \cdot y_2).$$

Побудуємо $f_4(x,y)$:

$f_4(x_1,y)=0$; $f_4(x_2,y)=x_2\cdot(\bar{y}_1\cdot\bar{y}_2)$;

$f_4(x_3,y)=x_3\cdot(\bar{y}_1\cdot y_2)$; $f_4(x_4,y)=x_4\cdot y_1$.

В результаті об'єднання цих функцій з допомогою додавання за модулем два маємо $f_4(x,y)$:

$$f_4(x,y)=x_2\cdot(\bar{y}_1\cdot\bar{y}_2)\oplus x_3\cdot(\bar{y}_1\cdot y_2)\oplus x_4\cdot y_1 \quad (6)$$

або $f_4(x,y)=x_2\cdot(\bar{y}_1\cdot\bar{y}_2)\vee x_3\cdot(\bar{y}_1\cdot y_2)\vee x_4\cdot y_1$.

З допомогою формул (3) – (6) створимо модель спрощеної операції:

$$O^{k*}=\begin{bmatrix} x_1\cdot(\overline{y_1\cdot y_2})\oplus x_2\cdot(y_1\cdot y_2)\\ x_1\cdot(y_1\cdot y_2)\oplus x_2\cdot(\bar{y}_1\cdot y_2)\oplus\\ \quad\oplus x_3\cdot(y_1\cdot\bar{y}_2)\oplus x_4\cdot(\bar{y}_1\cdot\bar{y}_2)\\ x_2\cdot(y_1\cdot\bar{y}_2)\oplus x_3\cdot(y_1\oplus y_2\oplus 1)\oplus\\ \quad\oplus x_4\cdot(\bar{y}_1\cdot y_2)\\ x_2\cdot(\bar{y}_1\cdot\bar{y}_2)\oplus x_3\cdot(\bar{y}_1\cdot y_2)\oplus x_4\cdot y_1 \end{bmatrix}. \quad (7)$$

Для створення моделі обробки сигналів інверсії функцій даної операції побудуємо таблицю істинності (табл. 5).

Таблиця 5 – **Таблиця істинності моделі обробки сигналів інверсії функцій для операції строгого стійкого криптографічного кодування**

Команди (аргумент y)				Параметри інверсії функцій			
y_1	y_2	y_3	y_4	$\bar{f}_1$	$\bar{f}_2$	$\bar{f}_3$	$\bar{f}_4$
0	0	0	0	**1**	**1**	**0**	**0**
0	0	0	1	**1**	**0**	**0**	**1**
0	0	1	0	**0**	**1**	**1**	**0**
0	0	1	1	**0**	**0**	**1**	**1**
0	1	0	0	**1**	**0**	**1**	**0**
0	1	0	1	**1**	**0**	**0**	**1**
0	1	1	0	**0**	**1**	**1**	**0**
0	1	1	1	**0**	**1**	**0**	**1**
1	0	0	0	**1**	**1**	**0**	**0**
1	0	0	1	**1**	**0**	**1**	**0**
1	0	1	0	**0**	**1**	**0**	**1**
1	0	1	1	**0**	**0**	**1**	**1**
1	1	0	0	**1**	**0**	**1**	**0**
1	1	0	1	**1**	**0**	**0**	**1**
1	1	1	0	**0**	**1**	**1**	**0**
1	1	1	1	**0**	**1**	**0**	**1**

За результатами мінімізації маємо:

$\bar{f}_1=\bar{y}_3$; $\bar{f}_2=y_2\cdot y_3\vee\bar{y}_2\cdot\bar{y}_4$;

$\bar{f}_3=y_1\cdot\bar{y}_4\cdot y_3\vee\bar{y}_1\cdot\bar{y}_2\cdot y_3\vee y_1\cdot\bar{y}_2\cdot y_4$;

$\bar{f}_4=\bar{y}_1\cdot y_4\vee y_2\cdot y_4\vee y_1\cdot\bar{y}_2\cdot y_3$.

$$\bar{O}^k=\begin{bmatrix} \bar{y}_3\\ y_2\cdot y_3\vee\bar{y}_2\cdot\bar{y}_4\\ y_1\cdot\bar{y}_4\cdot y_3\vee\bar{y}_1\cdot\bar{y}_2\cdot y_3\vee y_1\cdot\bar{y}_2\cdot y_4\\ \bar{y}_1\cdot y_4\vee y_2\cdot y_4\vee y_1\cdot\bar{y}_2\cdot y_3 \end{bmatrix}. \quad (8)$$

Підставимо (7) і (8) у (2) і отримаємо чотирьохрозрядну двохоперандну операцію строгого стійкого криптографічного кодування:

$$O^k=\begin{bmatrix} x_1\cdot(\overline{y_1\cdot y_2})\oplus x_2\cdot(y_1\cdot y_2)\\ x_1\cdot(y_1\cdot y_2)\oplus x_2\cdot(\bar{y}_1\cdot y_2)\oplus x_3\cdot(y_1\cdot\bar{y}_2)\oplus\\ \quad\oplus x_4\cdot(\bar{y}_1\cdot\bar{y}_2)\\ x_2\cdot(y_1\cdot\bar{y}_2)\oplus x_3\cdot(y_1\oplus y_2\oplus 1)\oplus x_4\cdot(\bar{y}_1\cdot y_2)\\ x_2\cdot(\bar{y}_1\cdot\bar{y}_2)\oplus x_3\cdot(\bar{y}_1\cdot y_2)\oplus x_4\cdot y_1 \end{bmatrix}\oplus$$

$$\oplus\begin{bmatrix} \bar{y}_3\\ y_2\cdot y_3\vee\bar{y}_2\cdot\bar{y}_4\\ y_1\cdot\bar{y}_4\cdot y_3\vee\bar{y}_1\cdot\bar{y}_2\cdot y_3\vee y_1\cdot\bar{y}_2\cdot y_4\\ \bar{y}_1\cdot y_4\vee y_2\cdot y_4\vee y_1\cdot\bar{y}_2\cdot y_3 \end{bmatrix};$$

$$O^k=\begin{bmatrix} x_1\cdot(\overline{y_1\cdot y_2})\oplus x_2\cdot(y_1\cdot y_2)\oplus\bar{y}_3\\ x_1\cdot(y_1\cdot y_2)\oplus x_2\cdot(\bar{y}_1\cdot y_2)\oplus x_3\cdot(y_1\cdot\bar{y}_2)\oplus\\ \quad\oplus x_4\cdot(\bar{y}_1\cdot\bar{y}_2)\oplus y_2\cdot y_3\vee\bar{y}_2\cdot\bar{y}_4\\ x_2\cdot(y_1\cdot\bar{y}_2)\oplus x_3\cdot(y_1\oplus y_2\oplus 1)\oplus\\ \quad\oplus x_4\cdot(\bar{y}_1\cdot y_2)\oplus y_1\cdot\bar{y}_4\cdot y_3\vee\\ \quad\vee\bar{y}_1\cdot\bar{y}_2\cdot y_3\vee y_1\cdot\bar{y}_2\cdot y_4\\ x_2\cdot(\bar{y}_1\cdot\bar{y}_2)\oplus x_3\cdot(\bar{y}_1\cdot y_2)\oplus x_4\cdot y_1\oplus\\ \quad\oplus\bar{y}_1\cdot y_4\vee y_2\cdot y_4\vee y_1\cdot\bar{y}_2\cdot y_3 \end{bmatrix} \quad (9)$$

Операція (9) забезпечує оброблення чотирьох біт інформації за критерієм строгого стійкого криптографічного кодування. Таким чином, дану узагальнену модель можна розглядати як узагальнену двохоперандну чотирьохрозрядну операцію з властивістю строгого стійкого криптографічного кодування. Запропоновану послідовність математичних перетворень, яка забезпечує побудову узагальненої моделі операцій можна розглядати як технологію побудови двохоперандної чотирьохрозрядної операції мінімальної складності з властивістю строгого стійкого криптографічного кодування.

Висновки

Запропонована технологія побудови двохоперандної чотирьохрозрядної операції мінімальної складності з властивістю строгого стійкого криптографічного кодування, яка перевірена шляхом створення однієї з двохоперандних чотирьохрозрядних операцій для потокового шифрування.

СПИСОК ЛІТЕРАТУРИ

1. В. М. Рудницький, Л. А. Шувалова, О. Б. Нестеренко. Побудова примітивів строгого стійкого кодування мінімальної складності. Вісник Черкаського державного технологічного університету №1, 2018, с. 21-26.
2. Manikandan V, Porkodi V, Mohammed AS, Sivaram M, "Privacy Preserving Data Mining Using Threshold Based Fuzzy cmeans Clustering", ICTACT Journal on Soft Computing, Volume 9, Issue 1, 2018, pp.1813-1816. DOI: 10.21917/ijsc.2018.0252
3. Saravanan S., Hailu M., Gouse G.M., Lavanya M., Vijaysai R. Optimized Secure Scan Flip Flop to Thwart Side Channel Attack in Crypto-Chip. *International Conference on Advances of Science and Technology*, ICAST 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Vol 274. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-15357-1_34

4. Amin Salih M., Yuvaraj D., Sivaram M., Porkodi V. Detection And Removal Of Black Hole Attack In Mobile Ad Hoc Networks Using Grp Protocol. *International Journal of Advanced Research in Computer Science*. Vol. 9, No 6. P. 1–6, DOI: http://dx.doi.org/10.26483/ijarcs.v9i6.6335
5. Mozhaev O. Multiservise network security metric / O. Mozhaev, H. Kuchuk, N. Kuchuk, M. Mozhaev, M. Lohvynenco // IEEE Advanced information and communication technologies-2017. Proc. of the 2th Int. Conf. – Lviv, 2017. – P. 133-136.
6. Kuchuk G., Kovalenko A., Komari I.E., Svyrydov A., Kharchenko V.. Improving big data centers energy efficiency: Traffic based model and method. Studies in Systems, Decision and Control, vol 171. Kharchenko, V., Kondratenko, Y., Kacprzyk, J. (Eds.). Springer Nature Switzerland AG, 2019. Pp. 161-183. DOI: http://doi.org/10.1007/978-3-030-00253-4_8
7. Svyrydov, A., Kuchuk, H., Tsiapa, O. (2018), "Improving efficienty of image recognition process: Approach and case study", Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018, pp. 593-597, DOI: http://dx.doi.org/10.1109/DESSERT.2018.8409201
8. Кучук Г.А. Метод мінімізації середньої затримки пакетів у віртуальних з'єднаннях мережі підтримки хмарного сервісу / Г.А. Кучук, А.А. Коваленко, Н.В. Лукова-Чуйко // Системи управління, навігації та зв'язку. – Полтава . ПНТУ, 2017. – Вип. 2(42). – С. 117-120.
9. Рудницький В.М. Синтез операцій криптографічного перетворення за критерієм строгого стійкого кодування / В.М. Рудницький, Л.А. Шувалова, О. Б. Нестеренко // Часопис "Вісник інженерної академії України". – Київ, 2016. – Вип. 3. – С.105-108.
10. Рудницький В.М. Метод синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування / В.М. Рудницький, Л.А. Шувалова, О.Б. Нестеренко // "Вісник ЧДТУ". - Черкаси, 2017. – Вип. 1. – С.5-10.
11. Шувалова Л.А. Синтез та аналіз криптографічних операцій за критерієм строгого стійкого кодування / Л.А. Шувалова, О.Б. Нестеренко // тези доповідей IV міжнародної науково-технічної конференції „Проблеми інформатизації", 3-4 листопада 2016р. – Черкаси: ЧДТУ; Баку: ВА ЗСАР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2016. – С. 14.
12. Бабенко В. Г., Лада Н. В., Лада С. В. Аналіз множин операцій, синтезованих на основі додавання за модулем два. Методи та засоби кодування, захисту й ущільнення інформації: тези доп. П'ятої міжнар. наук.- практ. конф., (Вінниця, 19–21 квіт. 2016). Вінниця: Нілан - ЛТД, 2016. С. 54–57.

Рецензент: д-р техн. наук, проф. С. Г. Семенов,
Національний технічний університет «ХПІ», Харків
Received (Надійшла) 06.06.2019
Accepted for publication (Прийнята до друку) 21.08.2019

Технология построения двухоперандной четырехразрядной операции минимальной сложности для строгого устойчивого криптографического кодирования

И. Н. Федотова-Пивень, Н. В. Лада, Г. В. Канашевич, М. О. Пустовит

Развитие методов строгого устойчивого криптографической кодирования как одного из направлений криптографической кодирования и декодирования на основе логических функций является важным, так как приводит к значительной неопределенности значение каждого бита незакодированный сообщение при попытках декодирования сообщения. В статье для защиты информационных ресурсов применены логические функции в операции матричного криптографического преобразования информации на основе сложения по модулю два. Разработана технология построения двухоперандной четырехразрядной операции минимальной сложности со свойством строгого устойчивого криптографического кодирования. Такое строгое устойчивое криптографическое кодирование приводит к значительной неопределенности значения каждого бита незакодированного сообщения при попытках декодирования закодированного сообщения. Технология проверена путем создания одной из двухоперандных четырехразрядный операций для потокового шифрования.

Ключевые слова: криптографическое преобразование, логические функции, сложение по модулю два, строгое устойчивое криптографическое кодирование.

The technology of building a two-operand four-bit operation of minimal complexity for strictly sustainable cryptographic coding

I. Fedotova-Piven, N. Lada, G. Kanashevych, M. Pustovit

In the article were applied logical functions in the operation matrix cryptographic transformation of information based on addition modulo two for the protection of the confidential information resources. It was developed a construction technology of the two-operand four-bit operation of minimal complexity with a property of strictly sustainable cryptographic coding. This construction technology consists in the fact that pair-wise inverting of a certain number of digits is performed and a half of digits of the input information is inverted, while taking into account the limitations that only one digit can be inverted in each transposition of the digits. Such strictly sustainable cryptographic coding leads to a large uncertainty in the value of each bit of the uncoded message when attempting to decode the encoded message. The two-operand four-bit operation with the strictly sustainable cryptographic coding property is created on the basis of one-operand operations with their sequential addition modulo two. A complete set of one-operand four-bit operations of minimal complexity contains 42 operations depending on the number of transpositions (zero, one and two transpositions). For the construction of this two-operand four-bit operation of minimal complexity with the strictly sustainable cryptographic coding property, 16 four-bit operations were chosen, obtained from the basic four-bit operations by one transposition in which only one bit is inverted. The truth tables were constructed for a simplified operation model without taking into account the signals of the inversion of functions, and then a model of a generalized operation was constructed taking into account the inversion of functions. The proposed technology for constructing a two-operand four-bit operation of minimal complexity with the strictly sustainable cryptographic coding property is verified by creating one of the two-operand four-bit operations for stream encryption.

Keywords: cryptographic transformation, logical functions, addition modulo two, strictly sustainable cryptographic encoding, matrix operations, mathematical model.