УДК 004. 056.55:004.312.2 **doi: 10.26906/SUNZ.2019.5.029**

Р. В. Бреус

Черкаський державний технологічний університет, Черкаси, Україна

СИНТЕЗ ДВОХРОЗРЯДНИХ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ СТРОГОГО СТІЙКОГО КРИПТОГРАФІЧНОГО КОДУВАННЯ ШЛЯХОМ ПЕРЕТВОРЕННЯ ДРУГОГО ОПЕРАНДА

На основі дослідження різних форм представлення двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування розроблено підхід до їх побудови на основі перетворення другого операнда шляхом застосування одноопераднних операцій. Застосувавши технологію перетворення другого операнда було отримано групу двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. У даній статті приведено одержану групу двохрозрядних двохоперандних операцій строгого стійкого криптографічного перетворення. Запропонований підхід до синтезу двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування шляхом перетворення другого операнда значно спрощує процес дослідження групи операцій строгого стійкого криптоперетворення.

Ключові слова: двохрозрядні двохоперандні операції, криптографічне перетворення, математичне моделювання, синтез операцій, класифікація операцій криптоперетворення.

Вступ

Постановка проблеми. У сучасному суспільстві технічний прогрес відіграє важливу роль, що, в свою чергу, призводить до збільшення комп'ютерних злочинів. Комп'ютерні системи і телекомунікації визначають надійність і потужність систем оборони і безпеки країни. Тому гостро постає питання захисту інформації.

Криптографічний захист інформації являється одним із найефективніших на сьогодні. Тому виникає необхідність вдосконалення існуючих та створення нових методів та засобів криптографічного захисту інформації, у зв'язку зі зростанням кіберзлочинів. Для досягнення даного результату необхідне покращення вже розроблених або створення нових алгоритмів криптоперетворення. Отже, дослідження та побудова нових операцій криптоперетворення на сьогоднішній день являється особливо актуальним.

Аналіз останніх досліджень і публікацій. Останнім часом велика увага приділяється одному з напрямів розвитку комп'ютерної криптографії, а саме – криптографічному кодуванню [1–3]. Також заслуговують уваги дослідження направлені на побудову операцій з заданими властивостями [4–6].

Особливої уваги заслуговують дослідження направлені на побудову операцій криптоперетворення які забезпечують максимальну невизначеність результатів шифрування [7–12].

Проте на сьогоднішній день залишилися не дослідженими процеси синтезу груп двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування.

Метою роботи є викладення результатів дослідження і синтезу двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування для побудови їх модифікацій на основі перетворення другого операнда.

Основний матеріал

Розглянемо одну з двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування, наприклад,

$$O_1 = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}. \quad (1)$$

Відповідно до [13] (1) можна представити як:

$$O_1 = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 0; \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1. \end{cases} \quad (2)$$

Аналіз виразу (2) показує, що зміна порядку одноопераднних перетворень в правій частині виразу приведе до зміни самої операції, наприклад,

$$O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = \left\{ \begin{array}{l} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \ \textit{якщо } k_1 = 0;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \textit{якщо } k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \ \textit{якщо } k_1 = 1;\ k_2 = 0; \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \textit{якщо } k_1 = 1;\ k_2 = 1; \end{array} \right\} \neq$$

$$\neq \left\{ \begin{array}{l} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \ якщо\ k_1 = 0;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \ якщо\ k_1 = 1;\ k_2 = 0; \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1 = 1;\ k_2 = 1; \end{array} \right\} = \quad (3)$$

$$= O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}.$$

Приклад (3) показує коректність нашого припущення.

Одним із самих простих способів перетворення другого операнду є виконання над ним одноопераднодної операції криптоперетворення.

Групу одноопераднодних операцій криптоперетворення, класифікованих на базові операції, операції перестановок та операції інверсії наведена наведених в табл. 1 [14].

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного кодування O_1^k та виконаємо над нею одноопераднодне криптографічне перетворення F_1.

Внаслідок даного перетворення ми отримуємо операцію строгого стійкого кодування O_1^k, що показано в наступному прикладі:

$$F_1(O_1^k) = \left\{ \begin{array}{l} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \ якщо\ k_1 = 0;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \ якщо\ k_1 = 1;\ k_2 = 0; \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1 = 1;\ k_2 = 1; \end{array} \right\} = \left\{ \begin{array}{l} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \ якщо\ k_1 = 0;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \ якщо\ k_1 = 1;\ k_2 = 0; \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1 = 1;\ k_2 = 1; \end{array} \right\} = O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}. \quad (4)$$

Таблиця 1 – **Класифікація одноопераднодних двохрозрядних операцій криптографічного перетворення інформації**

Класифікатор операцій	Операції інверсії			
	$\begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 1 \end{bmatrix}$
Базові операції	$F_1 = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_2 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_3 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_4 = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
	$F_5 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$	$F_6 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}$	$F_7 = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}$	$F_8 = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
	$F_9 = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}$	$F_{10} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$	$F_{11} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$	$F_{12} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$
Операції перестановок	$F_{13} = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{14} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{15} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{16} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
	$F_{17} = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$	$F_{18} = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$	$F_{19} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$	$F_{20} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$
	$F_{21} = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$	$F_{22} = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{23} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{24} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$

Аналогічно виконаємо перетворення над другим операндом двохоперандної операції строгого криптографічного кодування O_1^k за допомогою одноопераднодної операції криптографічного перетворення F_2. Це перетворення призводить до отримання операції строгого стійкого кодування O_5^k, що показано в прикладі (5). Якщо над другим операндом двохрозрядної двохоперандної операції строгого стійкого криптографічного кодування O_1^k виконати перетворення шляхом використання одноопераднодної криптографічної операції F_9, то буде отримана операція строгого стійкого кодування O_9^k, що відповідає прикладу (6). Зведені результати дослідження результатів перетворення другого операнда операції O_1^k за допомогою одноопераднодних операцій криптоперетворення F, наведених в табл. 1, представлено в табл. 2.

В табл. 2 представлені отримані двохрозрядні двохоперандні операції строгого стійкого криптографічного кодування класифікаковано на базові операції, операції перестановок та операції інверсії. Аналіз таблиці показав, що на основі перетворення другого операнду двохоперандної операції строгого стійкого криптографічного кодування за допомогою повної математичної групи одноопераднодних операцій буде

отримано повну математичну групу двохоперандних операцій строгого стійкого криптографічного кодування, придатних для практичного застосування. Наведені результати дозволяють значно спростити процес дослідження і синтезу груп операцій строгого стійкого криптографічного кодування:

$$F_5(O_1^k)=\left\{\begin{array}{l}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0;\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1;\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0;\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1;\end{array}\right\}=\left\{\begin{array}{l}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0;\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1;\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0;\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1;\end{array}\right\}=$$

$$=O_5^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \overline{k}_2\end{bmatrix}; \tag{5}$$

$$F_9(O_1^k)=\left\{\begin{array}{l}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \textit{ якщо } k_1=0;\ k_2=0;\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1;\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \textit{ якщо } k_1=1;\ k_2=1;\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0;\end{array}\right\}=\left\{\begin{array}{l}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \textit{ якщо } k_1=0;\ k_2=0;\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1;\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \textit{ якщо } k_1=1;\ k_2=0;\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1;\end{array}\right\}=$$

$$=O_9^k=\begin{bmatrix}x_1\cdot\overline{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\overline{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}. \tag{6}$$

Таблиця 2 – **Група двохоперандних операцій строгого криптографічного кодування після перетворення**

		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	$F_1=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	$O_1^k=\begin{bmatrix}x_1\cdot\overline{k}_1\ominus x_2\cdot k_1\\ x_1\cdot k_1\ominus x_2\cdot\overline{k}_1\end{bmatrix}\ominus\begin{bmatrix}k_2\\ \overline{k}_2\end{bmatrix}$	$O_2^k=\begin{bmatrix}x_1\cdot\overline{k}_1\ominus x_2\cdot k_1\\ x_1\cdot k_1\ominus x_2\cdot\overline{k}_1\end{bmatrix}\ominus\begin{bmatrix}\overline{k}_2\\ k_2\end{bmatrix}$	$O_3^k=\begin{bmatrix}x_1\cdot k_1\ominus x_2\cdot\overline{k}_1\\ x_1\cdot\overline{k}_1\ominus x_2\cdot k_1\end{bmatrix}\ominus\begin{bmatrix}k_2\\ \overline{k}_2\end{bmatrix}$	$O_4^k=\begin{bmatrix}x_1\cdot k_1\ominus x_2\cdot\overline{k}_1\\ x_1\cdot\overline{k}_1\ominus x_2\cdot k_1\end{bmatrix}\ominus\begin{bmatrix}\overline{k}_2\\ k_2\end{bmatrix}$
	$F_5=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}$	$O_5^k=\begin{bmatrix}x_1\cdot(\overline{k_1\ominus k_2})\ominus x_2\cdot(k_1\ominus k_2)\\ x_1\cdot(k_1\ominus k_2)\ominus x_2\cdot(\overline{k_1\ominus k_2})\end{bmatrix}\ominus\begin{bmatrix}k_2\\ \overline{k}_2\end{bmatrix}$	$O_6^k=\begin{bmatrix}x_1\cdot(\overline{k_1\ominus k_2})\ominus x_2\cdot(k_1\ominus k_2)\\ x_1\cdot(k_1\ominus k_2)\ominus x_2\cdot(\overline{k_1\ominus k_2})\end{bmatrix}\ominus\begin{bmatrix}\overline{k}_2\\ k_2\end{bmatrix}$	$O_7^k=\begin{bmatrix}x_1\cdot(k_1\ominus k_2)\ominus x_2\cdot(\overline{k_1\ominus k_2})\\ x_1\cdot(\overline{k_1\ominus k_2})\ominus x_2\cdot(k_1\ominus k_2)\end{bmatrix}\ominus\begin{bmatrix}k_2\\ \overline{k}_2\end{bmatrix}$	$O_8^k=\begin{bmatrix}x_1\cdot(k_1\ominus k_2)\ominus x_2\cdot(\overline{k_1\ominus k_2})\\ x_1\cdot(\overline{k_1\ominus k_2})\ominus x_2\cdot(k_1\ominus k_2)\end{bmatrix}\ominus\begin{bmatrix}\overline{k}_2\\ k_2\end{bmatrix}$
	$F_9=\begin{bmatrix}x_1\\ x_1\ominus x_2\end{bmatrix}$	$O_9^k=\begin{bmatrix}x_1\cdot\overline{k}_1\ominus x_2\cdot k_1\\ x_1\cdot k_1\ominus x_2\cdot\overline{k}_1\end{bmatrix}\ominus\begin{bmatrix}k_1\ominus k_2\\ \overline{k_1\ominus k_2}\end{bmatrix}$	$O_{10}^k=\begin{bmatrix}x_1\cdot\overline{k}_1\ominus x_2\cdot k_1\\ x_1\cdot k_1\ominus x_2\cdot\overline{k}_1\end{bmatrix}\ominus\begin{bmatrix}\overline{k_1\ominus k_2}\\ k_1\ominus k_2\end{bmatrix}$	$O_{11}^k=\begin{bmatrix}x_1\cdot k_1\ominus x_2\cdot\overline{k}_1\\ x_1\cdot\overline{k}_1\ominus x_2\cdot k_1\end{bmatrix}\ominus\begin{bmatrix}k_1\ominus k_2\\ \overline{k_1\ominus k_2}\end{bmatrix}$	$O_{12}^k=\begin{bmatrix}x_1\cdot k_1\ominus x_2\cdot\overline{k}_1\\ x_1\cdot\overline{k}_1\ominus x_2\cdot k_1\end{bmatrix}\ominus\begin{bmatrix}\overline{k_1\ominus k_2}\\ k_1\ominus k_2\end{bmatrix}$
Операції перестановок	$F_{13}=\begin{bmatrix}x_2\\ x_1\end{bmatrix}$	$O_{13}^k=\begin{bmatrix}x_1\cdot\overline{k}_2\ominus x_2\cdot k_2\\ x_1\cdot k_2\ominus x_2\cdot\overline{k}_2\end{bmatrix}\ominus\begin{bmatrix}k_1\\ \overline{k}_1\end{bmatrix}$	$O_{14}^k=\begin{bmatrix}x_1\cdot\overline{k}_2\ominus x_2\cdot k_2\\ x_1\cdot k_2\ominus x_2\cdot\overline{k}_2\end{bmatrix}\ominus\begin{bmatrix}\overline{k}_1\\ k_1\end{bmatrix}$	$O_{15}^k=\begin{bmatrix}x_1\cdot k_2\ominus x_2\cdot\overline{k}_2\\ x_1\cdot\overline{k}_2\ominus x_2\cdot k_2\end{bmatrix}\ominus\begin{bmatrix}k_1\\ \overline{k}_1\end{bmatrix}$	$O_{16}^k=\begin{bmatrix}x_1\cdot\overline{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\overline{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \overline{k}_1\end{bmatrix}$
	$F_{17}=\begin{bmatrix}x_2\\ x_1\ominus x_2\end{bmatrix}$	$O_{17}^k=\begin{bmatrix}x_1\cdot\overline{k}_2\ominus x_2\cdot k_2\\ x_1\cdot k_2\ominus x_2\cdot\overline{k}_2\end{bmatrix}\ominus\begin{bmatrix}k_1\ominus k_2\\ \overline{k_1\ominus k_2}\end{bmatrix}$	$O_{18}^k=\begin{bmatrix}x_1\cdot\overline{k}_2\ominus x_2\cdot k_2\\ x_1\cdot k_2\ominus x_2\cdot\overline{k}_2\end{bmatrix}\ominus\begin{bmatrix}\overline{k_1\ominus k_2}\\ k_1\ominus k_2\end{bmatrix}$	$O_{19}^k=\begin{bmatrix}x_1\cdot k_2\ominus x_2\cdot\overline{k}_2\\ x_1\cdot\overline{k}_2\ominus x_2\cdot k_2\end{bmatrix}\ominus\begin{bmatrix}k_1\\ \overline{k}_1\end{bmatrix}$	$O_{20}^k=\begin{bmatrix}x_1\cdot k_2\ominus x_2\cdot\overline{k}_2\\ x_1\cdot\overline{k}_2\ominus x_2\cdot k_2\end{bmatrix}\ominus\begin{bmatrix}\overline{k_1\ominus k_2}\\ k_1\ominus k_2\end{bmatrix}$
	$F_{19}=\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}$	$O_{21}^k=\begin{bmatrix}x_1\cdot(\overline{k_1\ominus k_2})\ominus x_2\cdot(k_1\ominus k_2)\\ x_1\cdot(k_1\ominus k_2)\ominus x_2\cdot(\overline{k_1\ominus k_2})\end{bmatrix}\ominus\begin{bmatrix}k_1\\ \overline{k}_1\end{bmatrix}$	$O_{22}^k=\begin{bmatrix}x_1\cdot(\overline{k_1\ominus k_2})\ominus x_2\cdot(k_1\ominus k_2)\\ x_1\cdot(k_1\ominus k_2)\ominus x_2\cdot(\overline{k_1\ominus k_2})\end{bmatrix}\ominus\begin{bmatrix}\overline{k}_1\\ k_1\end{bmatrix}$	$O_{23}^k=\begin{bmatrix}x_1\cdot(k_1\ominus k_2)\ominus x_2\cdot(\overline{k_1\ominus k_2})\\ x_1\cdot(\overline{k_1\ominus k_2})\ominus x_2\cdot(k_1\ominus k_2)\end{bmatrix}\ominus\begin{bmatrix}k_1\\ \overline{k}_1\end{bmatrix}$	$O_{24}^k=\begin{bmatrix}x_1\cdot(k_1\ominus k_2)\ominus x_2\cdot(\overline{k_1\ominus k_2})\\ x_1\cdot(\overline{k_1\ominus k_2})\ominus x_2\cdot(k_1\ominus k_2)\end{bmatrix}\ominus\begin{bmatrix}\overline{k}_1\\ k_1\end{bmatrix}$

Висновки

В результаті дослідження розроблено підхід до побудови двозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда. Застосування групи одноопераднних операцій для перетворення другого операнда дозволяє отримати групу двохрозрядних двохоперандних операцій строгого стійкого криптоперетворення. Розроблений підхід дозволяє значно спростити процес дослідження та синтезу групи операцій строгого стійкого криптоперетворення.

СПИСОК ЛІТЕРАТУРИ

1. Криптографическое кодирование: методы и средства реализации: монография / Рудницкий В.Н., Пивнева С.В., Бабенко В.Г., Миронец И.В. и др. // Тольят. гос. ун-т. – Тольятти, 2013. – 196 с.
2. Криптографическое кодирование: методы и средства реализации (часть 2): монография / В.Н. Рудницкий, В.Я. Мильчевич, В.Г. Бабенко, Р.П. Мельник, С.В. Рудницкий, О. Г. Мельник. – Х. : едрая усадьба плюс, 2014. – 224 с.
3. Криптографічне кодування: обробка та захист інформації: колективна монографія / під ред.. В.М. Рудницького. – Харків: ТОВ «ДІСА ПЛЮС», 2018. – 139 с.
4. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. Збірник наукових праць Харківського університету Повітряних Сил. Харків: ХУПС ім. І. Кожедуба, 2012 Вип. 4 (33). С. 198-200.
5. Мельник Р. П., Застосування операцій розширеного матричного криптографічного перетворення для захисту інформації / Р. П. Мельник // Системи обробки інформації. - 2012. - Вип. 9. - С. 145-147.
6. Синтез елементарних функцій перестановок, керованих інформацією / В. М. Рудницький, Т. В. Миронюк, О. Г. Мельник, В. П. Щербина // Безпека інформації. – Т. 20, № 3. – К.: НАУ, 2014. – С. 242–247.
7. 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.
8. Коваленко А. А., Кучук Г. А. Методи синтезу інформаційної та технічної структур системи управління об'єктом критичного застосування. *Сучасні інформаційні системи*. 2018. Т. 2, № 1. С. 22–27. DOI: https://doi.org/10.20998/2522-9052.2018.1.04
9. Рудницький, Н. Лада, С. Козловська, Технологія побудови двохоперандних операцій криптографічного перетворення інформації за результатами моделювання, Сучасні інформаційні системи, Т. 2, № 4, С. 26-30, 2018.
10. Рудницький В.М., Лада Н.В., Федотова-Півень І.М., Пустовіт М.О. Синтез обернених дворозрядних двохоперандних операцій строгого стійкого криптографічного кодування. Системи та методи обробки інформації. Збірник наукових праць. Київ: ДНДІ МВС України, 2018. Вип. 4(55). С. 76–81.
11. 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.
12. Semenov, S., Sira, O., Kuchuk, N. (2018), "Development of graphicanalytical models for the software security testing algorithm", Eastern-European Journal of Enterprise Technologies, Vol 2, No 4 (92), pp. 39-46, DOI: https://doi.org/10.15587/1729-4061.2018.127210
13. 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. Збірник наукових праць. Полтава: ПНТУ, 2018. Т. 6(52). С. 113–115.
14. 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. Збірник наукових праць. Полтава: ПНТУ, 2018. Т. 6(52). С. 113–115.

Рецензент: д-р техн. наук, проф. С. Г. Семенов,
Національний технічний університет «ХПІ», Харків
Received (Надійшла) 12.08.2019
Accepted for publication (Прийнята до друку) 11.09.2019

Синтез двухразрядных двухоперандных операций строгого стойкого криптографического кодирования путем преобразования второго операнда

Р. В. Бреус

На основании исследования различных форм представления двухразрядных двухоперандных операций строгого стойкого криптографического кодирования разработан подход к их построению путем преобразования второго операнда с помощью применения одноопераднных операций. Применив технологию преобразования второго операнда, была получена группа двухразрядных двухоперандных операций строгого устойчивого криптографического кодирования. В этой статье приведена полученная группа двухразрядных двухоперандных операций строгого устойчивого криптографического преобразования. Предложенный подход к синтезу двухразрядных двухоперандных операций строгого устойчивого криптографического кодирования путем преобразования второго операнда значительно упрощает процесс исследования группы операций строгого устойчивого криптопреобразования.

Ключевые слова: двухразрядные двухоперандные операции, криптографическое преобразование, математическое моделирование, синтез операций, классификация операций криптопреобразования.

Synthesising the two-bit two-operand operations of strict stable cryptographic coding by the second operand's conversion

R. Breus

Based on studying the different representation forms of two-bit two-operand operations of strict stable cryptographic coding, it was developed an approach to their construction based on the second operand transformation by the one-operand operations use. A group of two-bit two-operand operations of strictly stable cryptographic coding was obtained by using the second-operand conversion technology. The obtained group of two-bit two-operand operations of strict stable cryptographic transformation is presented in the article. The proposed approach for synthesizing the two-bit two-operand operations of strict stable cryptographic coding by the second operand transformation simplifies the research process of strict stable cryptographic conversion group of operations greatly.

Keywords: two-bit two-operand operations, cryptographic transformation, mathematical modeling, synthesis of operations, classification of cryptopreformation operations.