УДК 004.056.55:004.312.2 **doi: 10.20998/2522-9052.2018.4.04**

В. М. Рудницький[1], Н. В. Лада[1], С. Г. Козловська[2]

[1] Черкаський державний технологічний університет, Черкаси, Україна
[2] Східноєвропейський університет економіки і менеджменту, Черкаси, Україна

ТЕХНОЛОГІЯ ПОБУДОВИ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ ЗА РЕЗУЛЬТАТАМИ МОДЕЛЮВАННЯ

Самими універсальними операція криптоперетворення, з погляду застосування є двохоперандні операції, яким нажаль не приділялося достатньої уваги. **Метою статті** є розробка технології побудови математичних моделей двохоперандних операцій криптоперетворення, аналогічних моделям модифікованих операцій з точністю до перестановки, за результатами комп'ютерного моделювання. **Результати.** Розглянуті операції були розбиті на 24 набори двохоперандних операцій, по чотири операції в кожному наборі. Дані набори формувалися виходячи з наявності в них однакових одноопераднних двохрозрядних операцій криптоперетворення. Всім наборам двохоперандних операцій був присвоєний порядковий номер. Наведена і проілюстрована послідовність кроків переходу від результатів комп'ютерного моделювання до придатної в інженерній практиці формалізованої операції криптоперетворення відображає технологію побудови математичних моделей двохоперандних операцій криптографічного перетворення інформації. **Висновки.** Експериментально синтезовані 96 двохоперандних операцій криптографічного перетворення було класифіковано на 4 математичні групи операцій по 24 операції в кожній, а також виділили 24 набори двохоперандних операцій по 6 в кожній групі, виходячи з наявності в них однакових одноопераднних двохрозрядних операцій. На прикладі одного з наборів двохоперандних операцій розглянута послідовність математичних перетворень, які забезпечують побудову узагальнених математичних моделей криптоопераций. Послідовність кроків переходу від результатів комп'ютерного моделювання до придатної в інженерній практиці формалізованої операції криптоперетворення відображає технологію побудови математичних моделей двохоперандних операцій криптографічного перетворення інформації.

Ключові слова: криптографічне кодування; крипто перетворення; додавання за модулем два; перестановки; математична модель операції.

Вступ

Постановка проблеми. Сучасні наукові дослідження в сфері криптографічного захисту інформації все більше уваги приділяють аналізу та синтезу операцій, на основі яких будуються системи криптографічного захисту інформації. Збільшення кількості операцій, придатних для криптоперетворення, їх застосування замість, наприклад, стандартної операції додавання за модулем дає змогу підвищувати надійність та стійкість шифрування [1-2], що є надзвичайно актуальним в наш час.

Операції криптографічного перетворення інформації по аналогії з командами які реалізуються в комп'ютерних системах класифікуються по кількості операндів на одноопераднні, двохоперандні та багатоопераднні [3]. Одноопераднні операції криптографічного перетворення застосовуються в блокових шифрах. Двохоперандні операції застосовуються в блокових та потокових шифрах. Основною областю застосування багатоопераднних операцій є багатомірні примітиви блокового шифрування. Самими універсальними операція криптоперетворення, з погляду застосування є двохоперандні операції, яким нажаль не приділялося достатньої уваги.

Аналіз останніх досліджень і публікацій. Синтез двохоперандних операцій криптоперетворення може розвиватися по двох основних напрямах. Перший напрям полягає в модифікації операцій додавання за модулем на основі перестановок операндів і результатів виконання операцій. Результати даних досліджень представлено в роботах [4–6]. В роботах [7–8] запропоновано другий напрям синтезу двохоперандних операцій криптоперетворення, в основі якого лежить моделювання двоопераднних операцій криптоперетворення на основі одноопераднних. Проте отримані результати є розрізненими і не систематизованими.

Метою роботи є розробка технології побудови математичних моделей двохоперандних операцій криптоперетворення, аналогічних моделям модифікованих операцій з точністю до перестановки, за результатами комп'ютерного моделювання.

Основний матеріал

Математичні моделі операцій криптографічного додавання по модулю два з точністю до перестановки мають вигляд [9]:

$$O_1^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}; \quad O_2^{\oplus} = \begin{vmatrix} x_1 \oplus y_{1`} \\ x_2 \oplus y_2 \oplus 1 \end{vmatrix};$$

$$O_3^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_2 \oplus 1 \end{vmatrix}; \quad O_4^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_2 \end{vmatrix}.$$

де $x_{i.j} \in \{0, 1\}$ – операнд, $i \in \{1, 2\}$ – номер операнда, $j \in \{1, 2\}$ – номер розряду операнда, $\oplus$ – операція додавання за модулем два.

Результати обчислювального експерименту по моделюванню двохоперандних операцій криптоперетворення на основі двохрозрядних операцій крипто перетворення, були опубліковані в [10]. В процесі дослідження синтезованих 96 операцій [10], було виділено 4 математичні групи операцій по 24 операції в кожній. Результати даного дослідження наведені в табл. 1. Для подальшого дослідження, наведені в табл. 1 операції були розбиті на 24 набори двохоперандних операцій (НДО), по чотири операції в кожному наборі.

Таблиця 1 – **Результати моделювання операцій над двома операндами**

Група операцій 1		**Група операцій 2**		**Група операцій 3**		**Група операцій 4**	
НДО 1	**НДО 4**	**НДО 7**	**НДО 10**	**НДО 13**	**НДО 16**	**НДО 19**	**НДО 22**
$O_{1,7,13,19}$, $O_{7,1,19,13}$, $O_{13,19,1,7}$, $O_{19,13,7,1}$.	$O_{4,16,10,22}$, $O_{10,22,4,16}$, $O_{16,4,22,10}$, $O_{22,10,16,4}$.	$O_{1,8,13,20}$, $O_{8,13,20,1}$, $O_{13,20,1,8}$, $O_{20,1,8,13}$.	$O_{4,17,10,23}$, $O_{10,23,4,17}$, $O_{17,10,23,4}$, $O_{23,4,17,10}$.	$O_{1,10,16,19}$, $O_{10,19,1,16}$, $O_{16,1,19,10}$, $O_{19,16,10,1}$.	$O_{4,13,7,22}$, $O_{7,4,22,13}$, $O_{13,22,4,7}$, $O_{22,7,13,4}$.	$O_{1,7,15,21}$, $O_{7,1,21,15}$, $O_{15,21,7,1}$, $O_{21,15,1,7}$.	$O_{4,16,12,24}$, $O_{12,24,16,4}$, $O_{16,4,24,12}$, $O_{24,12,4,16}$.
НДО 2	**НДО 5**	**НДО 8**	**НДО 11**	**НДО 14**	**НДО 17**	**НДО 20**	**НДО 23**
$O_{2,20,14,8}$, $O_{8,14,20,2}$, $O_{14,8,2,20}$, $O_{20,2,8,14}$.	$O_{5,23,11,17}$, $O_{11,17,5,23}$, $O_{17,11,23,5}$, $O_{23,5,17,11}$.	$O_{2,19,14,7}$, $O_{7,2,19,14}$, $O_{14,7,2,19}$, $O_{19,14,7,2}$.	$O_{5,22,11,16}$, $O_{11,16,5,22}$, $O_{16,5,22,11}$, $O_{22,11,16,5}$	$O_{2,24,18,8}$, $O_{8,18,24,2}$, $O_{18,2,8,24}$, $O_{24,8,2,18}$.	$O_{5,21,9,17}$, $O_{9,5,17,21}$, $O_{17,9,21,5}$, $O_{21,17,5,9}$.	$O_{2,20,17,11}$, $O_{11,17,2,20}$, $O_{17,11,20,2}$, $O_{20,2,11,17}$.	$O_{5,23,8,14}$, $O_{8,14,23,5}$, $O_{14,8,5,23}$, $O_{23,5,14,8}$.
НДО 3	**НДО 6**	**НДО 9**	**НДО 12**	**НДО 15**	**НДО 18**	**НДО 21**	**НДО 24**
$O_{3,9,21,15}$, $O_{9,3,15,21}$, $O_{15,21,9,3}$, $O_{21,15,3,9}$.	$O_{6,18,24,12}$, $O_{12,24,18,6}$, $O_{18,6,12,24}$, $O_{24,12,6,18}$.	$O_{3,12,21,18}$, $O_{12,21,18,3}$, $O_{18,3,12,21}$, $O_{21,18,3,12}$.	$O_{6,15,24,9}$, $O_{9,6,15,24}$, $O_{15,24,9,6}$, $O_{24,9,6,15}$.	$O_{3,11,23,15}$, $O_{11,15,3,23}$, $O_{15,23,11,3}$, $O_{23,3,15,11}$.	$O_{6,14,20,12}$, $O_{12,20,14,6}$, $O_{14,12,6,20}$, $O_{20,6,12,14}$.	$O_{3,9,19,13}$, $O_{9,3,13,19}$, $O_{13,19,3,9}$, $O_{19,13,9,3}$.	$O_{6,18,22,10}$, $O_{10,22,6,18}$, $O_{18,6,10,22}$, $O_{22,10,18,6}$.

Дані набори формувалися виходячи з наявності в них однакових одноопераднних двохрозрядних операцій криптоперетворення. Всім наборам двохоперандних операцій був присвоєний порядковий номер.

Розглянемо перший НДО наведений в табл. 1. Даний набір включає в себе операції:

$$O_{1,7,13,19},\ O_{7,1,19,13},\ O_{13,19,1,7},\ O_{19,13,7,1}.$$

Умовно будемо вважати операцію $O_{1,7,13,19}$ основною, так як вона представлена першою в даному наборі. Дослідимо можливість побудови математичних моделей НДО №1, по аналогії з дослідженнями моделей модифікацій операцій з точністю до перестановки, наведеними в [11].

Математична модель основної операції першого НДО $O_{1,7,13,19}$ матиме вигляд:

$$O_{1,7,13,19}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}, & \text{якщо } k_1=0;\ k_2=0;\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, & \text{якщо } k_1=0;\ k_2=1;\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, & \text{якщо } k_1=1;\ k_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, & \text{якщо } k_1=1;\ k_2=1,\end{cases} \tag{1}$$

де k_1 і k_2 – команди управління криптографічним перетворенням.

Для встановлення сутності операції (1), її можна представити як:

$$O_{1,7,13,19}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}, & \text{якщо } k_1=0;\ k_2=0;\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, & \text{якщо } k_1=0;\ k_2=1;\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, & \text{якщо } k_1=1;\ k_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, & \text{якщо } k_1=1;\ k_2=1\end{cases}= \tag{2}$$

$$=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, & \text{якщо } k_1=0;\ k_2=0;\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, & \text{якщо } k_1=0;\ k_2=1;\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, & \text{якщо } k_1=1;\ k_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, & \text{якщо } k_1=1;\ k_2=1.\end{cases}$$

Таким чином, операцію $O_{1,7,13,19}$, представлену виразом (1) можна записати як:

$$O_{1,7,13,19}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0;\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1;\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

або

$$O_{1,7,13,19}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}. \quad (3)$$

Виходячи з виразу (3), операцію (1) можна представити таким чином:

$$O_{1,7,13,19}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_2\end{bmatrix}. \quad (4)$$

По аналогії з побудовою математичної моделі основної операції першого набору двохоперандних операцій $O_{1,7,13,19}$ дослідимо можливість побудови інших двохоперандних операцій даного набору.

Математична модель операції $O_{7,1,19,13}$, що є синтезованою на основі моделі основної операції $O_{1,7,13,19}$ першого набору двохоперандних операцій, представляються у вигляді:

$$O_{7,1,19,13}=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0;\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1;\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1.\end{cases} \quad (5)$$

Отже, операцію $O_{7,1,19,13}$, представлену виразом (5) можна представити у вигляді, що розкриває її сутність, а саме:

$$O_{7,1,19,13}=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=k_2=0;\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1;\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

або

$$O_{7,1,19,13}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}. \quad (6)$$

Виходячи з виразу (6), операцію (5) можна представити таким чином:

$$O_{7,1,19,13}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_2\oplus 1\end{bmatrix}. \quad (7)$$

Математична модель операції $O_{13,19,1,7}$, що є синтезованою на основі моделі основної операції $O_{1,7,13,19}$ першого набору двохоперандних операцій, матиме вигляд:

$$O_{13,19,1,7}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1;\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0;\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1.\end{cases} \quad (8)$$

Для встановлення сутності операції $O_{13,19,1,7}$, її можна представити аналогічно виразу (2) як:

$$O_{13,19,1,7}=$$

$$=\begin{cases}\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0;\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1;\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0;\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1.\end{cases}$$

Відповідно, операцію $O_{13,19,1,7}$ можна записати таким чином:

$$O_{13,19,1,7}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\end{bmatrix}. \quad (9)$$

Виходячи з виразу (9), операцію (8) можна представити таким чином:

$$O_{13,19,1,7}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_2\end{bmatrix}. \quad (10)$$

Математична модель операції $O_{19,13,7,1}$, що є синтезованою на основі моделі базової операції $O_{1,7,13,19}$ першого набору двохоперандних операцій, представляються у вигляді:

$$O_{19,13,7,1} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0; \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1. \end{cases} \quad (11)$$

Операцію (11) також можна представити як:

$$O_{19,13,7,1} =$$

$$= \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0; \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1. \end{cases}$$

Таким чином, операцію $O_{19,13,7,1}$ можна записати як:

$$O_{19,13,7,1} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}. \quad (12)$$

Таким чином, виходячи з виразу (12), операцію (11) можна представити таким чином:

$$O_{19,13,7,1} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_2 \oplus 1 \end{bmatrix}. \quad (13)$$

Наведена і проілюстрована послідовність кроків переходу від результатів комп'ютерного моделювання до придатної в інженерній практиці формалізованої операції криптоперетворення відображає технологію побудови математичних моделей двохоперандних операцій криптографічного перетворення інформації.

Висновки

Проведене дослідження дало змогу зробити наступні висновки.

1. Класифіковано чотири математичні групи операцій по двадцять чотири операції в кожній з експериментально синтезованих дев'яносто шости двохоперандних операцій криптографічного перетворення.

Виділено двадцять чотири набори двохоперандних операцій по 6 в кожній групі, виходячи з наявності в них однакових одноопераднних двохрозрядних операцій.

2. Отримана послідовність математичних перетворень, які забезпечують побудову узагальнених математичних моделей криптоопераций на прикладі одного з наборів двохоперандних операцій.

3. Представлена послідовність кроків переходу від результатів комп'ютерного моделювання до придатної в інженерній практиці формалізованої операції крипто перетворення, що відображає технологію побудови математичних моделей двохоперандних операцій криптографічного перетворення інформації.

СПИСОК ЛІТЕРАТУРИ

1. 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.
2. Рудницький В. М., Миронець І. В., Бабенко В. Г. Обґрунтування можливості розширення набору функцій перекодування інформації для захисту конфіденційних інформаційних ресурсів. Системи управління, навігації та зв'язку: зб. наук. пр. Київ: Центр. наук.-досл. ін.-т навігації і управл., 2010. Вип. 2 (14). С. 118-122.
3. Криптографическое кодирование: кол. моногр. / Под ред. В. Н. Рудницкого, В. Я. Мильчевича. Харьков: Щедрая усадьба плюс, 2014. 240 с.
4. Lada N. V. Застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах / N. V. Lada, S. H. Kozlovska // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2018. – Т. 1 (47). – С. 127-130.
5. Лада Н. В. Аналіз коректності взаємозв'язків між прямими та оберненими матричними моделями операцій криптографічного перетворення інформації. Системи управління, навігації та зв'язку:. Полтава : ПНТУ, 2015. Вип. 4 (36). С. 73-78.
6. Бабенко В. Г., Лада Н. В. Аналіз результатів виконання модифікованих операцій додавання за модулем два з точністю до перестановки. The scientific potential of the present: proceedings of the Internat. sci. conf., (St. Andrews, Scotland, UK, December, 1, 2016) / ed. N. P. Kazmyna. NGO «European Scientific Platform». Vinnytsia: PE Rogal ska I. O., 2016. С. 108-111. (Шотландия, Логос).
7. Криптографічне кодування: обробка та захист інформації: колективна монографія / під ред. В. М. Рудницького. Харків: ТОВ «ДІСА ПЛЮС», 2018. – 139 с.
8. Рудницький В. М., Лада Н. В., Бабенко В. Г. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія. Харків: ТОВ «ДІСА ПЛЮС», 2018. 184 с.
9. Рудницький В. М., Бабенко В. Г.,Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного перекодування інформації. Захист інформації : наук.-практ. журн. 2012. № 3 (56). С. 50-56.
10. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2014. Вип. 2 (118). С. 116-118.
11. Бабенко В. Г., Лада Н. В. Технологія дослідження операцій за модулем два. Smart and Young: щомісячний наук. журн. 2016. № 11–12. Ч. 1. С. 49–54.

REFERENCES

1. Rudnitsky, V.M., Babenko, V.G. and Rudnitsky, S.V. (2012), “The method of synthesis of matrix models of operations of cryptographic encoding and decoding of information”, *Collection of scientific works of HUPS*, Kharkiv, No. 4 (33), pp. 198-200.
2. Rudnitsky, V.M., Mironets, I.V. and Babenko, V.G. (2010), “Substantiation of the possibility of expanding the set of functions of re-coding information for the protection of confidential information resources”, *Control, navigation and communication systems*, Center. sciences Institute of Navigation and Management, Kyiv, Issue 2 (14), pp. 118-122.
3. Rudnitsky, V. N. and Milcevich, Ya. (2014), *Cryptographic encoding*, Generous Homestead Plus, Kharkiv, 240 p.
4. Lada N.V. and Kozlovska S.H. (2018), “Application of operations of cryptographic addition by module two with precision to permutation in stream ciphers”, C*ontrol, navigation and communication systems*, PNTU, Poltava, Issue 1 (47), pp. 127-130.
5. Lada, N.V. (2015), “Analysis of the correctness of the relationship between direct and inverse matrix models of operations of cryptographic information transformation”, C*ontrol, navigation and communication systems*, PNTU, Poltava, Issue 4 (36), pp. 73-78.
6. Babenko V.G. and Lada N.V. (2016), “Analysis of the results of the modified modification operation operations with accuracy up to permutation, *Proc. of the Int. sci. conf. NGO* «E*uropean Scientific Platform*», Vinnytsia, pp. 108-111.
7. Rudnitsky, V.M. (2018), *Cryptographic encoding: data processing and protection*, LLC "DISA PLUS", Kharkiv, 139 p.
8. Rudnitsky, V.M., Lada, N.V. and Babenko, V.G. (2018), *Cryptographic encoding: Synthesis of streaming encryption operations up to permutation*, LLC "DISA PLUS", Kharkiv, 184 p.
9. Rudnitsky, V.M., Babenko, V.G. and Rudnitsky, S.V. (2012), “The method of matrix models synthesis of cryptographic information re-encoding operations ", *Information Protection*, No. 3 (56), pp. 50-56.
10. Babenko, V.G. and Lada, N.V. (2014), “Synthesis and analysis of operations of cryptographic addition by module two”, *Information Processing Systems*, KhUPS, Kharkiv, No. 2 (118), pp. 116-118.
11. Babenko, V.G. and Lada, N.V. (2016), “Technology for the study of operations by module two”, *Smart and Young*, No. 11-12, Part 1, pp. 49-54.

Надійшла (received) 11.09.2018
Прийнята до друку (accepted for publication) 31.10.2018

Технология построения двухоперандных операций криптографического преобразования информации по результатам моделирования

В. Н. Рудницкий, Н. В. Лада, С. Г. Козловская

Самыми универсальными операция криптопреобразования, с точки зрения применения, являются двухоперандных операции, которым к сожалению не уделялось достаточного внимания. **Целью статьи** является разработка технологии построения математических моделей двухоперандных операций криптопреобразования, аналогичных моделям модифицированных операций с точностью до перестановки, по результатам компьютерного моделирования. **Результаты.** Рассмотрены операции были разбиты на 24 наборы двухоперандных операций, по четыре операции в каждом наборе. Данные наборы формировались исходя из наличия в них одинаковых одноперандних двухразрядных операций криптопреобразования. Всем наборам двухоперандных операций был присвоен порядковый номер. Приведенная и проиллюстрирована последовательность шагов перехода от результатов компьютерного моделирования к пригодной в инженерной практике формализованной операции криптопреобразования отражает технологию построения математических моделей двухоперандных операций криптографического преобразования информации. **Выводы.** Экспериментально синтезированные 96 двухоперандных операций криптографического преобразования были классифицированы на 4 математические группы операций по 24 операции в каждой, а также выделили 24 наборы двухоперандных операций по 6 в каждой группе, исходя из наличия в них одинаковых одноперандных двуразрядных операций. На примере одного из наборов двухоперандных операций рассмотрена последовательность математических преобразований, которые обеспечивают построение обобщенных математических моделей криптоопераций. Последовательность шагов перехода от результатов компьютерного моделирования к пригодной в инженерной практике формализованной операции криптопреобразования отражает технологию построения математических моделей двухоперандных операций криптографического преобразования информации.

Ключевые слова: криптографическое кодирование; криптопреобразования; сложение по модулю два; перестановки; математическая модель операции.

Technology of two operand operations construction of information cryptographic transformation by modeling results

V. Rudnytsky, N. Lada, S. Kozlovska

The most universal operation of cryptanalysis, from the point of view of application are two-step operations, which unfortunately were not given enough attention. **The purpose of the article** is to develop a technology for constructing mathematical models of two-operand operations of cryptographic, similar to models of modified operations with precision to permutations, based on computer simulation results. **Results.** The operations under consideration were broken down into 24 sets of double-action operations, in four operations in each set. These sets were formed on the basis of the presence of identical one-operand two-digit operations of cryptographic transformation in them. All sets of double-action operations were assigned a serial number. The illustrated and illustrated sequence of transition steps from the results of computer simulation to the applicable in engineering practice of the formalized operation of cryptographic transformation reflects the technology of constructing mathematical models of two-operand operations of cryptographic information transformation. **Conclusions.** Experimentally synthesized 96 two operand operations of cryptographic transformation were classified into 4 mathematical groups of operations for 24 operations in each, and also allocated 24 sets of two operand operations on 6 in each group, based on the presence of identical one operand two-bit operations in them. On the example of one of the sets of two-operand operations, a sequence of mathematical transformations is considered that provide the construction of generalized mathematical models of cryptographic operations. The sequence of steps of transition from the results of computer simulation to the applicable in engineering practice of the formalized operation of cryptographic transformation reflects the technology of constructing mathematical models of two-operand operations of cryptographic information transformation.

Keywords: cryptographic coding; cryptographic transformation; adding by module two; permutations, mathematical model of operation.