УДК 004.056.55:004.312.2

[0000-0003-3473-7433] **В. М. Рудницький**[1], *д.т.н., професор,*
e-mail: rvn_2008@ukr.net
[0000-0002-9671-108X] **О. Г. Мельник**[2], *к.т.н., ст. наук. співробітник,*
e-mail: melnyk.olja.2014@gmail.com
[0000-0002-5622-5642] **Р. П. Мельник**[2], *к.т.н.*
e-mail: indigo211212@gmail.com
[1]Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
[2]Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України
вул. Онопрієнка, 8, м. Черкаси, 18034, Україна

ТЕХНОЛОГІЯ ОПИСУ ЛІНІЙНИХ І НЕЛІНІЙНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

За результатами проведеного дослідження встановлено, що запропонована нами залежність розрахунку кількості операцій криптографічного перетворення, що базується на рекурентному поєднанні потужностей множин операцій меншої розрядності та елементарних функцій, є коректною і математично описує процес побудови множин нових операцій. Ґрунтуючись на результатах дослідження, можна вважати, що розробка єдиної технології синтезу та дослідження як лінійних, так і нелінійних операцій криптографічного перетворення інформації є можливою. Цей підхід дає можливість не тільки розраховувати кількість операцій криптографічного перетворення інформації, а й будувати самі операції шляхом поєднання відомих операцій криптоперетворення та елементарних функцій більшої розрядності.

Запропонований підхід створює передумови для розробки єдиної технології опису та синтезу як лінійних, так і нелінійних операцій криптоперетворення.

Ключові слова: *захист інформації, операції криптографічного перетворення, синтез операцій, розрядність, технологія синтезу.*

Постановка проблеми. На сьогодні найбільш ефективним способом захисту інформації від несанкціонованого доступу є криптографічні перетворення [1]. Основними їх задачами є забезпечення математичними методами такого захисту інформації, при якому навіть у випадках перехоплення викрадачами й обробки будь-якими способами з використанням останніх досягнень науки і техніки зміст інформації може бути розкритий тільки протягом певного заданого часу.

Одним із шляхів вдосконалення існуючих криптографічних систем захисту інформації та розробки нових криптографічних алгоритмів є розширення спектра операцій, на основі яких вони будуються. Тому задача синтезу нових операцій криптографічного перетворення інформації є актуальною.

Аналіз останніх досліджень. Серед останніх досліджень і публікацій варто виділити: [2, 3], де представлено результати проведеного обчислювального експерименту по знаходженню елементарних операцій для криптографічного кодування інформації, а також проведено розрахунок кількості елементарних операцій для криптографічного перетворення залежно від розрядності, [4–6], де викладено основні теоретичні й практичні аспекти криптографічного, стенографічного захисту інформації, та [7], що присвячена підвищенню ефективності алгоритмів комп'ютерної криптографії за рахунок розробки нових мікрокриптопримітивів на основі використання нових синтезованих операцій криптографічного перетворення інформації, де також представлено наукові результати нових методів синтезу функцій та операцій криптографічного перетворення інформації.

Однак у цих дослідженнях не було розглянуто питання щодо побудови операцій шляхом поєднання відомих операцій криптоперетворення та елементарних функцій більшої розрядності.

Метою роботи є дослідження залежності розрахунку кількості операцій, що базується на рекурентному поєднанні потужностей множин операцій меншої розрядності та елементарних функцій для опису процесу побу-

DOI: 10.24025/2306-4412.3.2019.178322

дови множин нових операцій, а також вивчення питання можливості розробки єдиної технології синтезу та дослідження як лінійних, так і нелінійних операцій криптографічного перетворення інформації.

Виклад основного матеріалу. Результати, отримані під час обчислювального експерименту щодо визначення дворозрядних логічних функцій за допомогою розробленого програмного комплексу [4], можна структурно представити у вигляді таблиці 1. У таблиці представлений повний набір логічних функцій двох змінних.

Таблиця 1 – **Логічні функції двох змінних**

x_2	x_1	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Для подальших досліджень нам необхідно представити логічні функції у вигляді логічних операцій, що їм відповідають. Зобразимо ці логічні операції двох змінних в аналітичному представленні (таблиця 2).

Таблиця 2 – **Аналітичне представлення логічної операції двох змінних**

0	**0**	**8**	$\overline{x}_1 \cdot \overline{x}_2$
1	$x_1 \cdot x_2$	**9**	$x_1 \oplus x_2 \oplus 1 = \overline{x_1 \oplus x_2}$
2	$x_1 \cdot \overline{x}_2$	**10**	$\overline{x}_1$
3	x_2	**11**	$x_1 \vee \overline{x}_2 = \overline{\overline{x}_1 \cdot x_2}$
4	$\overline{x}_1 \cdot x_2$	**12**	$\overline{x}_2$
5	x_1	**13**	$\overline{x}_1 \vee x_2 = \overline{x_1 \cdot \overline{x}_2}$
6	$x_1 \oplus x_2$	**14**	$\overline{x}_1 \vee \overline{x}_2 = \overline{x_1 \cdot x_2}$
7	$x_1 \vee x_2 = \overline{\overline{x}_1 \cdot \overline{x}_2}$	**15**	**1**

У системах захисту інформації використовуються тільки логічні функції, що мають однакову кількість нулів і одиниць у таблицях істинності [3], а саме 6 дворозрядних елементарних функцій (3, 5, 6, 9, 10, 12), що представлені в таблиці 3. Ці елементарні функції використовуються для синтезу дворозрядних операцій криптографічного перетворення.

Таблиця 3 – **Дворозрядні елементарні функції для синтезу операцій криптографічного перетворення інформації**

x_2	x_1	**3**	**5**	**6**	**9**	**10**	**12**
0	0	0	0	0	1	1	1
0	1	0	1	1	0	0	1
1	0	1	0	1	0	1	0
1	1	1	1	0	1	0	0
		x_2	x_1	$x_1 \oplus x_2$	$x_1 \oplus x_2 \oplus 1 = \overline{x_1 \oplus x_2}$	$\overline{x}_1$	$\overline{x}_2$

Оскільки криптографічні операції синтезуються на основі вибраних елементарних функцій та являють собою композицію відповідних функцій перетворення, то застосуємо дворозрядні елементарні функції для синтезу операцій криптографічного перетворення інформації. Приклад поєднання елементарних функцій в операції криптографічного перетворення представлений у таблиці 4.

DOI: 10.24025/2306-4412.3.2019.178322

Таблиця 4 – **Результати застосування дворозрядних елементарних функцій для синтезу операцій криптографічного перетворення інформації**

x_2	x_1	$F_{3,5}=\begin{bmatrix}x_2\\x_1\end{bmatrix}$		$F_{6,5}=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$		$F_{3,6}=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$		$F_{5,3}=\begin{bmatrix}x_1\\x_2\end{bmatrix}$		$F_{5,6}=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$		. . .
0	0	0	0	0	0	0	0	0	0	0	0	
0	1	0	1	1	1	0	1	1	1	1	1	
1	0	1	0	1	0	1	1	0	0	0	1	. . .
1	1	1	1	0	1	1	0	1	1	1	0	
		x_2	x_1	$x_1\oplus x_2$	x_1	x_2	$x_1\oplus x_2$	x_1	x_2	x_1	$x_1\oplus x_2$	. . .

Виходячи з наведеного прикладу поєднання елементарних функцій в операції криптографічного перетворення, що наведені в таблиуі 4, сформуємо повну групу дворозрядних операцій криптографічного перетворення інформації, представлену в таблиці 5.

Таблиця 5 – **Повна група дворозрядних операцій криптографічного перетворення інформації**

№	операція	№	операція	№	операція	№	операція
1	$F_{3,5}=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	**7**	$F_{3,10}=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}$	**13**	$F_{12,5}=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}$	**19**	$F_{12,10}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$
2	$F_{6,5}=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	**8**	$F_{6,10}=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}$	**14**	$F_{9,5}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\end{bmatrix}$	**20**	$F_{9,10}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$
3	$F_{3,6}=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	**9**	$F_{3,9}=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}$	**15**	$F_{12,6}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}$	**21**	$F_{12,9}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
4	$F_{5,3}=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	**10**	$F_{5,12}=\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}$	**16**	$F_{10,3}=\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}$	**22**	$F_{10,12}=\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}$
5	$F_{5,6}=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	**11**	$F_{5,9}=\begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}$	**17**	$F_{10,6}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}$	**23**	$F_{10,9}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
6	$F_{6,3}=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	**12**	$F_{6,12}=\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}$	**18**	$F_{9,3}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}$	**24**	$F_{9,12}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}$

Проаналізувавши наукові дослідження [7-8], можна зробити припущення, що використання операцій криптографічного перетворення інформації більшої розрядності дозволить зменшити час криптографічної обробки інформації. Тому спробуємо отримати на основі дворозрядних операцій криптографічного перетворення інформації трирозрядні операції. Приклад синтезу трирозрядної операції криптографічного перетворення інформації представлено в таблиці 6.

Таблиця 6 – **Приклад синтезу трирозрядної операції криптографічного перетворення інформації**

x_3	x_2	x_1					
0	0	0	0	0	0	$F_{3,5}=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	$F=\begin{bmatrix}x_3\\\begin{cases}F_{3,5}=\begin{bmatrix}x_2\\x_1\end{bmatrix}, & \text{якщо } x_3=0\\ F_{3,6}=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}, & \text{якщо } x_3=1\end{cases}\end{bmatrix}$
0	0	1	0	0	1		
0	1	0	0	1	0		
0	1	1	0	1	1		
1	0	0	1	0	0	$F_{3,6}=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	
1	0	1	1	0	1		
1	1	0	1	1	1		
1	1	1	1	1	0		

DOI: 10.24025/2306-4412.3.2019.178322

В роботах [7-9] висвітлено результати проведеного обчислювального експерименту, в ході якого було знайдено 70 елементарних функцій для криптографічного перетворення інформації. Однак форми представлення поєднання елементарних функцій в операції базуються на використанні різних математичних апаратів, що створює непереборні складності в одночасному застосуванні всіх класифікованих та досліджених операцій криптоперетворення.

На сьогодні кількість операцій криптоперетворення визначається через факторіальну залежність потужності множини кодових слів. У цих розрахунках відсутнє значення потужностей елементарних функцій. Можна допустити, що, знайшовши спосіб поєднання множин потужностей кодових слів та елементарних функцій при розрахунку граничної кількості операцій криптоперетворення, будуть створені передумови для розробки єдиного підходу до синтезу як лінійних, так і нелінійних операцій.

Проекспериментуємо з множинами кодових слів та елементарних функцій.

Кількість трирозрядних операцій визначається за формулою $K_3^o = 2^3! = 8!$

Кількість трирозрядних елементарних функцій визначається за формулою $K_3^\phi = C_{2^3}^{2^2} = C_8^4 = \frac{8!}{4!(8-4)!} = 70$.

Визначимо кількість дворозрядних операцій: $K_2^o = 2^2! = 4! = 24$.

Якщо трирозрядні операції задавати як:

x_3	x_2	x_1		
0	0	0	$F_{2,i}$	$F_{3,k} = \begin{bmatrix} x_3 \\ \begin{cases} F_{2,i}, \text{ якщо } x_3 = 0 \\ F_{2,j}, \text{ якщо } x_3 = 1 \end{cases} \end{bmatrix}$ $i, j \in \{1, 2, ..., 4!\}$, $k \in \{1, 2, ..., 8!\}$
0	0	1		
0	1	0		
0	1	1		
1	0	0	$F_{2,j}$	
1	0	1		
1	1	0		
1	1	1		

$$\frac{K_3^o}{K_2^o \cdot K_2^o} = \frac{8!}{4! \cdot 4!} = \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8}{(1 \cdot 2 \cdot 3 \cdot 4) \cdot (1 \cdot 2 \cdot 3 \cdot 4)} = \frac{5 \cdot 6 \cdot 7 \cdot 8}{1 \cdot 2 \cdot 3 \cdot 4} = \frac{5 \cdot 7 \cdot 2}{1} = 70$$

Оскільки $K_3^\phi = 70$, то можна допустити, що: $K_3^o = K_2^o \cdot K_2^o \cdot K_3^\phi$.

Виходячи з виразу, отримаємо модель синтезу трирозрядної операції:

x_3	x_2	x_1		
0	0	0	$F_{2,i}$	$F_{3,k} = \begin{bmatrix} f_{3,n} \\ \begin{cases} F_{2,i}, \text{ якщо } f_{3,n} = 0 \\ F_{2,j}, \text{ якщо } f_{3,n} = 1 \end{cases} \end{bmatrix}$ $i, j \in \{1, 2, ..., 4!\}$, $k \in \{1, 2, ..., 8!\}$, $n \in \{1, 2, ..., 70\}$
0	0	1		
0	1	0		
0	1	1		
1	0	0	$F_{2,j}$	
1	0	1		
1	1	0		
1	1	1		

Перевіримо цю модель синтезу для розрахунку кількості дворозрядних операцій криптоперетворення інформації.

Оскільки кількість дворозрядних операцій $K_2^o = 2^2! = 4! = 24$, то кількість дворозрядних елементарних функцій буде визначатися як $K_2^\phi = C_{2^2}^{2^1} = C_4^2 = 6$; кількість однорозрядних операцій – $K_1^o = 2^1! = 2! = 2$, тоді кількість дворозрядних операцій – $K_2^o = K_1^o \cdot K_1^o \cdot K_2^\phi = (K_1^o)^2 \cdot K_2^\phi = 2^2 \cdot 6 = 24$.

Кількість трирозрядних операцій – $K_3^o = 2^3! = 8!$, кількість трирозрядних елементарних функцій – $K_3^\phi = C_{2^3}^{2^2} = C_8^4 = \frac{8!}{4!(8-4)!} = 70$.

Кількість дворозрядних операцій – $K_2^o = 2^2! = 4! = 24$.

DOI: 10.24025/2306-4412.3.2019.178322

x_2	x_1		
0	0	0	$F_{2,i}$
0	1	0	
1	0	1	$F_{2,j}$
1	1	1	

$$F_{2,k} = \begin{bmatrix} f_{2,n} \\ \begin{cases} F_{1,i}, \text{ якщо } f_{2,n} = 0 \\ F_{1,j}, \text{ якщо } f_{2,n} = 1 \end{cases} \end{bmatrix}$$

$i, j \in \{1, 2\}$, $k \in \{1, 2, ..., 4!\}$, $n \in \{1, 2, ..., 6\}$

Розрахуємо кількість дворозрядних операцій:

$$K_2^o = K_1^o \cdot K_1^o \cdot K_2^\phi = (K_1^o)^2 \cdot K_2^\phi = 2^2 \cdot 6 = 24.$$

Кількості дворозрядних операцій збіглися.

Перевіримо вираз для розрахунку кількості чотирирозрядних операцій криптоперетворення інформації.

Кількість чотирирозрядних операцій – $K_4^o = 2^4! = 16!$

Кількість чотирирозрядних елементарних функцій –

$$K_4^\phi = C_{2^4}^{2^3} = C_{16}^8 = \frac{16!}{8! \cdot 8!} = 12870.$$

Кількість трирозрядних операцій – $K_3^o = 2^3! = 8! = 40320$.

$$K_4^o = K_3^o \cdot K_3^o \cdot K_4^\phi.$$

Отриманий результат дозволяє стверджувати, що запропонована залежність розрахунку кількості операцій, яка базується на рекурентному поєднанні потужностей множин операцій меншої розрядності та елементарних функцій, є коректною і математично описує процес побудови множин нових операцій. Виходячи з цього, можна стверджувати, що можливо розробити єдину технологію синтезу та дослідження як лінійних, так і нелінійних операцій криптографічного перетворення інформації.

Висновок. Запропонований підхід дає можливість:

- розраховувати кількість операцій криптографічного перетворення інформації;
- будувати самі операції шляхом поєднання відомих операцій криптоперетворення та елементарних функцій більшої розрядності;
- створює передумови для розробки єдиної технології опису та синтезу як лінійних, так і нелінійних операцій криптоперетворення.

Список літератури

[1] Thomas W. Cusick, and Pantelimon Stănică, *Cryptographic Boolean functions and applications.* Academic Press, 2009.

[2] В. Г. Бабенко, С. В. Рудницький, та Р. П. Мельник, "Визначення множини трирозрядних елементарних операцій криптографічного перетворення", *Вісник інженерної академії України*, вип. 3 (4), с. 77–79, 2012.

[3] В. Н. Рудницкий, Р. П. Мельник, и О. Г. Мельник, "Повышение быстродействия систем защиты информации", на *междунар. науч.-практ. конф. Чрезвычайные ситуации: теория, практика, инновации «ЧС – 2012»*. Гомель: ГГТУ им. П. О. Сухого, 2012, с. 224.

[4] В. Н. Рудницкий, С. В. Пивнева, В. Г. Бабенко, И. В. Миронец, А. В. Дмитришин, и Ю. В. Барышев, *Криптографическое кодирование: методы и средства реализации:* монография. Тольятти, 2013.

[5] В. Н. Рудницкий, В. Я. Мильчевич, В. Г. Бабенко, Р. П. Мельник, С. В. Рудницкий, и О. Г. Мельник, *Криптографическое кодирование: методы и средства реализации (часть 2):* монография. Харьков: Щедрая усадьба плюс, 2014.

[6] *Криптографическое кодирование:* колл. монография / под ред. В. Н. Рудницкого, и В. Я. Мильчевича. Харьков: Щедрая усадьба плюс, 2014.

[7] *Криптографічне кодування: обробка та захист інформації* / під ред. В. М. Рудницького. Харків: ДІСА ПЛЮС, 2018.

[8] В. М. Рудницький, І. В. Миронець, та В. Г. Бабенко, "Систематизація повної множини логічних функцій для криптографічного перетворення інформації", *Системи обробки інформації*, вип. 8 (98), с. 184–188, 2011.

[9] В. М. Рудницький, В. Г. Бабенко, С. В. Рудницький, "Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації", *Збірник наукових праць Харківського університету Повітряних Сил*, вип. 4 (33), с. 198-200, 2012.

DOI: 10.24025/2306-4412.3.2019.178322

[10] В. М. Рудницький, В. Г. Бабенко, та С. В. Рудницький, "Метод синтезу матричних моделей операцій криптографічного перекодування інформації", *Захист інформації*, № 3 (56), с. 50-56, 2012.

References

[1] Thomas W. Cusick, and Pantelimon Stănică, *Cryptographic Boolean functions and applications.* Academic Press, 2009.

[2] V. G. Babenko, S. V. Rudnyckyj, and R. P. Melnyk, "Determination of the set of three-element elementary operations of cryptographic transformation", *Visnyk inzhenernoyi akademiyi Ukrayiny*, no. 3 (4), pp. 77-79, 2012 [in Ukrainian].

[3] V. M. Rudnyckyj, R. P. Melnyk, and O. G. Melnyk, "Improving the performance of information security systems", in *Coll. Materials Internat. Sci.-Pract. Conf. "Chrezvychainyie situatsiyi: teoriya, praktika, innovatsiyi" "ChS – 2012"*. Gomel: GGTU im. P. O. Sukhogo, 2012, p. 224 [in Russian].

[4] V. N. Rudnyckyj, S. V. Pivneva, V. G. Babenko, I. V. Mironets, A. V. Dmitrishyn, and Yu. V. Baryshev, *Cryptographic coding: methods and means of implemen-tation:* monograph, Toliatty, 2013 [in Russian].

[5] V. N. Rudnickyj, V. Ya. Milchevich, V. G. Babenko, R. P. Melnik, S. V. Rudnickyj, and O. G. Melnik, *Cryptographic coding: methods and means of implementation (part 2):* monograph. Kharkiv: Shchedraia usadba plius, 2014 [in Russian].

[6] *Cryptographic coding:* coll. monograph, V. N. Rudnickyi and V. Ya. Milchevich, Eds. Kharkiv: Shchedraia usadba plius, 2014 [in Russian].

[7] *Cryptographic encoding: processing and protecting information*, V. M. Rudnyckyi, Ed. Kharkiv: DISA PLIUS, 2018 [in Ukrainian].

[8] V. M. Rudnyckyj, I. V. Myronets, and V. G. Babenko, "Systematization of a complete set of logical functions for the cryptographic transformation of information", *Systemy obrobky informatsii*, no. 8 (98), pp. 184-188, 2011 [in Ukrainian].

[9] V. M. Rudnyckyj, V. G. Babenko, and S. V. Rudnyckyj, "Method of synthesis of matrix models of operations of cryptographic encoding and decoding of information", *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl*, no. 4 (33), pp. 198-200, 2012 [in Ukrainian].

[10] V. M. Rudnyckyj, V. G. Babenko, and S. V. Rudnyckyj, "Method of synthesis of matrix models of operations of cryptographic transcoding of information", *Zakhyst informatsii*, no. 3 (56), pp. 50-56, 2012 [in Ukrainian].

V. M. Rudnytskyi[1], *D. Tech. Sc., professor,*
e-mail: rvn_2008@ukr.net
O. G. Melnyk[2], *Ph. D., senior researcher,*
e-mail: melnyk.olja.2014@gmail.com
R. P. Melnyk[2], *Ph. D.,*
e-mail: indigo211212@gmail.com
[1]Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine
[2]Cherkasy Institute of Fire Safety named after Chornobyl Heroes
of National University of Civil Defence of Ukraine,
Onoprienko str., 8, Cherkasy, 18034, Ukraine

TECHNOLOGY OF DESCRIBING LINEAR AND NONLINEAR CRYPTOGRAPHIC TRANSFORMATIONS

The paper deals with the study of the dependence of the calculation of the number of operations, based on recurrent combination of capacities of sets of operations of lower bit rate and elementary functions to describe the process of construction of sets of new operations. The possibility of developing a single technology for the synthesis and investigation of both linear and nonlinear operations of

DOI: 10.24025/2306-4412.3.2019.178322

cryptographic transformation of information is studied. An attempt has been made to obtain three-bit operations based on two-bit operations of cryptographic information conversion.

For this purpose, logical functions are presented in the form of logical operations of two variables corresponding to them in analytical representation. Two-bit elementary functions in the operation of cryptographic information transformation are combined. The study calculates the number of two-bit, three-bit and four-bit elementary functions, two-bit, three-bit and four-bit operations.

According to the results of the study, it is found that our proposed dependence of the calculation of the number of operations of cryptographic transformation, based on recurrent combination of capacities of sets of operations of lower bit rate and elementary functions, is correct and mathematically describes the process of constructing the sets of new operations. Based on the results of this study, it can be considered that the development of a single technology for the synthesis and investigation of both linear and nonlinear operations of cryptographic transformation of information is possible. This approach allows not only to calculate the number of operations of cryptographic information conversion, but also to construct the operations themselves by combining known cryptographic transformation operations and elementary higher bit functions.

The proposed approach creates the preconditions for the development of a single technology for the description and synthesis of both linear and nonlinear crypto-transformation operations.

Keywords: *information protection, operations of cryptographic transformation, synthesis of operations, digit capacity, technology of synthesis.*

Стаття надійшла 27.06.2019
Прийнято 19.07.2019

DOI: 10.24025/2306-4412.3.2019.178322