УДК 004.056.55:004.312.2 DOI: 10.30748/soi.2019.156.13

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

[1] *Черкаський державний технологічний університет, Черкаси*
[2] *Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля, Черкаси*

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

В статті застосовано логічні функції в операції матричного криптографічного перетворення інформації на основі додавання за модулем два для захисту інформаційних ресурсів. Розроблено технологію побудови оберненої двохоперандної чотирьохрозрядної операції мінімальної складності з властивістю строгого стійкого криптографічного кодування. Таке строге стійке криптографічне кодування є суттєвим для зменшення будь-якої кореляції між значеннями бітів незакодованого і закодованого повідомлення при спробах декодування закодованого повідомлення.

Ключові слова: *криптографічне перетворення, логічні функції, додавання за модулем два, матричні операції, математична модель, обернена операція.*

Вступ

Постановка проблеми. Створення нових надійних швидкодіючих методів криптографічного перетворення (КП) на основі логічних функцій від великої кількості змінних важливе для розвитку криптографії. Розвиток методів строгого стійкого криптографічного кодування як одного з напрямків КП на основі логічних функцій є важливим, тому що приводить до значної невизначеності значення кожного біта незакодованого повідомлення при спробах декодування повідомлення [1].

Аналіз останніх досліджень і публікацій. У криптографії лавинний ефект (ЛЕ) відноситься до бажаної властивості криптографічних алгоритмів (КА), зазвичай блокових шифрів (БШ) та криптографічних хеш-функцій (КХФ) [2–3]. ЛЕ проявляється, якщо в середньому половина вихідних бітів змінюється щоразу, коли один вхідний біт змінює значення. Якщо БШ або КХФ не мають значного ЛЕ, то вони мало рандомізовані і криптоаналітик може робити прогнози про дані входу, маючи тільки дані виходу, і частково або повністю розкрити КА [2]. ЛЕ обраховується за формулою [2]:

$$\text{ЛЕ} = \frac{Кількість\_змінених\_біт\_в\_шифротексті}{Загальна\_кількість\_біт\_в\_шифротексті}.$$

Отже, для високоякісних БШ невелика зміна або ключа, або відкритого тексту повинна привести до різкої зміни шифротексту [4].

КП є повним, якщо кожен вихідний біт залежить від всіх вхідних біт [5]. Строгий лавинний критерій, який забезпечує строге стійке криптографічне кодування, був введений Вебстером і Таваресом [5], щоб об'єднати ідеї повноти КП і ЛЕ.

Щоб відповідати строгому лавинному критерію, кожен вихідний біт повинен змінюватися з ймовірністю 0,5 щоразу, коли один вхідний біт змінює значення. Тобто зміна значення будь-якого окремого біта вхідного вектора даних повинна привести до зміни рівно половини значень вихідного вектора даних, так як ЛЕ = 50% є суттєвим для зменшення будь-якої кореляції між комбінаціями на вході і виході і не дає витоку інформації [6]. Тому будь-яке значення ЛЕ, близьке до 0,5, завжди вважається показником якості КП [6]. Це означає, зокрема, що не існує функції з меншою кількістю біт, яка є хорошим наближенням до даної функції і використання якої суттєво скоротило б обсяг роботи, необхідної для декодування повідомлення.

В БШ при виконанні симетричного шифрування залежність ключа і вихідних даних робиться якомога складнішою з допомогою S-боксів (таблиць підстановок), як нелінійних компонентів, які призводять до сильної плутанини при спробах дешифрування повідомлення та забезпечують безпеку передачі даних [6]. Побудова оптимальних S-боксів є найголовнішою темою, яка цікавить експертів з питань безпеки [6].

Прямі одноопернадні чотирьохрозрядні операції мінімальної складності з властивістю строгого стійкого криптографічного кодування розроблені та частково досліджені в [1; 7–9].

Але оскільки КП складається з прямої і оберненої операції, залишається не вирішеною актуальна задача розробки методів створення оберненої двохоперандної чотирьохрозрядної операції мінімальної складності для строгого стійкого криптографічного кодування.

Метою статті є розробка технології побудови оберненої двохоперандної чотирьохрозрядної операції мінімальної складності для строгого стійкого криптографічного кодування.

Основний матеріал

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

Знайдемо обернену операцію для прямої чотирьохрозрядної двохоперандної операції O^d з властивістю строгого стійкого криптографічного кодування:

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

Для синтезу операції, оберненої до (1), необхідно побудувати обернені чотирьохрозрядні одноопераднді операції до операцій $F_7^4 - F_{22}^4$ (2). Для побудови обернених операцій строгого стійкого криптографічного кодування застосуємо метод синтезу операцій оберненого матричного криптографічного перетворення [9].

Даний метод забезпечує побудову обернених одноопераднних матричних операцій довільної кількості аргументів. Результати побудови наведено в табл. 1.

Таблиця 1

Результати побудови вибраних обернених чотирьохрозрядних одноопераднних операцій строгого стійкого криптографічного кодування

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

Синтезуємо обернену операцію для застосування в потокових шифрах, з врахуванням можливості використання в прямому та оберненому каналах шифрування однакових гамуючих послідовностей. В загальному вигляді модель можна представити:

$$O=\begin{cases} F_7^{4d}, & для\ k_1=0;\ k_2=0, k_3=0;\ k_4=0;\\ F_8^{4d}, & для\ k_1=0;\ k_2=0, k_3=0;\ k_4=1;\\ F_9^{4d}, & для\ k_1=0;\ k_2=0, k_3=1;\ k_4=0;\\ F_{10}^{4d}, & для\ k_1=0;\ k_2=0, k_3=1;\ k_4=1;\\ F_{11}^{4d}, & для\ k_1=0;\ k_2=1, k_3=0;\ k_4=0;\\ F_{12}^{4d}, & для\ k_1=0;\ k_2=1, k_3=0;\ k_4=1;\\ F_{13}^{4d}, & для\ k_1=0;\ k_2=1, k_3=1;\ k_4=0;\\ F_{14}^{4d}, & для\ k_1=0;\ k_2=1, k_3=1;\ k_4=1;\\ F_{15}^{4d}, & для\ k_1=1;\ k_2=0, k_3=0;\ k_4=0;\\ F_{16}^{4d}, & для\ k_1=1;\ k_2=0, k_3=0;\ k_4=1;\\ F_{17}^{4d}, & для\ k_1=1;\ k_2=0, k_3=1;\ k_4=0;\\ F_{18}^{4d}, & для\ k_1=1;\ k_2=0, k_3=1;\ k_4=1;\\ F_{19}^{4d}, & для\ k_1=1;\ k_2=1, k_3=0;\ k_4=0;\\ F_{20}^{4d}, & для\ k_1=1;\ k_2=1, k_3=0;\ k_4=1;\\ F_{21}^{4d}, & для\ k_1=1;\ k_2=1, k_3=1;\ k_4=0;\\ F_{22}^{4d}, & для\ k_1=1;\ k_2=1, k_3=1;\ k_4=1. \end{cases} \quad (2)$$

Як видно з табл. 1, моделі спрощених операцій прямого та оберненого перетворення співпадають (2). Побудуємо таблицю істинності для синтезу моделі обробки сигналів інверсії функцій. Результати побудови наведено в табл. 2.

Побудуємо модель обробки сигналів інверсії. За результатами мінімізації отримано:

$$\overline{f}_1=\overline{(y_1\cdot y_2)\oplus y_3};$$
$$\overline{f}_2=\overline{y}_2\cdot y_4\vee y_2\cdot(y_1\oplus y_3);$$
$$\overline{f}_3=y_1\cdot\overline{y}_4\vee\overline{y}_1\cdot\overline{y}_2\cdot y_3\vee\overline{y}_1\cdot y_2\cdot y_4;$$
$$\overline{f}_4=\overline{y}_1\cdot\overline{y}_4\vee y_1\cdot y_2\cdot y_4\vee y_1\cdot\overline{y}_2\cdot y_3;$$
$$\overline{O}^r=\begin{bmatrix}\overline{(y_1\cdot y_2)\oplus y_3}\\ \overline{y}_2\cdot y_4\vee y_2\cdot(y_1\oplus y_3)\\ y_1\cdot\overline{y}_4\vee\overline{y}_1\cdot\overline{y}_2\cdot y_3\vee\overline{y}_1\cdot y_2\cdot y_4\\ \overline{y}_1\cdot\overline{y}_4\vee y_1\cdot y_2\cdot y_4\vee y_1\cdot\overline{y}_2\cdot y_3\end{bmatrix} \quad (3)$$

Таблиця 2

Таблиця істинності параметрів інверсії моделі операції

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

На основі виразів (2–3) побудуємо обернену чотирьохрозрядну двохоперандну операцію строгого стійкого криптографічного кодування:

$$O^r=\begin{bmatrix}x_1\cdot(\overline{y_1\cdot y_2})\oplus x_2\cdot(y_1\cdot y_2)\\ x_1\cdot(y_1\cdot y_2)\oplus x_2\cdot(\overline{y}_1\cdot y_2)\oplus x_3\cdot(y_1\cdot\overline{y}_2)\oplus x_4\cdot(\overline{y}_1\cdot\overline{y}_2)\\ x_2\cdot(y_1\cdot\overline{y}_2)\oplus x_3\cdot(y_1\equiv y_2)\oplus x_4\cdot(\overline{y}_1\cdot y_2)\\ x_2\cdot(\overline{y}_1\cdot\overline{y}_2)\oplus x_3\cdot(\overline{y}_1\cdot y_2)\oplus x_4\cdot y_1\end{bmatrix}\oplus\begin{bmatrix}\overline{(y_1\cdot y_2)\oplus y_3}\\ \overline{y}_2\cdot y_4\vee y_2\cdot(y_1\oplus y_3)\\ y_1\cdot\overline{y}_4\vee\overline{y}_1\cdot\overline{y}_2\cdot y_3\vee\overline{y}_1\cdot y_2\cdot y_4\\ \overline{y}_1\cdot\overline{y}_4\vee y_1\cdot y_2\cdot y_4\vee y_1\cdot\overline{y}_2\cdot y_3\end{bmatrix}$$

$$O^r=\begin{bmatrix}x_1\cdot(\overline{y_1\cdot y_2})\oplus x_2\cdot(y_1\cdot y_2)\oplus\overline{(y_1\cdot y_2)\oplus y_3}\\ x_1\cdot(y_1\cdot y_2)\oplus x_2\cdot(\overline{y}_1\cdot y_2)\oplus x_3\cdot(y_1\cdot\overline{y}_2)\oplus x_4\cdot(\overline{y}_1\cdot\overline{y}_2)\oplus\overline{y}_2\cdot y_4\vee y_2\cdot(y_1\oplus y_3)\\ x_2\cdot(y_1\cdot\overline{y}_2)\oplus x_3\cdot(y_1\equiv y_2)\oplus x_4\cdot(\overline{y}_1\cdot y_2)\oplus y_1\cdot\overline{y}_4\vee\overline{y}_1\cdot\overline{y}_2\cdot y_3\vee\overline{y}_1\cdot y_2\cdot y_4\\ x_2\cdot(\overline{y}_1\cdot\overline{y}_2)\oplus x_3\cdot(\overline{y}_1\cdot y_2)\oplus x_4\cdot y_1\oplus\overline{y}_1\cdot\overline{y}_4\vee y_1\cdot y_2\cdot y_4\vee y_1\cdot\overline{y}_2\cdot y_3\end{bmatrix} \quad (4)$$

Операції (1) і (4) забезпечують реалізацію одного з варіантів паралельного чотирьохбітового потокового шифрування, в результаті якого буде досягатися максимальна відсутність кореляції між двійковими комбінаціями не закодованого і закодованого повідомлення і забезпечуватиметься відсутність витоку інформації.

Висновки

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

Список літератури

1. Рудницький В.М. Побудова примітивів строгого стійкого кодування мінімальної складності / В.М. Рудницький, Л.А. Шувалова, О.Б. Нестеренко // Вісник Черкаського державного технологічного університету. – 2018. – № 1. – С. 21-26.

2. Drashti E. Study of avalanche effect in AES / E. Drashti, O. Vadaviya, Purvi H. Tandel // National Conference on Recent Advances in Engineering for Sustainability. – May 2015.

3. Vyakaranal S. Performance Analysis of Symmetric Key Cryptographic Algorithms / S. Vyakaranal, S. Kengond // 2018 International Conference on Communication and Signal Processing (ICCSP). – Chennai. – 2018. – P. 0411-0415. https://doi.org/10.1109/ICCSP.2018.8524373.

4. Kumar Amish. Effective implementation and avalanche effect of AES / Amish Kumar, Mrs. Namita Tiwari // International Journal of Security, Privacy and Trust Management (IJSPTM). – August 2012. – Vol. 1, No. 3/4. – P. 31-35.

5. Cusick T.W. Cryptographic Boolean Functions and Applications / T.W. Cusick, P. Stanica. – Amsterdam, The Netherlands: Elsevier, 2009.

6. A New 1D Chaotic Map and β-Hill Climbing for Generating Substitution-Boxes / Ahmad M. Alzaidi, M.N. Doja, E.A. Solami, M.M.S. Beg // IEEE Access. – 2018. – Vol. 6. – P. 55405-55418. https://doi.org/10.1109/ACCESS.2018.2871557.

7. 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.

8. 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.

9. 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". – 2016. – С. 14.

10. Рудницький В.М. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації / В.М. Рудницький, В.Г. Бабенко, С.В. Рудницький // Збірник наукових праць Харківського університету Повітряних Сил. – Вип. 4 (33). – Х.: ХУПС ім. І. Кожедуба, 2012. – С. 198-200.

References

1. Rudnitskyi, V.M., Shuvalova, L.A. and Nesterenko, O.B. (2018), "Pobudova prymityviv strohoho stiikoho koduvannia minimalnoi skladnosti" [Creation of primitives of strict sustainable coding of minimal complexity], *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu, Seria: Tehnichni nauky*, No. 1, pp. 21-26.

2. Drashti, E., Vadaviya, O. and Tandel, Purvi H. (2015), Study of avalanche effect in AES, *National Conference on Recent Advances in Engineering for Sustainability.*

3. Vyakaranal, S. and Kengond, S. (2018), Performance Analysis of Symmetric Key Cryptographic Algorithms, *International Conference on Communication and Signal Processing (ICCSP),* Chennai, pp. 0411-0415. https://doi.org/10.1109/ICCSP.2018.8524373.

4. Kumar, Amish and Mrs. Tiwari, Namita (2012), Effective implementation and avalanche effect of AES, *International Journal of Security, Privacy and Trust Management (IJSPTM)*, Vol. 1, No. 3/4, pp. 31-35.

5. Cusick, T.W. and Stanica, P. (2009), *Cryptographic Boolean Functions and Applications*, Elsevier, Amsterdam, The Netherlands.

6. Alzaidi, M. Ahmad, Doja, M.N., Solami, E.A. and Beg, M.M.S. (2018), A New 1D Chaotic Map and β-Hill Climbing for Generating Substitution-Boxes, *IEEE Access*, Vol. 6, pp. 55405-55418. https://doi.org/10.1109/ACCESS.2018.2871557.

7. Rudnitskyi, V.M., Shuvalova, L.A. and Nesterenko, O.B. (2016), "Syntez operatsii kryptohrafichnoho peretvorennia za kryteriiem strohoho stiikoho koduvannia" [Synthesis of operations of cryptographic transformation by the criterion of strict sustainable coding], *Bulletin of engineering academy of Ukraine*, No. 3, pp. 105-108.

8. Rudnitskyi, V.M., Shuvalova, L.A. and Nesterenko, O.B. (2017), "Metod syntezu operatsii kryptohrafichnoho peretvorennia za kryteriiem strohoho stiikoho koduvannia" [The method of synthesis of cryptographic conversion operations according to the criterion of strict sustainable coding], *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu*, No. 1, pp. 5-10.

9. Shuvalova, L.A. and Nesterenko, O.B. (2016), "Syntez ta analiz kryptohrafichnykh operatsii za kryteriiem strohoho stiikoho koduvannia" [Synthesis and analysis of cryptographic operations by the criterion of strict sustainable coding], *Tezy dopovidei IV mizhnarodnoi naukovo-tekhnichnoi konferentsii "Problemy informatyzatsii"*, pp. 14.

10. Rudnitskyi, V.M., Babenko, V.G. and Rudnitskyi, S.V. (2012), "Metod syntezu matrychnykh modelei operatsii kryptohrafichnoho koduvannia ta dekoduvannia informatsii" [The synthesis method of matrix models of cryptographic operations data encoding and decoding], *Scientific works of Kharkiv National Air Force University,* No. 4(33), pp. 198-200.

Надійшла до редколегії 26.12.2018
Схвалена до друку 22.01.2019

Відомості про авторів:

Федотова-Півень Ірина Миколаївна
кандидат технічних наук доцент
доцент кафедри Черкаського державного
технологічного університету,
Черкаси, Україна
https://orcid.org/0000-0002-0512-6118

Лада Наталія Володимирівна
кандидат технічних наук
асистент кафедри Черкаського державного
технологічного університету,
Черкаси, Україна
https://orcid.org/0000-0002-7682-2970

Мельник Ольга Григорівна
кандидат технічних наук доцент
доцент кафедри Інституту пожежної безпеки
ім. Героїв Чорнобиля Національного університету
цивільного захисту України,
Черкаси, Україна
https://orcid.org/0000-0002-9671-108X

Пустовіт Михайло Олександрович
старший викладач кафедри
Інституту пожежної безпеки ім. Героїв Чорнобиля
Національного університету цивільного захисту України,
Черкаси, Україна
https://orcid.org/0000-0001-5313-1459

Information about the authors:

Iryna Fedotova-Piven
Candidate of Technical Sciences Associate Professor
Senior Lecturer of Department of Cherkasy
State Technological University,
Cherkasy, Ukraine
https://orcid.org/0000-0002-0512-6118

Nataliia Lada
Candidate of Technical Sciences
Assistant Lecturer of Department
of Cherkasy State Technological University,
Cherkasy, Ukraine
https://orcid.org/0000-0002-7682-2970

Olga Melnyk
Candidate of Technical Sciences Associate Professor
Senior Lecturer of Department of Cherkasy Institute of Fire
Safety named after Chornobyl Heroes of National University
of Civil Defense of Ukraine,
Cherkasy, Ukraine
https://orcid.org/0000-0002-9671-108X

Mykhailo Pustovit
Senior Instructor of Department of Cherkasy Institute of Fire
Safety named after Chornobyl Heroes of National University
of Civil Defense of Ukraine,
Cherkasy, Ukraine
https://orcid.org/0000-0001-5313-1459

МОДЕЛИРОВАНИЕ ОБРАТНОЙ ДВУХОПЕРАНДНОЙ ЧЕТЫРЕХРАЗРЯДНОЙ ОПЕРАЦИИ МИНИМАЛЬНОЙ СЛОЖНОСТИ ДЛЯ СТРОГОГО УСТОЙЧИВОГО КРИПТОГРАФИЧЕСКОГО КОДИРОВАНИЯ

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

В статье применены логические функции в операции матричного криптографического преобразования информации на основе сложения по модулю два для защиты информационных ресурсов. Разработана технология построения обратной двухоперандной четырехразрядной операции минимальной сложности со свойством строгого устойчивого криптографической кодирования. Такое строгое устойчивое криптографическое кодирование является существенным для уменьшения любой корреляции между значениями битов незакодированного и закодированного сообщения при попытках декодирования закодированного сообщения.

Ключевые слова: *криптографическое преобразование, логические функции, сложение по модулю два, матричные операции, математическая модель, обратная операция.*

MODELING A REVERSE TWO-OPERAND FOUR-DIGIT OPERATION OF MINIMAL COMPLEXITY FOR STRICTLY SUSTAINABLE CRYPTOGRAPHIC CODING

I. Fedotova-Piven, N. Lada, O. Melnik, M. Pustovit

The article is devoted to the modeling of matrix operations of cryptographic transformation of information. The logical functions were applied 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 reverse two-operand four-digit operation of minimal complexity with a property of strictly sustainable cryptographic coding. Initially, the reverse four-digit single-operand operations of minimal complexity were constructed by the method of synthesis of reverse matrix cryptographic transformations. A model of a simplified two-operand four-digit operation of minimal complexity was constructed without taking into account the signals of the inversion of functions, then a truth table was constructed for the synthesis of the inverse function signal processing model. A model for processing inversion signals is constructed. As a result of minimization, a reverse four-digit two-operand operation of minimal complexity of strictly sustainable cryptographic coding is constructed. Such strictly sustainable cryptographic coding is essential for reducing any correlation between the values of digits of an unencoded and coded message when attempting to decode a coded message. The proposed technology for constructing a reverse two-operand four-digit operation of minimal complexity with the strictly sustainable cryptographic coding property is verified by creating one of the two-operand four-digit operations for stream encryption. The applying of proposed technology of constructing a reverse two-operand four-digit operation of minimal complexity with the strictly sustainable cryptographic coding property allows to construct of highly reliable systems of cryptographic information protection systems and to improve their cryptographic strength.

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