УДК 621.391

В.М. Рудницький, В.Г. Бабенко

Черкаський державний технологічний університет, Черкаси

МОДЕЛЬ УНІФІКОВАНОГО ПРИСТРОЮ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

Робота присвячена розробці моделі уніфікованого пристрою криптографічного перетворення інформації, принцип роботи якого оснований на застосуванні синтезованих наборів спеціалізованих логічних функцій, і який здатний забезпечувати двостороннє криптографічне перетворення інформації, тобто як кодування, так і декодування оброблюваної інформації, в залежності від сигналу управління.

Ключові слова: *комбінаційна схема, спеціалізовані логічні функції, криптографічне перетворення.*

Вступ

Постановка проблеми. Останнім часом коло задач криптографії значно розширилось завдяки стрімкому розвитку комунікаційних технологій та їх поширення в усі сфери діяльності. Поряд з традиційним та відкритим шифруванням, окремим напрямом є розробка методів і алгоритмів задач щодо захисту інформації від несанкціонованого її перетворення при передаванні по каналам зв'язку (імітозахист, хеш-функції, аутентифікація, цифровий підпис та ін.) [3]. Упровадження в усі сфери життєдіяльності суспільства та держави інформаційних технологій зумовило поширення великих масивів інформації в обчислювальних та інформаційних мережах, автоматизованих та технічних засобів обробки інформації, що в свою чергу загострило проблему захисту інформації та визначило необхідність розвитку методів і засобів захисту інформації.

Аналіз досліджень та публікацій. Протягом багатьох років криптографія слугувала виключно військовим цілям. Сьогодні звичайні користувачі отримують можливість звертатися до засобів, які дозволяють захистити себе від несанкціонованого доступу до конфіденційної інформації, застосовуючи методи комп'ютерної криптографії [1]. До появи комп'ютерів криптографія складалась із алгоритмів на символьній основі. Різноманітні криптографічні алгоритми або заміняли одні символи на інші або переставляли символи.

Сьогодні все значно складніше, але філософія залишається попередньою. Перша зміна полягає в тому, що алгоритми почали працювати з бітами, а не символами. Це важливо хоча б з точки зору алфавіту – з 26 елементів до двох. Більшість хороших криптографічних алгоритмів до цього часу комбінує підстановки та перестановки.

Шкідливі впливи на інформацію в процесі функціонування комп'ютерних систем різного призначення відбуваються з ціллю порушення її конфіденційності, цілісності і доступності. Вирішення задач, пов'язаних з попередженням впливу безпосередньо на інформацію, відбувається в рамках комплексної проблеми забезпечення безпеки інформації і має достатньо розвинену науково-методичну базу [2].

В основі криптографії лежить сукупність методів перетворення даних, направлених на те, щоб зробити інформацію, яка передається або обробляється, даремною для зловмисника. Для того, щоб приховати зміст інформації, що передається, застосовують два типи перетворень: кодування та шифрування.

З практичної точки зору важливими також є наступні принципи архітектурної безпеки: неперервність захисту в просторі та часі, неможливість обминути захисні засоби, дотримання стандартів, використання апробованих рішень, ієрархічна організація інформаційних систем з невеликим числом сутностей на кожному рівні, посилення найслабшої ланки, неможливість переходу в небезпечний стан, мінімізація привілеїв, розділення обов'язків, каскадність оборони, різноманітність захисних засобів, простота і керованість інформаційної системи [1, 2].

Мета статті. Мета роботи полягає у розробці моделі уніфікованого пристрою криптографічного перетворення інформації, основаного на реалізації синтезованих наборів спеціалізованих логічних функцій, який здатний забезпечувати двостороннє криптографічне перетворення інформації, тобто як кодування, так і декодування оброблюваної інформації, в залежності від сигналу управління.

Виклад основного матеріалу

Основною задачею дослідження є побудова пристрою криптографічного перетворення інформації, який може реалізувати повну множину спеціалізованих логічних функцій для кодування-декодування інформації.

В основу розробки пристрою кодування-декодування покладемо факт взаємної відповідності функцій кодування функціям декодування [4], що дозволить зменшити кількість команд управління за рахунок заміни команди декодування однією функцією на команду кодування відповідною функцією.

Для забезпечення функціонування пристрою криптографічного кодування необхідно ідентифікувати вибрані функції. Ідентифікація може бути реалізована на основі двох підходів: ідентифікація функції; ідентифікація операції, на основі якої отримана функція.

Другий підхід більш пріоритетний порівняно з першим, так як його реалізація полягає в побудові уніфікованого пристрою кодування-декодування інформації на основі спеціалізованих блоків.

Як математичний апарат дуже зручно та ефективно застосувати алгебру Буля для аналізу і синтезу комбінаційних схем. Відомо, що булеві функції визначають логіку роботи комбінаційних схем наступного виду (рис. 1), де $x_1 - x_n$, $F \in \{0,1\}$.

Рис. 1. Загальний вигляд комбінаційної схеми

Відповідно другому підходу потрібно розбити функції [5] на групи, реалізація яких і буде формувати спеціалізовані блоки уніфікованого пристрою. Ідентифікація операції полягає у визначенні всіх типів операцій, що використовуються у синтезованих моделях спеціалізованих функцій. Спираючись на це, можемо ідентифікувати в якості базових операцій такі як інверсія, заміна простої функції на складну та перестановка функцій. Розглянемо функції криптографічного кодування інформації, які синтезуються на основі інверсії правильно розміщених функцій. До даної групи спеціалізованих логічних функцій входять $\vec{F}_1$, $\vec{F}_3$, $\vec{F}_4$, $\vec{F}_5$.

Реалізація чотирьох варіантів інверсії двохрозрядного коду вимагає використання двох сигналів управління k_1 і k_2. Виходячи з простоти представлення, закодуємо сигнали управління наступним чином:

$k_1 = 0;\ k_2 = 0$ – вихідні функції неінвертовані;

$k_1 = 0;\ k_2 = 1$ – інверсія першої вихідної функції;

$k_1 = 1;\ k_2 = 0$ – інверсія другої вихідної функції;

$k_1 = 1;\ k_2 = 1$ – інверсія двох вихідних функцій.

Враховуючи вище сказане, модель функції кодування $\vec{F}_{1,3,4,5}$ буде представлена як:

$$\vec{F}_{1,3,4,5}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, & \text{якщо} \quad k_1 = 0,\ k_2 = 0; \\ \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix}, & \text{якщо } k_1 = 0,\ k_2 = 1; \\ \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix}, & \text{якщо} \quad k_1 = 1,\ k_2 = 0; \\ \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}, & \text{якщо} \quad k_1 = 1,\ k_2 = 1. \end{cases}$$

Тобто в даному випадку n=4, а саме x_1 , x_2 , k_1, k_2 – вхідні сигнали, при чому x_1, x_2 – інформаційні входи, де x_1 – значення першого розряду інформації, а x_2 – значення другого розряду інформації. Тоді відповідно задекларуємо і два вихідних сигнали Y_1 – для першого розряду, Y_2 – для другого розряду закодованої інформації. Побудуємо таблицю істинності для функції кодування $\vec{F}_{1,3,4,5}$ (табл. 1), яка ставить у відповідність кожному набору вхідних сигналів значення вихідних сигналів .

Для отримання логічних функцій, які описують вихідні сигнали, ми провели мінімізацію описаної моделі функцій $\vec{F}_{1,3,4,5}$ з використанням методу діаграм Вейча та отримали наступний результат:

$$y_1 = x_1\overline{k}_1 \cup \overline{x}_1 k_1;$$
$$y_2 = x_2\overline{k}_2 \cup \overline{x}_2 k_2.$$

Тобто спеціалізований блок, який виконує всі чотири варіанти інверсії двохрозрядного коду, будуватиметься на основі реалізації даних визначених логічних функцій та матиме відповідно два інформаційні виходи.

Таблиця 1

Таблиця істинності моделі $\vec{F}_{1,3,4,5}$

X_1	X_2	K_1	K_2	$У_1$	$У_2$
0	0	0	0	**0**	**0**
0	0	0	1	**1**	**0**
0	0	1	0	**0**	**1**
0	0	1	1	**1**	**1**
0	1	0	0	**1**	**0**
0	1	0	1	**0**	**0**
0	1	1	0	**1**	**1**
0	1	1	1	**0**	**1**
1	0	0	0	**0**	**1**
1	0	0	1	**1**	**1**
1	0	1	0	**0**	**0**
1	0	1	1	**1**	**0**
1	1	0	0	**1**	**1**
1	1	0	1	**0**	**1**
1	1	1	0	**1**	**0**
1	1	1	1	**0**	**0**

Розглянемо функції криптографічного кодування інформації, які виконують всі види перестановок. До даної групи спеціалізованих логічних функцій входять $\vec{F}_2$, $\vec{F}_6$, $\vec{F}_7$, $\vec{F}_8$.

Для реалізації чотирьох варіантів перестановки з врахуванням інверсії двохрозрядного коду достатньо двох сигналів управління k_1 і k_2 . Коди сигналів управління можна представити наступним чином:

$k_1 = 0;\ k_2 = 0$ – вихідні функції переставлені та неінвертовані;

$k_1 = 0;\ k_2 = 1$ – вихідні функції переставлені та інвертована перша вихідна функція;

$k_1 = 1;\ k_2 = 0$ – вихідні функції переставлені та інвертована друга вихідна функція;

$k_1 = 1;\ k_2 = 1$ – вихідні функції переставлені та інвертовані.

Виходячи з вище сказаного, функція кодування $\vec{F}_{2,6,7,8}$ буде представлена як:

$$\vec{F}_{2,6,7,8}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}, & \text{якщо } k_1 = 0,\ k_2 = 0; \\ \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix}, & \text{якщо } k_1 = 0,\ k_2 = 1; \\ \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix}, & \text{якщо } k_1 = 1,\ k_2 = 0; \\ \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}, & \text{якщо } k_1 = 1,\ k_2 = 1. \end{cases}$$

Побудувавши таблицю істинності для даної моделі функції кодування та виконавши мінімізацію за допомогою діаграм Вейча для першої та другої функцій виходу, отримаємо:

$$y_1 = \overline{x}_2 k_2 \vee x_2\overline{k}_2 ;$$
$$y_2 = \overline{x}_1 k_1 \vee x_1\overline{k}_1 .$$

Дані логічні функції покладемо в основу синтезу спеціалізованого блоку перестановок спеціалізованих функцій.

Проведемо синтез узагальненої моделі функції $\vec{F}_{1,2,3,4,5,6,7,8}$, яка поєднує функції інверсії та перестановки. Дана модель міститиме вісім функцій, тому для її реалізації потрібно принаймні три сигнали управління. Для опису інверсії використаємо два сигнали управління, а третій сигнал задамо як ознаку перестановки функцій. Коди сигналів управління можна задати наступним чином:

$k_1 = 0;\ k_2 = 0;\ k_3 = 0$ – вихідні функції непереставлені та неінвертовані;

$k_1 = 0;\ k_2 = 0;\ k_3 = 1$ – вихідні функції переставлені та неінвертовані;

$k_1 = 0;\ k_2 = 1;\ k_3 = 0$ – вихідні функції непереставлені та інвертована перша вихідна функція;

$k_1 = 0;\ k_2 = 1;\ k_3 = 1$ – вихідні функції переставлені та інвертована перша вихідна функція;

$k_1 = 1;\ k_2 = 0;\ k_3 = 0$ – вихідні функції непереставлені та інвертована друга вихідна функція;

$k_1 = 1;\ k_2 = 0;\ k_3 = 1$ – вихідні функції переставлені та інвертована друга вихідна функція;

$k_1 = 1;\ k_2 = 1;\ k_3 = 0$ – вихідні функції непереставлені та інвертовані;

$k_1 = 1;\ k_2 = 1;\ k_3 = 1$ – вихідні функції переставлені та інвертовані.

Векторне представлення даної моделі матиме вигляд:

$$\vec{F}_{1,2,3,4,5,6,7,8}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{cases}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } k_1=0,\ k_2=0,\ k_3=0;\\ \begin{pmatrix}x_1\oplus 1\\x_2\end{pmatrix}, \text{якщо } k_1=0,\ k_2=1,\ k_3=0;\\ \begin{pmatrix}x_1\\x_2\oplus 1\end{pmatrix}, \text{якщо } k_1=1,\ k_2=0,\ k_3=0;\\ \begin{pmatrix}x_1\oplus 1\\x_2\oplus 1\end{pmatrix}, \text{якщо } k_1=1,\ k_2=1,\ k_3=0;\\ \begin{pmatrix}x_2\\x_1\end{pmatrix}, \text{ якщо } k_1=0,\ k_2=0,\ k_3=1;\\ \begin{pmatrix}x_2\oplus 1\\x_1\end{pmatrix}, \text{якщо } k_1=0,\ k_2=1,\ k_3=1;\\ \begin{pmatrix}x_2\\x_1\oplus 1\end{pmatrix}, \text{якщо } k_1=1,\ k_2=0,\ k_3=1;\\ \begin{pmatrix}x_2\oplus 1\\x_1\oplus 1\end{pmatrix}, \text{якщо } k_1=1,\ k_2=1,\ k_3=1.\end{cases}$$

Побудувавши таблицю істинності узагальненої моделі $\vec{F}_{1,2,3,4,5,6,7,8}$ та виконавши мінімізацію за допомогою діаграм Вейча функцій виходу, які залежать в даному випадку від п'яти аргументів, а саме x_1, x_2 – інформаційні входи, а k_1, k_2, k_3 – сигнали управління, отримаємо наступні логічні функції інформаційних виходів:

$$y_1 = x_1\bar{k}_2\bar{k}_3 \vee \bar{x}_1k_2\bar{k}_3 \vee \bar{x}_2k_2k_3 \vee x_2\bar{k}_2k_3;$$

$$y_2 = x_2\bar{k}_1\bar{k}_3 \vee x_1\bar{k}_1k_3 \vee \bar{x}_2k_1\bar{k}_3 \vee \bar{x}_1k_1k_3.$$

Спеціалізований блок, який реалізує як всі варіанти інверсії, так і перестановки функцій, описуватиметься вище зазначеними булевими виразами.

Для реалізації спеціалізованого блоку заміни простої функції на складну розглянемо два випадки: заміни застосована лише для першої вхідної функції або лише для другої вхідної функції.

Проведемо синтез узагальненої моделі функції $\vec{F}_{1,2,3,4,5,6,7,8,9,11,13,14,18,20,23,24}$, яка враховує інверсії та перестановки, а також можливість заміни першої функції на складну. Для реалізації даної моделі достатньо чотирьох сигналів управління. Опис кодів сигналів управління запишемо як:

$k_1 = 0;\ k_2 = 0$ – вихідні функції неінвертовані;

$k_1 = 0;\ k_2 = 1$ – інверсія першої вихідної функції;

$k_1 = 1;\ k_2 = 0$ – інверсія другої вихідної функції;

$k_1 = 1;\ k_2 = 1$ – інверсія двох вихідних функцій;

$k_3 = 0$ – функції прямі;

$k_3 = 1$ – функції переставлені;

$k_4 = 0$ – обидві функції прості;

$k_4 = 1$ – перша функція складна.

Булеві функції інформаційних виходів узагальненої моделі функції $\vec{F}_{1,2,3,4,5,6,7,8,9,11,13,14,18,20,23,24}$ після мінімізації матимуть вигляд:

$$y_1 = \bar{x}_1x_2\bar{k}_2k_4 \vee x_2\bar{k}_2k_3\bar{k}_4 \vee x_1\bar{k}_2\bar{k}_3\bar{k}_4 \vee x_1\bar{x}_2\bar{k}_2k_4 \vee \vee\bar{x}_1\bar{x}_2k_2 \vee \bar{x}_2k_2k_3\bar{k}_4 \vee \bar{x}_1k_2\bar{k}_3\bar{k}_4 \vee x_1x_2k_2k_4;$$

$$y_2 = \bar{x}_1\bar{x}_2k_1 \vee \bar{x}_1k_1k_3 \vee x_2\bar{k}_1\bar{k}_3 \vee x_1x_2\bar{k}_1 \vee x_1\bar{x}_2k_1\bar{k}_3 \vee \vee x_1\bar{x}_2\bar{k}_1k_3.$$

Проведемо синтез узагальненої моделі функції $\vec{F}_{1,2,3,4,5,6,7,8,10,12,15,16,17,19,21,22}$, яка враховує інверсії та перестановки, а також можливість заміни другої функції на складну. Для реалізації даної моделі достатньо чотирьох сигналів управління. Опис кодів сигналів управління запишемо як:

$k_1 = 0;\ k_2 = 0$ – вихідні функції неінвертовані;

$k_1 = 0;\ k_2 = 1$ – інверсія першої вихідної функції;

$k_1 = 1;\ k_2 = 0$ – інверсія другої вихідної функції;

$k_1 = 1;\ k_2 = 1$ – інверсія двох вихідних функцій;

$k_3 = 0$ – функції прямі;

$k_3 = 1$ – функції переставлені;

$k_4 = 0$ – обидві функції прості;

$k_4 = 1$ – друга функція складна.

Інформаційні виходи даної узагальненої моделі функції описуватимуться наступними мінімізованими логічними виразами:

$$y_1 = x_1\bar{k}_2\bar{k}_3 \vee x_2\bar{k}_2k_3 \vee \bar{x}_2k_2k_3 \vee \bar{x}_1k_2\bar{k}_3;$$

$$y_2 = \bar{x}_1\bar{x}_2k_1 \vee \bar{x}_1k_1k_3\bar{k}_4 \vee x_2\bar{k}_1\bar{k}_3\bar{k}_4 \vee \vee\bar{x}_1x_2\bar{k}_1k_4 \vee x_1x_2\bar{k}_1k_3\bar{k}_4 \vee x_1x_2k_1k_4 \vee \vee x_1\bar{x}_2k_1\bar{k}_3\bar{k}_4 \vee x_1\bar{x}_2\bar{k}_1k_4 \vee x_1\bar{x}_2\bar{k}_1k_3.$$

Таким чином, для синтезу моделі уніфікованого пристрою криптографічного перетворення інформації, принцип роботи якого оснований на застосуванні синтезованих наборів спеціалізованих логічних функцій, потрібно провести узагальнення всіх визначених нами спеціалізованих блоків, котрі будуть реалізувати всі ідентифіковані операції, що забезпечать реалізацію повної множини спеціалізованих логічних функцій при мінімальній кількості вхідних сигналів, так як будемо використовувати проведену поблокову мінімізацію логічних функцій.

Виходячи з того, що уніфікований пристрій буде синтезований на основі поєднання трьох спеціалізованих блоків: блок інверсії, перестановки та блок заміни простої функції на складну, потрібно визначити порядок поєднання даних спеціалізованих блоків, тобто порядок виконання ідентифікованих операцій. Визначимо послідовність застосування операцій як заміна, перестановка, інверсія, тобто спочатку проводиться визначення застосування операції заміни функції, потім порядку розміщення функції, а саме, наявність перестановки або її відсутності і , нарешті, застосування інверсії до вихідних функцій. Так як визначені нами функції інформаційних виходів кожного із блоків достатньо складні, то для спрощення запису формул введемо додаткові позначення, які допоможуть структуризувати загальну модель уніфікованого пристрою.

Нехай x^* – функція виходу спеціалізованого блоку, який перетворює просту функцію в складену, Y_1^*, Y_2^* – функції виходу блоку заміни простої функцію на складну; Y_1^{**}, Y_2^{**} – функції виходу блоку перестановки та Y_1^{***}, Y_2^{***} – функції виходу блоку інверсії, а Y_1, Y_2 – інформаційні виходи уніфікованого пристрою. Тоді модель уніфікованого пристрою криптографічного перетворення інформації з використанням введених позначень можна описати як:

$$Y_1 = Y_1^{***} = Y_1^{**}\bar{k}_4 \vee \bar{Y}_1^{**}k_4,$$

де $Y_1^{**} = Y_1^{*}\bar{k}_3 \vee Y_2^{*}k_3,$

де $Y_1^{*} = x_1\bar{k}_1 \vee x^{*}k_1, \quad Y_2^{*} = x_2\bar{k}_2 \vee x^{*}k_2,$

де в свою чергу $x^{*} = x_1\bar{x}_2 \vee \bar{x}_1x_2.$

$$Y_2 = Y_2^{***} = Y_2^{**}\bar{k}_5 \vee \bar{Y}_2^{**}k_5,$$

де $Y_2^{**} = Y_2^{*}\bar{k}_3 \vee Y_1^{*}k_3,$

де $Y_1^{*} = x_1\bar{k}_1 \vee x^{*}k_1, \quad Y_2^{*} = x_2\bar{k}_2 \vee x^{*}k_2,$

де в свою чергу $x^{*} = x_1\bar{x}_2 \vee \bar{x}_1x_2.$

Розроблена комбінаційна схема згідно описаних математичних моделей представлена на рис. 2.

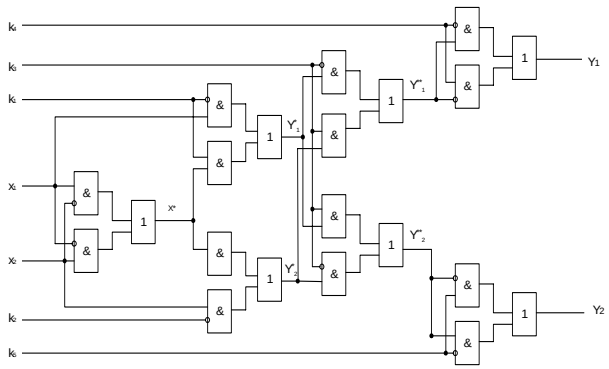

Рис. 2. Комбінаційна схема уніфікованого пристрою

Висновки

Результати аналізу та математичного моделювання дозволили визначити загальні закономірності побудови спеціалізованих блоків, які реалізують ідентифіковані операції перетворення інформації на основі використаних функцій кодування.

Сукупність синтезованих математичних моделей наборів функцій кодування представляє собою методику синтезу узагальненої математичної моделі уніфікованого пристрою криптографічного перетворення інформації та побудови комбінаційної схеми, що реалізує задану модель функцій.

Розроблена модель уніфікованого пристрою криптографічного перетворення інформації може знайти практичне застосування в системах захисту інформації в якості додаткового блоку, що дозволить підвищити швидкодію обробки інформації.

Список літератури

1. Безбогов А.А. Криптографическая защита информации: Учебное пособие / А.А. Безбогов, А.Я. Яковлев, В.Н. Шамкин. – Тамбов: ТГТУ, 2006. – 140 с.

2. Фергюссон Нильс. Практическая криптография: пер. с англ. / Нильс Фергюссон, Брюс Шнайер. – М.: Вильямс, 2005. – 424 с.

3. Бабенко В.Г. Алгоритми синтезу логічних функцій для систем захисту інформації / В.Г. Бабенко, Т.В. Дахно, В.М. Рудницький // Інтегровані інформаційні технології та системи (ІТС-2007). – К.: НАУ, 2007. – С. 46-48.

4. Бабенко В.Г. Результати моделювання логічних функцій для криптографії / В.Г. Бабенко, Т.В. Дахно, В.М. Рудницький // Сучасні інформаційні системи. Проблеми і тенденції розвитку: Зб. матеріалів конференції. – Х.: ХНУРЕ, 2007. – С. 421-422.

5. Рудницький В.М. Синтез математичних моделей пристроїв декодування інформації для криптографічних систем / В.М. Рудницький, В.Г. Бабенко // Системи обробки інформації. – Х.: ХУПС, 2009. – Вип. 2(76). – С. 124-128.

6. Рудницький В.М. Визначення множини логічних функцій для синтезу цифрових пристроїв систем захисту інформації / В.М. Рудницький, Н.М. Пантелєєва, В.Г. Бабенко // Системи управління, навігації та зв'язку. – К.: ЦНДІ НіУ, 2008. – Вип. 4(8). – С. 155-157.

Надійшла до редколегії 29.04.2008

Рецензент: д-р техн. наук, проф. І.В. Чумаченко, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

МОДЕЛЬ УНИФИЦИРОВАННОГО УСТРОЙСТВА КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ

В.Н. Рудницкий, В.Г. Бабенко

Работа посвящена разработке модели унифицированного устройства криптографического преобразования информации, принцип работы которого основан на использовании синтезированных наборов специализированных логических функций и которое способно обеспечивать двустороннее криптографическое превращение информации, то есть как кодировка, так и декодирование обрабатываемой информации, в зависимости от сигнала управления.

Ключевые слова: *комбинационная схема, специализированные логические функции, криптографическое преобразование.*

MODEL OF UNIFICATION DEVICE OF CRYPTOGRAPHIC TRANSFORMATION OF INFORMATION

V.M. Rudnitskiy, V.G. Babenko

Work is devoted development of model of unification device of cryptographic transformation of information, principle of work of which is based on the use of synthesized sets of the specialized boolean functions. The device is able to provide bilateral cryptographic transformation of information, that both code and decoding of the processed information, depending on the signal of management.

Keywords: *combinational circuit, specialized boolean functions, cryptographic transformation.*