УДК 519.714

В. М. Рудницький, *д.т.н., професор,*
С. В. Бурмістров, *аспірант,*
О. С. Шемшур, *викладач*
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
sergijburmistrov@yandex.ua

ОСОБЛИВОСТІ БУДОВИ БЛОКУ ОТРИМАННЯ ЗВОРОТНОГО КЛЮЧА В ШИФРУВАЛЬНИХ ПРИСТРОЯХ

Описано призначення, принцип роботи та особливості будови блоку отримання зворотного ключа в шифрувальних пристроях, призначених для посимвольного кодування текстової інформації. Принципову схему блоку розраховано шляхом приведення до мінімізації систем частково визначених булевих функцій (БФ) в ортогональній формі представлення (ОРФП).

Ключові слова: *шифрувальні пристрої, функції кодування, функції декодування, фіксований ключ кодування, фіксований ключ декодування.*

Одними із найбільш розповсюджених шифрувальних пристроїв є апарати, призначені для посимвольного кодування текстової інформації. Активна реалізація цих пристроїв почалася ще до появи електронних пристроїв в 20-х роках минулого століття [1] і привела безпосередньо до створення перших комп'ютерів [2] на початку Другої світової війни.

Принцип роботи цих пристроїв полягає в тому, що під час кодування інформації один символ заміняється на інший із використовуваного алфавіту.

Досить тривалий термін експлуатації цих шифрувальних пристроїв [1] в комерційних мережах вказує на достатньо високий рівень захисту даного методу шифрування в модифікованому вигляді (табл. 1).

Таблиця 1

Залежність зростання кількості варіантів посимвольного кодування при зростанні розрядності сигналу, що передається

№ п/п	Розрядність сигналу, що передається	Кількість варіантів посимвольного кодування
1	2	24
2	3	40320
3	4	$2{,}09228*10^{13}$
4	5	$2{,}63131*10^{35}$
5	6	$1{,}26887*10^{89}$

Метою роботи є створення уніфікованої схеми прийомної і передаючої частини шифрувального пристрою для посимвольного кодування текстової інформації в модифікованому вигляді.

Суть методу шифрування в модифікованому вигляді можна показати на простому прикладі. Візьмемо текстову інформацію, що складається з алфавіту, який містить 8 знаків, наприклад:

$$\{a_0^{\arg}=0, a_1^{\arg}=1, a_2^{\arg}=2,..., a_7^{\arg}=7\}.$$

Нехай шифрувальний пристрій передає символи у вигляді бінарних машинних кодів. Для задання указаного алфавіту в машинних кодах достатньо 3 розрядів (n=3):

$$n=\log_2 8=3,$$

де n – кількість аргументів у машинному коді.

Нехай на деякому етапі шифрування відбулось кодування повного алфавіту початкової інформації (табл. 2), де $\{a_0^{\arg}, a_1^{\arg},..., a_7^{\arg}\}$ – початкові незакодовані символи, а $\{a_0^{in}, a_1^{in},..., a_7^{in}\}$ – відповідні їм закодовані символи, що належать тому ж алфавіту.

Стовпчики в таблиці f_1^{in}, f_2^{in}, f_3^{in} називаються функціями кодування і в сумі складають фіксований ключ кодування.

Таблиця 2

Приклад посимвольного кодування інформації

№ початкового символу	Бінарний код початкового символу			Бінарний код символу, що передається			№ символу, що передається
$a_0^{\arg}$	0	0	0	0	1	1	$a_0^{in} = a_3^{\arg}$
$a_1^{\arg}$	0	0	1	1	1	0	$a_1^{in} = a_6^{\arg}$
$a_2^{\arg}$	0	1	0	0	0	1	$a_2^{in} = a_1^{\arg}$
$a_3^{\arg}$	0	1	1	1	1	1	$a_3^{in} = a_7^{\arg}$
$a_4^{\arg}$	1	0	0	0	1	0	$a_4^{in} = a_2^{\arg}$
$a_5^{\arg}$	1	0	1	0	0	0	$a_5^{in} = a_0^{\arg}$
$a_6^{\arg}$	1	1	0	1	0	0	$a_6^{in} = a_4^{\arg}$
$a_7^{\arg}$	1	1	1	1	0	1	$a_7^{in} = a_5^{\arg}$
	$\uparrow$ $f_3^{\arg}$	$\uparrow$ $f_2^{\arg}$	$\uparrow$ $f_1^{\arg}$	$\uparrow$ f_1^{in}	$\uparrow$ f_2^{in}	$\uparrow$ f_3^{in}	
	Початкові функції аргументів			Функції кодування			

Фіксований ключ кодування описується системою логічних рівнянь:

$$\begin{cases} f_1^{in} = F_1(f_1^{\arg}, f_2^{\arg}, f_3^{\arg}) \\ f_2^{in} = F_2(f_1^{\arg}, f_2^{\arg}, f_3^{\arg}) \\ f_3^{in} = F_3(f_1^{\arg}, f_2^{\arg}, f_3^{\arg}) \end{cases} \quad (1)$$

Для пристрою оптимальною кількістю функцій кодування є кількість, що дорівнює розрядності машинного коду ($n = 3$), що передається, а розрядність функції кодування становить $2^n = 8$.

Ідея посимвольного методу шифрування в модифікованому вигляді полягає в тому, що на кожний наступний символ ($n = 3$), що передається, використовується новий ключ – поточний фіксований ключ кодування.

Відповідно, пристрій, що виконує кодування, повинен містити такі апаратні блоки (рис. 1):

1. Блок формування поточного фіксованого ключа. Даний блок призначений для задання номерів функцій кодування f_i^{in} на кожний із модулів шифрування для поточного символу($n = 3$), що передається.
2. Модулі шифрування f_i^{in}. Ці модулі виконують безпосередньо кодування символів ($n = 3$), що передаються, на основі поточного фіксованого ключа кодування. Вони повинні працювати синхронно.

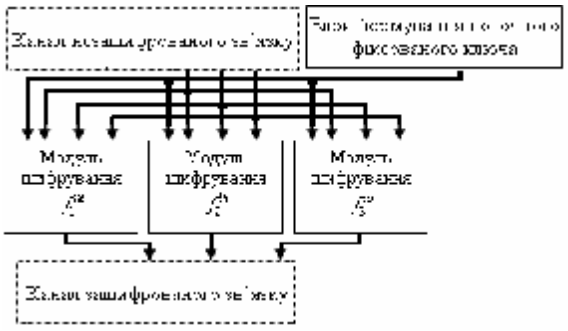

Рис. 1. Загальна схема пристрою кодування

Для виконання зворотної дії – процесу декодування потрібно закодованим символам повернути первинне істинне значення (табл. 3).

Стовпчики в таблиці f_1^{out}, f_2^{out}, f_3^{out} називаються функціями декодування і в сумі складають фіксований ключ кодування.

Таблиця 3

Приклад посимвольного декодування інформації

№ закодованого символу	Бінарний код закодованого символу			Бінарний код декодованого символу			№ декодованого символу
$a_0^{in\_arg}$	0	0	0	1	0	1	$a_0^{out} = a_5^{in\_arg} = a_5^{arg}$
$a_1^{in\_arg}$	0	0	1	0	1	0	$a_1^{out} = a_2^{in\_arg} = a_2^{arg}$
$a_2^{in\_arg}$	0	1	0	1	0	0	$a_2^{out} = a_4^{in\_arg} = a_4^{arg}$
$a_3^{in\_arg}$	0	1	1	0	0	0	$a_3^{out} = a_0^{in\_arg} = a_0^{arg}$
$a_4^{in\_arg}$	1	0	0	1	1	0	$a_4^{out} = a_6^{in\_arg} = a_6^{arg}$
$a_5^{in\_arg}$	1	0	1	1	1	1	$a_5^{out} = a_7^{in\_arg} = a_7^{arg}$
$a_6^{in\_arg}$	1	1	0	0	0	1	$a_6^{out} = a_1^{in\_arg} = a_1^{arg}$
$a_7^{in\_arg}$	1	1	1	0	1	1	$a_7^{out} = a_3^{in\_arg} = a_3^{arg}$
	$\uparrow f_3^{in\_arg}$	$\uparrow f_2^{in\_arg}$	$\uparrow f_1^{in\_arg}$	$\uparrow f_1^{out}$	$\uparrow f_2^{out}$	$\uparrow f_3^{out}$	
	Початкові функції для декодування інформації			Функції декодування			

Фіксований ключ декодування описується системою:

$$\begin{cases} f_1^{out} = F_1(f_1^{in\_arg}, f_2^{in\_arg}, f_3^{in\_arg}) \\ f_2^{out} = F_2(f_1^{in\_arg}, f_2^{in\_arg}, f_3^{in\_arg}) \\ f_3^{out} = F_3(f_1^{in\_arg}, f_2^{in\_arg}, f_3^{in\_arg}) \end{cases} \quad (2)$$

Значення поточного фіксованого ключа декодування не дорівнює значенню поточного фіксованого ключа кодування, але напряму від нього залежить.

Відповідно, пристрій, що виконує декодування, на відміну від пристрою кодування, в своїй будові дещо відрізняється (рис. 2):

1. Блок формування поточного фіксованого ключа. По будові – аналогічний як і в пристрої шифрування.
2. Модулі дешифрування f_i^{out}. По будові дані модулі аналогічні модулям шифрування f_i^{in}.
3. Блок обчислення фіксованого ключа декодування. Даний блок на апаратному рівні обчислює на основі поточного фіксованого ключа кодування – поточний фіксований ключ декодування.

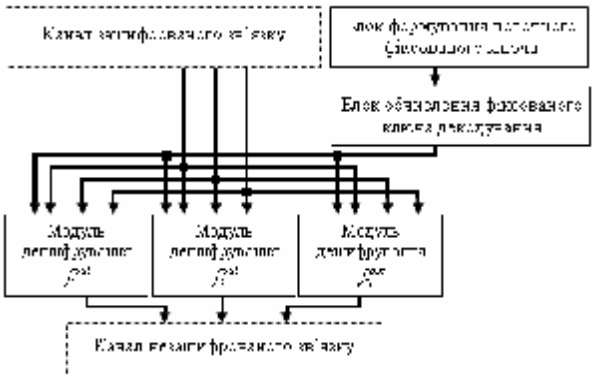

Рис. 2. Загальна схема пристрою декодування

Фактично, основне призначення фіксованого ключа декодування – знайти залежність функцій f_1^{out}, f_2^{out}, f_3^{out} від f_1^{in}, f_2^{in}, f_3^{in} та обчислювати результат вказаної залежності на апаратному рівні. Умовно назвемо дану задачу – задача отримання зворотного фіксованого ключа шифрування.

Залежність функцій одна від одної $F(f_1^{out}, f_2^{out}, f_{31}^{out}) = F(f_1^{in}, f_2^{in}, f_3^{in})$ не є функціональною залежністю. Тому **актуальною проблемою** є розробка методу обчислення розв'язку задачі отримання зворотного фіксованого ключа шифрування.

Пропонується звести розв'язок задачі до процесу мінімізації системи частково визначених булевих функцій (ЧО СБФ) [5,6]. Функції f_i^{in} є восьмирозрядними машинними кодами. Тому значення всіх 3 функцій $\{f_1^{in}, f_2^{in}, f_3^{in}\}$ можна прийняти як 24-розрядний рядок аргументів в таблиці істинності (ТІ) ЧО СБФ. Відповідно значення функцій $\{f_1^{out}, f_2^{out}, f_3^{out}\}$ записують у відповідні рядки результату ТІ ЧО СБФ. Якщо для деякого рядка аргументу відсутні значення рядків результату, їх позначають як невизначені (значком *) (табл. 4).

Таблиця 4

Таблиця істинності системи частково визначених булевих функцій для розв'язку задачі отримання зворотного фіксованого ключа шифрування

№ рядка таблиці істинності	Значення рядків аргументів			Значення частково визначених булевих функцій		
	f_1^{in}	f_2^{in}	f_3^{in}	f_1^{out}	f_2^{out}	f_3^{out}
0	00000000	00000000	00000000	********	********	********
1	00000000	00000000	00000001	********	********	********
2	00000000	00000000	00000010	********	********	********
3	00000000	00000000	00000011	********	********	********
…	…	…	…	…	…	…
1 006 644	00001111	01011100	00110100	********	********	********
1 006 645	00001111	01011100	00110101	00001111	11000101	01010011
1 006 646	00001111	01011100	00110110	00001111	11000101	01100011
1 006 647	00001111	01011100	00110111	********	********	********
…	…	…	…	…	…	…
16 777 213	11111111	11111111	11111101	********	********	********
16 777 214	11111111	11111111	11111110	********	********	********
16 777 215	11111111	11111111	11111111	********	********	********

Як наслідок, отримують таблицю істинності ЧО СБФ, яка має 24 стовпчики аргументів, для 24 частково визначених БФ. ТІ ЧО СБФ має 16 777 216 рядків. Зважаючи на розміри таблиці істинності БФ, ця задача розв'язана лише машинним способом.

Ця задача розв'язана на основі методу мінімізації в ортогональній формі представлення, запропонованого в [3; 4; 5; 6]. Кожна із булевих функцій $f(x_1,x_2,x_3,\ldots,x_{24})$ ЧО СБФ для даного випадку має досить низький ступінь визначеності:

$$k = \frac{n!}{2^n} \cdot 100\% = \frac{8!}{2^{24}} \cdot 100\% = 0{,}24\%,$$

де n – кількість аргументів в кожній із булевих функцій $\{f_i^{in}, f_i^{out}\}$ ($n=8$), k – ступінь визначеності БФ.

Тому розв'язок системи має досить високий рівень мінімізації.

Для отримання максимальної швидкодії блоку було розглянуто лише результати, що мають максимально можливу швидкодію. Для цього випадку отримано 124 рівноцінних розв'язки, що мають рівень мінімізації. Результати мінімізації наведено в табл. 5 в порівнянні з використанням в схемі класичної програмованої логічної матриці.

Додатково можна вказати, що за рахунок спрощення дублюючих ланцюгів схеми отримано економію використання логічних елементів приблизно 4,47%.

Таблиця 5

Результати мінімізації в ортогональній формі представлення

№ п/п	Отримані результати	Кількість літерал у схемі S_L	Кількість доданків у схемі S_{AD}	Кількість умовних транзисторів
1	Схема на основі використання програмованої логічної матриці	967 680	40 320	1 008 024
2	Схема на основі використання ортогональної форми представлення	169 100	9 873	178 997
3	Ступінь мінімізації	17,47%	24,48%	17,75%

Висновки:

1. З метою уніфікації приймально-передавальних кодуючих апаратів в схему шифрувальних пристроїв для посимвольного кодування текстової інформації в модифікованому вигляді запропоновано в схемі прийомної частини блок обчислення фіксованого ключа декодування. Даний блок обчислює ключ на апаратному рівні на основі поточного фіксованого ключа кодування.
2. Схема блоку обчислення фіксованого ключа декодування розрахована шляхом зведення задачі до мінімізації системи частково визначених булевих функцій. З метою отримання максимальної швидкодії блоку кінцева схема має вигляд дворівневої комбінаційної схеми логічних елементів.
3. В порівнянні з використанням аналогічної схеми на основі стандартної програмованої логічної матриці отримано ущільнення схеми в 5,63 разу.

Список літератури

1. Stripp Alan (1993) The enigma machine: its mechanism and use. In: F. H. Hinsley and Alan Stripp (Eds.). Codebreakers: The Inside Story of Bletchley Park, pp. 83–88.
2. Copeland B. J. Colossus: the first electronic computer: the secrets of Bletchley Park's code-breaking computers / B. Jack Copeland. – Oxford : OUP, 2006. – 462 p.
3. Кочкарев Ю. А Минимизация булевых функций по частям / Ю. А. Кочкарев, С. В. Бурмистров, С. Ф. Аксенов // Радиоэлектронные и компьютерные системы. – 2012. – № 4. – С. 110–116.
4. Кочкарев Ю. А. Минимизация частично определенных булевых функций в ортогональной форме представления / Ю. А. Кочкарев, С. В. Бурмистров, С. Ф. Аксенов // Прикладная радиоэлектроника. – 2013. – Т. 12, № 3. – С. 413–420.
5. Кочкарев Ю. А. Минимизация систем полностью определенных булевых функций в ортогональной форме представления / Ю. А. Кочкарев, В. Н. Рудницкий, С. В. Бурмистров // Эвристические алгоритмы и распределенные вычисления в прикладных задачах : кол. монография под ред. проф. Мельникова. – Вып. 2. – Ульяновск, 2013. – С. 87–100.
6. Рудницкий В. Н. Распараллеливание процесса минимизации систем частично или полностью определенных булевых функций с большим числом переменных / В. Н. Рудницкий, С. В. Пивнева, С. В. Бурмистров // Вектор науки Тольяттинского государственного университета. – 2014. – № 1. – С. 27–30.

References

1. Stripp, Alan (1993) The enigma machine: its mechanism and use. In: F. H. Hinsley and Alan Stripp (Eds.). Codebreakers: The Inside Story of Bletchley Park, pp. 83–88.
2. Copeland, B. J. (2006) Colossus: the first electronic computer: the secrets of Bletchley Park's code-breaking computers. Oxford: OUP, 462 p.

3. Kochkarev, Yu. A., Burmistrov, S. V. and Aksyonov, S. F. (2012) Minimization of Boolean functions in parts. *Radioelektronnye i komp'juternye sistemy*, (4), pp.110–116 [in Russian].
4. Kochkarev, Yu. A., Burmistrov, S. V. and Aksyonov, S. F. (2013) Minimization of partially defined Boolean functions in the form of orthogonal representations. *Prikladnaya radioelektronika*, 12 (3), pp. 413–420 [in Russian].
5. Kochkarev, Yu. A., Rudnickij, V. M. and Burmistrov, S. V. (2013) Minimization of systems of completely defined Boolean functions in the form of orthogonal representations. In: prof. Melnikov (Ed.). Heuristic algorithms and distributed computing in applications, issue 2. Ulyanovsk, pp. 87–100 [in Russian].
6. Rudnyckij, V. M., Pivneva, S. V. and Burmistrov, S. V. (2014) Parallelization of the process of minimizing of the systems of partially or fully defined Boolean functions with more variables. *Vector nauki Tollyatinskogo gosudarstvennogo universiteta*, (1), pp. 27–30 [in Russian].

V. M. Rudnyts'kyy, *Dr.Tech.Sc., professor,*
S. V. Burmistrov, *post-graduate student,*
O. S. Shemshur, *lecturer*
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine
sergijburmistrov@yandex.ua

FEATURES OF ARRANGEMENT OF THE UNIT FOR FEEDBACK KEY RECEIPT IN ENCRYPTION DEVICES

In the paper a modified scheme of discrete encryption device for encoding the spelling of text information on the basis of a fixed key coding-decoding is offered.

The essence of a modified method for coding textual information in the form of a digital signal using a fixed key is shown. The optimal encoding of functions that make up a fixed key, and fairly high potential of this method of encryption for its use in commercial networks are analyzed.

In developing of the device one of the basic principles of cryptographic devices construction – opening of device structure does not allow a third person to read coded alerts – is considered.

The structure and purpose of the main constituents of the device and detailed method for calculation of circuit unit for feedback key receipt are specified.

This technical problem is reduced to the problem of the system of Boolean functions minimization in orthogonal form of representation of a large number of arguments.

In order to standardize transceiver transmitting-coding units in the scheme of encryption devices for spelling of coding textual information in a modified form the calculation unit with fixed decoding key is offered. This unit calculates the key in hardware.

The scheme of calculation unit with fixed decoding key is calculated by reducing the problem to minimize the system of partially marked Boolean functions in order to maximize the performance of the unit diagram looks like the ultimate 2-level combinational circuit logic elements.

Compared to using a similar scheme based on a standard programmable logic matrix a compaction scheme in 5.63 times is obtained.

Keywords: *encryption devices, encoding functions, decoding functions, fixed encryption key, fixed decoding key.*

Рецензенти: С. М. Первунінський, д.т.н., професор,
С. В. Голуб, д.т.н., професор