УДК 681.385.63 (088.8)

Бойченко О. В., *к.т.н.*; **Дробик О. В.,** *к.т.н.*; **Торошанко Я. І.,** *к.т.н.*

БАГАТОСТУПЕНЕВИЙ ШИФРАТОР З РЕГУЛЯРНИМИ ЗВ'ЯЗКАМИ

Бойченко О. В., Дробик О. В., Торошанко Я. І. Багатоступеневий шифратор з регулярними зв'язками. Розглянуті способи побудови цифрового пристрою шифрації. Запропонована структура шифратора з регулярними зв'язками, показана можливість скорочення апаратних витрат при його схемній реалізації.

Ключові слова: ШИФРАТОР, АПАРАТНІ ВИТРАТИ, РЕГУЛЯРНІСТЬ СТРУКТУРИ

Бойченко О. В., Дробик А. В., Торошанко Я. И. Многоступенчатый шифратор с регулярными связями. Рассмотрены способы построения цифрового устройства шифрации. Предложена структура шифратора с регулярными связями, показана возможность сокращения аппаратных расходов при его схемной реализации.

Ключевые слова: ШИФРАТОР, АППАРАТНЫЕ РАСХОДЫ, РЕГУЛЯРНОСТЬ СТРУКТУРЫ

Boychenko O. V., Drobyk O. V., Toroshanko Ya. I. Multistage coder with regular connections. The methods for the construction of digital coder are considered. The structure of coder with regular connections is proposed; the possibility is shown for the reduction of hardware expenses when circuit implementation.

Key words: SCRAMBLER, HARDWARE EXPENSES, STRUCTURAL REGULARITY

Постановка задачі. Шифратор, як операційний блок обчислювальної техніки, виконує функцію перетворення унарного 2^n-розрядного двійкового коду в n-розрядний позиційний код в тій чи іншій системі числення. В унарному коді кожне число представляється у вигляді коду "1" тільки в одному розряді числа. Прикладом шифратора є комбінаційна схема, яка перетворює сигнали від клавіш клавіатури комп'ютера у 7- чи 8-бітовий код відповідного символа. Входами такого шифратора є лінії від кожної клавіші.

Область використання шифраторів значно менша ніж у іншого операційного блоку обчислювальної техніки – дешифратора, який виконує зворотну функцію – перетворення n-розрядного позиційного коду в унарний код. Широке використання дешифраторів в системах адресації пам'яті та інших цифрових пристроях обумовило велику кількість робіт щодо їх оптимальної побудови за різними критеріями: апаратні витрати, надійність, швидкодія, контроль, тощо [1...4].

Щодо шифраторів, то такі роботи проводились в дуже незначній мірі і в науково-технічній літературі практично не висвітлювались. З постійним розвитком технологій мікроелектроніки, ростом ступеню інтеграції і мікромініатюризації схем і елементів ЕОМ зникли стримуючі фактори апаратної реалізації шифраторів (значна кількість входів-виходів, габаритні показники, тощо). Практично відсутні такі стримуючі фактори при використанні пристроїв шифрації у складі великих інтегральних схем (ВІС), в яких вхідні сигнали шифратора формуються в самій ВІС іншими її вузлами.

Тому питання розробки принципів побудови логічних схем шифраторів, що дозволяють скоротити апаратні витрати, підвищити надійність їх функціонування є актуальними і представляють інтерес для фахівців та розробників цифрових пристроїв.

Крім того, під час проектування операційних пристроїв обчислювальної техніки окрім основних факторів (апаратні витрати, швидкодія, надійність) важливу роль відіграють такі вимоги, як регулярність структури, можливість розширення по розрядності, по числу аргументів, тощо.

Умовне графічне позначення шифратора показане на рис.1.

Він має 2^n входів ($x_0, x_1, ..., x_{2^n-1}$) та n виходів ($y_0, y_1, ..., y_{n-1}$), де 2^n – розрядність вхідного числа, n – розрядність вихідного числа.

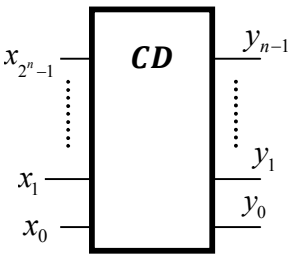

Рис. 1. Шифратор

В кожен момент часу активним може бути тільки один із входів. Кожному *L*-му входові відповідає *n*-розрядне число *L*, яке формується на виходах шифратора.

Відомі шифратори будуються на основі логічних елементів "АБО" [3, 4]. Кожен j-й розряд y_j вихідного числа формується як диз'юнкція входів шифратора, двійкові номери яких в j-му розряді містять "1":

$$\begin{cases} y_0 = x_1 \vee x_3 \vee x_5 \vee x_7 \vee ... \vee x_{2^n-1}; \\ y_1 = x_2 \vee x_3 \vee x_6 \vee x_7 \vee x_{10} \vee x_{11} \vee ... \vee x_{2^n-2} \vee x_{2^n-1}; \\ . \\ y_{n-1} = x_{2^{n-1}} \vee x_{2^{n-1}+1} \vee ... \vee x_{2^n-2} \vee x_{2^n-1}. \end{cases} \quad (1)$$

Побудова такого шифратора пов'язана зі значними апаратними витратами, які суттєво зростають при збільшенні розрядності вихідного числа шифратора (надалі – розрядності шифратора). Як випливає із (1), при збільшенні розрядності n шифратора на "1", кількість входів у елементів "АБО" для кожного вихідного розряду зростає вдвоє.

Ступенева структура шифратора, яка пропонується, дозволяє скоротити апаратні витрати, а також дає можливість збільшувати розрядність вхідних і вихідних слів без перебудови уже спроектованої і діючої схеми шифратора.

Такий шифратор складається із $n-1$ ступенів шифрації [5]. На кожному i-му ступені (i =1,…,$n-1$) формується значення відповідного i-го розряду вихідного числа, а також здійснюється формування входів для молодшого $i-1$-го ступеню шифрації. При цьому кількість входів $i-1$-го ступеню зменшується вдвічі у порівнянні із i-м ступенем. Зауважимо, що на 1-му ступені формується значення двох молодших розрядів шифратора, а саме 1-го та 0-го (див. далі).

На рис. 2 показана схема $n-1$-го та $n-2$-го (старших) ступенів шифратора. Ступінь $n-1$ складається із 2^{n-1}-входового елементу "АБО" (A^{n-1}) та 2^{n-1} 2-входових елементів "АБО" ($B_0^{n-1} ... B_{2^{n-1}-1}^{n-1}$). В позначеннях елементів А і В верхній індекс вказує на номер ступеня шифратора, нижній індекс – порядковий номер елемента В.

Входами старшого $n-1$-го ступеню є входи шифратора. Входи, номери яких містять у старшому розряді "1" ($x_{2^{n-1}} ... x_{2^n-1}$), підключаються до елемента "АБО" (A^{n-1}), на виході якого формується значення старшого розряду вихідного числа y_{n-1}, як диз'юнкція старшої половини входів (n-1)-го ступеню згідно виразу (2):

$$y_{n-1} = \bigvee_{i=2^{n-1}}^{2^n-1} x_i . \quad (2)$$

На виходах елементів $B_0^{n-1} ... B_{2^n-1}^{n-1}$ формуються відповідно нижнім індексам входи наступного – ($n-2$)-го ступеня шифратора. Кожен із елементів $B_0^{n-1} ... B_{2^n-1}^{n-1}$ об'єднує по 2 входи, двійкові номери яких відрізняються тільки старшими – ($n-1$)-ми розрядами.

Іншими словами, молодші $n-1$ розрядів $(n-1)$-го ступеня представляють собою номери входів наступного – $(n-2)$-го ступеня (входи $x_0^{n-2} \ldots x_{2^{n-2}-1}^{n-2}$).

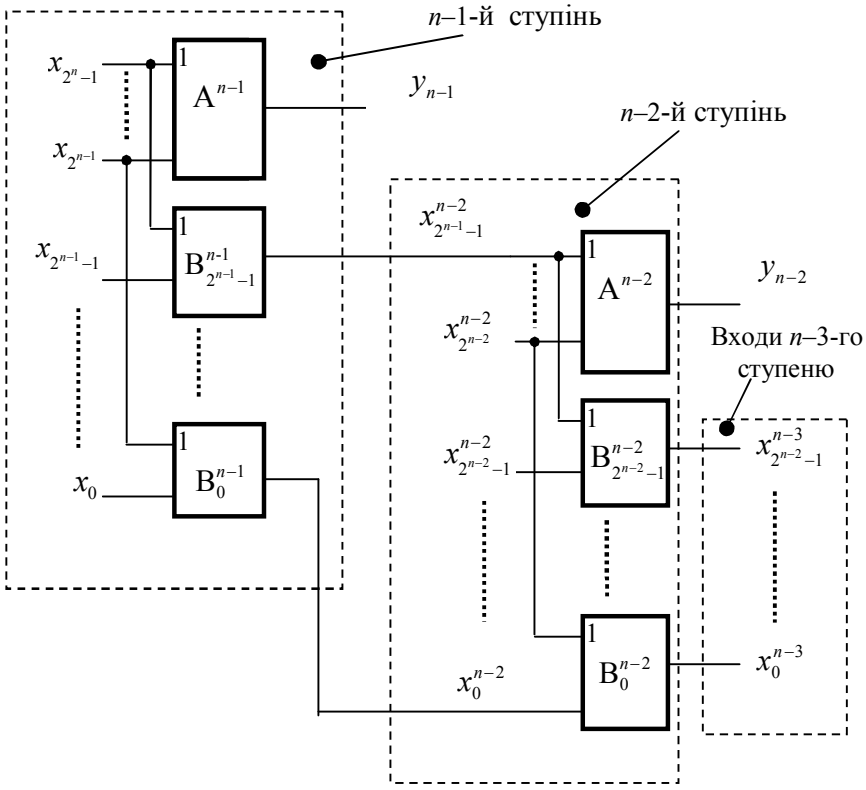

Рис. 2. Старші ступені шифратора

Таким же чином будується $(n-2)$-ий ступінь з тією різницею, що кількість входів цього ступеня вдвічі менша, ніж у $(n-1)$-му ступені. На виході елемента "АБО" A^{n-2} формується значення $(n-2)$-го розряду шифратора y_{n-2}, а на виходах елементів $B_0^{n-2} \ldots B_{2^{n-2}-1}^{n-2}$ – значення входів $(n-3)$-го ступеня $x_0^{n-3} \ldots x_{2^{n-3}-1}^{n-3}$, відповідно.

На рис. 3 показана схема 1-го ступеня шифратора. Виходи x_0^0 та x_1^0 позначені по аналогії з попередніми ступенями. Вихід x_1^0 елемента B_1^1 є виходом 0-го розряду шифратора.

Як бачимо, логічний елемент B_0^1 у схемі 1-го ступеня не використовується. Аналізуючи схеми наступних ступенів приходимо до висновку, що в кожному i-у ступені 2-входові елементи "АБО", на яких формуються входи x_0^{i-1} (входи з номером "0") для молодшого $i-1$-го ступеню, не використовуються і можуть бути видалені. Враховуючи сказане, уточнена схема i-го та i–1-го ступенів матиме вигляд, показаний на рис. 4.

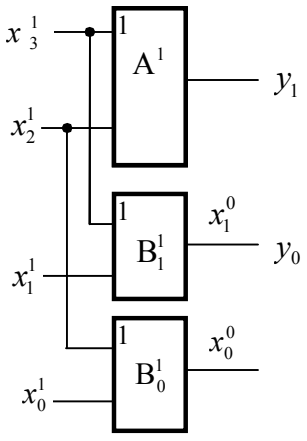

Рис. 3. 1-й ступінь шифратора

Приклад побудови ступеневого шифратора. Розглянемо побудову 4-розрядного шифратора. Входами такого шифратора будуть $x_0, x_1, x_2, \ldots, x_{14}, x_{15}$. Кількість ступенів шифрації – 3.

До 8-входового логічного елемента *3-го ступеня* A^3 будуть підключені старші 8 входів шифратора, а саме $x_8, x_9, \ldots, x_{15}$. На його виході цього елемента формується значення 3-го розряду шифратора y_3. Кількість 2-входових елементів "АБО", на яких формуються входи 2-го ступеня – 7 ($B_1^3, B_2^3, \ldots, B_7^3$). До елемента B_1^3 підключаються входи x_1 та x_9 і на на ньому формується вхід x_1^2; до елемента B_2^3 – входи x_2 та x_{10}, на ньому формується вхід x_2^2; і т.д., – до елемента B_7^3 підключаються входи x_7 та x_{15}, на ньому формується вхід x_7^2.

2-й ступінь містить 4-входовий елемент "АБО" A^2, до якого підключені входи $x_4^2, x_5^2, x_6^2, x_7^2$ і на його виході формується значення 2-го розряду шифратора y_2. Кількість 2-входових елементів "АБО", на яких формуються входи 1-го ступеня – 3 (B_1^2, B_2^2, B_3^2). До елемента B_1^2 підключаються входи x_1^2 та x_5^2 і на на ньому формується вхід x_1^1; до елемента B_2^2 – входи x_2 та x_6^2, на ньому формується вхід x_2^1; до елемента B_3^2 – входи x_3^2 та x_7^2, на ньому формується вхід x_3^1.

Побудова *1-го ступеня* показана на рис. 3 (за виключенням елемента B_0^1).

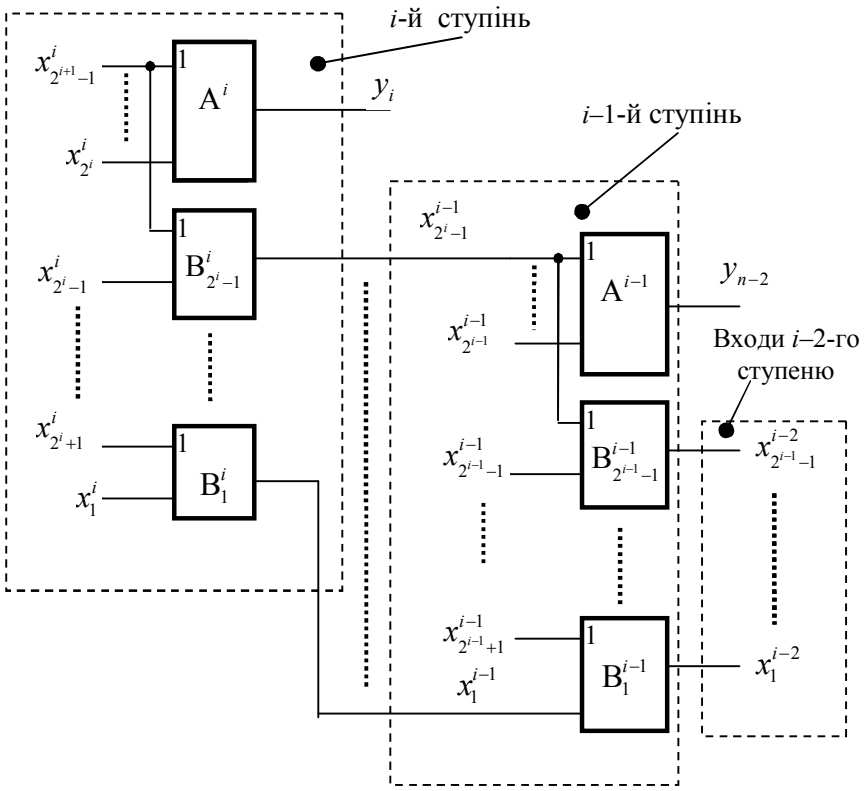

Рис. 4. Уточнена схема шифратора

Порівняльна характеристика складності пристроїв шифрації. Для оцінки апаратних витрат на побудову розглянутих схем використаємо таку міру, як "*ціна по Квайну*", яка представляє собою сумарну кількість входів усіх логічних елементів цифрової комбінаційної схеми, побудованої у відповідному базисі [3] .

Ціна по Квайну C_1 описаного в [5] багатоступеневого шифратора (див. рис. 2 і 3) визначається по закону геометричної прогресії [6], як сумарна ціна всіх його ступенів, згідно формулі

$$C_1 = \frac{a_1(q^m - 1)}{q - 1} = 4(2^{n-1} - 1), \quad (3)$$

де $a_1 = 4$ – перший член прогресії (ціна 1-го ступеня, див. рис. 3);
$m = n - 1$ – число членів прогресії (число ступенів шифрації);
$q=2$ – знаменник геометричної прогресії.

Для запропонованої схеми шифратора з вилученими в кожному ступені 2-входовими елементами B_0^i (рис. 4) апаратні витрати (ціна по Квайну) будуть визначатися таким виразом:

$$C_2 = 4(2^{n-1} - 1) - 2(n - 1). \quad (4)$$

Ціна по Квайну шифратора, побудованого згідно виразів (1) визначається як

$$C_3 = n \cdot 2^{n-1}. \quad (5)$$

Висновки: Аналізуючи вирази (3), (4) і (5) можна зробити висновок, що у порівнянні із прямим способом формування виходів згідно (1) апаратні витрати на побудову багатоступеневих шифраторів суттєво зменшуються при зростанні розрядності (числа входів) шифратора. Так, $C_1 \le C_3$ уже при $n = 3$, $C_2 \le C_3$ – при $n = 2$.

Розглядаючи структуру багатоступеневого шифратора, зауважимо наступне:

1) Ступені з номерами від 1 до i-1 представляють собою i-розрядний шифратор, входи якого формуються на більш старшому ступені.

2) Збільшення розрядності уже спроектованого шифратора здійснюється шляхом підключення до його входів схем наступних ступенів без будь-яких змін у схемі уже існуючого спроектованого шифратора.

Сказане забезпечує регулярність структури цифрового пристрою, а також суттєво спрощує реалізацію розширення шифратора по числу вхідних аргументів та розрядності вихідного слова.

Література

1. Калабеков Б. А. Цифровые устройства и микропроцессорные системы / Б. А. Калабеков. – М.: Горячая линия-Телеком, 2003. – 336 с.

2. Угрюмов Е. П. Цифрова схемотехніка / Е. П. Угрюмов. – [2-е изд.]. – С.-Пб.: БХВ-Петербург, 2007. – 782 с.

3. Самофалов К. Г. Цифровые ЭВМ: Теория и проектирование / К. Г. Самофалов, В. И. Корнейчук, В. П. Тарасенко ; под общ. ред. К. Г. Самофалова. – К.: Вища школа, 1989. – 424 с.

4. Майоров С. А. Принципы организации цифровых машин / С. А. Майоров, Г. И. Новиков. – Ленинград: Машиностроение, 1974. – 431 с.

5. Авторское свидетельство СССР на изобретение № 783786, МПК G 06 F 5/02. Шифратор. / Бойчев О. Н. (Болгария), Корнейчук В. И., Сушко В. В., Тарасенко В. П., Торошанко Я. И. (Украина); заявитель Киевский политехнический институт; заявл. 09.06.1978; опубл. 30.11.1980; бюл. № 44.

6. Выгодский М. Я. Справочник по элементарной математике / М. Я. Выгодский. – М.: Наука, 1964. – 420 с.