УДК 004.312.2

АППАРАТНЫЙ ГЕНЕРАТОР ПЕРЕСТАНОВОК

Н. И. Кушниренко, к. т. н. В. Я. Чечельницкий

Одесский национальный политехнический университет
Украина, г. Одесса
victor@net.opu.ua

Приведен алгоритм работы и принцип построения аппаратного генератора перестановок элементов на базе мультиплексоров. Такой генератор характеризуется повышенным быстродействием, так как построен без использования регистров сдвига, которые присутствуют в прототипах и замедляют их работу как минимум в два раза.

Ключевые слова: генератор перестановок, аппаратная сложность, быстродействие.

Генераторы перестановок широко используются в вычислительной, информационно-измерительной радиотехнике, в разнообразных системах кодирования и шифрования, а также аналоговой и цифровой телефонии для защиты информации от несанкционированного доступа.

Программной реализации генератора перестановок посвящено много публикаций, например [1—3], но для реализации различных аппаратных алгоритмов шифрования необходимы аппаратные генераторы перестановок, которые невозможно построить на базе программных алгоритмов. В литературе встречаются некоторые алгоритмы построения аппаратных генераторов перестановок, но все они используют регистры сдвига [4—7]. При этом для очередной генерации перестановки необходимо несколько тактовых сигналов, чтобы выполнить очередной сдвиг элементов, что значительно замедляет работу всей схемы.

В данной работе рассматривается алгоритм работы и схема построения аппаратного генератора перестановок, выполненного на коммутаторах (мультиплексорах) без применения регистров сдвига. Причем использовать его можно как для последовательной генерации перестановок, с помощью синхроимпульсов, так и для генерации перестановки, номер которой задается кодовым словом. При этом очередная перестановка генерируется за один такт работы схемы.

Рассмотрим методы генерирования всех $n!$ перестановок множества M, которое состоит из n элементов (1, 2, 3, …, n). Для n=2 существует всего две перестановки:

$$\begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix}. \qquad (1)$$

Реализовать данные перестановки можно с помощью обыкновенного коммутатора (переключателя) или мультиплексора. Для данного случая была спроектирована схема генератора перестановок.

Для создания генератора перестановок большего порядка (n=3) на базе генератора перестановок меньшего порядка (n=2) необходимо добавить новый разряд (число 3) к уже существующим разрядам. Добавлять этот разряд необходимо слева или справа от существующей перестановки или между всеми разрядами перестановки, например для (1) это будет:

$$\begin{matrix} (3) & 1 & 2 \\ (3) & 2 & 1 \end{matrix}, \qquad (2)$$

$$\begin{matrix} 1 & 2 & (3) \\ 2 & 1 & (3) \end{matrix}, \qquad (3)$$

$$\begin{matrix} 1 & (3) & 2 \\ 2 & (3) & 1 \end{matrix}. \qquad (4)$$

В данном случае будут сгенерированы следующие перестановки (3), (4), (5)

$$\begin{array}{ccc} 3 & 1 & 2 \\ 3 & 2 & 1 \\ 1 & 2 & 3 \\ 2 & 1 & 3 \\ 1 & 3 & 2 \\ 2 & 3 & 1 \end{array} \quad (5)$$

Данные перестановки не являются лексиграфическими и антилексиграфическими, тем не менее, они обеспечивают полный класс перестановок данного порядка. Для перестановки (5) была разработана схема генератора перестановок.

Аналогичным образом, используя генератор перестановок меньшего порядка, можно реализовать генератор перестановок для n=4 и генераторы перестановок большего порядка. Построенная в работе схема генерирует последовательно следующие перестановки:

4	3	1	2	3	1	2	4	3	4	1	2	3	1	4	2
4	3	2	1	3	2	1	4	3	4	2	1	3	2	4	1
4	1	2	3	1	2	3	4	1	4	2	3	1	2	4	3
4	2	1	3	2	1	3	4	2	4	1	3	2	1	4	3
4	1	3	2	1	3	2	4	1	4	3	2	1	3	4	2
4	2	3	1	2	3	1	4	2	4	3	1	2	3	4	1.

Для реализации генератора перестановок любого порядка необходимо k_{DC} счетчиков и k_{MC} мультиплексоров:

$$k_{DC} = n - 1;\ k_{MS} = \sum_{i=2}^{n} i\,. \quad (6)$$

В заключение следует отметить, что скорость работы предложенного генератора перестановок определяется только скоростью переключения счетчиков и мультиплексоров и как минимум в 2 раза превышает скорость работы аналогов [4—7].

Для реализации генератора фиксированной перестановки необходимо на управляющие входы мультиплексоров подать сигналы не от счетчиков, а соответствующие цифровые коды, которые и будут определять номер очередной перестановки. При этом необходимость в счетчиках отпадает, а сложность всего устройства определяется только количеством мультиплексоров.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Липский В. Комбинаторика для программистов. — Москва: Мир, 1988.

2. Носов, В. А. Комбинаторика и теория графов. — Москва: МГУ имени М. В. Ломоносова, 1999.

3. Кнут Д. Э. Искусство программирования, том. 3. Сортировка и поиск = The Art of Computer Programming, vol. 3. Sorting and Searching.— Москва: «Вильямс», 2007.

4 Сотов Л. С. Формирователи перестановок с управляемой цикловой структурой // Гетеромагнитная микроэлектроника.— 2011.— № 9. — С. 43—55.

5. Sotov L. S. The hardware implementation of permutation instructions of bits of the data // Гетеромагнитная микроэлектроника.— 2011.— № 10.— С. 25—50.

6. Sotov L. S., Achkacov V. N. The universal module of manipulation in bits of the data in microprocessors // Гетеромагнитная микроэлектроника.— 2011.— № 11.— С. 57—73.

7. Соболев С. С. Модель генератора перестановок на основе управляемого циклического сдвига // Вестник Воронежского государственного университета.— 2012.— № 1.— С. 73—81.

N. I. Kushnirenko, V. Ya. Chechelnytskiy

A hardware generator of permutations.

The paper presents an algorithm and a scheme of the hardware generator of permutations based on multiplexers. Such scheme is characterized by increased speed of operation, since it is designed without the use of shift registers, which are present in existing prototypes and slow down their operation at least two times.

Keywords: *generator of permutations, hardware complexity, high performance.*