РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 390 049** (13) **C1**

(51) МПК
G06F 7/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2008139529/09, 07.10.2008**

(24) Дата начала отсчета срока действия патента:
07.10.2008

(45) Опубликовано: **20.05.2010** Бюл. № **14**

(56) Список документов, цитированных в отчете о поиске: **RU 2320000 C1, 20.03.2008. US 20070277085 A1, 29.11.2007. US 6105114, 15.08.2000. US 20030145272 A1, 31.07.2003.**

Адрес для переписки:
410012, г.Саратов, ул. Московская, 155, СГУ, ПЛО, Н.В. Романовой

(72) Автор(ы):
Молодченко Жанна Анатольевна (RU),
Сотов Леонид Сергеевич (RU),
Харин Валерий Николаевич (RU)

(73) Патентообладатель(и):
Государственное образовательное учреждение высшего профессионального образования "Саратовский государственный университет им. Н.Г. Чернышевского" (RU)

(54) ПАРАЛЛЕЛЬНЫЙ ДЕШИФРАТОР УПРАВЛЯЕМОЙ ТРАНСПОЗИЦИИ ИНФОРМАЦИИ, ХРАНИМОЙ В ПЕРСОНАЛЬНОЙ ЭВМ

(57) Реферат:

Изобретение относится к области кодирования информации и может быть использовано в вычислительной технике и в системах защиты информации от несанкционированного доступа. Техническим результатом является возможность высокоскоростного параллельного преобразования форматов блоков данных методом транспозиции с использованием управляющих кодов. Дешифратор управляемой транспозиции информации, хранимой в персональной ЭВМ, содержит К уровней узлов дешифрации, регистр управляющих кодов, содержащий биты управляющих кодов. Узлы дешифрации выполнены на одинаковых логических элементах, имеющих первый и второй входы данных X_1, X_2, первый и второй выходы данных Y_1, Y_2 и вход управляющего кода COD. 3 ил.

RU 2390049 C1

RU 2390049 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 390 049** (13) **C1**

(51) Int. Cl.
G06F 7/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2008139529/09, 07.10.2008**

(24) Effective date for property rights:
07.10.2008

(45) Date of publication: **20.05.2010 Bull. 14**

Mail address:
410012, g.Saratov, ul. Moskovskaja, 155, SGU, PLO, N.V. Romanovoj

(72) Inventor(s):
Molodchenko Zhanna Anatol'evna (RU),
Sotov Leonid Sergeevich (RU),
Kharin Valerij Nikolaevich (RU)

(73) Proprietor(s):
Gosudarstvennoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija "Saratovskij gosudarstvennyj universitet im. N.G. Chernyshevskogo" (RU)

(54) PARALLEL DECODER FOR CONTROLLED TRANSPOSITION OF INFORMATION STORED ON PERSONAL COMPUTER

(57) Abstract:

FIELD: information technology.

SUBSTANCE: decoder for controlled transposition of information stored on a personal computer has K levels of decoding units, a control code register which contains control code bits. The decoding units are made from the same logical elements having first and second data inputs X_1, X_2, first and second data outputs Y_1, Y_2 and a control code COD input.

EFFECT: possibility of high-speed parallel conversion of formats of data blocks through transposition using control codes.

3 dwg

RU 2390049 C1

RU 2390049 C1

Устройство относится к области кодирования информации и может быть использовано в вычислительной технике и в системах защиты информации от несанкционированного доступа.

Известно устройство линейного дешифратора (см. патент РФ № 2032937, МПК G06F 11/00), содержащее К уровней узлов дешифрации (К - разрядность информационного входа дешифратора). В устройство введено К элементов НЕ, а каждый узел дешифрации выполнен в виде мажоритарного элемента. Каждый уровень дешифрации содержит 2i мажоритарных элементов $\left(i = \overline{1,K}\right)$. Вход выборки дешифратора соединен с первыми входами первого и второго мажоритарных элементов первого уровня. Выход каждого мажоритарного элемента i-го уровня соединен с первыми входами пары мажоритарных элементов (i+1)-го уровня, выходы мажоритарных элементов k-го уровня являются выходами дешифратора, информационные входы которого соединены с входами элементов НЕ и соответственно с вторыми входами четных мажоритарных элементов уровней с первого по k-й. Вторые входы нечетных мажоритарных элементов которых соединены соответственно с выходами элементов НЕ. Третьи входы нечетных мажоритарных элементов всех уровней соединены с первым управляющим входом дешифратора, второй управляющий вход которого соединен с третьими входами четных мажоритарных элементов всех уровней.

Однако это устройство функционально не решает задачу управляемой транспозиции данных.

Известен коммутатор на базе коммутационной матрицы, основанной на комбинационной схеме, аналогичной предлагаемой (http: //www.unix.com.ua/lsok/glava_7.htm). Коммутационная матрица состоит из уровней двоичных переключателей, которые соединяют свой вход с одним из двух выходов в зависимости от значения бита тэга. Переключатели первого уровня управляются первым битом тэга, второго - вторым и т.д.

Недостатком использования такой матрицы в качестве дешифратора управляемой транспозиции является невозможность параллельной обработки всего входного блока данных. Если составной канал передачи данных невозможно построить из-за занятости выходного порта или промежуточного коммутационного элемента, то данные должны накапливаться в их источнике, в данном случае - во входном блоке порта, принявшего эти данные. Таким образом, скорость преобразования входных данных существенно уменьшается.

Наиболее близким к предлагаемому решению является дешифратор управляемой побитовой транспозиции информации, хранимой в персональной ЭВМ (см. патент РФ № 2320000, МПК G06F 7/76). Дешифратор содержит К уровней узлов дешифрации, каждый уровень дешифрации содержит 2^i элементов $\left(i = \overline{1,K}\right)$, регистр управляющих кодов, сдвиговый регистр данных, двойной буферный регистр накопления и хранения форматированных данных, блок управления, генератор тактовых импульсов. Вход выборки дешифратора соединен с первыми входами первого и второго элементов первого уровня. Элемент первого уровня реализует логическую функцию $Y_1=X$, $Y_2 = \overline{X}$, остальные элементы реализуют логическую функцию $Y_1 = \overline{X_1} \times X_2, Y_2 = X_1 \times X_2$. Вход X элемента первого уровня соединен с выходом первого бита регистра управляющих кодов, входы X_1 остальных элементов i-го уровня соединены с выходом i-го бита регистра управляющих кодов, входы X_2 остальных элементов i-го уровня соединены с выходами элементов i-1 уровня, причем вход двойного буферного регистра накопления и хранения форматированных данных

соединен с выходом сдвигового регистра данных, а входы разрешения записи этого регистра соединены с выходами последнего уровня дешифрации. Генератор тактовых импульсов соединен с блоком управления, который своими входами и выходами соединен с буферным регистром накопления и хранения форматированных данных, входным сдвиговым регистром данных, регистром управляющих кодов.

Недостатком данного дешифратора является последовательное преобразование данных, которое происходит за N тактовых импульсов генератора, что при больших значениях N значительно снижает быстродействие.

Задачей настоящего решения является ускорение процесса форматирующего преобразования произвольной транспозиции информации за счет одновременной (параллельной) перестановки входного вектора данных (α_1, α_2, …, α_N), при минимизации логических вентилей матрицы дешифратора.

Техническим результатом является возможность высокоскоростного параллельного преобразования форматов блоков данных методом транспозиции с использованием управляющих кодов.

Поставленная задача достигается тем, что дешифратор управляемой транспозиции информации, хранимой в персональной ЭВМ, содержащий K уровней узлов дешифрации, регистр управляющих кодов, содержащий биты управляющих кодов, согласно решению содержит $N=2^K$ входов данных и выполнен с возможностью перестановки вектора входных данных длиной N параллельно. Для этого узлы дешифрации выполнены на одинаковых логических элементах, имеющих первый и второй входы данных X_1, X_2, первый и второй выходы данных Y_1, Y_2 и вход управляющего кода COD, причем каждый логический элемент электрически соединен входом COD с соответствующим битовым выходом регистра управляющих кодов, каждый логический элемент i-го уровня дешифрации $\left(i = \overline{1, K-1}\right)$ с номером j электрически соединен первым выходом данных Y_1 с первым входом данных X_1 элемента i+1 уровня дешифрации с номером j, а вторым выходом данных Y_2 со вторым входом данных X_2 элемента i+1 уровня дешифрации с номером $j+(-1)^{\mathrm{INT}\left(\frac{j-0,5}{2^{K-i-1}}\right)}\cdot 2^{K-i-1}$, входы данных элементов первого уровня дешифрации являются входами данных дешифратора, выходы данных элементов K-го уровня дешифрации являются выходами данных дешифратора, где i - номер уровня дешифрации, j - номер уровня логического элемента, INT - функция выделения целой части числа.

Изобретение поясняется чертежами, где на фиг.1 приведена блок-схема устройства, на фиг.2 - логический элемент узла дешифратора, на фиг.3 - граф, иллюстрирующий работу матрицы дешифратора, где

1) регистр управляющих кодов;

2) матрица дешифратора;

3) X_1, X_2 - первый и второй входы данных узла дешифрации;

4) Y_1, Y_2 - первый и второй выходы данных узла дешифрации;

5) COD - вход управляющего кода.

Предлагаемый параллельный дешифратор управляемой транспозиции информации состоит из регистра управляющих кодов 1 и матрицы дешифратора 2 (фиг.1), выполняющей функцию перестановки вектора данных (α_1, α_2, …, α_N). Матрица дешифратора выполнена на одинаковых логических элементах, имеющих два входа данных X_1, X_2, два выхода данных Y_1, Y_2 и вход управляющего кода COD (см. фиг.2).

Каждый логический элемент осуществляет транспозицию данных $Y_1=X_2$, $Y_2=X_1$ при высоком логическом уровне на входе COD или передает данные без изменения $Y_1=X_1$, $Y_2=X_2$ при низком логическом уровне на входе COD. Входы кодов матрицы дешифратора соединены с выходами регистра управляющих кодов. Число логических элементов матрицы дешифратора $L=N/2\cdot K$, где $K=\log_2 N$ - уровней дешифрации.

Работа дешифратора поясняется графом, представленным на фиг.3, выполненным для N=16, К=4. Логические элементы фиг.2 располагаются в вершинах графа. На входы данных элементов первого уровня дешифрации подаются элементы входного вектора данных ($\alpha_1, \alpha_2, \ldots, \alpha_N$). Каждый элемент i-го уровня дешифрации с номером j электрически соединен первым выходом данных с первым входом данных элемента i+1 уровня дешифрации с номером $j+(-1)^{INT\left(\frac{j-0,5}{2^{K-i-1}}\right)}\cdot 2^{K-i-1}$. Выходы данных элементов К-го уровня дешифрации являются выходами данных дешифратора.

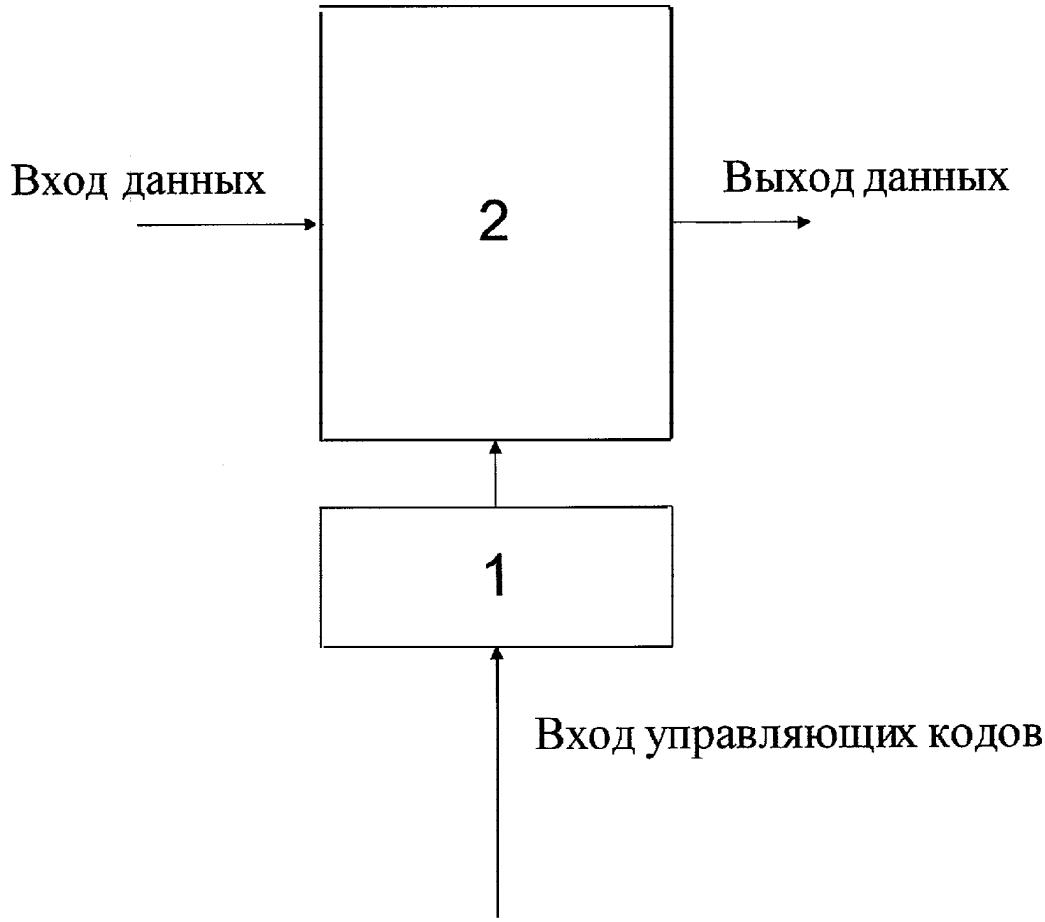
Устройство работает следующим образом. Перед началом преобразования в регистр управляющих кодов записывается $N/2\cdot\log_2 N$ бит управляющих кодов, каждый их которых управляет соответствующим логическим элементом узла дешифратора. На входы дешифратора подаются элементы входного вектора данных. Через время задержки преобразования на выходах дешифратора появляется перестановка входного вектора данных. Время задержки выполнения перестановки Т определяется временем задержки на логическом элементе узла матрицы дешифратора τ и числом уровней дешифрации K:$T=K\cdot\tau$.

Таким образом, перестановка входного вектора данных длиной N в соответствии с управляющими кодами в регистре управляющих кодов выполняется параллельно, что обеспечивает высокую скорость преобразования. Число логических элементов дешифратора $N/2\cdot\log_2 N$ растет практически линейно с ростом N, что делает технически возможным перестановку больших блоков данных. Число возможных перестановок, осуществляемых данным дешифратором, $2^{N/2\cdot\log_2 N} < N!$, т.к. данный дешифратор не реализует полное множество возможных перестановок вектора входных данных.

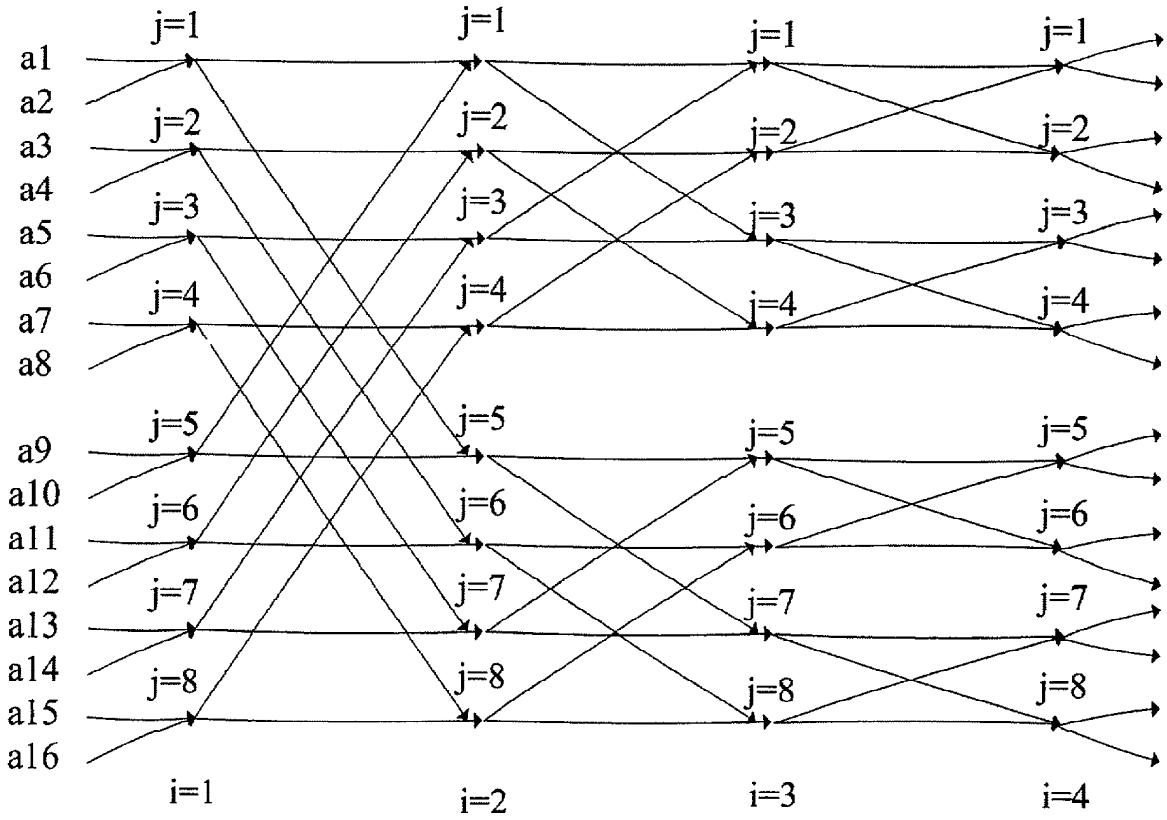
Формула изобретения

Дешифратор управляемой транспозиции информации, хранимой в персональной ЭВМ, содержащий узлы дешифрации, которые образуют К уровней, регистр управляющих кодов, содержащий биты управляющих кодов, отличающийся тем, что он содержит $N=2^K$ входов данных и выполнен с возможностью перестановки вектора входных данных длиной N параллельно, при этом узлы дешифрации выполнены на одинаковых логических элементах, имеющих первый и второй входы данных X_1, X_2, первый и второй выходы данных Y_1, Y_2 и вход управляющего кода COD и осуществляющих транспозицию данных на входах данных $Y_1=X_2$, $Y_2=X_1$ при высоком логическом уровне на входе COD или передающих данные на входах данных без изменения $Y_1=X_1$, $Y_2=X_2$ при низком логическом уровне на входе COD, причем каждый логический элемент электрически соединен входом COD с соответствующим битовым выходом регистра управляющих кодов, каждый логический элемент i-го уровня дешифрации $\left(i=\overline{1,K-1}\right)$ с номером j электрически соединен первым выходом данных Y_1 с первым входом данных X_1 элемента i+1 уровня дешифрации с номером j, а вторым выходом данных Y_2 со вторым входом данных X_2 элемента i+1

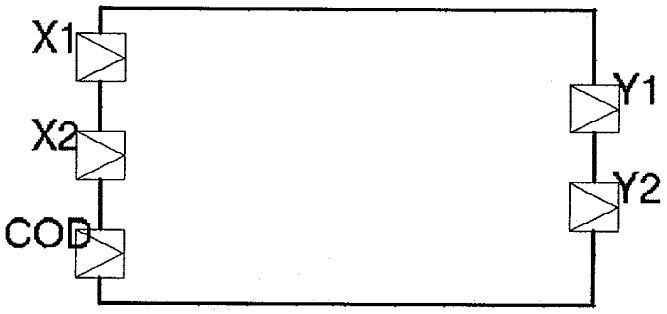
уровня дешифрации с номером $j + (-1)^{INT\left(\frac{j-0,5}{2^{K-i-1}}\right)} \cdot 2^{K-i-1}$, входы данных элементов первого уровня дешифрации являются входами данных дешифратора, выходы данных элементов К-го уровня дешифрации являются выходами данных дешифратора, где i - номер уровня дешифрации, j - номер уровня логического элемента, INT - функция выделения целой части числа.


Вход данных
2
Выход данных
1
Вход управляющих кодов

Фиг. 1


a1
a2
a3
a4
a5
a6
a7
a8
a9
a10
a11
a12
a13
a14
a15
a16
j=1
j=2
j=3
j=4
j=5
j=6
j=7
j=8
i=1
i=2
i=3
i=4

Фиг. 2



Фиг. 3