РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 445 681** (13) **C2**

(51) МПК
G06F 7/523 (2006.01)
G06F 7/72 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2009146603/08, 15.12.2009**

(24) Дата начала отсчета срока действия патента:
15.12.2009

Приоритет(ы):
(22) Дата подачи заявки: **15.12.2009**

(43) Дата публикации заявки: **20.06.2011** Бюл. № 17

(45) Опубликовано: **20.03.2012** Бюл. № 8

(56) Список документов, цитированных в отчете о поиске: **RU 2299460 C1, 05.10.2005. RU 2015537 C1,30.06.1994. WO 2008028529 A1, 13.03.2008.**

Адрес для переписки:
355009, Ставропольский край, г.Ставрополь, ул. Пушкина, 1, Ставропольский государственный университет, научно-исследовательская часть

(72) Автор(ы):
Копытов Владимир Вячеславович (RU),
Петренко Вячеслав Иванович (RU),
Сидорчук Алеся Вячеславна (RU)

(73) Патентообладатель(и):
Государственное образовательное учреждение высшего профессионального образования "Ставропольский государственный университет" (RU)

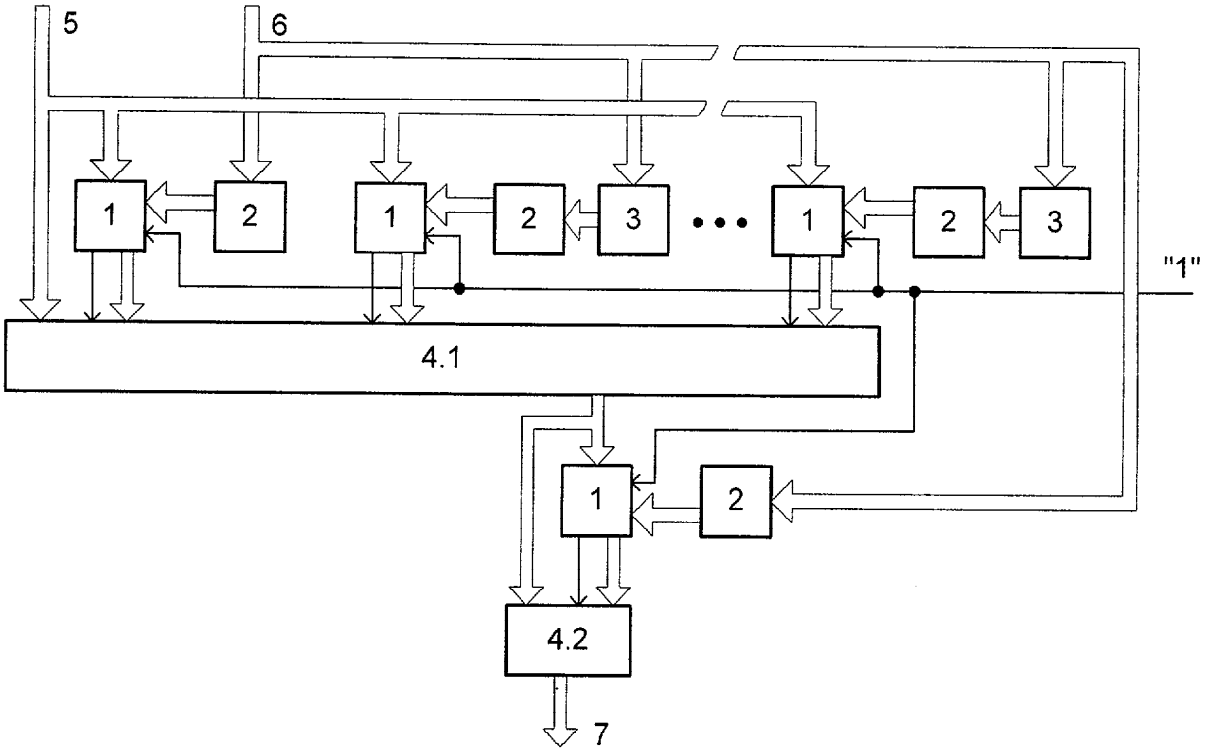
(54) УМНОЖИТЕЛЬ НА ДВА ПО МОДУЛЮ

(57) Реферат:

Изобретение относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах, а также в устройствах для формирования элементов конечных полей и в криптографических приложениях. Техническим результатом является расширение диапазона значений входных чисел. Устройство содержит сумматоры, умножители, инверторы и мультиплексоры. 1 ил.

RU 2445681 C2

RU 2445681 C2



1-сумматор

2-инвертор

3-умножитель

4.1, 4.2-мультиплексоры

Фиг. 1

RU 2445681 C2

RU 2445681 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 445 681** (13) **C2**

(51) Int. Cl.
G06F 7/523 (2006.01)
G06F 7/72 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2009146603/08, 15.12.2009**

(24) Effective date for property rights:
15.12.2009

Priority:
(22) Date of filing: **15.12.2009**

(43) Application published: **20.06.2011** Bull. 17

(45) Date of publication: **20.03.2012 Bull. 8**

Mail address:
355009, Stavropol'skij kraj, g.Stavropol', ul. Pushkina, 1, Stavropol'skij gosudarstvennyj universitet, nauchno-issledovatel'skaja chast'

(72) Inventor(s):
Kopytov Vladimir Vjacheslavovich (RU),
Petrenko Vjacheslav Ivanovich (RU),
Sidorchuk Alesja Vjacheslavna (RU)

(73) Proprietor(s):
Gosudarstvennoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija "Stavropol'skij gosudarstvennyj universitet" (RU)

(54) DOUBLER BY MODULE

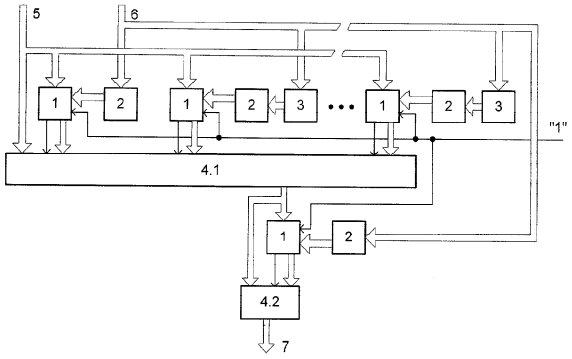
(57) Abstract:

FIELD: information technologies.

SUBSTANCE: invention may be used in digital computing devices, and also in devices to generate elements of end fields and in cryptographic applications. The device comprises summators, multipliers, inverters and multiplexors.

EFFECT: expanded range of input number values.

1 dwg



1-сумматор
2-инвертор
3-умножитель
4.1, 4.2-мультиплексоры

Фиг. 1

RU 2445681 C2

RU 2445681 C2

Изобретение относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах, а также в устройствах для формирования элементов конечных полей и в криптографических приложениях.

Известен умножитель на два по модулю, содержащий сумматор и мультиплексор (см. патент РФ №2015537, кл. G06F 7/49, 30.06.1994).

Недостатком данного устройства являются его ограниченные функциональные возможности, а именно ограниченный диапазон значений входных чисел x ($0<x\leq p-1$, где p - значение модуля, по которому производится вычисление).

Наиболее близким по технической сущности к заявляемому изобретению является умножитель на два по модулю, содержащий n сумматоров, n инверторов, (n-1) умножителей и мультиплексор (см. патент РФ №2299460, кл. G06F 7/72, 20.05.2007).

Недостатком данного устройства является ограниченный диапазон значений входных чисел x ($0<x\leq\{n/2)p-1$, где p - модуль, n - размер умножителя, определяемый количеством сумматоров).

Цель изобретения - увеличение диапазона значений входных чисел.

Для достижения поставленной цели в умножитель на два по модулю, состоящий из n сумматоров, n инверторов, n-1 умножителей, и первого мультиплексора, имеющего n+1 информационных и n управляющих входов, причем вход записи двоичного кода числа, подключен к первому информационному входу первого мультиплексора и первым входам всех n сумматоров, выход переноса i-го сумматора подключен к i-му управляющему входу первого мультиплексора, информационный выход i-го сумматора подключен к (i+1)-му информационному входу первого мультиплексора, где i=1, …, n, вход записи двоичного кода модуля подключен к входу первого инвертора и к входу каждого умножителя, j-й умножитель производит умножение значения на своем входе на величину (j+1), где j=1, …, n-1, выход 7-го умножителя подключен к входу (j+1)-го инвертора, выход i-го инвертора подключен ко второму входу i-го сумматора, к входу переноса каждого сумматора подключен вход записи логической единицы, дополнительно введены (n+1)-й сумматор, (n+1)-й инвертор и второй мультиплексор, имеющий два информационных и один управляющий вход, причем выход первого мультиплексора, сдвинутый на один разряд в сторону старшего, подключен к первому информационному входу (n+1)-го сумматора и первому информационному входу второго мультиплексора, вход записи двоичного кода модуля подключен к входу (n+1)-го инвертора, выход которого подключен ко второму информационному входу (n+1)-го сумматора, на вход переноса которого подана логическая единица, выход переноса (n+1)-го сумматора соединен с управляющим входом второго мультиплексора, второй информационный вход которого соединен с информационным выходом сумматора, выход второго мультиплексора является выходом умножителя.

Сущность изобретения заключается в реализации следующего способа умножения на два по модулю.

Пусть требуется умножить число x на два и сформировать остаток r получившегося выражения по модулю p.

Число x лежит в пределах $0<x\leq np-1$. Перед умножением на два формируется остаток r1 по модулю p двоичного числа x. Для этого x одновременно сравнивается со значениями p, 2p, …, ip, …, np путем вычитания из x этих значений. Таким образом получаются разности $x_1=x-p$, $x_2=x-2p$,… $x_i=x-ip$, …, $x_N=x-np$. То значение x_i,, где i=1, …, n, которое окажется больше 0 и меньше p, и будет результатом формирования остатка r1 по модулю p двоичного числа x. Получившееся значение r1 умножается на

два и снова приводится по модулю p тем же способом.

На чертеже представлена схема умножителя на два по модулю.

Умножитель на два по модулю содержит n+1 сумматоров 1, n+1 инверторов 2, n-1 умножителей 3, 1 мультиплексор 4.1, имеющий n управляющих и (n+1) информационных входов и 1 мультиплексор 4.2, имеющий 1 управляющий и 2 информационных входа. Вход 5 служит для подачи двоичного кода числа x, вход 6 служит для подачи двоичного кода модуля p. Выходы переноса первых n сумматоров 1 подключены к управляющим входам мультиплексора 4.1, а их информационные выходы подключены к информационным входам мультиплексора 4.1. Информационный выход мультиплексора 4.1 подключен к информационному входу (n+1)-го сумматора 1 и информационному входу мультиплексора 4.2. Выход переноса (n+1)-го сумматора 1 подключен к управляющему входу мультиплексора 4.2, информационный выход (n+1)-го сумматора 1 подключен к информационному входу мультиплексора 4.2. Выход мультиплексора 4.2 подключен к выходу 7 и является выходом устройства.

Умножитель на два по модулю работает следующим образом.

На вход 5 подается код числа из диапазона $0<x\leq np-1$, где x - умножаемое число, p - модуль, n - размер умножителя, определяемый количеством сумматоров 1. Данный код поступает на первые входы первых n сумматоров 1 и на первый информационный вход мультиплексора 4.1. Со входа 6 код модуля (подается на входы умножителей 3, на вход первого и (n+1)-го инвертора 2, причем значение модуля в k-м умножителе умножается на значение i=(k+1), где k=1,…, n-1. С выхода k-го умножителя 3 код произведения ixp поступает на вход (k+1)-го инвертора 2. В j-м инверторе 2 поступающий на его вход код переводится в инверсный код, который подается на второй вход j-го сумматора 1, где j,…, n+1. Таким образом, на второй вход каждого сумматора 1 поступает инверсный код значения i×p, где i=1,…, n - номер сумматора. На вход переноса каждого сумматора 1 поступает код числа «1», служащий для перевода инверсного кода модуля в дополнительный код.

В общем виде n сумматоров 1 осуществляют операцию, описываемую выражением: $c = x + \overline{i \times p} + 1$, где c - результат суммирования, x - число, i - номер сумматора, p - модуль. Старший разряд сформированного значения c поступает на выход переноса сумматора 1, остальные разряды представляют разность x - i×p и поступают на информационный выход сумматора 1. (n+1)-ый сумматор 1 осуществляют операцию, описываемую выражением: $m = 2c + \overline{p} + 1$, где m - результат суммирования, x - число, p - модуль. Старший разряд сформированного значения m поступает на выход переноса сумматора 1, остальные разряды представляют разность x-p и поступают на информационный выход сумматора 1.

До тех пор, пока значение x превышает значение i×p, на выходе переноса i-го сумматора 1 будет формироваться «1», которая будет поступать на i-й управляющий вход мультиплексора 4.1. При превышении значением i×p значения x на выходе переноса i-го сумматора 1 сформируется «0». При поступлении на i-й управляющий вход мультиплексора 4.1 символа «0» с выхода переноса i-го сумматора 1 мультиплексор 4.1 переключит на вход (n+1)-го сумматора 1 и на первый вход мультиплексора 4.2, со сдвигом разрядов на один в сторону старшего разряда, информационный вход, на который подается значение с информационного выхода (i-1)-го сумматора 1. Мультиплексор 4.2 переключит на выход 7 информационный вход с мультиплексора 4.1, если $2c<p$, или информационный вход с сумматора 1, если $2c\geq p$. В последнем случае на выходе мультиплексора 4.2 будет значение $m=2c-p$. Данное

значение будет представлять результат умножения числа x на два по модулю ρ.

Рассмотрим работу умножителя на примере.

Пусть $x = 15_{10} = 01111_2$, $p = 4_{10} = 00100_2$, $\overline{p} = 11011_2$. Как показано выше, i-й сумматор 1 формирует значение $c = x + \overline{i \times p} + 1$, поэтому для второго сумматора $i \times p = 2 \times p = 8_{10} = 01000_2$, $\overline{i \times p} = 10111_2$, для третьего сумматора $i \times p = 3 \times p = 12_{10} = 01100_2$, $\overline{i \times p} = 10011_2$, для четвертого сумматора $i \times p = 4 \times p = 16_{10} = 10000_2$, $\overline{i \times p} = 01111_2$.

Тогда первый сумматор 1 сформирует значение $c_1=01111_2+11011_2+1=101011_2$, второй $c_2=01111_2+10111_2+1=100111_2$, третий - $c_3=01111_2+10011_2+1=100011_2$, четвертый - $c_4=01111_2+01111_2+1=011111_2$.

Как видно из примера, на выходах переноса первых трех сумматоров 1 сформировано значение «1», на выходе же четвертого сумматора 1 сформировано значение «0», поэтому на выход мультиплексора 4.1 поступит значение с информационного выхода третьего сумматора 1, равное $00011_2=3_{10}$.

Полученное значение умножается на 2, путем сдвига разрядов на один в сторону старшего. На первый информационный вход мультиплексора 4.2 и на первый информационных вход сумматора 1 поступает значение 0110_2. (n+1)-ый сумматор 1 формирует значение $m = 2c + \overline{p} + 1 = 0110_2 + 1011_2 + 1 = 100010_2$ Т.к. на выходе переноса сумматора 1 сформировано значение «1», поэтому на выход мультиплексора 4.2 поступит значение с информационного выхода сумматора 1, равное $0010_2=2_{10}$. Так как (15)(mod 4)=3, (3×2)(mod 4)=2, то правильность работы устройства очевидна.

Формула изобретения

Умножитель на два по модулю, состоящий из n сумматоров, n инверторов, n-1 умножителей и первого мультиплексора, имеющего n+1 информационных и n управляющих входов, причем первый информационный вход первого мультиплексора подключен к первым входам всех n сумматоров, выход переноса i-го сумматора подключен к i-му управляющему входу первого мультиплексора, информационный выход i-го сумматора подключен к (i+1)-му информационному входу первого мультиплексора, где i=1, …, n, вход записи двоичного кода модуля подключен к входу первого инвертора и к входу каждого умножителя, j-й умножитель производит умножение значения на своем входе на величину (j+1), где j=1, …, n-1, выход j-го умножителя подключен к входу (j+1)-го инвертора, выход i-го инвертора подключен ко второму входу i-го сумматора, к входу переноса каждого сумматора подключен вход записи логической единицы, отличающийся тем, что в него дополнительно введены (n+1)-й сумматор, (n+1)-й инвертор и второй мультиплексор, имеющий два информационных и один управляющий вход, причем вход записи двоичного кода числа подключен к первому информационному входу первого мультиплексора и первым входам всех n сумматоров, выход первого мультиплексора подключен со сдвигом на один разряд в сторону старшего к первому информационному входу (n+1)-го сумматора и первому информационному входу второго мультиплексора, вход записи двоичного кода модуля подключен к входу (n+1)-го инвертора, выход которого подключен ко второму информационному входу (n+1)-го сумматора, на вход переноса которого подана логическая единица, выход переноса (n+1)-го сумматора соединен с управляющим входом второго мультиплексора, второй

информационных вход которого соединен с информационным выходом сумматора, выход второго мультиплексора является выходом умножителя.