РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 299 460** (13) **C1**

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

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2005130894/09, 05.10.2005**

(24) Дата начала отсчета срока действия патента:
05.10.2005

(45) Опубликовано: **20.05.2007 Бюл. № 14**

(56) Список документов, цитированных в отчете о поиске: **RU 2015537 C1, 30.06.1994. RU 2023290 C1, 15.11.1994. RU 2143723 C1, 27.12.1999. SU 1667055 A1, 30.07.1991. JP 2002251137, 06.09.2002. EP 0145533 A, 19.06.1985.**

Адрес для переписки:
355017, г.Ставрополь, ул. Артема, 2, СВИСРВ, НИО

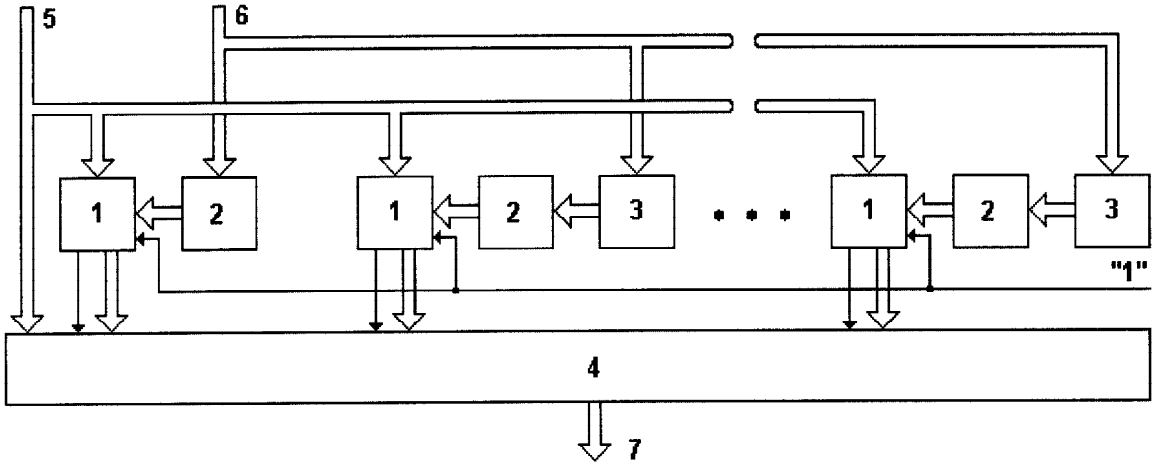
(72) Автор(ы):
Петренко Вячеслав Иванович (RU),
Кузьминов Юрий Владимирович (RU)

(73) Патентообладатель(и):
Петренко Вячеслав Иванович (RU),
Кузьминов Юрий Владимирович (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. Техническим результатом является расширение функциональных возможностей за счет расширения диапазона значений входных чисел. Устройство содержит сумматоры, инверторы, умножители, мультиплексор. 1 ил.



RU 2299460 C1

RU 2299460 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 299 460** (13) **C1**

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

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2005130894/09, 05.10.2005**

(24) Effective date for property rights: **05.10.2005**

(45) Date of publication: **20.05.2007 Bull. 14**

Mail address:
355017, g.Stavropol', ul. Artema, 2, SVISRV, NIO

(72) Inventor(s):
Petrenko Vjacheslav Ivanovich (RU),
Kuz'minov Jurij Vladimirovich (RU)

(73) Proprietor(s):
Petrenko Vjacheslav Ivanovich (RU),
Kuz'minov Jurij Vladimirovich (RU)

(54) MODULUS MULTIPLIER BY TWO

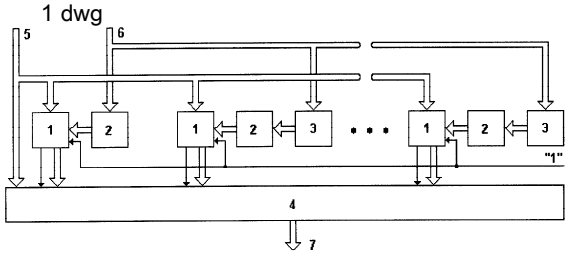
(57) Abstract:

FIELD: computer engineering, possible use in digital computing devices, and also in devices for forming elements of finite fields.

SUBSTANCE: device contains adders, inverters, multipliers, multiplexer.

EFFECT: expanded functional capabilities due to expanded range of input number values.

1 dwg



RU 2299460 C1

RU 2299460 C1

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

Известен умножитель на два по модулю, содержащий два сумматора, элементы ИЛИ-НЕ и элементы ИЛИ с соответствующими связями (см. Пухальский Т.И., Новосельцева Т.Я. Проектирование дискретных устройств на интегральных микросхемах. Справочник. М.: Радио и связь, 1990, с.205, рис.3.131).

Недостатком данного устройства является низкое быстродействие.

Наиболее близким по технической сущности к заявляемому изобретению является 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).

Цель изобретения - расширение функциональных возможностей умножителя на два по модулю за счет расширения диапазона значений входных чисел.

Известно, что любое число x, представленное в двоичной форме, можно умножить на два путем сдвига всех разрядов числа на один в сторону старшего с записью значения "0" в младший разряд. При проведении вычислений по модулю p значение $a=2x$ сравнивается со значением модуля. Если полученное значение $a\geq p$, то из a вычитается значение модуля p, а полученное в результате значение $a_1=a-p$ вновь сравнивается со значением p. Если и в этом случае значение $a_1\geq p$, то из a_1 вновь вычитается значение p, а полученное в результате значение $a_2=a_1-p$ сравнивается со значением p. Данные операции проводятся до тех пор, пока значение a_n, полученное на n-м шаге вычислений, не станет меньше значения модуля p. В этом случае значение a_n является результатом умножения числа x на два по модулю p. Если уже на первом шаге входное значение $a<p$, значение a остается без изменений и является результатом умножения числа x на два по модулю.

Предлагаемый умножитель на два по модулю осуществляет данный метод путем параллельного выполнения n операций (где n - размер умножителя, определяемый количеством входящих в его состав сумматоров), в ходе i-й операции значение $a=2x$ сравнивается со значением $i\times p$ путем вычисления разности $a-i\times p$, где $i=1, ..., n$. Как только при выполнении i-й операции значение полученной разности станет отрицательным, результатом умножения числа x на два по модулю будет являться значение разности, полученное в результате (i-1)-й операции. Диапазон значений входных чисел x для данного умножителя определяется размером умножителя и находится в пределах $0<x\leq(n/2)p-1$.

На чертеже представлена схема умножителя на два по модулю.

Умножитель на два по модулю содержит n сумматоров 1, n инверторов 2, (n-1) умножителей 3 и мультиплексор 4. Вход 5 служит для подачи двоичного кода числа x, вход 6 служит для подачи двоичного кода модуля p. Выходы переноса сумматоров 1 подключены к управляющим входам мультиплексора 4, информационные выходы сумматоров 1 подключены к информационным входам мультиплексора 4. Выход 7 является выходом устройства.

Умножитель на два по модулю работает следующим образом.

На вход 5 подается код числа из диапазона $0<x\leq(n/2)p-1$, где x - умножаемое число, p - модуль, n - размер умножителя, определяемый количеством сумматоров 1. Данный код поступает на первые входы сумматоров 1 и на первый информационный вход мультиплексора 4. Со входа 6 код модуля p подается на входы умножителей 3 и на вход первого 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 значения $i\times p$ 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 $j=1, ..., n$. Таким образом, на второй вход каждого сумматора 1 поступает инверсный код

значения $i \times p$, где i - номер сумматора. На третий вход каждого сумматора 1 поступает код числа "1", служащий для перевода инверсного кода модуля в дополнительный код.

В общем виде сумматор 1 осуществляет операцию, описываемую выражением: $c = 2x + \overline{i \times p} + 1$, где c - результат суммирования, x - число, умножаемое на два по модулю, i - номер сумматора, p - модуль. Старший разряд сформированного значения c поступает на выход переноса сумматора 1, остальные разряды представляют разность $2x-i \times p$ и поступают на информационный выход сумматора 1.

До тех пор, пока значение 2x превышает значение $i \times p$, на выходе переноса i-го сумматора 1 будет формироваться "1", которая будет поступать на i-й управляющий вход мультиплексора 4. При превышении значением $i \times p$ значения 2x на выходе переноса i-го сумматора 1 сформируется "0". При поступлении на i-й управляющий вход мультиплексора 4 символа "0" с выхода переноса i-го сумматора 1 мультиплексор 4 проключит на выход 7 информационный вход, на который подается значение с информационного выхода (i-1)-го сумматора 1. Данное значение будет представлять результат умножения числа x на два по модулю p.

Рассмотрим работу умножителя на примере.

Пусть $x=7_{10}=00111_2$, $2x=14_{10}=01110_2$, $p=4_{10}=00100_2$, $\overline{p}=11011_2$. Как показано выше, i-й сумматор 1 формирует значение $c = 2x + \overline{i \times p} + 1$, 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 $c_1=01110_2+11011_2+1=101010_2$, второй $c_2=01110_2+10111_2+1=100110_2$, третий - $c_3=01110_2+10011_2+1=100010_2$, четвертый - $c_4=01110_2+01111_2+1=011110_2$.

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 7 мультиплексора поступит значение с информационного выхода третьего сумматора 1, равное $00010_2=2_{10}$. Так как $(7 \times 2) \pmod 4 = 2$, то правильность работы устройства очевидна.

Пусть теперь $x=3_{10}=0011_2$, $2x=6_{10}=0110_2$, $p=7_{10}=0111_2$, $\overline{p}=1000_2$. В этом случае первый сумматор 1 сформирует значение $c_1=0110_2+1000_2+1=01111_2$. Так как уже первый сумматор на выходе переноса формирует символ "0", на выход 7 мультиплексора поступит значение со входа 5 умножителя, то есть $2x=0110_2=6_{10}=(3 \times 2) \pmod 7$.

Формула изобретения

Умножитель на два по модулю, состоящий из сумматора и мультиплексора, отличающийся тем, что в него дополнительно введены (n-1) сумматоров, (n-1) умножителей и n инверторов, причем вход записи двоичного кода числа, сдвинутого на один разряд в сторону старшего, подключен к первому информационному входу мультиплексора и первым входам всех сумматоров, выход переноса i-го сумматора подключен к i-му управляющему входу мультиплексора, информационный выход i-го сумматора подключен к (i+1)-му информационному входу 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 третьему входу каждого сумматора подключен вход записи логической единицы, выход мультиплексора является выходом умножителя.