РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 299 461** (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: **2005130895/09, 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 Al, 30.07.1991. JP 2002251137, 06.09.2002. EP 0145533 A, 19.06.1985.**

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

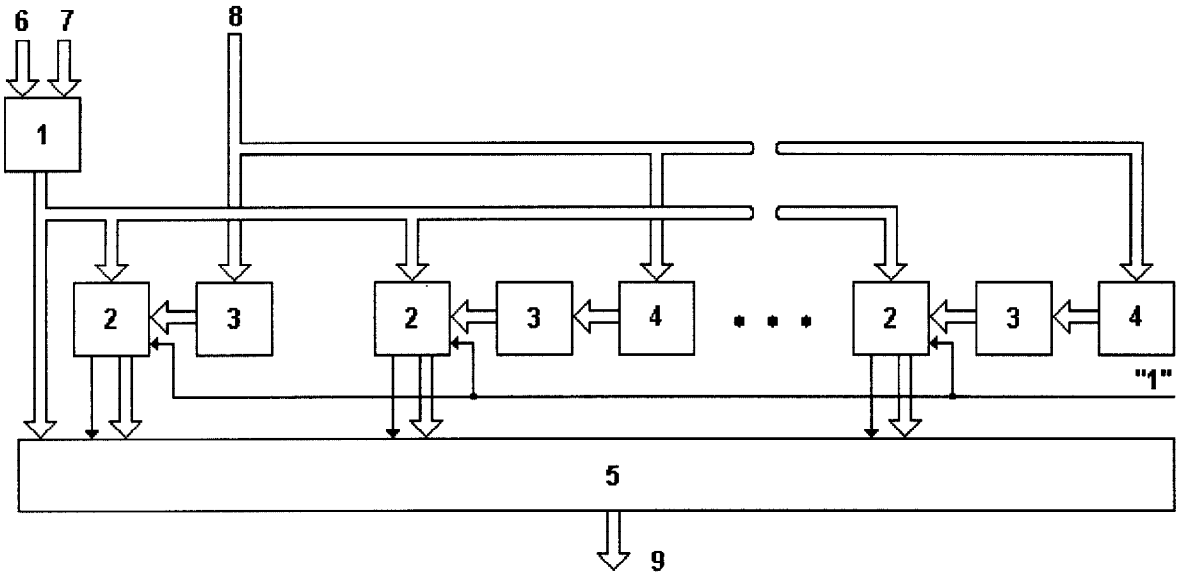
(72) Автор(ы):
Петренко Вячеслав Иванович (RU),
Кузьминов Юрий Владимирович (RU)

(73) Патентообладатель(и):
Петренко Вячеслав Иванович (RU),
Кузьминов Юрий Владимирович (RU)

(54) УМНОЖИТЕЛЬ 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. Устройство содержит умножитель, сумматоры, инверторы, умножители на константу, мультиплексор. 1 ил.



RU 2299461 C1

RU 2299461 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 299 461** (13) **C1**

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

(12) ABSTRACT OF INVENTION

Based on Article 13, par. 3 of the Patent law of the Russian Federation of September 23, 1992, #3517-I the patent owner undertakes to transfer the exclusive right to the invention (assign the patent), on generally practiced conditions, to the first person - citizen of the Russian Federation or a Russian legal person who expresses such a wish and conveys it to the patent owner and the Federal executive body for Intellectual Property.

(21), (22) Application: **2005130895/09, 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, NIO, SVIS RV

(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 MULTIPLEXER

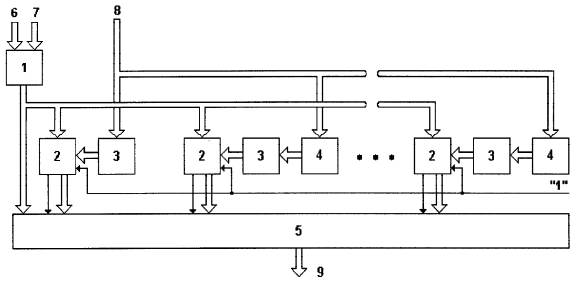
(57) Abstract:

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

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

EFFECT: expanded functional capabilities.

1 dwg



RU 2299461 C1

RU 2299461 C1

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

Известно устройство для умножения чисел по модулю, содержащее два входных регистра, два дешифратора, три группы элементов ИЛИ, четыре группы элементов И, табличный вычислитель значений вида $\alpha'\beta'(\mathrm{mod}\ p/2)+p/2$, пять элементов ИЛИ, два элемента И и шифратор (см. АС СССР №1187161, кл. G06F 7/49, 23.10.1985).

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).

Недостатками 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), а также отсутствие возможности умножения на число, отличное от двух.

Цель изобретения - расширение функциональных возможностей умножителя на два по модулю за счет обеспечения возможности производить вычисление произведения двух чисел, отличных от двух.

Цель достигается путем перемножения значений входных чисел x и y, представленных в двоичной форме, с последующим приведением полученного значения $z=x\times y$ по модулю p в соответствии со следующим алгоритмом.

При проведении вычислений по модулю p значение $z=x\times y$ сравнивается со значением модуля p. Если полученное значение $z\geq p$, то из z вычитается значение модуля p, а полученное в результате значение $z_1=z-p$ вновь сравнивается со значением p. Если и в этом случае значение $z_1\geq p$, то из z_1 вновь вычитается значение p, а полученное в результате значение $z_2=z_1-p$ сравнивается со значением p. Данные операции проводятся до тех пор, пока значение z_n, полученное на n-м шаге вычислений, не станет меньше значения модуля p. В этом случае значение z_n является результатом умножения числа x на число y по модулю p. Если уже на первом шаге входное значение $z<p$, значение z остается без изменений и является результатом умножения числа x на число y по модулю p.

Предлагаемый умножитель 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 $z=x\times y$ сравнивается со значением $i\times p$ путем вычисления разности $z-i\times p$, где $i=1, ..., n$. Как только при выполнении i-й операции значение полученной разности станет отрицательным, результатом умножения числа x на число y по модулю p будет являться значение разности, полученное в результате (i-1)-й операции. Диапазон значений входных чисел x и y для данного умножителя определяется размером умножителя и находится в пределах $[0, ..., (n/4)p-1]$.

На чертеже представлена схема умножителя по модулю.

Умножитель по модулю содержит умножитель 1, n сумматоров 2, n инверторов 3, (n-1) умножителей на константу 4 и мультиплексор 5. Входы 6 и 7 служат для подачи двоичных кодов умножаемых чисел x и y, вход 8 служит для подачи двоичного кода модуля p. Выход 9 является выходом устройства.

Умножитель по модулю работает следующим образом.

На вход 6 подается двоичный код числа x, на вход 7 - двоичный код числа y, причем оба числа принадлежат диапазону $[0, ..., (n/4)p-1]$, где p - модуль, n - размер умножителя, определяемый количеством сумматоров 2. Данные коды подаются на вход умножителя 1, который на выходе формирует двоичный код числа $z=x\times y$. Код числа z поступает на первые входы сумматоров 2 и на первый информационный вход мультиплексора 5. Со входа 8 двоичный код модуля p подается на входы умножителей на

константу 4 и на вход первого инвертора 3, причем значение модуля в k-м умножителе умножается на значение i=(k+1), где k=1, ..., n-1. С выхода k-го умножителя на константу 4 код значения i×p поступает на вход (k+1)-го инвертора 3. В j-м инверторе 3 поступающий на его вход код переводится в инверсный код, который подается на второй вход j-го сумматора 2, где j=1, ..., n. Таким образом, на второй вход каждого сумматора 2 поступает инверсный код значения i×p, где i - номер сумматора. На третий вход каждого сумматора 2 поступает код числа «1», служащий для перевода инверсного кода модуля в дополнительный код.

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

До тех пор, пока значение z превышает значение i×p, на выходе переноса i-го сумматора 2 будет формироваться «1», которая будет поступать на i-й управляющий вход мультиплексора 5. При превышении значением i×p значения z на выходе переноса i-го сумматора 2 сформируется «0». При поступлении на i-й управляющий вход мультиплексора 5 символа «0» с выхода переноса i-го сумматора 2 мультиплексор 5 проключит на выход 9 информационный вход, на который подается значение с информационного выхода (i-1)-го сумматора 2. Данное значение будет представлять результат умножения числа x на число y по модулю p.

Рассмотрим работу умножителя на примере.

Пусть $x=5_{10}=00101_2$, $y=3_{10}=00011_2$, $z=x\times y=15_{10}=01111_2$, $p=4_{10}=00100_2$, $\bar{p} = 11011_2$. Как показано выше, i-й сумматор 2 формирует значение $c = z + \overline{i \times p} + 1$, 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 2 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 - $c_4=01110_2+01111_2+1=011111_2$.

Как видно из примера, на выходах переноса первых трех сумматоров 2 сформировано значение «1», на выходе же четвертого сумматора 2 сформировано значение «0», поэтому на выход 9 мультиплексора 5 поступит значение с информационного выхода третьего сумматора 2, равное $00011_2=3_{10}$. Так как $(5\times3)(\mathrm{mod}\ 4)=3$, то правильность работы устройства очевидна.

Пусть теперь $x=4_{10}=00100_2$, $y=3_{10}=00011_2$, $z=x\times y=12_{10}=01100_2$, $p=15_{10}=01111_2$, $\bar{p} = 10000_2$. В этом случае первый сумматор 2 сформирует значение $c_1=01100_2+10000_2+1=011101_2$. Так как уже первый сумматор на выходе переноса формирует символ «0», на выход 9 мультиплексора поступит значение с выхода умножителя 1, то есть $z=x\times y=01100_2=12_{10}=(4\times3)(\mathrm{mod}\ 15)$.

Формула изобретения

Умножитель по модулю, состоящий из сумматора и мультиплексора, отличающийся тем, что в него введены умножитель, (n-1) сумматоров, (n-1) умножителей на константу, n инверторов, причем вход записи двоичного кода первого из умножаемых чисел подключен к первому входу умножителя, вход записи двоичного кода второго умножаемого числа подключен ко второму входу умножителя, выход умножителя 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 на константу, j-й умножитель на константу производит умножение значения на своем входе на величину (j+1), где j=1, ..., n-1, выход j-го умножителя на константу 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 устройства.