



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК

G06F 7/72 (2024.08); G06F 7/523 (2024.08)

(21)(22) Заявка: 2024115290, 04.06.2024

(24) Дата начала отсчета срока действия патента:
04.06.2024

Дата регистрации:
23.10.2024

Приоритет(ы):

(22) Дата подачи заявки: 04.06.2024

(45) Опубликовано: 23.10.2024 Бюл. № 30

Адрес для переписки:

355017, г. Ставрополь, ул. Пушкина, 1, ФГАОУ
ВО "Северо-Кавказский федеральный
университет", Алиханов Анатолий Алиевич

(72) Автор(ы):

Петренко Вячеслав Иванович (RU),
Небесская Мария Валерьевна (RU)

(73) Патентообладатель(и):

Федеральное государственное автономное
образовательное учреждение высшего
образования "Северо-Кавказский
федеральный университет" (RU)

(56) Список документов, цитированных в отчете
о поиске: RU 2653310 C1, 07.05.2018. RU
2652450 C1, 26.04.2018. RU 2797164 C1,
31.05.2023. RU 2589361 C1, 10.07.2016. US
20050033790 A1, 10.02.2005.

(54) УМНОЖИТЕЛЬ ПО МОДУЛЮ

(57) Реферат:

Изобретение относится к вычислительной
технике. Технический результат заключается в
повышении быстродействия устройства.
Технический результат достигается за счет того,
что устройство содержит ключи, сумматоры,
трехвходовые сумматоры, которые содержат
одноразрядные полные сумматоры и $(m+1)$ -
разрядный сумматор, и пятивходовые
мультиплексоры; при этом при вычислении

произведения чисел по модулю P путем
последовательного выполнения $(n/2)$ операций,
где n – количество разрядов входного числа A ,
приведение результатов вычисления по
произвольному модулю на каждой ступени
преобразования выполняется за один шаг,
одновременно с операцией суммирования
промежуточных вычислений. 2 ил.

RU 2 829 089 C1

RU 2 829 089 C1



ФИГ. 1

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) ABSTRACT OF INVENTION

(52) CPC

G06F 7/72 (2024.08); G06F 7/523 (2024.08)

(21)(22) Application: 2024115290, 04.06.2024

(24) Effective date for property rights:
04.06.2024Registration date:
23.10.2024

Priority:

(22) Date of filing: 04.06.2024

(45) Date of publication: 23.10.2024 Bull. № 30

Mail address:

355017, g. Stavropol, ul. Pushkina, 1, FGAOU VO
"Severo-Kavkazskij federalnyj universitet",
Alikhanov Anatolij Alievich

(72) Inventor(s):

Petrenko Viacheslav Ivanovich (RU),
Nebesskaia Mariia Valerevna (RU)

(73) Proprietor(s):

Federalnoe gosudarstvennoe avtonomnoe
obrazovatelnoe uchrezhdenie vysshego
obrazovaniia "Severo-Kavkazskii federalnyi
universitet" (RU)

(54) MODULUS MULTIPLIER

(57) Abstract:

FIELD: computer engineering.

SUBSTANCE: device comprises switches, adders, three-input adders, which contain single-bit full adders and $(m+1)$ -bit adder, and five-input multiplexers; wherein when calculating the product of numbers modulo P by successively performing $(n/2)$ operations, where n is the number of bits of the input number A ,

reduction of calculation results by an arbitrary modulus at each conversion stage is performed in one step, simultaneously with the operation of summation of intermediate calculations.

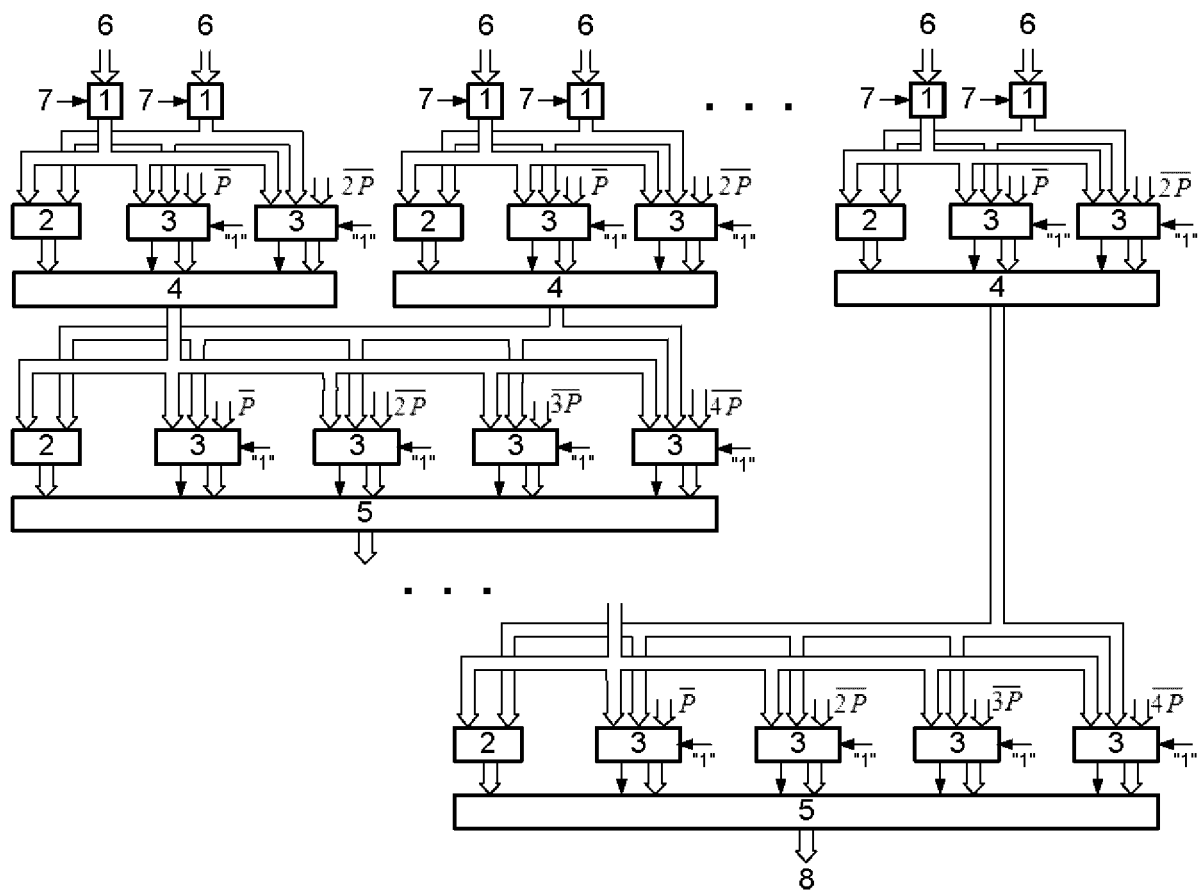
EFFECT: faster operation of the device.

1 cl, 2 dwg

RU 2 829 089

C1

RU 2 829 089 C1



Фиг. 1

Область техники, к которой относится изобретение

Изобретение относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах, в криптографических приложениях, а также в устройствах цифровой обработки сигналов и в системах управления.

Уровень техники

Известен умножитель на два по модулю, содержащий сумматор и мультиплексор [1]. Устройство представляет собой решение в области умножения чисел на два по произвольному модулю. В его состав входят сумматор и мультиплексор, которые совместно обеспечивают повышенную эффективность и быстродействие процесса умножения. Недостатком данного устройства являются его ограниченные функциональные возможности, а именно отсутствие возможности умножения на число, отличное от двух.

Известно устройство для умножения чисел по произвольному модулю, содержащее сумматоры, мультиплексоры, ключи, блоки сдвига, инвертор и сумматор по модулю [2]. Устройство является эффективным решением для умножения чисел по произвольному модулю. Это устройство предлагает расширенные функциональные возможности, которые могут быть применены в цифровых вычислительных устройствах и системах для формирования элементов конечных полей. Недостатком данного устройства является низкое быстродействие, так как умножение осуществляется за $(n-1)$ последовательных шагов преобразования, где n – разрядность устройства.

Наиболее близким по технической сущности к заявляемому изобретению является умножитель по модулю, содержащий ключи, сумматоры, мультиплексоры [3], выбранный в качестве прототипа. Умножитель по модулю позволяет умножать два числа по произвольному модулю за $n/2$ этапов преобразования, образующих ступени преобразования, где n – разрядность устройства, одновременно обрабатывая два разряда множимого. Однако на каждой ступени преобразования приведение результатов вычисления по произвольному модулю выполняется за два шага, вначале выполняется операция суммирования промежуточных вычислений, а затем осуществляется приведение полученного значения по модулю, что снижает быстродействие устройства.

Техническим результатом изобретения является повышение быстродействия.

Раскрытие сущности изобретения

Для достижения технического результата в умножитель по модулю, содержащий входы кодов множимого, входы кодов множителя, выходы кодов произведения, $n/2$ ступеней преобразования, где n – разрядность устройства, причем первая ступень преобразования содержит $n/2$ узлов, а $(2 \dots n/2)$ -е ступени преобразования содержат по одному узлу, каждый узел преобразования первой ступени преобразования содержит первый и второй ключи, двухвходовый сумматор и трехвходовый мультиплексор, а узлы преобразования $(2 \dots n/2)$ -й ступеней преобразования содержат двухвходовые сумматоры и пятивходовые мультиплексоры, информационные входы всех ключей первой ступени преобразования соединены со входами кода множителя, управляющие входы соединены с соответствующими разрядами кода множимого, информационные выходы первых ключей каждого узла первой ступени преобразования соединены с первыми информационными входами соответствующих двухвходовых сумматоров со сдвигом на один разряд в сторону старших, информационные выходы вторых ключей каждого узла первой ступени преобразования соединены со вторыми информационными входами соответствующих двухвходовых сумматоров, информационные выходы двухвходовых сумматоров соединены с первыми информационными входами соответствующих трехвходовых мультиплексоров, информационные выходы

трехвходового мультиплексора первого узла первой ступени преобразования соединены со сдвигом на два разряда в сторону старших с первыми информационными входами двухвходового сумматора второй ступени преобразования, информационные выходы трехвходовых мультиплексоров j -го узла первой ступени преобразования, где $j=2 \dots n/2$,
 5 соединены со вторыми информационными входами двухвходовых сумматоров j -й ступени преобразования, информационные выходы двухвходовых сумматоров j -й ступени преобразования соединены с первыми информационными входами соответствующих пятивходовых мультиплексоров, информационные выходы пятивходовых мультиплексоров j -й ступени преобразования, где $j=2, \dots, n/2-1$ соединены
 10 со сдвигом на два разряда в сторону старших с первыми информационными входами двухвходовых сумматоров $(j+1)$ -й ступени преобразования, а $n/2$ -й ступени преобразования являются выходами кодов произведения дополнительно введены на первой ступени преобразования в каждый узел первый и второй трехвходовые сумматоры, а на $(2 \dots n/2)$ -й ступени преобразования введены первый, второй, третий и
 15 четвертый трехвходовые сумматоры, причем первые информационные входы первых и вторых трехвходовых сумматоров первой ступени преобразования соединены с информационными выходами первых ключей соответствующего узла со сдвигом на один разряд в сторону старших, вторые информационные входы соединены с информационными выходами вторых ключей соответствующего узла, на третьи
 20 информационные входы первых трехвходовых сумматоров подается инверсный код модуля, а на третьи информационные входы вторых трехвходовых сумматоров подается инверсный код удвоенного модуля, информационные выходы первых трехвходовых сумматоров соединены со вторыми информационными входами соответствующих трехвходовых мультиплексоров, информационные выходы вторых трехвходовых
 25 сумматоров соединены с третьими информационными входами соответствующих трехвходовых мультиплексоров, выходы переноса первых трехвходовых сумматоров соединены с первыми управляющими входами соответствующих трехвходовых мультиплексоров, выходы переноса вторых трехвходовых сумматоров соединены со вторыми управляющими входами соответствующих трехвходовых мультиплексоров,
 30 первые информационные входы первых, вторых, третьих и четвертых трехвходовых сумматоров второй ступени преобразования соединены со сдвигом на два разряда в сторону старших с информационными выходами трехвходового мультиплексора первого узла первой ступени преобразования, вторые информационные входы первого, второго, третьего и четвертого трехвходовых сумматоров j -й ступени преобразования,
 35 где $j=2 \dots n/2$, соединены с информационными выходами трехвходового мультиплексора j -го узла первой ступени преобразования, на третьи информационные входы первых, вторых, третьих и четвертых трехвходовых сумматоров j -й ступени преобразования, подаются соответственно инверсные коды модуля, инверсные коды удвоенного модуля, инверсные коды утроенного модуля и инверсные коды учетверенного модуля, на входы
 40 переноса всех трехвходовых сумматоров подается сигнал логической единицы, причем каждый трехвходовый сумматор содержит m полных одноразрядных сумматоров и $(m+1)$ -разрядный сумматор, $(1 \dots m)$ -й разряды информационных выходов которого являются информационными выходами трехвходового сумматора, а $(m+1)$ -й разряд является выходом переноса трехвходового сумматора, первые информационные входы
 45 полных одноразрядных сумматоров соединены с соответствующими разрядами первых информационных входов трехвходового сумматора, вторые информационные входы соединены с соответствующими разрядами вторых информационных входов трехвходового сумматора, третьи информационные входы соединены с

соответствующими разрядами третьих информационных входов трехвходового сумматора, информационные выходы $(1 \dots m)$ -го полных одноразрядных сумматоров соединены с $(1 \dots m)$ -м разрядами первых информационных входов $(m+1)$ -разрядного сумматора, а выходы переноса соединены с $(2 \dots m+1)$ -м разрядами вторых информационных входов $(m+1)$ -разрядного сумматора, первый разряд которых соединен со входом переноса трехвходового сумматора, на $(m+1)$ -й разряд первых информационных входов $(m+1)$ -разрядного сумматора подается сигнал логического нуля.

Сущность изобретения заключается в реализации следующего способа вычисления произведения чисел A и B по модулю P . Пусть

$$(A \cdot B) \equiv R \pmod{P}, \quad (1)$$

где A – неотрицательное целое число, являющееся множимым;

B – неотрицательное целое число, являющееся множителем, причем $B < P$;

P – неотрицательное целое число, называемое модулем;

R – неотрицательное целое число, являющееся остатком от произведения чисел A и B по модулю P , $R < P$.

При этом пусть

$$A = a_{n-1} \cdot 2^{n-1} + a_{n-2} \cdot 2^{n-2} + a_{n-3} \cdot 2^{n-3} + a_{n-4} \cdot 2^{n-4} + \dots + a_3 \cdot 2^3 + a_2 \cdot 2^2 + a_1 \cdot 2 + a_0, \quad (2)$$

$$B = b_{m-1} \cdot 2^{m-1} + \dots + b_1 \cdot 2 + b_0, \quad (3)$$

$$P = p_{m-1} \cdot 2^{m-1} + \dots + p_1 \cdot 2 + p_0, \quad (4)$$

$$R = r_{m-1} \cdot 2^{m-1} + \dots + r_1 \cdot 2 + r_0, \quad (5)$$

где $a_i, i = \overline{0, n-1}$ – коэффициенты, принимающие значение 0 или 1 в зависимости от значения числа A ;

n – количество разрядов в представлении множимого, n – четное;

$b_i, i = \overline{0, m-1}$ – коэффициенты, принимающие значение 0 или 1 в зависимости от значения числа B ;

$p_i, i = \overline{0, m-1}$ – коэффициенты, принимающие значение 0 или 1 в зависимости от значения модуля P ;

$r_i, i = \overline{0, m-1}$ – коэффициенты, принимающие значение 0 или 1 в зависимости от значения остатка R ;

m – количество разрядов в представлении множителя B , модуля P и остатка R .

Представим произведение чисел A и B следующим образом:

$$A \cdot B = (a_{n-1} \cdot 2^{n-1} + a_{n-2} \cdot 2^{n-2} + a_{n-3} \cdot 2^{n-3} + a_{n-4} \cdot 2^{n-4} + \dots + a_3 \cdot 2^3 + a_2 \cdot 2^2 + a_1 \cdot 2 + a_0) \cdot B. \quad (6)$$

Перепишем выражение (6) следующим образом:

$$A \cdot B = (a_{n-1} \cdot 2^{n-1} \cdot B + a_{n-2} \cdot 2^{n-2} \cdot B + a_{n-3} \cdot 2^{n-3} \cdot B + a_{n-4} \cdot 2^{n-4} \cdot B + \dots + a_3 \cdot 2^3 \cdot B + a_2 \cdot 2^2 \cdot B + a_1 \cdot 2 \cdot B + a_0 \cdot B), \quad (7)$$

Преобразуем выражение (7) в следующий вид, объединив по два соседних слагаемых:

$$A \cdot B = (a_{n-1} \cdot 2^{n-1} \cdot B + a_{n-2} \cdot 2^{n-2} \cdot B) + (a_{n-3} \cdot 2^{n-3} \cdot B + a_{n-4} \cdot 2^{n-4} \cdot B) + \dots + (a_3 \cdot 2^3 \cdot B + a_2 \cdot 2^2 \cdot B) + (a_1 \cdot 2 \cdot B + a_0 \cdot B), \quad (8)$$

Из каждой суммы в скобках в выражении (8) вынесем 2^i за скобки, где $i = \overline{0, n-2}$, принимает только четные значения:

$$A \cdot B = 2^{n-2}(a_{n-1} \cdot 2 \cdot B + a_{n-2} \cdot B) + 2^{n-4}(a_{n-3} \cdot 2 \cdot B + a_{n-4} \cdot B) + \dots \\ \dots + 2^2(a_3 \cdot 2 \cdot B + a_2 \cdot B) + (a_1 \cdot 2 \cdot B + a_0 \cdot B), \quad (9)$$

В выражении (9) перед каждой из $n/2$ образовавшихся сумм вида

($a_{i+1} \cdot 2 \cdot B + a_i \cdot B$), получаем множитель 2^i , где $i = \overline{0, n/2 - 2}$, принимает только четные значения.

Далее вынесем в (9) наименьшую ненулевую степень 2 за скобки:

$$A \cdot B = 2^2(2^{n-4}(a_{n-1} \cdot 2 \cdot B + a_{n-2} \cdot B) + 2^{n-6}(a_{n-3} \cdot 2 \cdot B + a_{n-4} \cdot B) + \dots \\ \dots + (a_3 \cdot 2 \cdot B + a_2 \cdot B)) + (a_1 \cdot 2 \cdot B + a_0 \cdot B), \quad (10)$$

Выполняя последовательно преобразование (10) $(n/2) - 2$ раз получим:

$$A \cdot B = 2^2(2^2 \dots (2^2(a_{n-1} \cdot 2 \cdot B + a_{n-2} \cdot B) + (a_{n-3} \cdot 2 \cdot B + a_{n-4} \cdot B)) + \dots \\ \dots + (a_3 \cdot 2 \cdot B + a_2 \cdot B)) + (a_1 \cdot 2 \cdot B + a_0 \cdot B), \quad (11)$$

где 2^2 встречается $(n/2) - 1$ раз.

Тогда выражение (1) может быть представлено в следующем виде:

$$A \cdot B \equiv (2^2(2^2 \dots (2^2(a_{n-1} \cdot 2 \cdot B + a_{n-2} \cdot B) + (a_{n-3} \cdot 2 \cdot B + a_{n-4} \cdot B)) + \dots \\ \dots + (a_3 \cdot 2 \cdot B + a_2 \cdot B)) + (a_1 \cdot 2 \cdot B + a_0 \cdot B)) \bmod P. \quad (12)$$

Из теории чисел известно, что операция приведения по модулю инвариантна к сложению и умножению, т. е. величина остатка не зависит от того, вычислен ли он от суммы (произведения) или от каждого слагаемого (сомножителя), а затем соответствующие частичные остатки просуммированы (перемножены) и от результата вычислен остаток по модулю.

Исходя из вышесказанного, выражение (12) может быть вычислено следующим образом.

Вначале на первой ступени преобразования одновременно в $(n/2)$ узлах вычисляют величины t_{1i} , $i = \overline{1, n/2}$:

$$t_{11} = (a_{n-1} \cdot 2 \cdot B + a_{n-2} \cdot B) \bmod P, \\ t_{12} = (a_{n-3} \cdot 2 \cdot B + a_{n-4} \cdot B) \bmod P, \quad (13) \\ \dots, \\ t_{1(n/2)} = (a_1 \cdot 2 \cdot B + a_0 \cdot B) \bmod P.$$

На второй ступени преобразования вычисляют величину

$$t_2 = (2^2 t_{11} + t_{12}) \bmod P. \quad (14)$$

Аналогичным образом производят вычисления на последующих ступенях преобразования.

На последней $(n/2)$ -й ступени преобразования вычисляют величину

$$t_{n/2} = (2^2 t_{n/2-1} + t_{1(n/2)}) \bmod P, \quad (15)$$

которая и является искомым произведением чисел A и B по модулю P .

Операция приведения по модулю P на первой ступени преобразования во всех узлах выполняется исходя из следующих соображений.

По определению величина множителя B лежит в диапазоне $0 \leq B \leq P-1$. Поэтому значение любой величины t_{1i} в (13) до приведения ее по модулю находится в диапазоне от 0 до $3P-3$.

Приведение по модулю величины t_{1i} , $i = \overline{1, n/2}$ осуществляется по следующим

правилам:

$$t_{1i} \pmod{P} = t_{1i}, \text{ если } 0 \leq t_{1i} < P, \quad (16)$$

$$t_{1i} \pmod{P} = t_{1i} - P, \text{ если } P \leq t_{1i} < 2P,$$

$$t_{1i} \pmod{P} = t_{1i} - 2P, \text{ если } 2P \leq t_{1i} \leq (3P - 3),$$

Условия попадания значения t_{1i} в один из указанных в (16) интервалов определяются значениями сигналов переноса на выходах переноса сумматоров, осуществляющих операцию вычитания ($t_{1i} - kP$), где $k=1, 2$ в соответствии с таблицей 1.

Таблица 1.

t_{1i}	$t_{1i} - P$	$t_{1i} - 2P$
$0 \leq t_{1i} < P$	0	0
$P \leq t_{1i} < 2P$	1	0
$2P \leq t_{1i} < (3P - 3)$	1	1

Таким образом, если значение сигналов переноса равно «1» на выходах переноса двух сумматоров, то $t_{1i} \pmod{P} = t_{1i} - 2P$, если значение сигнала переноса равно «1» на выходах переноса одного сумматора, то $t_{1i} \pmod{P} = t_{1i} - P$. Если значение сигналов переноса равно «0» на выходах переноса двух сумматоров, то тогда $t_i \pmod{P} = t_i$, т.е.

операция вычитания не выполняется.

Операция приведения по модулю P на второй и последующих ступенях преобразования выполняется следующим образом. Значение величин $t_i, i = \overline{2, n/2}$ в (14), (15) до приведения по модулю находится в диапазоне от 0 до $5P-5$.

Приведение по модулю P величины $t_i, i = \overline{2, n/2}$ осуществляется по следующим правилам

$$t_i \pmod{P} = t_i, \text{ если } 0 \leq t_i < P, \quad (17)$$

$$t_i \pmod{P} = t_i - P, \text{ если } P \leq t_i < 2P,$$

$$t_i \pmod{P} = t_i - 2P, \text{ если } 2P \leq t_i < 3P,$$

$$t_i \pmod{P} = t_i - 3P, \text{ если } 3P \leq t_i < 4P,$$

$$t_i \pmod{P} = t_i - 4P, \text{ если } 4P \leq t_i \leq (5P-5).$$

Условия попадания значения t_i в один из указанных в (17) интервалов определяются значениями сигналов переноса на выходах переноса сумматоров, осуществляющих операцию вычитания ($t_i - kP$), где $k=1, 2, 3, 4$ в соответствии с таблицей 2.

Таблица 2.

t_i	$t_i - P$	$t_i - 2P$	$t_i - 3P$	$t_i - 4P$
$0 \leq t_i < P$	0	0	0	0
$P \leq t_i < 2P$	1	0	0	0
$2P \leq t_i < 3P$	1	1	0	0
$3P \leq t_i < 4P$	1	1	1	0
$4P \leq t_i \leq (5P-5)$	1	1	1	1

Таким образом, если значение сигналов переноса равно «1» на выходах переноса всех четырех сумматоров, то $t_i \pmod{P} = t_i - 4P$, если значение сигналов переноса равно «1» на выходах переноса трех сумматоров, то

$$t_i \pmod{P} = t_i - 3P, \text{ если значение сигналов переноса равно «1» на выходах переноса}$$

двух сумматоров, то $t_i \pmod P = t_i - 2P$, если значение сигнала переноса равно «1» на выходах переноса одного сумматора, то

$t_i \pmod P = t_i - P$. Если значение сигналов переноса равно «0» на выходах переноса всех четырех сумматоров, то тогда $t_i \pmod P = t_i$, т.е. операция вычитания не выполняется.

В устройстве прототипе на каждой ступени преобразования приведение результатов вычисления по произвольному модулю по выражениям (13)-(15) выполняется за два шага – вначале выполняется операция суммирования промежуточных вычислений, а затем осуществляется приведение полученного значения по модулю. В предлагаемом устройстве операция суммирования промежуточных вычислений и операция приведения по модулю выполняются одновременно.

Краткое описание чертежей

На фиг. 1 представлена схема умножителя по модулю.

Умножитель по модулю содержит входы кодов множимого 7, входы кодов множителя 6, выходы кодов произведения 8, $n/2$ ступеней преобразования, где n - разрядность кода множимого. Первая ступень преобразования содержит $n/2$ узлов включающих n ключей 1, $n/2$ сумматоров 2, n трехвходовых сумматоров 3 и $n/2$ трехвходовых мультиплексоров 4. Вторая и последующая ступени преобразования содержат каждая сумматор 2, четыре трехвходовых сумматора 3 и пятивходовый мультиплексор 5. Управляющие входы ключей 1 соединены с соответствующими разрядами входов кода множимого 7, а информационные входы соединены со входами кода множителя 6. Информационные выходы первого ключа 1 каждого узла первой ступени преобразования соединены со сдвигом на один разряд в сторону старших с первыми информационными входами сумматора 2, а также первого и второго трехвходовых сумматоров 3 этого же узла. Информационные выходы второго ключа 1 каждого узла первой ступени преобразования соединены со вторыми информационными входами сумматора 2 и первого и второго трехвходовых сумматоров 3. На третьи информационные входы первых трехвходовых сумматоров 3 подается инверсный код модуля, а на третьи информационные входы вторых трехвходовых сумматоров подается инверсный код удвоенного модуля. Информационные выходы сумматора 2 каждого узла первой ступени преобразования соединены с первыми информационными входами трехвходового мультиплексора 4. Информационные выходы первых трехвходовых сумматоров 3 соединены со вторыми информационными входами соответствующих трехвходовых мультиплексоров 4, информационные выходы вторых трехвходовых сумматоров 3 соединены с третьими информационными входами соответствующих трехвходовых мультиплексоров 4, выходы переноса первых трехвходовых сумматоров 3 соединены с первыми управляющими входами соответствующих трехвходовых мультиплексоров 4, выходы переноса вторых трехвходовых сумматоров 3 соединены со вторыми управляющими входами соответствующих трехвходовых мультиплексоров 4. Информационные выходы трехвходового мультиплексора 4 первого узла первой ступени преобразования соединены со сдвигом на два разряда в сторону старших с первыми информационными входами сумматора 2, первого, второго, третьего и четвертого трехвходовых сумматоров 3 второй ступени преобразования. Информационные выходы трехвходового мультиплексора 4 j -го узла первой ступени преобразования, где $j=2, \dots, n/2$, соединены со вторыми информационными входами сумматора 2, первого, второго, третьего и четвертого трехвходовых сумматоров 3 j -й ступени преобразования. На третьи информационные входы первого, второго, третьего и четвертого трехвходовых сумматоров 3 j -й ступени преобразования, подаются

соответственно инверсные коды модуля, инверсные коды удвоенного модуля, инверсные коды утроенного модуля и инверсные коды учетверенного модуля. На входы переноса трехвходовых сумматоров 3 всех ступеней преобразования подается сигнал логической единицы. Информационные выходы сумматора 2, первого, второго, третьего и четвертого трехвходовых сумматоров 3 j -й ступени преобразования, соединены соответственно с первым, вторым, третьим, четвертым и пятым информационными входами пятивходового мультиплексора 5 этой же ступени преобразования, а выходы переносов первого, второго, третьего и четвертого трехвходовых сумматоров 3 соединены соответственно с первым, вторым, третьим и четвертым управляющими входами пятивходового мультиплексора 5. Информационные выходы пятивходового мультиплексора 5 j -й ступени преобразования, где $j=2, \dots, n/2-1$, соединены со сдвигом на два разряда в сторону старших с первыми информационными входами сумматора 2, первого, второго, третьего и четвертого трехвходовых сумматоров 3 $(j+1)$ -й ступени преобразования. Информационные выходы пятивходового мультиплексора 5 $n/2$ -й ступени преобразования соединены с выходами кодов произведения 8 устройства.

На фиг. 2 представлена схема трехвходового сумматора.

Трехвходовый сумматор содержит m полных одноразрядных сумматоров $9.1 \div 9.m$ и $(m+1)$ -разрядный сумматор 10, $(1 \dots m)$ -й разряды информационных выходов которого являются информационными выходами трехвходового сумматора 3, а $(m+1)$ -й разряд является выходом переноса трехвходового сумматора 3. Первые, вторые и третьи информационные входы полных одноразрядных сумматоров $9.1 \div 9.m$ соединены с соответствующими разрядами первых, вторых и третьих информационных входов трехвходового сумматора 3. Информационные выходы полных одноразрядных сумматоров $9.1 \div 9.m$ соединены соответственно с $(1 \dots m)$ -м разрядами первых информационных входов $(m+1)$ -разрядного сумматора 10, а выходы переноса соединены соответственно со $(2 \dots m+1)$ -м разрядами вторых информационных входов $(m+1)$ -разрядного сумматора 10, первый разряд которых соединен со входом переноса трехвходового сумматора 3. На $(m+1)$ -й разряд первых информационных входов $(m+1)$ -разрядного сумматора 10 подается сигнал логического нуля.

30 **Осуществление изобретения.**

Умножитель по модулю работает следующим образом (см. Фиг. 1).

На вход 7 устройства подается n -разрядный двоичный код множимого A . На вход 6 устройства подается m -разрядный код множителя B . На третьи информационные входы первых и вторых трехвходовых сумматоров 3 первой ступени преобразования подается инверсный код модуля и соответственно инверсный код удвоенного модуля. На входы переноса первых и вторых трехвходовых сумматоров 3 всех узлов первой ступени преобразования подается логическая единица. На третьи информационные входы первых, вторых, третьих и четвертых трехвходовых сумматоров 3 второй и последующих ступеней преобразования подается соответственно инверсный код модуля, инверсный код удвоенного модуля, инверсный код утроенного модуля и инверсный код учетверенного модуля.

Вначале на первой ступени преобразования одновременно в $(n/2)$ узлах вычисляют величины t_{1i} $i = \overline{1, n/2}$, где i – номер узла:

$$\begin{aligned} t_{11} &= (a_{n-1} \cdot 2 \cdot B + a_{n-2} \cdot B) \bmod P, \\ t_{12} &= (a_{n-3} \cdot 2 \cdot B + a_{n-4} \cdot B) \bmod P, \\ &\dots, \\ t_{1(n/2)} &= (a_1 \cdot 2 \cdot B + a_0 \cdot B) \bmod P. \end{aligned}$$

Умножение разрядов множимого a_i на множитель B осуществляется с помощью ключей 1. Умножение множителя B на 2 осуществляется путем сдвига разрядов на один в сторону старших с информационных выходов первых ключей 1 каждого узла при подключении к первым информационным входам сумматоров 2, первым
 5 информационным входам первых и вторых трехвходовых сумматоров 3 соответствующего узла. Параллельно сумматор 2, первый и второй трехвходовые сумматоры 3 каждого узла первой ступени преобразования осуществляют суммирование значений $a_i \cdot 2 \cdot B$ и $a_{i-1} \cdot B$, а первый и второй трехвходовые сумматоры 3 еще приводят
 10 получившиеся суммы по модулю путем одновременного вычитания из нее значений P и $2P$ и трехвходового мультиплексора 4 соответствующего узла, осуществляющего коммутацию на выходы, поступивших на его информационные входы значений сигналов переноса, в соответствии с таблицей 1.

В результате на выходах всех узлов первой ступени преобразования образуются значения t_{1i} , $i = \overline{1, n/2}$ в соответствии с выражением (13).
 15

На второй ступени преобразования осуществляется вычисление значения $t_2 = (2^2 t_{11} + t_{12}) \bmod P$, где t_{11} и t_{12} значения на выходах первого и второго узла первой ступени преобразования. Умножение значения t_{11} на 2^2 осуществляется сдвигом разрядов кода
 20 t_{11} на два в сторону старшего. Приведение по модулю P осуществляется аналогичным образом путем одновременного вычитания из суммы значений модуля, удвоенного модуля, утроенного модуля и учетверенного модуля и выбором окончательного значения с помощью пятивходового мультиплексора 4 в зависимости от управляющих сигналов, подаваемых на его вход в соответствии с таблицей 2. Операция вычитания
 25 осуществляется с помощью соответствующих трехвходовых сумматоров 3 на третьи информационные входы которых подается в инверсном виде код соответствующих значений модуля, а на вход переноса подается сигнал логической единицы, преобразуя инверсный код в дополнительный.

Трехвходовый мультиплексор 4 в зависимости от комбинаций сигналов на его
 30 управляющих входах, коммутирует на свой выход сигнал с одного из своих трех информационных входов. Пятивходовый мультиплексор 5 в зависимости от комбинаций сигналов на его управляющих входах, коммутирует на свой выход один из своих пяти информационных входов в соответствии с таблицей 2.

Трехвходовые сумматоры 3 (см. Фиг. 2) суммируют коды чисел, поступающие на их
 35 первые и вторые информационные входы и одновременно вычитают из этой суммы коды чисел, поступающие на их третьи информационные входы. Так как на входы переноса этих сумматоров подается сигнал логической единицы, а на третьи информационные входы поступают инверсные коды значений модуля (удвоенного модуля, утроенного модуля или учетверенного модуля), то в результате образуются
 40 соответствующие дополнительные коды, которые и приводят к реализации операции вычитания. На выходах каждого из m полных одноразрядных сумматоров $9.1 \div 9.m$ трехвходовых сумматоров 3 формируется сигнал частичной суммы и сигналы сквозного переноса трех чисел, поступающих на их входы. В результате на информационных
 45 выходах полных одноразрядных сумматоров $9.1 \div 9.m$ образуются поразрядные сигналы частичной суммы, а на выходах переноса образуются поразрядные сигналы сквозного переноса. Сигналы частичной суммы с информационных выходов полных одноразрядных сумматоров $9.1 \div 9.m$ поступают на $(1, \dots, m)$ -й разряды первых информационных входов $(m+1)$ -разрядного сумматора 10, на $(m+1)$ -й разряд которого

подается сигнал логического нуля. Сигналы с выходов переноса полных одноразрядных сумматоров $9.1 \div 9.m$ поступают на $(2, \dots, (m+1))$ -й разряды вторых информационных входов $(m+1)$ -разрядного сумматора 10, на первый разряд которого поступает сигнал логической единицы, преобразуя инверсный код модуля в дополнительный. В результате на $(1, \dots, m)$ -ом разрядах информационных выходов $(m+1)$ -разрядного сумматора 10 образуется значение суммы в соответствии с (13), (14) или (15), причем значение формируемое на $(m+1)$ -м разряде информационных выходов $(m+1)$ -разрядного сумматора 10 является сигналом переноса.

Аналогичные вычисления производятся и на последующих ступенях преобразования. В результате этих вычислений на выходе последней $(n/2)$ -й ступени преобразования образуется значение произведения чисел A и B по модулю P .

Так как на каждой ступени преобразования осуществляется обработка одновременно двух разрядов множимого, то через $(n/2)$ шагов преобразований на выходе кода произведения 8 устройства сформируется двоичный код произведения чисел A и B по модулю P . При этом приведение результатов вычисления по произвольному модулю на каждой ступени преобразования выполняется за один шаг, одновременно с операцией суммирования промежуточных вычислений, что повышает быстродействие устройства.

Источники информации

1. Умножитель на два по модулю. Патент РФ №2015537, МПК G06F 7/49 (1990.01), опубл. 30.06.1994.

2. Устройство для умножения чисел по произвольному модулю. Патент РФ №2316042, МПК G06F 7/523 (2006.01), G06F 7/72 (2006.01), опубл. 27.01.2008. Бюл. № 3.

3. Умножитель по модулю. Патент РФ №2751802, МПК G06F 7/72 (2006.01), G06F 7/523 (2006.01), опубл. 19.07.2021. Бюл. № 20.

(57) Формула изобретения

Умножитель по модулю, содержащий входы кодов множимого, входы кодов множителя, выходы кодов произведения, $n/2$ ступеней преобразования, где n - разрядность устройства, причем первая ступень преобразования содержит $n/2$ узлов, а $(2 \dots n/2)$ -е ступени преобразования содержат по одному узлу, каждый узел преобразования первой ступени преобразования содержит первый и второй ключи, двухвходовый сумматор и трехвходовый мультиплексор, а узлы преобразования $(2 \dots n/2)$ -й ступеней преобразования содержат двухвходовые сумматоры и пятивходовые мультиплексоры, информационные входы всех ключей первой ступени преобразования соединены со входами кода множителя, управляющие входы соединены с соответствующими разрядами кода множимого, информационные выходы первых ключей каждого узла первой ступени преобразования соединены с первыми информационными входами соответствующих двухвходовых сумматоров со сдвигом на один разряд в сторону старших, информационные выходы вторых ключей каждого узла первой ступени преобразования соединены со вторыми информационными входами соответствующих двухвходовых сумматоров, информационные выходы двухвходовых сумматоров соединены с первыми информационными входами соответствующих трехвходовых мультиплексоров, информационные выходы трехвходового мультиплексора первого узла первой ступени преобразования соединены со сдвигом на два разряда в сторону старших с первыми информационными входами двухвходового сумматора второй ступени преобразования, информационные выходы трехвходовых мультиплексоров j -го узла первой ступени преобразования, где $j=2 \dots n/2$, соединены со вторыми информационными входами двухвходовых сумматоров j -й ступени

преобразования, информационные выходы двухвходовых сумматоров j -й ступени преобразования соединены с первыми информационными входами соответствующих пятивходовых мультиплексоров, информационные выходы пятивходовых мультиплексоров j -й ступени преобразования, где $j=2, \dots, n/2-1$, соединены со сдвигом на два разряда в сторону старших с первыми информационными входами двухвходовых сумматоров $(j+1)$ -й ступени преобразования, а $n/2$ -й ступени преобразования являются выходами кодов произведения, отличающийся тем, что в него введены на первой ступени преобразования в каждый узел первый и второй трехвходовые сумматоры, а на $(2 \dots n/2)$ -й ступени преобразования введены первый, второй, третий и четвертый трехвходовые сумматоры, причем первые информационные входы первых и вторых трехвходовых сумматоров первой ступени преобразования соединены с информационными выходами первых ключей соответствующего узла со сдвигом на один разряд в сторону старших, вторые информационные входы соединены с информационными выходами вторых ключей соответствующего узла, на третьи информационные входы первых трехвходовых сумматоров подается инверсный код модуля, а на третьи информационные входы вторых трехвходовых сумматоров подается инверсный код удвоенного модуля, информационные выходы первых трехвходовых сумматоров соединены со вторыми информационными входами соответствующих трехвходовых мультиплексоров, информационные выходы вторых трехвходовых сумматоров соединены с третьими информационными входами соответствующих трехвходовых мультиплексоров, выходы переноса первых трехвходовых сумматоров соединены с первыми управляющими входами соответствующих трехвходовых мультиплексоров, выходы переноса вторых трехвходовых сумматоров соединены со вторыми управляющими входами соответствующих трехвходовых мультиплексоров, первые информационные входы первых, вторых, третьих и четвертых трехвходовых сумматоров второй ступени преобразования соединены со сдвигом на два разряда в сторону старших с информационными выходами трехвходового мультиплексора первого узла первой ступени преобразования, вторые информационные входы первого, второго, третьего и четвертого трехвходовых сумматоров j -й ступени преобразования, где $j=2 \dots n/2$, соединены с информационными выходами трехвходового мультиплексора j -го узла первой ступени преобразования, на третьи информационные входы первых, вторых, третьих и четвертых трехвходовых сумматоров j -й ступени преобразования подаются соответственно инверсные коды модуля, инверсные коды удвоенного модуля, инверсные коды утроенного модуля и инверсные коды учетверенного модуля, на входы переноса всех трехвходовых сумматоров подается сигнал логической единицы, причем каждый трехвходовый сумматор содержит m полных одноразрядных сумматоров и $(m+1)$ -разрядный сумматор, $(1 \dots m)$ -й разряды информационных выходов которого являются информационными выходами трехвходового сумматора, а $(m+1)$ -й разряд является выходом переноса трехвходового сумматора, первые информационные входы полных одноразрядных сумматоров соединены с соответствующими разрядами первых информационных входов трехвходового сумматора, вторые информационные входы соединены с соответствующими разрядами вторых информационных входов трехвходового сумматора, третьи информационные входы соединены с соответствующими разрядами третьих информационных входов трехвходового сумматора, информационные выходы $(1 \dots m)$ -го полных одноразрядных сумматоров соединены с $(1 \dots m)$ -м разрядами первых информационных входов $(m+1)$ -разрядного сумматора, а выходы переноса соединены с $(2 \dots m+1)$ -м разрядами вторых информационных входов $(m+1)$ -разрядного сумматора, первый разряд которых соединен

со входом переноса трехвходового сумматора, на $(m+1)$ -й разряд первых информационных входов $(m+1)$ -разрядного сумматора подается сигнал логического нуля.

5

10

15

20

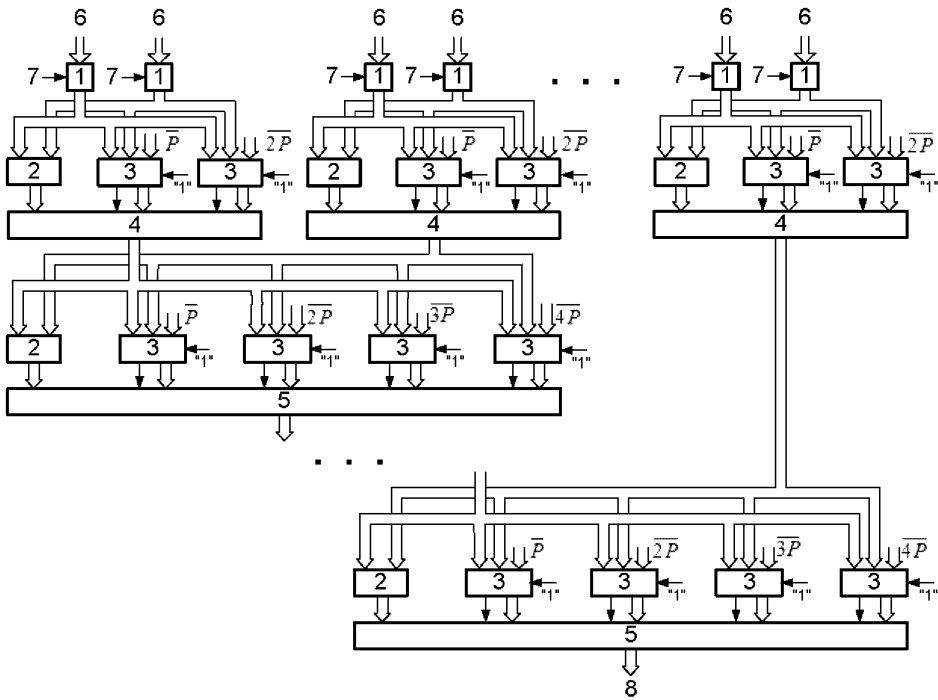
25

30

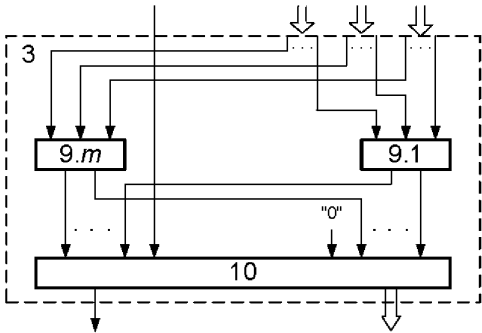
35

40

45



Фиг. 1



Фиг. 2