РЕСПУБЛИКА КАЗАХСТАН

(19) **KZ** (13) **B** (11) **35765**
(51) ***G06F 7/52*** (2006.01)
G05F 7/535 (2006.1)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ИЗОБРЕТЕНИЯ
К ПАТЕНТУ

(21) 2022/0270.1
(22) 03.05.2022
(45) 15.07.2022, бюл. №28
(76) Тынымбаев Сахыбай
(56) KZ 35623 B, 21.02.2022;
SU 1633495 A1, 07.03.1991;
SU 736095 A1, 25.05.1980;
KZ 30983 A4, 15.03.2016

А.А. Джуманов, Быстродействующее устройство приведения числа по модулю на трехсумматорном формирователе частичных остатков, НАО АУЭС, 2019 г.

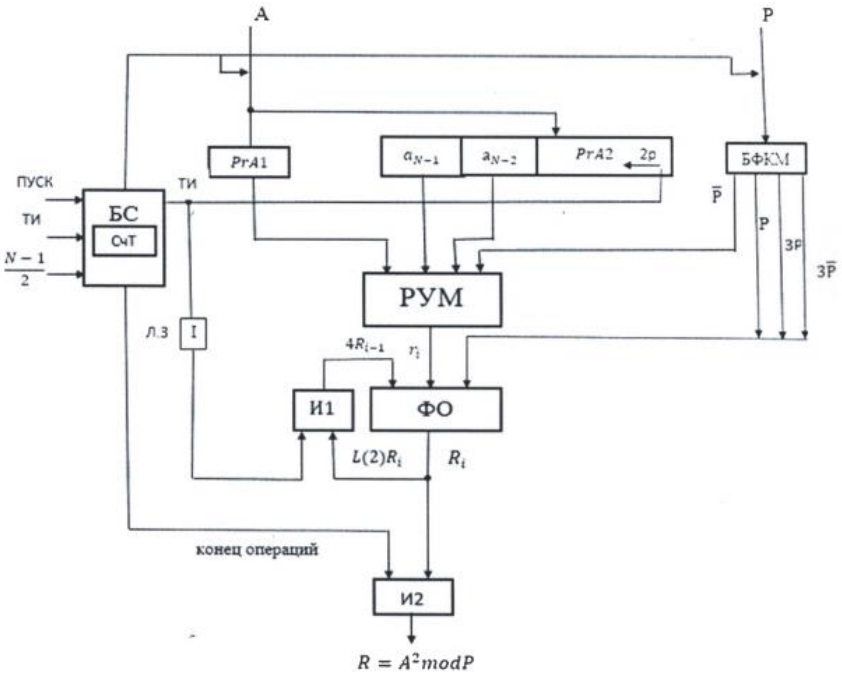
(54) **БЫСТРОДЕЙСТВУЮЩЕЕ УСТРОЙСТВО МОДУЛЬНОГО ВОЗВЕДЕНИЯ ЧИСЕЛ В КВАДРАТ**

(57) Изобретение относится к вычислительной технике и может быть использовано в устройствах для формирования элементов конечных полей в криптографических приложениях.

Для построения устройства модульного возведения чисел в квадрат в состав устройства входят регистры РгА1 и сдвигающий регистр РгА2 с цепями сдвига влево на два разряда влево, блок формирователя кратных модулю (БФКМ), разрядный умножитель по модулю (РУМ), где формируются текущие остатки $r_i = (2A \cdot a_i + A \cdot a_{i-1})$ modP. ФО исходя из значений остатки r_i $4R_{i-1}$ и кратных модулей Р, $\overline{P}$ и 2Р, $2\overline{P}$ и 3Р, $3\overline{P}$ формирует частичный остаток исходя из соотношения $R_i = (4R_{i-1} + r_i)$modP.

Техническим результатом предложенных схемных решений является повышение быстродействия устройства модульного возведения в квадрат два раза.

(19) KZ (13) B (11) 35765



Фигура 1

Изобретение относится к вычислительной технике и может быть использовано в устройствах для формирования элементов конечных полей в криптографических приложениях.

Прототипом служит «Устройство модульного возведения в квадрат [Патент KZ №35623, опубликован 22.04.2022 бюллетень №16, МПК G06F 7/72]. В состав устройства входят регистры РгА1 и РгА2, где хранятся разряды возводимого числа А в квадрат, регистр РгР для хранения модуля Р, сумматор СМ1 для суммирования предыдущего остатка с числом А, также формирователь остатка ФО и регистр остатка РгR, блоки логических схем И1÷И5, блок синхронизаций БС.

Недостатком такого устройства является низкое быстродействие. Для модульного возведения числа А в квадрат потребуются N тактовых импульсов.

Технической задачей изобретения является разработка быстродействующего устройства модульного возведения в квадрат.

Техническим результатом является построение устройства модульного возведения чисел в квадрат, где результат формируется за N/2 тактов.

Для достижения технического результата в состав устройства вводится блок разрядного умножителя по модулю (РУМ) и в блок формирователя остатков ФО вводятся дополнительный двоичный сумматор и схема сравнения.

На фигуре 1 приведена функциональная схема быстродействующего модульного возведения чисел в квадрат. В состав устройства входят регистры для числа А РгА1 и РгА2. Регистр РгА2 имеет цепи сдвига влево на два разряда, блок формирования кратных модулю Р, 3Р, $3\overline{P}$ (БФКМ), разрядный умножитель по модулю (РУМ), формирователь остатков (ФО), имеющий в своем составе регистр для хранения текущих остатков РгR, блоки логических схем И1 и И2, линия задержки ЛЗ, блок синхронизации БС, в состав которого входит вычитающий счетчик тактовых импульсов СчТИ. На входы БС подается сигнал «ПУСК», тактовые импульсы ТИ, двоичный код числа сдвигов $\frac{N-1}{2}$. На выходах БС формируются очередные тактовые импульсы и сигнал «Конец операций».

На фигуре 2 приведена функциональная схема РУМ, который состоит из сумматоров СМ1 и СМ2, блоков схем И1 и И2, И5 и И6, блока схемы ИЛИ1, а также схем ИЛИ2, И3, И4. На входы блоков схемы И1, И2 из РгА2 подаются значения битов a_i и a_{i-1}.

На входы блока схем И1 подается значение А из регистра РгА со сдвигом на один разряд в сторону старших разрядов, а на второй вход схемы И1 подается значение a_i из регистра РгА2. На вход схемы И2 подается значение А из регистра РгА без сдвига, а на второй вход схемы И2 подается значение бита a_{i-1}. При этом на выходе СМ1 формируется сумма на формуле $S_{CM1}=L(1)A\cdot a_i+ A\cdot a_{i-1}$. При $a_i=a_{i-1}=1$ $S_{CM1}=2A+A=3A$. При значении $a_i=1$ $a_{i-1}=0$, $S_{CM1}=2A$. При значении $a_i=0$ $a_{i-1}=1$, то $S_{CM1}=A$ и при $a_i=a_{i-1}=0$ $S_{CM1}=0$. Значение S_{CM1} подается на левые входы сумматора СМ2, где осуществляется вычитание из S_{CM1} значение модуля 2Р или Р в зависимости от сочетания битов a_i и a_{i-1}, тем самым осуществляется приведение числа S_{CM1} по модулю Р. При $a_i=1$ и $\overline{a}_{i-1}=1$ схема И3 вырабатывает единичный сигнал, который разрешает схеме И5 значение $2\underline{P}$ передать на правые входы сумматора СМ2. При этом в сумматоре СМ2 выполняется операция $r_i=S_{CM1}+2\overline{P}+1$, где сигнал +1 поступает из выхода схемы ИЛИ2.

При значении $a_i = 1$ и $a_{i-1} = 1$ схемы И4 выработает единичный сигнал, который позволит переключении значения модуля $\overline{P}$ с схемы И6 на правые входы сумматора СМ2. При этом сумматором СМ2 выполняется операция $r_i= S_{CM1} + \overline{P} + 1$.

На фигуре 3 приведена функциональная схема формирователя остатков ФО, который состоит из сумматоров СМ3 и СМ4, схем сравнения СС-1, СС-2 и СС-3, блоков схем И1÷И5 и И7÷И12 блоков схем ИЛИ1, ИЛИ2, ИЛИ4, ИЛИ5, схем И6 и ИЛИ3.

На правые входы сумматора СМ3 подается из РУМ значение остатка r_i, а на левые входы с выходов регистра остатка РгR подается R_{i-1} со сдвигом на два разряда – $4R_{i-1}$ и на выходе СМ3 получим $Si=4R_{i-1}+r_i$, который приводится по модулю Р.

Для приведения числа S_i по модулю Р необходимо выработать управляющие сигналы с помощью которых осуществляется передача на правые входы сумматора СМ4 значение одного из кратных $4\overline{P}$, $3\overline{P}$, $2\overline{P}$ или $\overline{P}$. Для этого S_i сравнивается со значениями кратких модулю 4Р, 3Р, 2Р, Р на схемах сравнения СС-1, СС-2. При этом S_i подается на левые входы схем сравнений СС-3, СС-2, СС-1. На схеме СС-1 сравнивается S_i со значениями Р либо 3Р, на схеме СС-2 S_i сравнивается со значениями 4Р либо 2Р. Выбор для сравнения одного из Р либо 3Р и 4Р либо 2Р определяется в результате сравнения S_i со значениями 3Р на схеме сравнения СС-3. При сравнении S_i с 3Р, если $S_i<3P$, то на выходе 1 СС-3 формируется сигнал “1”, который подается на левые входы блока схем И1 и И3. При этом на правые входы СС-1 и СС-2 поступают соответственно значения Р и 2Р, которые сравниваются со значением S_i.

При сравнении S_i с 3Р, если $S_i\geq3P$, то на выходе 2 СС-3 формируется единичный сигнал, который через схемы И2 и И4 обеспечивает подключение значений 3Р и 4Р соответственно на правые входы СС-1 и СС-2. При этом на схеме СС-1 S_i сравнивается со значением модуля 3Р, а на схеме СС-2 Si сравнивается со значением модуля 4Р.

При сравнении S_i с Р на СС-1, если $S_i<P$, то на его выходе “1” формируется сигнал “1”, который блоком схем значение S_i через блока схем ИЛИ5 передается на вход регистра остатка РгR. При этом $R_i= S_i\text{mod}P=S$.

При сравнении S_i с Р на СС-1, если $S_i\geq P$, то на его выходе 2 формируется единичный сигнал, который передается на вход логической схемы И6.

При сравнении S_i со значением 2Р на схеме СС-2, (при этом $S_i<3P$) если $S_i<2P$, то на его выходе 1 формируется единичный сигнал, который передается на вход схемы И6. На выходе И6

формируется управляющий сигнал, который (при наличии единичного сигнала с выхода 1 СС-2) переключает значение $\overline{P}$ на правые входы СМ4. При этом выполняется операция $R_i = S_i + \overline{P} + 1$.

При сравнении S_i с 2P, если $S_i \geq 2P$, то на его выходе 2 схемы сравнения СС-2 вырабатывается сигнал 1 и при наличии сигнала с выхода 1 СС-3 значение $2\overline{P}$ передается на вход сумматора СМ4, где выполняется операция $R_i = S_i + 2\overline{P} + 1$.

При сравнении S_i со значением 3P на схеме СС-1, если $S_i \geq 3P$, то на его выходе 2 формируется единичный сигнал, который передается на вход схемы И6.

При сравнении S_i со значением 4P на схеме СС-2, если выполняется условие $r_i < 4P$ на выходе 1 СС-2 формируется единичный уровень, то он подается на второй вход схемы И6 при этом высокий уровень с выхода И6 подается на вход блока схем И9 на другие входы подведены “1” сигнал с выхода 2 СС-3 и значение $3\overline{P}$. При этом с выхода схем И9 на правые входы СМ4 подается значение $3\overline{P}$ и сумматором выполняется операция $R_i = S_i + 3\overline{P} + 1$.

При сравнении S_i со значением 4P выполняется условие $r_i \geq 4P$, то с выхода 2 СС-2 единичный сигнал подается на вход блока схем И10. На остальной вход подается значение $4\overline{P}$ и единичный сигнал с выхода 2 схемы СС-3. При этом в сумматоре СМ4 выполняется операция $R_i = S_i + 4\overline{P} + 1$ и результат R_i принимается в регистр РгR. Очередным тактовым импульсом ТИ остаток R_i со сдвигом на два разряда подается на правые входы сумматора СМ3 либо сигналом “Конец операций” выдается на выход схемы.

Рассмотрим работу быстродействующего устройства модульного возведения чисел в квадрат.

По сигналу “Пуск” двоичный код числа сдвигов принимается в счетчик тактовых сигналов и принимает операнд А в регистры РгА1 и РгА2. Значение модуля Р принимается в блок формирования кратных по модулю Р (БФКМ), где формируется значение 3P и $3\overline{P}$. После приема операндов содержимое регистра РгА1 и старшие разряды a_{N-1} a_{N-2} из регистра Рг2 подаются в РУМ. В РУМ также подается из значение $\overline{P}$. Внутри РУМ из модуля $\overline{P}$ формируется $2\overline{P}$ путем сдвига $\underline{P}$ на один разряд влево. В РУМ формируется $r_i = (L(1)A \cdot a_{N-1} + A \cdot a_{i-1}) \bmod P$. Далее значение r_i подается на вход ФО. Поскольку на первом шаге $R_i = 0$, то $R_1 = r_1 \bmod P = r_1$, который запоминается в регистре остатка РгR. После чего БС выдает в схему тактовый импульс ТИ1, который сдвигает разряды регистра РгА2 на два разряда влево. При этом в операцию вступают биты a_{N-3} a_{N-4} и содержимое регистра РгА1. В РУМ формируется r_2. Тактовый сигнал также вычитает единицу из показания счетчика СТИ и задерживает тактовый сигнал на время формирования r_i в РУМ и передает содержимое регистра остатка РгR со сдвигом на два разряда влево в ФО. В ФО формируется R_2. Аналогично формируются R_3, R_4 ...

После поступления тактового импульса ТИ $\frac{N-1}{2}$ содержимое регистра РгА2 сдвигается на два разряда влево и в РУМ принимается число А из РгА1 и младшие разряды из регистра РгА2 и в РУМ формируется остаток r_{N-1}, который подается в ФО. На вход ФО подается остаток из регистра РгR со сдвигом на два разряда влево. В регистре РгR формируется остаток $R_{\frac{N-1}{2}}$. После поступления последнего тактового импульса СчТИ обнуляется и БС выработает сигнал “Конец операции”, который выдает содержимое РгR на выход через блок схем И2.

Рассмотрим пример выполнения операций $R = A^2 \bmod P$.

Пусть $A = 54_{10} = \{\overset{a_5\ a_4\ a_3\ a_2\ a_1\ a_0}{1\ 1\ 0\ 1\ 1\ 0}_2$; P=63; N=6.

Вычисления в десятичной системе приведен в таблице 1.

Таблица 1.

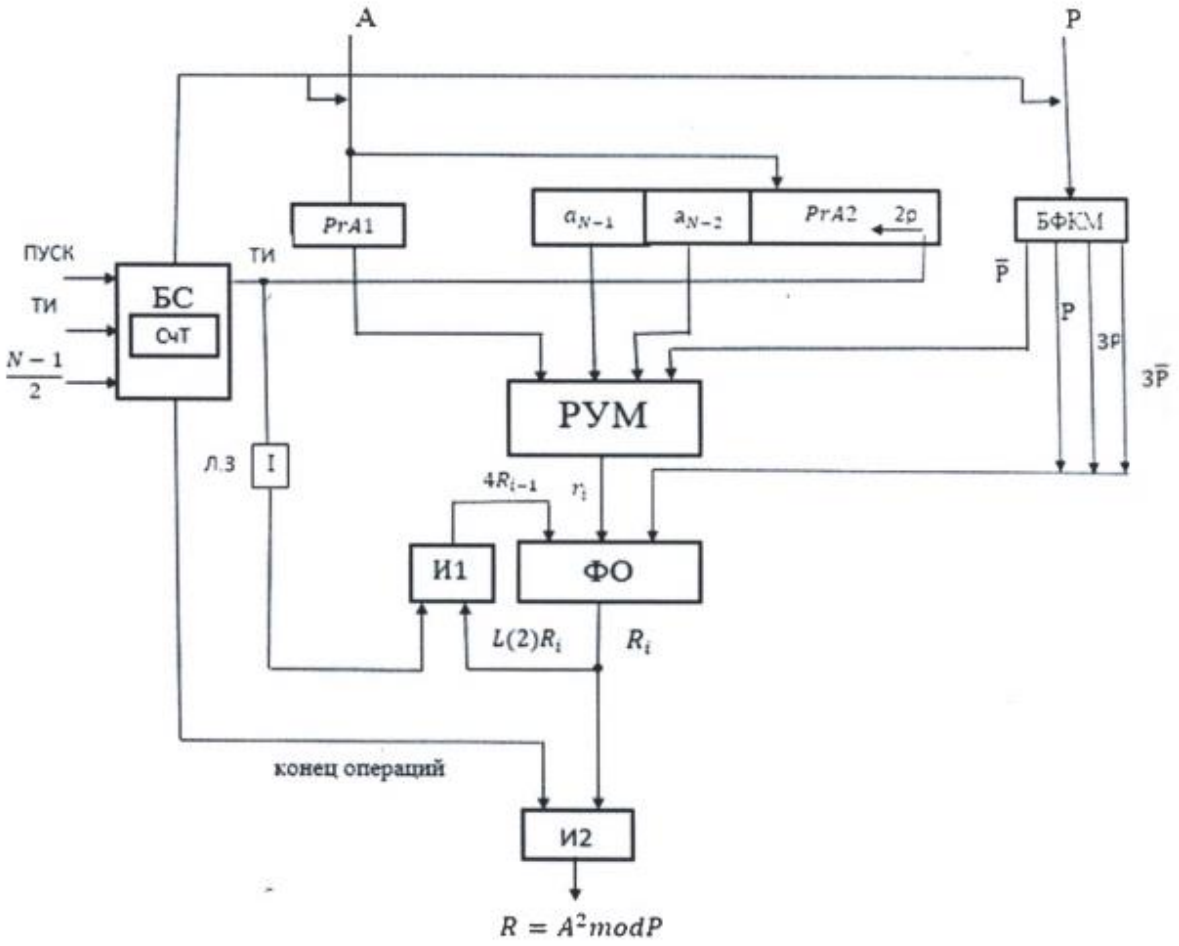
Последовательность вычисления $R = A^2 \bmod P$

ТИ	$a_i\ a_{i-1}$	РУМ	ФО
ПУСК	$a_5=1$ $a_4=1$	$r_1 = (2A \cdot a_5 + A \cdot a_4) \bmod P = 3A \bmod 63 = 162 \bmod 63 =$ 36;	$R_1 = (4R_0 + r_1) \bmod 63 =$ $(0+r_1) \bmod 63 = 36$
ТИ1	$a_3=0$ $a_2=1$	$r_2 = (2A \cdot a_3 + A \cdot a_2) \bmod P = A \bmod 63 = 54$;	$R_2 = (4R_1 + r_2) \bmod 63 =$ $(144+54) \bmod 63 = 9$
ТИ2	$a_1=1$ $a_0=0$	$r_3 = (2A \cdot a_1 + A \cdot a_0) \bmod P = 2A \bmod 63 = 108 \bmod 63 =$ 45	$R_3 = (4R_2 + r_3) \bmod 63 =$ $(36+45) \bmod 63 = 18$

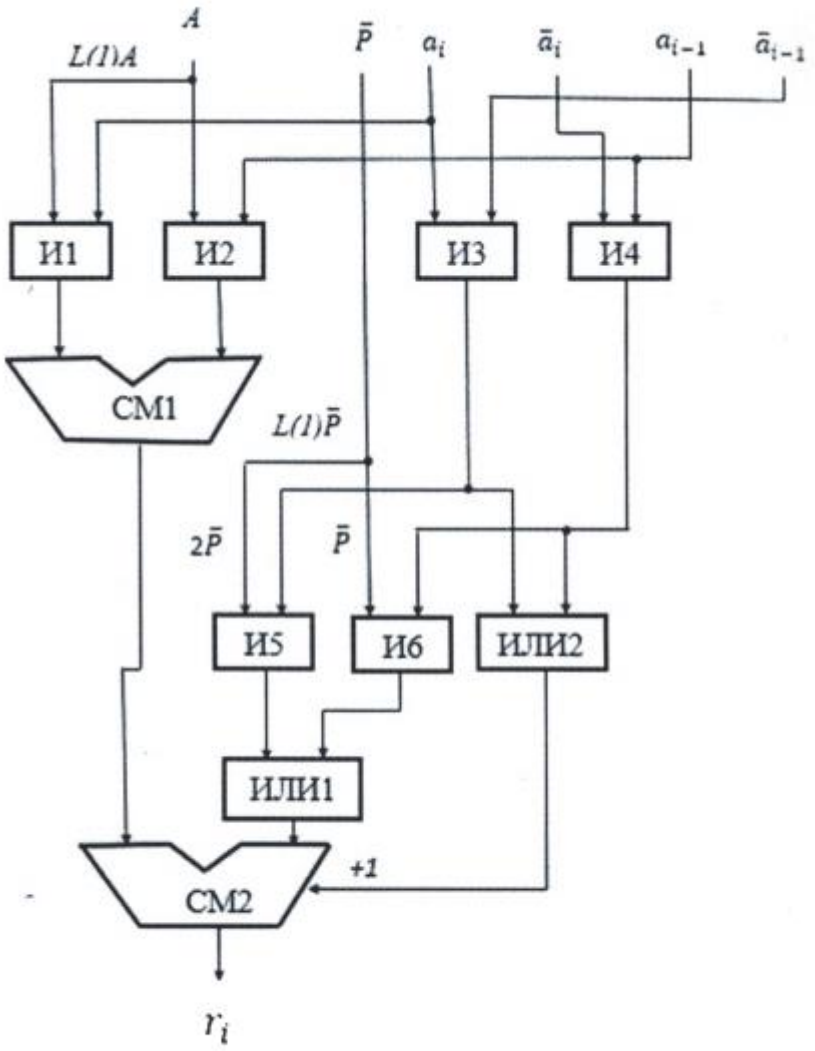
Проверка: $R = A^2 \bmod P = 54^2 \bmod 63 = 2916 \bmod 63 = 18_{10}$.

ФОРМУЛА ИЗОБРЕТЕНИЯ

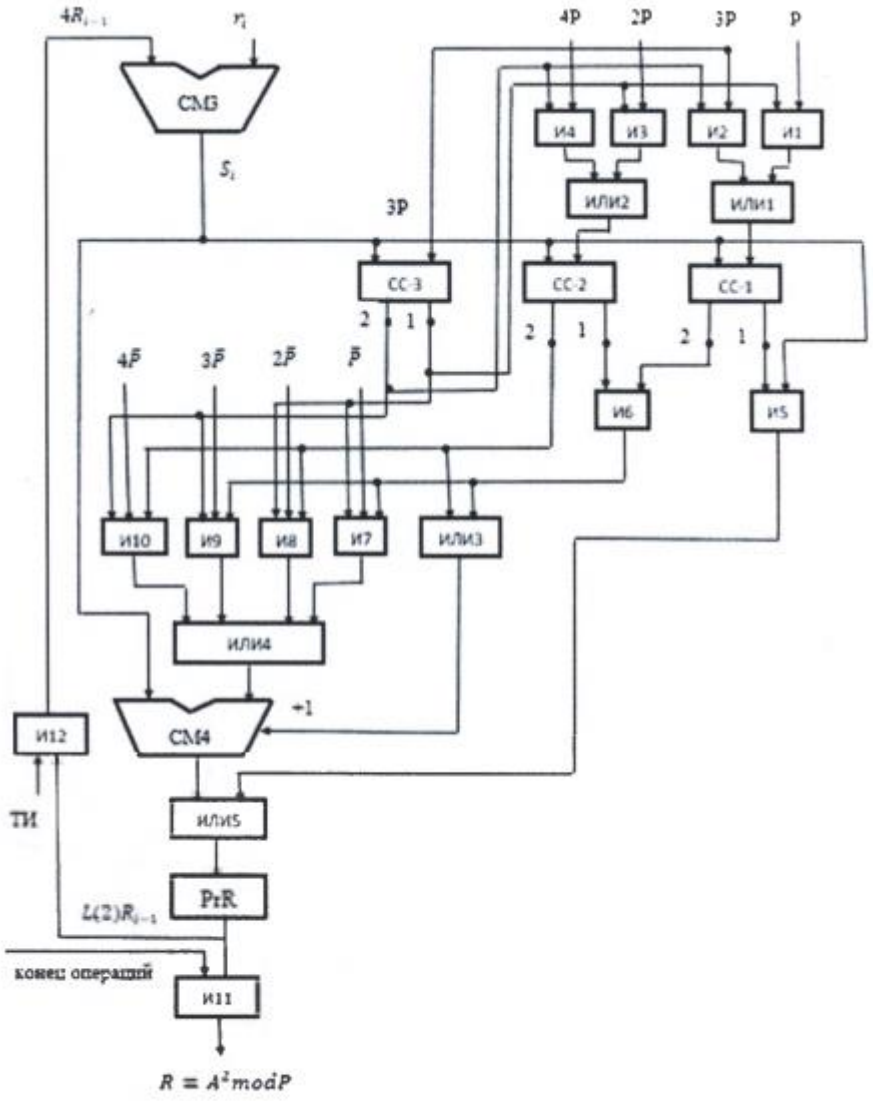
Быстродействующее устройство модульного возведения чисел в квадрат содержащее регистры РгА1 и РгА2 для хранения возводимого в квадрат числа А, остатка РгR, регистра модуля РгР, сумматора и формирователя остатков и схем И, ***отличающееся*** тем, что в состав устройства введен разрядный умножитель по модулю (РУМ), блок формирования кратных модулю (БФКМ), где выходы регистров РгА1, РгА2 и БФКМ связаны с РУМ, в котором формируются остатки $r_i = (2A \cdot a_i + A \cdot a_{i-1})$ modP; выходы РУМ, БФКМ и регистра остатков РгR связаны со входом ФО, где формируются остатки $R_i = (4R_{i-1} + r_i)$modP.



Фигура 1


A
L(1)A
$\bar{P}$
a_i
$\bar{a}_i$
a_{i-1}
$\bar{a}_{i-1}$
И1
И2
И3
И4
СМ1
L(1)$\bar{P}$
2$\bar{P}$
$\bar{P}$
И5
И6
ИЛИ2
ИЛИ1
+1
СМ2
r_i

Фигура 2



Фигура 3

Верстка Д. Женысова
Корректор Г. Косанова