РЕСПУБЛИКА КАЗАХСТАН

(19) **KZ** (13) **B** (11) **35623**
(51) ***G06F 7/72*** (2006.01)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ИЗОБРЕТЕНИЯ
К ПАТЕНТУ

(21) 2022/0111.1
(22) 21.02.2022
(45) 22.04.2022, бюл. №16
(72) Тынымбаев Сахыбай; Ибраимов Маргулан Касенович; Мукашева Асель Коптлеувна; Әділбекқызы Сайран; Намазбаев Тимур Адильканович
(73) Тынымбаев Сахыбай
(56) SU 1633495 A1, 07.03.1991
SU 736095 A1, 25.05.1980
KZ 30983 A4, 15.03.2016
EP 0145533 A1, 16.03.1988

(54) **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 модульного возведения чисел в квадрат в устройстве имеются регистр РгА1 для хранения числа А и сдвигающий регистр РгА2 с цепями сдвига влево на один разряд, а также сумматор СМ1, где выполняется операция $C_i = 2R_{i-1} + a_i * A$ и формирователь остатков ФО, где C_i приводится по модулю Р.

Техническим результатом предлагаемых схемных решений является упрощение структуры ФО, путем замены сумматора и мультиплексоров схемами сравнения.

(19) KZ (13) B (11) 35623

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

Прототипом служит «Устройство модульного возведения чисел в квадрат» [Патент KZ № 35493 бюллетене №5 от 04.02.2022г. МПК 606F7/72]

В состав такого устройства входят сдвигающий регистр (РгА) с цепями сдвига влево на один разряд, регистр модуля РгР, накапливающие частичные и промежуточные формирователи, блоки схем И1-И7, блоки схемы ИЛИ, линий задержки Л3, блок синхронизаций (БС).

Недостатком такого устройства является сложность технической реализации, что приводит к снижению надежности работы и повышению стоимости.

Технической задачей изобретения является разработка устройства модульного возведения чисел в квадрат с более высокой надежностью и низкой стоимостью.

Техническим результатом является построение устройства модульного введения чисел в квадрат с минимальными аппаратными затратами.

Для достижения технического результата из устройства исключаются мультиплексоры и двоичный сумматор, с вводом в состав устройства двух схем сравнения.

На фигуре 1 приведена функциональная схема модульного возведения чисел в квадрат. В состав устройства входят регистры РгА1 и РгА2, куда подается число А. РгА2 имеет цепи сдвига влево на один разряд, регистр РгР для хранения модуля Р, сумматор СМ1 для суммирования значений 2Ri-, с числом А, формирователь остатка (ФО), регистр остатка РгR, блоки логических схем И1-И5, линий задержки Л3, блок синхронизаций БС, в состав которого входит вычитающий счетчик тактовых сигналов СчТИ. На вход БС подается сигнал «ПУСК», тактовые импульсы ТИ, двоичный код числа сдвига N-1. На выходах БС выдаются тактовые сигналы ТИ, «Конец операций».

На фигуре 2 приведена функциональная схема ФО, который состоит из двух схем сравнений СС-1 и СС-2, двоичного сумматора СМ2, блоков логических схем И1, И3, И4, И5, ИЛИ1 и ИЛИ3, логической схемы И2, ИЛИ2.

На вход схемы ФО значение Ci = $2R_{i-1} + a_i * A$ поступает с выходов сумматора СМ1, который подается на левые входа сумматора СМ2 и на левые входы схем сравнений СС-1 и СС-2. Кроме C_i на вход ФО подается значения модулей Р и $\overline{P}$ из РгР. Значение Р со сдвигом влево на один разряд подается на правый вход СС-1, а на правый вход СС-2 значение Р. Схемой сравнения СС-1 значение C_i сравнивается со значением 2Р и при выполнении условий $C_i \geq 2P$ на его входе 2 формируется единичный сигнал. При этом на его правом выходе 1 формируется сигнал 0. Единичный сигнал на выходе 1 СС-1 вырабатывается при выполнении условий$C_i \geq 2P$. Схемой СС2 значение C_i сравнивается со значением Р. На выходе 2 схемы СС-2 формируется единичный сигнал при условии $C_i \geq P$. Единичный сигнал на выходе 1 схемы СС-2 формируется при условии $C_i < P$.

Выход 2 СС-1 связан со входами блока логических схем И4, на вторые входы которого подается значение $2\overline{P}$. Выход 2 схемы СС-2 так же связан со входом схемы ИЛИ2. При выполнении условий $C_i < 2P$ на выходе 1 СС-1 формируется единичный сигнал, который подается на первый вход схемы И2. При условиях $C_i \geq 2P$ на втором выходе СС-2 формируется единичный сигнал, который так же подается на вход схемы И2. При этом на выходе схем И2 формируется единичный сигнал, который подается на вход блока схем И5 и на вход схемы ИЛИ2. На второй вход блока схем И5 подается значение $\overline{P}$. Как видно из фигуры 2 выходы блоков схем И4 и И5 через блок схем ИЛИ1 связаны с правым входом СМ2, а выход схем ИЛИ2 связан с младшим разрядом сумматора СМ2. При $C_i \geq 2P$ сигнал с выхода 2 СС-1 разрешает прохождению значений $2\overline{P}$ на правый вход СМ2 и в сумматоре выполняется операция $R_i = C_i + 2\overline{P} + 1$. При выполнении условия $2P > C_i \geq 2P$ единичный сигнал с выхода схемы И2 разрешает передачу значений $\overline{P}$ на правые входы СМ2 и в сумматоре выполняется операция $C_i = C_i + \overline{P} + 1$. При выполнении условия $C_i < P$ на первом выходе СС-1 формируется единичный сигнал, который разрешает прохождению C_i на выход блока схем И3. При этом значение C_i через блок схем ИЛИ3 выдается на выход и $R_i = C_i$.

Рассмотрим работу модульного возведения чисел в квадрат. По сигналу «ПУСК» возводимое число в квадрат А с помощью блока схем И3 принимается в регистры РгА1 и РгА2, значения модуля Р посредством блока схемы И4 принимается в регистр РгР и подается в схему ФО. Затем число А из РгА1 при $a_{N-1} = 1$ через блок схем И5 подается на правый вход сумматора СМ1, где суммируется с нулем.

При этом на выходе СМ1 формируется число $C_0=0+A*a_{N-1}$, которое подается на вход ФО и на его выходах формируется остаток $R_0=A$ и запоминается в регистре остатка РгR.

К моменту формирования R_0 БС выдает на выход первый тактовый импульс ТИ1, который сдвигает содержимое $Р_ГА2$ на один разряд влево и уменьшает на единицу показания Сч ТИ. Одновременно задержанный ТИ1 на Л2 подается на вход блока схем И6, на второй вход которого подается остаток со сдвигом на один разряд влево содержимого регистра $Р_ГR$ - L(1) R_0. С выхода блока схем И6 значение $2R_0$ подается на левые входы сумматора СМ1, где суммируется с $A*a_{N-2}$ формируя $C_1=2R_0+A*a_{N-2}$. Далее C_1 подается на вход ФО, где формируется остаток $R_1=C_1 mod P$, который запоминается в $Р_ГR$.

Аналогично формируются другие остатки. После подачи тактового импульса ТИ N-1 в сумматоре СМ1 формируются $C_{N-2}=2R_{N-2}+A*a_0$ и C_{N-2} приводится по молью Р и результат $R= C_{N-2} mod P$ запоминается в $Р_ГR$. Показание СчТИ обнуляется и БС выработает сигнал «Конец операций», по

которому содержимое $P_I R$ через блока схем И5 выдается на выход.

Рассмотрим пример выполнения операции $R=A^2 modP$.

Пусть $A=45_{10}=\begin{cases} a_5 a_4\ a_3 a_2 a_1 a_0 \\ 1\ 0\ \ 1\ 1\ 0\ 1_2 \end{cases}$

$P=70_{10}$; $N=6$

Порядок вычисления в десятичной системе счислена приведен в табл.1.

Таблица 1.

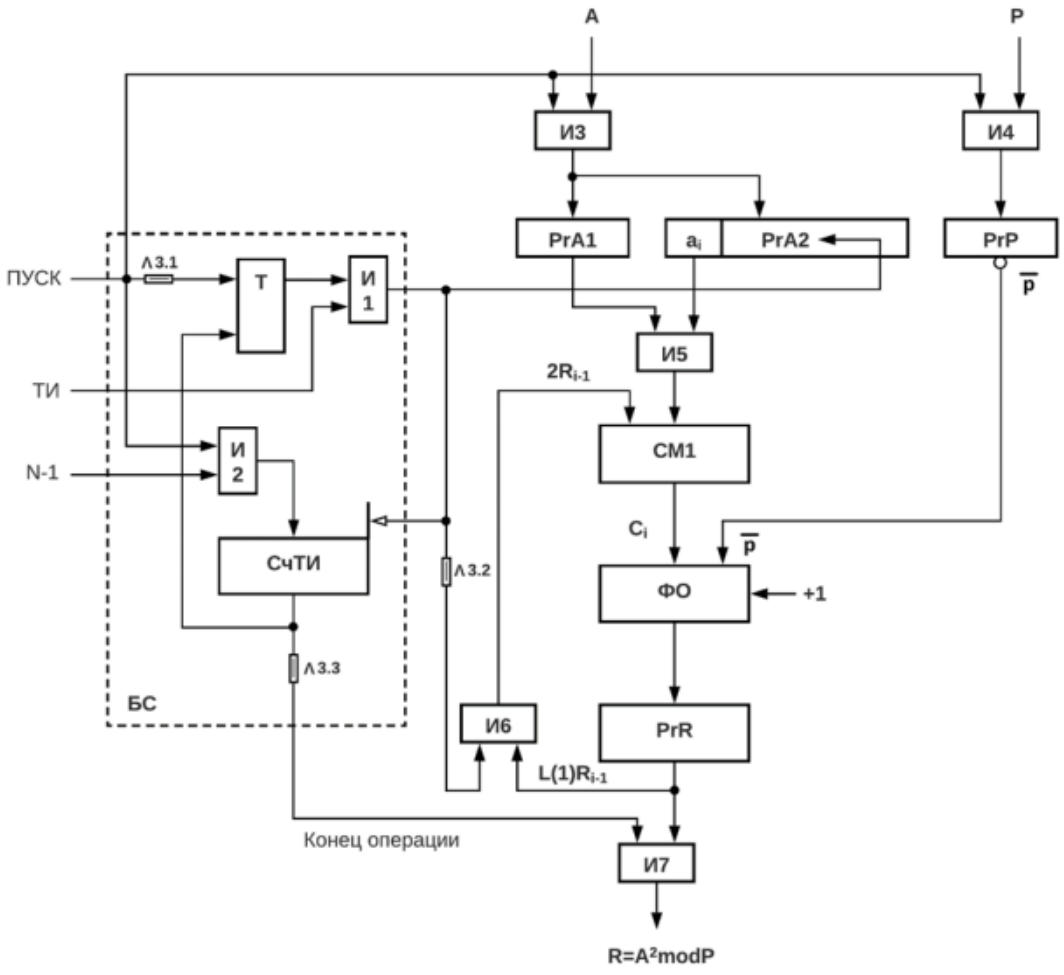
Порядок вычисления $R=A^2 modP$

ТИ	a_i	$C_i=2R_{i-1}+a_i\&A$	$R_i=C_i modP$
ПУСК	$a_5=1$	$C_0=0+A=45_{10}$	$R_0=C_0 modP=45 mod 75=45_{10}$
ТИ1	$a_4=0$	$C_1=2R_0+a_4*A=90+0=90$	$R_1=C_1 modP=90 mod 70=20_{10}$
ТИ2	$a_3=1$	$C_2=2R_1+a_3*A=40+45=85$	$R_2=C_2 modP=85 mod 70=15_{10}$
ТИ3	$a_2=1$	$C_3=2R_2+a_2*A=30+45=75_{10}$	$R_3=C_3 modP=75-70=5_{10}$
ТИ4	$a_1=0$	$C_4=2R_3+0=10_{10}$	$R_4=C_4 modP=10-70=10_{10}$
ТИ5	$a_0=1$	$C_5=2R_4+a_0*A=20+45=65_{10}$	$R_5=C_5 modP=65 mod 70=65_{10}$

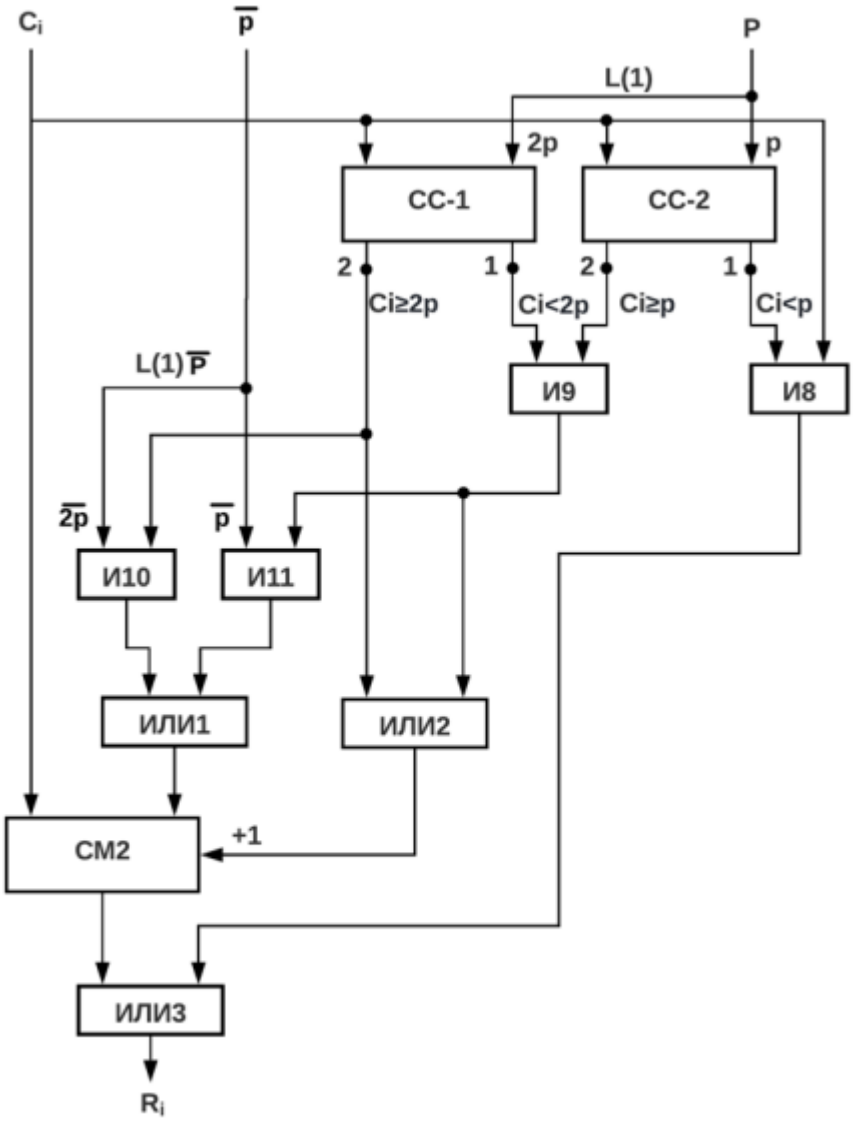
Проверка $A^2 modP=45^2_{10}$ $mod 70_{10}=2025_{10} mod 70_{10}=65_{10}$

ФОРМУЛА ИЗОБРЕТЕНИЯ

Устройство модульного возведения чисел в квадрат, содержащее регистры, двоичных сумматоров, мультиплексоров и блоков логических схем И и ИЛИ, ***отличающееся*** тем, что регистры для хранения числа А возводимого в квадрат по модулю регистры PrA1 и PrA2 по входу связаны связаны с блоком логических схем И3 через которого принимается число А, выходы регистра PrA1 и старший бит регистра PrA2 связаны со входами блока схем И5, входы сумматора СМ1 связаны с выходами блока схем И5 и И6, выходы сумматора СМ1 связаны со входами ФО, а вторые входы которого связаны с выходами регистра PrP, вход регистра PrP связан с выходом блока И4 через которого принимается значение модуля Р, выход схемы ФО связан со входом регистра PrR, а его выходы связаны со входами блоков И6 и И7, вторые входы их связаны с БС, в ФО выходы СМ1 связаны с левыми входами СМ2 и левыми входами схем сравнения СС-1 и СС-2, а также с информационными входами блока И8, а второй вход блока схем И8 связан с правым выходом СС-2, правые входы смем СС-1 и СС-2 связаны с выходами регистра PrP, выходы блока схем И8 связаны с информационными входами блока схем ИЛИ3, выход 1 схемы СС-1 и выход 2 схемы СС-2 связаны со входами схемы И9, входы блока схем И10 и И11 связаны с выходами регистра PrP, при этом на управляющий вход блока схем И10 связан с выходом 2 схемы СС-1, а управляющий блок схемы И1 связан с выходом схемы И9, входы схем ИЛИ2 связаны с выходом 2 схемы СС-1 и с выходом логической схемы И9, выход схемы ИЛИ2 связан с младшим разрядом СМ2, выходы сумматора СМ2 связаны со входами схемы ИЛИ3 через которого подается результат R_i на вход регистра PrR.


A
P
И3
И4
PrA1
a_i
PrA2
PrP
$\overline{P}$
ПУСК
Λ3.1
Т
И 1
ТИ
N-1
И 2
СчТИ
Λ3.2
Λ3.3
БС
И5
$2R_{i-1}$
СМ1
C_i
$\overline{P}$
ФО
+1
И6
PrR
$L(1)R_{i-1}$
Конец операции
И7
$R=A^2 modP$

Фигура 1



Фигура 2

Верстка Д. Женысова
Корректор Г. Косанова