РЕСПУБЛИКА КАЗАХСТАН

(19) **KZ** (13) **B** (11) **36585**
(51) ***G06F 7/00*** (2006.01)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ИЗОБРЕТЕНИЯ
К ПАТЕНТУ

(21) 2022/0718.1
(22) 14.11.2022
(45) 17.05.2024, бюл. №20
(72) Тынымбаев Сахыбай; Гнатюк Сергей Александрович; Бердибаев Рат Шындалиевич; Мукашева Асель Коптлеувна; Шайкулова Актоты Алиевна; Утешев Ілияс Жақсылықұлы
(73) Некоммерческое акционерное общество «Алматинский университет энергетики и связи имени Гумарбека Даукеева»
(74) Құрманғали Болат Серікұлы
(56) KZ35765 B, 15.07.2022
EP0449349 A1, 02.10.1991
CN114785507 A, 22.07.2022
UA51512 U, 26.07.2010

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

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

Сокращение количества шагов для возведения N-разрядного числа в квадрат по модулю достигается путем умножения на каждом шаге на два члена его полинома ($a+a_1{}^{2^1}+\ldots a_{n-1}{}^{2^{n-1}}+a_n{}^{2^n}$) с последующим приведением их по модулю. Для этого в состав устройства вводят регистр RgA с цепями сдвига на два разряда вправо, блок формирования и хранения кратных модулю (БФХКМ), накапливающий формирователь частичных остатков (НФЧО), формирователь разрядных остатков (ФРО), накапливающий сумматор остатков по модулю (НСОМ).

Техническим результатом предложенного является ускорение возведения чисел в квадрат по модулю.

(19) KZ (13) B (11) 36585

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

Прототипом устройства является устройство модульного возведения чисел в квадрат [Патент KZ 35493, опубликовано бюл. № 5 от 04.02.2022 МПК: G06F 7/72].

В состав устройства входят сдвигающий регистр PrA, где хранится возводимое число А в квадрат, регистр PrP, где хранится код модуля Р, накапляющий формирователь частичных остатков (НФЧО), накапливающий формирователь промежуточных остатков (НФПО), блоки схем И, ИЛИ, блок синхронизации (БС).

Недостатком устройства является его низкое быстродействие - для возведения N-разрядного числа в квадрат требуется N шагов.

Технической задачей изобретения является сокращение количества шагов для возведения N-разрядного числа в квадрат по модулю.

Техническим результатом предложенного является ускорение возведения чисел в квадрат по модулю.

Для достижения технического результата число А на каждом шаге умножается на два члена полинома $A = (a_0 + a_1 2^1 + \cdots + a_{n-1} 2^{n-1} + a_n 2^n)$ с приведением их по модулю Р. Для этого в состав устройства вводятся регистр числа А (RgA) с цепями сдвига на два разряда вправо, блок формирования и хранения кратных модулю (БФХКМ), накапливающий формирователь частичных остатков (НФЧО), формирователь разрядных остатков (ФРО), накапливающий сумматор остатков по модулю (НСМО).

На фигуре 1 приведена функциональная схема устройства модульного возведения числа в квадрат. В состав устройства входят сдвигающий регистр RgA с цепями сдвига вправо на два разряда, блок формирования и хранения значений кратных модулю Р ($P \dots 7P$ и $\bar{P} \dots 7\bar{P}$), формирователь частичных остатков (НФЧО), где вычисляются частичные остатки r_i, разрядный умножитель по модулю (РУМ), накапливающий сумматор остатков по модулю (НСОМО) с регистром для хранения промежуточных остатков RgR, блок синхронизации БС, в состав которого входит вычитающий счетчик тактовых импульсов (СчТИ). На вход БС подается сигнал «ПУСК»; тактовые испульси (ТИ), двоичный код числа сдвига N/2, с выходов БС выдаются ТИ и сигнал «конец операций» (КО при СчТИ: = 0).

Рассмотрим работу предложенного устройства модульного возведения числа в квадрат, где число А в каждом шаге умножается на его два разряда a_{i-1}, a_i с с приведением их по модулю. По сигналу «ПУСК» операнды А и Р посредством блоков логических схем И1 и И2 принимаются в регистр RgA и в БФХКМ, где формируются и запоминаются значения модуля и кратные числа к модулю ($P, 2P \dots 7P$ и $\bar{P}, 2\bar{P} \dots 7\bar{P}$). Задержанным сигналом «ПУСК» на Л3.1 число А из RgA через блок схем И3 передается со сдвигом вправо на два разряда через блок схем ИЛИ3 на вход НФЧО и без сдвига число А также передается через блок схем ИЛИ4 на входы РУМ. Одновременно задержанным сигналом «ПУСК» биты младших разрядов $a_1 a_2$ числа А также передается через блоков схем И4, И5 и ИЛИ1, ИЛИ2 на вход РУМ. В результате на выходе НФЧО формируется остаток $r_0 = 4A mod P$, которые запоминаются в регистре R_gr. Параллельно в РУМ формируется остаток $r_0{}^I = [(2a_1 + a_0)A] mod P$ и передается в НСМО, где формируется промежуточный остаток $R_0 = (0 + r_0^I) mod P$, который запоминается в RgR. К этому моменту БС выдает на выход ТИ1, сдвигающий содержимое RgA на два разряда в сигнсторону младшего разряда записав в младшие разряда RgA биты $a_3 a_2$ и эти биты непосредственно подаются на входы РУМ. На время сдвига регистра RgA ТИ1 задерживается линией задержкой Л3.2 и с выхода Л3.2 подается на вход блока схем И6. При этом одновременно содержимое R_gr передается на вход НФЧО и через блок схем И7 и ИЛИ4 передается на вход РУМ.

В ФЧО формируется остаток $r_i = 4r_{i-1} mod P = 4r_0 mod P$, а в РУМ формируется остаток $r_1{}^I = [(2a_3 + a_2)r_0] mod P$ и передается на вход НСМО, где формируется промежуточный остаток $R_1 = (r_1^I + R_0) mod P$. После отдачи ТИ1 показание счетчика СчТИ уменьшается на единицу.

Аналогично формируются r_2, r_3 в НФЧО и $r_2{}^I, r_3{}^I$ в РУМ и R_2, r_3 в блоке НСМО. После подачи ТИ $_{N/2-1}$ в блоке НФЧО формируется остаток $r_{\frac{N}{2}-1}$, в РУМ остаток r_{N-1}, а в RgR посредством СМО формируется результат. После подачи тактовых испульса ТИ $_{N/2-1}$ показание счетчика СЧТИ обнуляется и БС вырабатает сигнал «конец операций», по которому результат выдается на ввход через блока схем И8.

На фигуре 2 приведена функциональная схема умножителя чисел на четыре по модулю, которая состоит из двоичного сумматора СМ; двух схем сравнения СС-1 и СС-2; блоков логических схем И1÷И5, И8; схем И6, И7, ИЛИ3; блоков логических схем ИЛИ1, ИЛИ2, ИЛИ3 и НЕ.

Из БФХКМ модуль 2Р поступает на вход схемы СС-1. На правые входы СС-2 поступает значение модуля Р через блок схем И1 и ИЛИ1 или значение 3Р через блок схем И2 и ИЛИ1. Значение А или r_i, сдвинитое на два разряда в сторону старших разрядов обозначим через 4Х.

Значение 4Х подается на правые входы сумматора СМ через блок схем И8 и на левые входы схем СС-1 и СС-2. Схемой СС-1 сравнивается код 4Х с кодом 2Р. Если при этом 4Х ≥2Р, то на выходе 2 схемы СС-1 формируется единичный сигнал 1, который подается на управляющий вход блока схем И2, разрешая прохождение разрядов кратных модуля 3Р на правые входы схемы СС-2. При этом на выходе 1 схемы СС-1 – сигнал 0, который блокирует прохождение разрядов модуля Р через блок схемы И1 на входы схемы СС-2 и через схемы И6, НЕ приводит к формированию 1 на правом входе схемы И7.

При сравнении кода 4Х с кодом 2Р, если имеет место неравенство 4Х < 2Р, на выходе 1 схемы СС-1

формируется сигнал 1, разрешая прохождение разрядов кратных модуля P через схемы И1 на правые входы схемы СС-2. При этом на выходе 2 схемы СС-1 – сигнал 0, который блокирует прохождение 3P через блок схем И2 на входы схемы СС-2.

При выполнения условия 4X ≥2P схемой СС-2 осуществляется сравнение кода 4X с кодом 3P. Если при этом 4X ≥3P, то на выходе 1 схемы СС-2 установится сигнал 1, который подается на вход схемы ИЛИ3 и на управляющие входы блока схем И4, разрешая прохождение обратного кода $2\bar{P}$, поданного на информационные входы И4, на вход сумматора СМ через блок схем ИЛИ2. На выходе схемы ИЛИ3 формируется сигнал 1, разрешающий прохождение 2X через блок схемы И8 на сумматор СМ, и прохождение которого через схему И7 на вход +1 сумматора СМ разрешается единичным сигналом с выхода схемы НЕ. При этом сумматором СМ выполняется операция $R = 4X + 2\bar{P} + 1$.

Если при выполнения условия 4X ≥2P при сравнении кода 4X с кодом 3P на схеме СС-2 оказывается, что 4X ≥3P, то на выходе 2 схемы СС-2 установится сигнал 1, который подается на вход системы ИЛИ3 и на управляющие входы блока схем И5, разрешая прохождение обратного кода $3\bar{P}$, поданного на информационные входы И5, на вход сумматора СМ через блок схем ИЛИ2. На выходе схемы ИЛИ3 формируется сигнал 1, разрешающий прохождение 4X через блок схемы И8 на сумматор СМ, прохождение которого через схему И7 на вход +1 сумматора СМ разрешается единичным сигиалом с выхода схемы НЕ. При этом сумматором СМ выполняется операция R=4X+3$\bar{P}$+1.

При выполнения условия 4X<2P схемой СС-2 осуществляется сравнение кода 2X с кодом модуля P. Если при этом 4X≥P, то на выходе 2 схемы СС-2 установится сигнал 1, который подается на вход схемы ИЛИ3 и на управляющие входы блока схем И3, разрешая прохождение обратного кода $\bar{P}$, поданного на информационные входы И3, на вход сумматора СМ через блок схем ИЛИ2. На выходе схемы ИЛИ3 формируется сигнал 1, разрешающий прохождение 2X через блок схемы И8 на сумматор СМ, прохождение которого через схему И7 на вход +1 сумматора СМ разрешается единичным сигналом с выхода схемы НЕ. При этом сумматором СМ выполняется операция R=4X+$\bar{P}$+1.

Если при выполнении условия 4X<2P при сравнении 4X с кодом P на схеме СС-2 оказывается, что 4X<P , то на выходе СС-2 установится сигнал 1, который подается на входы схем ИЛИ3 и И6. На выходе схемы ИЛИ3 формируется сигнал 1, разрешающий прохождение 2X через блок схемы И8 на сумматор СМ, прохождение которого через схему И7 на вход +1 сумматора СМ запрещается нулевым сигналом с выхода схемы НЕ. При этом сумматором СМ выполняется операция R=4X+0=4X, т.к. на второй вход сумматора СМ не подаются кратные модули $\bar{P}$, $2\bar{P}$, $3\bar{P}$, заблокированные нулевыми управляющими сигналами на блоках схем И3, И4, И5.

Функциональная схема умножителя чисел A или r_i на двухразрядный код $a_{i+1}a_i$ числа A по модулю P приведена на фигуре 3. Умножитель содержит сумматоры СМ-1 и СМ-2, схем сравнения СС-1 и СС-2, блоков логических схем И1÷И4 и ИЛИ1 и блоков схем ИЛИ2, ИЛИ3, а также логических схем И5 и И6. Умножение числа A на двухразрядный код $a_{i+1}a_i$ числа A осуществляется блоками схем И1 и И2 и сумматором СМ-1. На выходе сумматора получаем число $C=2Aa_{i+1}+Aa_i$ в зависимости от значения битов a_{i+1} и a_i. Основная часть схем умножителя служит для приведения числа C по модулю P. Число C подается на левые входы схем сравнения СС-2 и СС-1 и на левые входы сумматора СМ2. На схеме СС-1 числа C сравнивается с прямым кодом модуля P, а на схеме СС-2 сравнивается со значением 2P. Значение 2P получаем путем подачи его на входы СС-2 со сдвигом на один разряд влево.

При C<P на выходе 1 СС-1 вырабатывается сигнал «1», который передает значение C на выход схемы через блока схем ИЛИ3. При 2P>C>P на выходе схемы И5 вырабатывается высокий уровень, что разрешает прохождению значения $\bar{P}$ на правые входы сумматора СМ2. При этом сигнал «1» с выхода схемы И5 также через логические схемы ИЛИ1 подается в младший разряд сумматора СМ-2, где выполняется операция $r_i'=C+\bar{P}+1$

При соотношении C≥2P на выходе 2 СС-2 вырабатывается единичный сигнал, который приводит к выполнению операции $r_i'=C+2\bar{P}+1$.

Функциональная схема НСОМ приведена на фигуре 4, который состоит из сумматоров СМ-1 и СМ-2 и мультиплексора MS. В сумматоре СМ-1 формируется сумма $S=r_i'+R_{i-1}$, которая приводится по модулю P сумматором СМ-2 и мультиплексором. При S>P на выходе мультиплексора MS формируется остаток $R_i=S-P$. При условии S<P значение R_i определятся величиной $S=r_i'+R_{i-1}$.

Рассмотрим пример модульного возведения чисел в квадрат.

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

$P=51_{10}$; $2P=102_{10}$; $3P=153_{10}$; $4P=204_{10}$; $5P=255_{10}$; $6P=306_{10}$

Последовательность вычисления $R=A^2 modP$ приведена в таблице 1, где для удобства все вычисления производится в десятичной системе счисления.

Таблица 1.

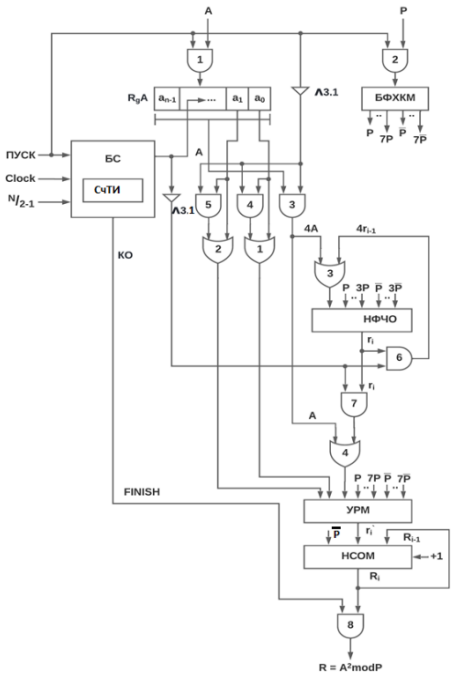
Последовательность вычисления R=A2modP

	FDR	РУМ	
ПУСК	r_1=4AmodP=180mod51= =180-3P=180-151=27 Rgr:=27	r_1'=(a_0·A)modP= =45mod51=45	R_1=(r_1'+R_0)modP= =45mod51=45
ТИ1	r_2=(4r_1)modP=108mod2P= =6 Rgr:=6	r_2'=(3·27)modP= =81-51=30	R_2=(r_2'+R_1)modP= =(30+45)mod51= =75-51=24
ТИ2	r_3=(4r_2)modP=24mod51=24	r_3'=(2·6)modP=12	R_3=(r_3'+R_2)modP= =(12+24)mod51=36

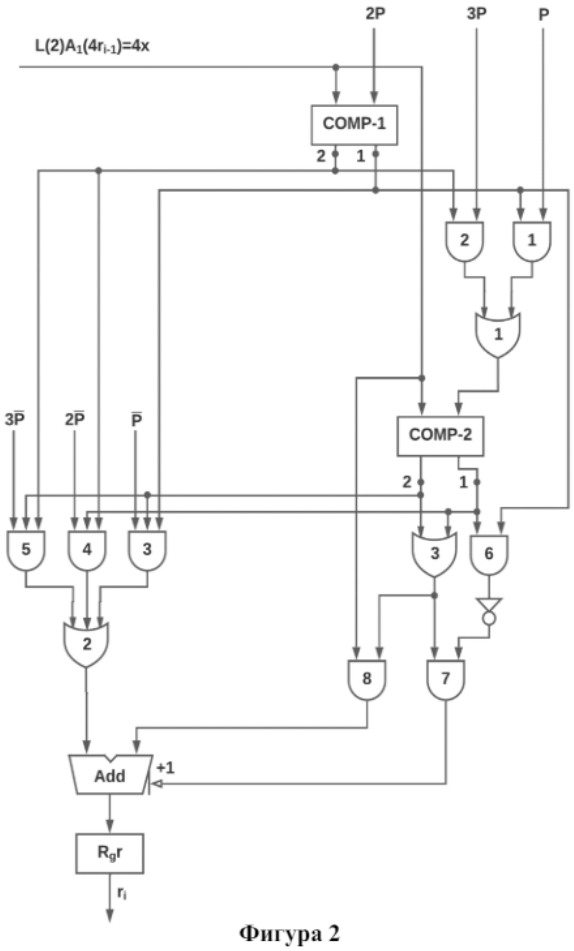
Проверка $R=A^2 mod51=2025mod51=36_{10}$

ФОРМУЛА ИЗОБРЕТЕНИЯ

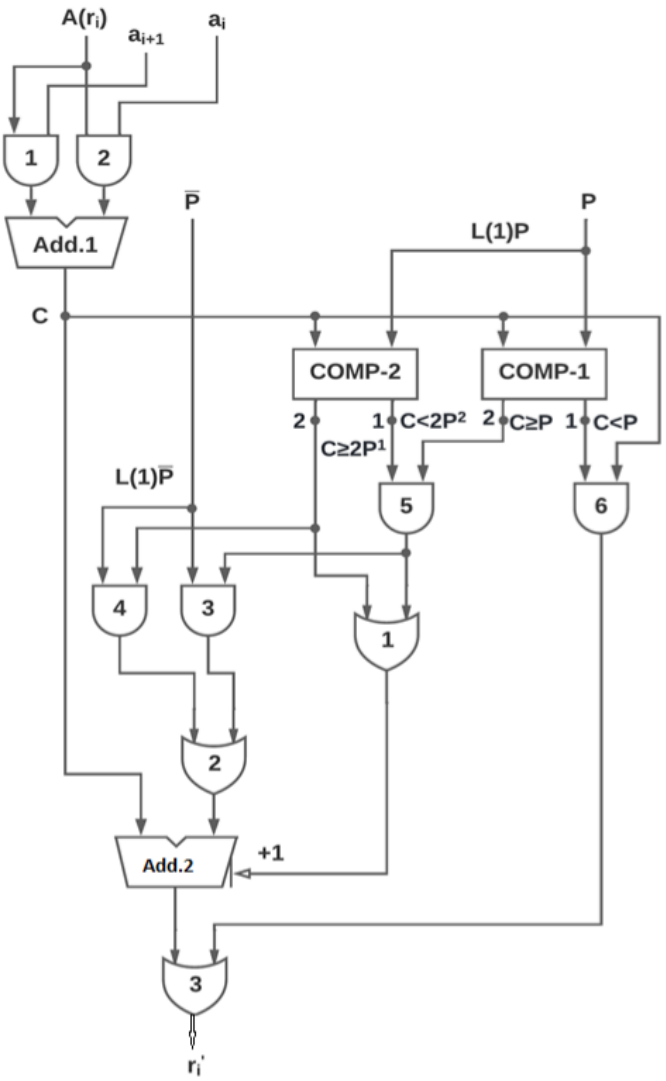
Быстродействующее устройство модульного возведения в квадрат, содержащее формирователь частичных остатков, сумматор по модулю, сдвигающий регистр возводимого числа в квадрат, регистр модуля, ***отличающееся*** тем, что в состав устройства введен накапливающий формирователь частичных остатков НФЧО, накапливающий сумматор по модулю, сдвигающий регистр РгА с цепями сдвига по два разряда вправо, блок формирования и хранения кратных модулю (БФХКМ), умножитель числа А или r_i на двухразрядный код по модулю (УРМ); прямые и инверсные выходы БФХКМ связаны со входами НФЧО, УРМ и НСОМ, информационные выходы RgA связаны также со входами НФЧО и УРМ; информационные выходы НФЧО связаны со входом НФЧО и УРМ, младшие разряды RgA также связаны со входом УРМ; выходы УРМ связаны со входом НСОМ, а выходы НСОМ через накапливающий регистр связаны также связаны со входом НСОМ.



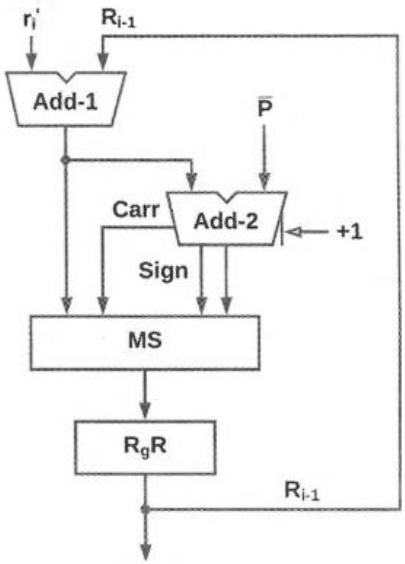
Фигура 1


2P
3P
P
L(2)A1(4ri-1)=4x
COMP-1
2
1
2
1
1
3P̄
2P̄
P̄
COMP-2
2
1
5
4
3
3
6
2
8
7
Add
+1
RgR
ri

Фигура 2


A(ri)
ai+1
ai
1
2
Add.1
P̄
P
L(1)P
C
COMP-2
COMP-1
2
1 C<2P2
C≥2P1
2 C≥P
1 C<P
L(1)P̄
5
6
4
3
1
2
Add.2
+1
3
ri'

Фигура 3



Фигура 4

Верстка Д. Женысова
Корректор Г. Косанова