УКРАЇНА

(19) **UA** (11) **110913** (13) **C2**

(51) МПК
G06F 7/52 (2006.01)
G06F 7/523 (2006.01)

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки: **a 2015 05097**
(22) Дата подання заявки: **25.05.2015**
(24) Дата, з якої є чинними права на винахід: **25.02.2016**
(41) Публікація відомостей про заявку: **26.10.2015, Бюл.№ 20**
(46) Публікація відомостей про видачу патенту: **25.02.2016, Бюл.№ 4**

(72) Винахідник(и):
Горбенко Іван Дмитрович (UA),
Краснобаєв Віктор Анатолійович (UA),
Курчанов Валерій Микитович (UA),
Янко Аліна Сергіївна (UA),
Кошман Сергій Олександрович (UA),
Горбенко Юрій Іванович (UA)

(73) Власник(и):
Горбенко Іван Дмитрович,
пр. Л. Свободи, 50-а, к. 68, м. Харків, 61204 (UA),
Краснобаєв Віктор Анатолійович,
вул. Астрономічна, 35-б, к. 24, м. Харків, 61085 (UA),
Курчанов Валерій Микитович,
вул. Зіньківська, 36-А, кв. 20, м. Полтава, 36009 (UA),
Янко Аліна Сергіївна,
вул. Великотирнівська, 36, корп. 3, к. 122, м. Полтава, 36014 (UA),
Кошман Сергій Олександрович,
вул. Енгельса, 19, к. 409, м. Харків-12, 61012 (UA),
Горбенко Юрій Іванович,
пр. Л. Свободи, 50-а, к. 68, м. Харків, 61204 (UA)

(56) Перелік документів, взятих до уваги експертизою:
RU 2006919 C1, 30.01.1994
RU 2018936 C1, 30.08.1994
SU 1095178 A1, 30.05.1984
SU 1126950 A1, 30.11.1984
SU 1149254 A1, 07.04.1985
US 5742530 A, 21.04.1998
US 5073870 A, 17.12.1991
US 5121431 A, 09.06.1992
RU 2023290 C1, 15.11.1994
SU 922731 A1, 23.04.1982

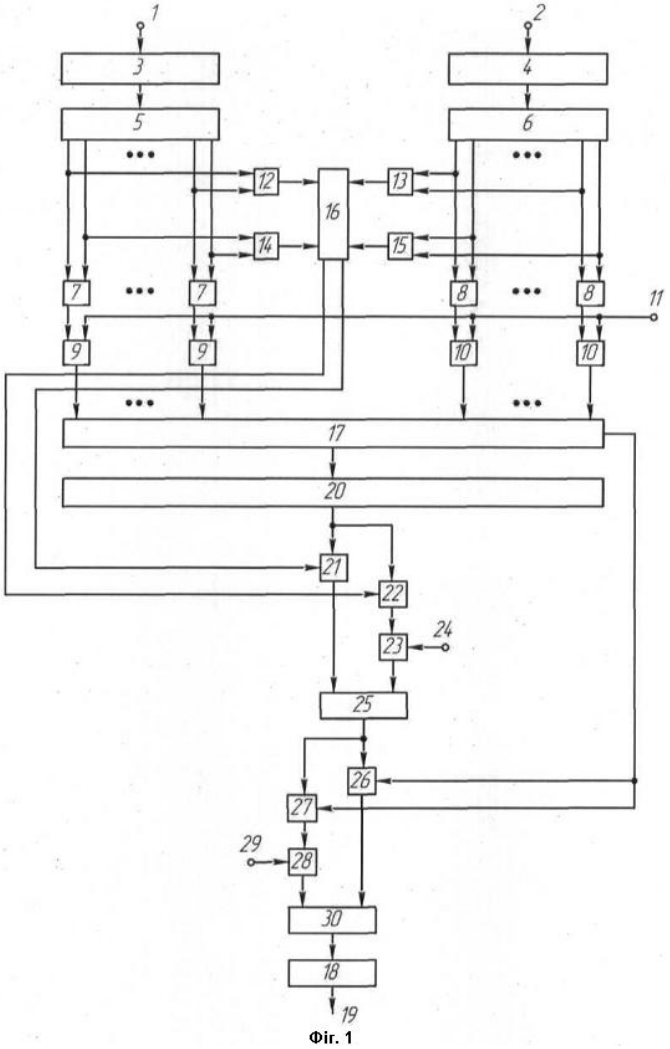
UA 110913 C2

(54) ПРИСТРІЙ ДЛЯ МНОЖЕННЯ ЛИШКІВ a_i ТА b_i ЧИСЕЛ ЗА МОДУЛЕМ m_i

(57) Реферат:

Винахід належить до області обчислювальної техніки та автоматики і призначена для множення лишків a_i та b_i числа за довільним модулем m_i системи залишкових класів (СЗК). Пристрій для множення лишків a_i та b_i чисел за модулем m_i містить перший і другий вхідні регістри, вихідний регістр, перший і другий дешифратори, першу та другу групи елементів АБО, кожна з

яких містить $\frac{m_i - 1}{2}$ елементів АБО, першу та другу групи елементів І, кожна з яких містить $\frac{m_i - 1}{2}$ елементів І, комутатор, суматор за модулем два, перший, другий, третій і четвертий елементи АБО, додатково введені шифратор, третя, четверта та п'ята групи елементів І, група ключових елементів, суматор за модулем m_i, суматор за модулем $\frac{m_i - 1}{2}$, третя та четверта групи елементів АБО. Технічним результатом, що досягається даним винаходом, є розширення функціональних можливостей пристрою за рахунок можливості виконання операції множення не тільки в додатній, а і у від'ємній числових областях.



Фіг. 1

Винахід належить до області обчислювальної техніки та автоматики і призначена для множення лишків a_i та b_i числа за довільним модулем m_i, системи залишкових класів (СЗК).

Відомий пристрій (аналог) для множення лишків a_i та b_i числа за довільним модулем m_i СЗК (а.с. СРСР № 885999, кл G 06 F 7/72, Б.В. № 44, 1981 р.). Він містить вхідні регістри, дешифратори, групи елементів АБО, групи елементів І, суматор за модулем два, елементи І та АБО, комутатори та вихідний регістр.

Недоліком аналога є низькі функціональні можливості пристрою, які полягають у тому, що множення лишків a_i та b_i числа за довільним модулем m_i СЗК виконується тільки в області додатних чисел.

Відомий пристрій (аналог) для множення лишків a_i та b_i числа за модулем m_i СЗК (а.с. СРСР № 896620 кл G 06 F 7/72, Б.В. № 1, 1982 р.). Пристрій містить перший і другий вхідні та вихідний регістри, перший і другий дешифратори, першу та другу групи елементів АБО, першу та другу групи елементів І, елементи І та АБО, комутатор.

Недоліком аналога є низькі функціональні можливості пристрою, які полягають у тому, що множення лишків a_i та b_i числа за довільним модулем m_i СЗК виконується тільки в області додатних чисел.

Найбільш близьким за технічною суттю і результатом, що досягається (прототипом), є пристрій для множення у СЗК (а.с. СРСР № 922731, кл G 06 F 7/39, Б.В. № 15, 1982 р.). Пристрій-прототип містить перший і другий вхідні регістри, вихідний регістр, перший і другий дешифратори, першу та другу групи елементів АБО, кожна з яких містить $\frac{m_i-1}{2}$ (для m_i непарного числа, або $\frac{m_i}{2}$ - для m_i парного числа) елементів АБО, першу та другу групи елементів І, кожна з яких містить $\frac{m_i-1}{2}$ елементів І, комутатор, суматор за модулем два, елементи АБО та І. При цьому перший і другий входи пристрою підключено до входів відповідно першого та другого вхідних регістрів, виходи яких підключено до входів відповідно першого та другого дешифраторів. Перший та (m_i-1)-й виходи першого та другого дешифраторів підключено до входів перших елементів АБО першої та другої груп елементів АБО, другий та (m_i-2)-й виходи першого та другого дешифраторів підключено до входів других елементів АБО першої та другої груп елементів АБО і т.д., а виходи($\left(\frac{m_i-1}{2}\right)$-го та $\left(\frac{m_i+1}{2}\right)$-го першого та другого дешифраторів підключено до входів $\left(\frac{m_i-1}{2}\right)$-х елементів АБО першої та другої груп елементів АБО. Виходи елементів АБО першої та другої груп підключено до перших входів елементів І відповідно першої та другої груп, до других входів яких підключена керуюча шина пристрою. Виходи $\left(1\div\frac{m_i-1}{2}\right)$ першого та другого дешифраторів підключено до входів першого та другого елементів АБО, а виходи $\left(\frac{m_i+1}{2}\div m_i-1\right)$ першого та другого дешифраторів підключені до входів відповідно третього та четвертого елементів АБО. Виходи першого та другого елементів АБО підключено до першого та другого нульових входів суматора за модулем два, а виходи третього та четвертого елементів АБО підключено до першого та другого одиничних входів суматора за модулем два. Виходи елементів І першої та другої груп підключені відповідно до першої та другої груп входів комутатора, а вихід вихідного регістра є виходом пристрою.

Недоліком прототипу - низькі функціональні можливості пристрою, які полягають у тому, що множення лишків a_i та b_i числа за довільним модулем m_i СЗК виконується тільки в області додатних чисел.

Задача винаходу - розширення функціональних можливостей пристрою за рахунок можливості виконання операції множення лишків a_i та b_i числа за довільним модулем m_i СЗК не тільки в додатній, а і у від'ємній числових областях.

Поставлена задача вирішується тим, що у пристрій для множення лишків a_i та b_i чисел за модулем m_i, що містить перший і другий вхідні регістри, вихідний регістр, перший і другий дешифратори, першу та другу групи елементів АБО, кожна з яких містить $\frac{m_i-1}{2}$ елементів АБО,

першу та другу групи елементів І, кожна з яких містить $\frac{m_i-1}{2}$ елементів І, комутатор, суматор за модулем два, перший, другий, третій и четвертий елементи АБО. При цьому перший і другий входи пристрою підключено до входів відповідно першого та другого вхідних регістрів, виходи яких підключено до входів відповідно першого та другого дешифраторів, перший та (m_i-1)-й виходи першого та другого дешифраторів підключено до входів відповідних перших двох входових елементів АБО першої та другої груп елементів АБО, другий та (m_i-2)-й виходи першого та другого дешифраторів підключено до входів відповідних других елементів АБО першої та другої груп елементів АБО і т.д., а виходи $\left(\frac{m_i-1}{2}\right)$-го та $\left(\frac{m_i+1}{2}\right)$-го першого та другого дешифраторів підключено до входів відповідних $\left(\frac{m_i-1}{2}\right)$-х елементів АБО першої та другої груп, виходи елементів АБО першої та другої груп підключено до перших входів відповідних елементів І відповідно першої та другої груп, до других входів яких підключена керуюча шина пристрою, виходи $1\div\frac{m_i-1}{2}$ першого та другого дешифраторів підключено до входів відповідно першого та другого елементів АБО, а виходи $\frac{m_i+1}{2}\div m_i-1$ першого та другого дешифраторів підключені до входів відповідно третього та четвертого елементів АБО. Виходи першого та другого елементів АБО підключено до першого та другого нульових входів суматора за модулем два, а виходи третього та четвертого елементів АБО підключено до першого та другого одиничних входів суматора за модулем два. Виходи елементів І першої та другої груп підключені відповідно до першої та другої груп входів комутатора, а вихід вихідного регістру є виходом пристрою, додатково введено шифратор, третю, четверту та п'яту групи елементів І, групу ключових елементів, суматор за модулем m_i, суматор за модулем $\frac{m_i-1}{2}$, третю та четверту групи елементів АБО. При цьому, перші виходи комутатора підключені до входів шифратора, виходи якого підключено до перших (інформаційних) входів елементів І третьої та четвертої груп, до других входів яких підключено відповідно нульовий та одиничний виходи суматора за модулем два, виходи елементів І четвертої групи підключено до першої групи входів суматора за модулем m_i, до другої групи входів якого підключена шина подачі значення m_i виходи елементів І третьої групи та суматора за модулем m_i через елементи АБО третьої групи підключені до перших (інформаційних) входів ключових елементів групи та елементів І п'ятої групи, виходи яких підключено до перших входів суматор за модулем $\frac{m_i-1}{2}$, до других входів якого підключена шина подачі значення $\frac{m_i-1}{2}$. Другий вихід комутатора підключено до других (заборонених) входів ключових елементів групи та до других (відкриваючих) входів елементів І п'ятої групи, виходи ключових елементів групи та суматора за модулем $\frac{m_i-1}{2}$ через елементи АБО четвертої групи підключено до входу вихідного регістра.

Введення вказаних ознак дозволяє розширити функціональні можливості пристрою за рахунок представлення результату операції множення лишків a_i та b_i числа за довільним модулем m_i одночасно, як в додатній, так і в від'ємній числових областях.

Для вирішення винаходу вихідні лишки a_i та b_i числа за модулем m_i представляються у так званій штучній формі (ШФ)

$a_i^{'}(b_i^{'}) = a_i(b_i) + \frac{m_i}{2}$, для m_i парного числа, або

$a_i^{'}(b_i^{'}) = a_i(b_i) + \frac{m_i-1}{2}$, для m_i непарного числа.

У прийнятому поданні чисел (ШФ) будемо мати справу тільки з додатними числами. Числа в інтервалі $\left[0,\frac{m_i-1}{2}\right]$ відображають від'ємні числа, а в інтервалі $\left[\frac{m_i+1}{2},m_i-1\right]$ - додатні числа. Схема представлення лишків a_i та b_i числа за модулем m_i=11 у ШФ $a_i^{'}$ і $b_i^{'}$ представлена в табл. 1.

Таблиця 1

Значення лишків a_i і b_i у ШФ a_i' і b_i'

$a_i(b_i)$	$a_i'(b_i')$	$a_i(b_i)$	$a_i'(b_i')$
-5	0	1	6
-4	1	2	7
-3	2	3	8
-2	3	4	9
-1	4	5	10
0	5	-	-

В цьому випадку маємо, що $-\frac{m_i-1}{2} \le a_i$, $b_i \le \frac{m_i-1}{2}$ та $0 \le a_i', b_i' \le m_i - 1$.

Для множення лишків a_i' та b_i' числа за модулем m_i, у винаході, як і у прототипі, використовуються властивості симетрії повної арифметичної таблиці множення лишків a_i та b_i числа за модулем m_i відносно вертикалі і горизонталі, що проходять між числами $\frac{m_i-1}{2}$ і $\frac{m_i+1}{2}$ для m_i - непарного числа, або за числом $\frac{m_i}{2}$ - - для m_i парного числа, де m_i - модуль таблиці, а також відносно лівої діагоналі цієї таблиці. Використання цих властивостей дає змогу на 75 % зменшити кількість елементів І з повної арифметичної таблиці множення лишків a_i' та b_i' числа за модулем m_i. Для прикладу в таблиці 2 дана повна арифметична таблиця множення лишків a_i' та b_i' за модулем m_i=11, в таблиці 3 дано представлення чисел a_i' та b_i' в коді $a_i' = [\gamma_{a_i'}; (a_i')^*]$ та $b_i' = [\gamma_{b_i'}; (b_i')^*]$ табличного множення (КТМ).

Таблиця 2

Повна арифметична таблиця множення лишків a_i' та b_i' за модулем m_i=11

b_i' \ a_i'	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	6	7	9
3	0	3	6	9	1	4	1	10	2	5	8
4	0	4	8	2	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Таблиця 3

Представлення чисел у КТМ

Представлення чисел $a_i^{'}(b_i^{'})$ у КТМ			
Представлення числа $a_i^{'}(b_i^{'})$ у десятковому коді	Представлення числа $a_i^{'}(b_i^{'})$ у двійковому коді	Код табличного множення	
		Символ $\gamma_{a_i^{'}}(\gamma_{b_i^{'}})$	Число $(a_i^{'})^*$, $(b_i^{'})^*$
1	0001	0	001
2	0010	0	010
3	0011	0	011
4	0100	0	100
5	0101	0	101
6	0100	1	101
7	0111	1	100
8	1000	1	011
9	1001	1	010
10	1010	1	001

Величини 0 і m_i можна не кодувати, так як результат множення на ці величини дає нуль, і в цьому випадку операція буде виконана швидше простим аналізом лишків $a_i^{'}$ та $b_i^{'}$. У цьому випадку табл. 1 та табл. 2 приймають вигляд табл. 4 та табл. 5.

Таблиця 4

Значення лишків a_i і b_i у ШФ $a_i^{'}$ і $b_i^{'}$

$a_i(b_i)$	$a_i^{'}(b_i^{'})$	$a_i(b_i)$	$a_i^{'}(b_i^{'})$
-4	1	1	6
-3	2	2	7
-2	3	3	8
-1	4	4	9
0	5	5	10

Таблиця 5

Арифметична таблиця множення лишків $a_i^{'}$ та $b_i^{'}$ за модулем m_i =11

$b_i^{'}$ \ $a_i^{'}$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	6	7	9
3	3	6	9	1	4	1	10	2	5	8
4	4	8	2	5.	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1.	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

У винаході множення лишків $a_i^{'}$ та $b_i^{'}$ за модулем m_i здійснюється у КТМ. Алгоритм множення наступний. Якщо множники $a_i^{'}=[\gamma_{a_i^{'}};(a_i^{'})^*]$ та $b_i^{'}=[\gamma_{b_i^{'}};(b_i^{'})^*]$ представлені у КТМ, тоді результат множення $c_i^{'}=a_i^{'}\cdot b_i^{'}=[\gamma_{a_i^{'}};(a_i^{'})^*]\cdot[\gamma_{b_i^{'}};(b_i^{'})^*]=[\gamma_{c_i^{'}};(c_i^{'})^*]$ цих чисел визначається наступним чином. По значеннях 0,25 повної таблиці 5 (наприклад, за другим квадрантом) визначається результат множення виду $[(a_i^{'})^*\cdot(b_i^{'})^*]\,\mathrm{mod}\,m_i=[\gamma_{c_i^{'}};(c_i^{'})^*]$, де $1\le(a_i^{'})^*$, $(b_i^{'})^*$ та $(c_i')^*\le\frac{m_i-1}{2}$, для m_i непарного числа. Після цього, якщо $\gamma_{a_i^{'}}=\gamma_{b_i^{'}}$, тоді індекс $\gamma_{c_i^{'}}$, не треба інвертувати, а якщо $\gamma_{a_i^{'}}\neq\gamma_{b_i^{'}}$, тоді індекс $\gamma_{c_i^{'}}$ треба інвертувати ($0\to1$ або $1\to0$).

У випадку такого кодування індекс КТМ визначається наступним чином

$$\gamma_{a_i}(\gamma_{b_i},\gamma_{c_i})=\begin{cases}0,\text{якщо}\ 1\le a_i^{'}(b_i^{'},c_i^{'})\le\dfrac{m_i-1}{2}\\ 1,\text{якщо}\ \dfrac{m_i-1}{2}\le a_i^{'}(b_i^{'},c_i^{'})\le m_i-1\end{cases}.$$

З урахуванням вищеозначеного таблиця рішень $c_i^{'}=a_i^{'}\cdot b_i^{'}=[\gamma_{a_i^{'}};(a_i^{'})^*]\cdot[\gamma_{b_i^{'}};(b_i^{'})^*]=[\gamma_{c_i^{'}};(c_i^{'})^*]$ комутатора (другий квадрант табл. 5) пристрою, що працює за модулем щ^{ш} 11, має вигляд таблиці 6. Тобто таблиця, що визначає результат множення виду $[(a_i^{'})^*\cdot(b_i^{'})^*]\,\mathrm{mod}\,m_i=[\gamma_{c_i^{'}};(c_i^{'})^*]$ має наступний вигляд.

Таблиця 6

Таблиця комутатора пристрою за модулем m_i =11

$(b_i^{'})^*$ \ $(a_i^{'})^*$		1	2	3	4	5
		10	9	8	7	6
1	10	1	2	3	4	5
2	9	2	4	6	8	10
3	8	3	6	9	1	4
5	7	4	8	2	5	9
5	6	5	10	4	9	3

Відомо, що для чисел $a_i^{'}$ та $b_i^{'}$, представлених у ШФ, виконуються умови

$(a_i\cdot b_i)'=a_i^{'}b_i^{'}$, (1)

$(a_i\cdot b_i)'=a_i^{'}b_i^{'}+\frac{m_i-1}{2}$. (2)

Для перевірки результату операції множення $c_i^{'}=a_i^{'}\cdot b_i^{'}=[\gamma_{a_i^{'}};(a_i^{'})^*]\cdot[\gamma_{b_i^{'}};(b_i^{'})^*]=[\gamma_{c_i^{'}};(c_i^{'})^*]$ використовується співвідношення (3)

$(a_i\cdot b_i)'=a_i\cdot b_i+\frac{m_i-1}{2}$. (3)

Співвідношення (1) і (2) є алгоритмом за яким працює винахід. Вихідні шини (перші виходи) комутатора об'єднують групи елементів I яким присвоюють однакові (від 1 до m_i-1) значенням $(a_i\cdot b_i)'=a_i^{'}b_i^{'}$. Другий вихід комутатора об'єднує всі елементи I, яким присвоюють значення $(a_i\cdot b_i)'=a_i\,b_i+\frac{m_i-1}{2}$. Сигнал другого виходу комутатора використовується для корекції значення $(a_i\cdot b_i)'=a_i^{'}b_i^{'}$ перших виходів комутатора, щоб отримати результат операції множення у вигляді $(a_i\cdot b_i)'=a_i^{'}b_i^{'}+\frac{m_i-1}{2}$.

На кресленні представлена блок-схема пристрою множення лишків a_i та b_i числа за модулем m_i, де: 1, 2 - перший та другий входи пристрою; 3, 4 - перший та другий вхідні регістри; 5, 6 - перший та другий дешифратори (пристрої для перетворення двійкового коду чисел а\ та Ц

в унітарний); 7, 8 - перша та друга групи елементів АБО; 9, 10 - перша та друга групи елементів І; 11 - керуюча шина пристрою; 12, 13, 14 і 15 - перший, другий, третій і четвертий елементи АБО; 16 - суматор за модулем два; 17 - комутатор (табличний пристрій для визначення результату операції $[(a_i^{'})*\cdot(b_i^{'})*]\mathrm{mod}m_i$; 18 - вихідний регістр; 19 - вихід пристрою; 20 - шифратор (пристрій для перетворення унітарного коду значення результату операції $[(a_i^{'})*\cdot(b_i^{'})*]\mathrm{mod}m_i$ у двійковий код); 21, 22 - третя та четверта групи елементів І; 23 - суматор за модулем m_i (суматор призначений для інвертування значення $[(a_i^{'})*\cdot(b_i^{'})*]\mathrm{mod}m_i$ за модулем m_i тобто, на виході суматора отримуємо значення $m_i-[(a_i^{'})*\cdot(b_i^{'})*]\mathrm{mod}m_i$; 24 - шини подачі значення модуля m_i, у двійковому коді; 25 - третя група елементів АБО; 26 - група ключових елементів; 27 - п'ята група елементів І; 28 - суматор за модулем $\frac{m_i-1}{2}$; 29 - шини подачі значення $\frac{m_i-1}{2}$ у двійковому коді; 30 - четверта група елементів АБО.

Перший 1 і другий 2 входи пристрою підключено до входів відповідно першого 3 та другого 4 вхідних регістрів, виходи яких підключено до входів відповідно першого 5 та другого 6 дешифраторів, перший та (m_i-1)-й виходи першого 5 та другого 6 дешифраторів підключено до входів перших елементів АБО першої 7 та другої 8 груп елементів АБО, другий та (m_i-2)-й виходи першого 5 та другого 6 дешифраторів підключено до входів других елементів АБО першої 7 та другої 8 груп елементів АБО і т.д., а виходи $(\frac{m_i-1}{2})$-го та $(\frac{m_i+1}{2})$-го першого 5 та другого 6 дешифраторів підключено до входів $(\frac{m_i-1}{2})$-х елементів АБО першої 7 та другої 8 груп елементів АБО, виходи елементів АБО першої 7 та другої 8 груп підключено до перших входів елементів І відповідно першої 9 та другої 10 груп, до других входів яких підключена керуюча шина 11 пристрою, виходи $1\div\frac{m_i-1}{2}$ першого 5 та другого 6 дешифраторів підключено до входів відповідно першого 12 та другого 13 елементів АБО, а виходи $\frac{m_i-1}{2}\div m_i-1$ першого 5 та другого 6 дешифраторів підключені до входів відповідно третього 14 та четвертого 15 елементів АБО, виходи першого 12 та другого 13 елементів АБО підключено до першого та другого нульових входів суматора 16 за модулем два, а виходи третього 14 та четвертого 15 елементів АБО підключено до першого та другого одиничних входів суматора 16 за модулем два. Виходи елементів І першої 9 та другої 10 груп підключені відповідно до першої та другої груп входів комутатора 17, а вихід вихідного 18 регістра є виходом 19 пристрою. Перші виходи комутатора 17 підключені до входів шифратора 20, виходи якого підключено до перших (інформаційних) входів елементів І третьої 21 та четвертої 22 груп, до других (керуючих) входів яких підключено відповідно нульовий та одиничний виходи суматора 16 за модулем два. Виходи елементів І четвертої 22 групи підключено до першої групи входів суматора 23 за модулем m_i, до другої групи входів якого підключені шини 24 подачі значення m_i. Виходи елементів І третьої 21 групи та суматора 23 за модулем m_i, через елементи АБО третьої 25 групи підключені до перших (інформаційних) входів ключових елементів 26 групи та елементів І п'ятої 27 групи, виходи яких підключено до перших входів суматор 28 за модулем $\frac{m_i-1}{2}$, до других входів якого підключені шини 29 подачі значення $\frac{m_i-1}{2}$. Другий вихід комутатора 17 до других (заборонених) входів ключових елементів 26 групи та до других (відкриваючих) входів елементів І п'ятої 27 групи. Виходи ключових елементів 26 групи та суматора 28 за модулем $\frac{m_i-1}{2}$ через елементи АБО четвертої 30 групи підключено до входу вихідного 18 регістру.

Пристрій функціонує наступним чином. За входами 1 і 2 до пристрою у двійковому коді поступають значення першого $a_i^{'}$ та другого $b_i^{'}$ чисел. З виходів першого 5 і другого 6 дешифраторів значення першого $a_i^{'}$ та другого $b_i^{'}$ чисел в унітарному коді, через відповідні елементи АБО першої 7 і другої 8 груп, надходять до входів відповідних елементів І першої 9 і другої 10 груп. Сигнал шини 11 відкриває відповідну пару елементів І 9 і 10 груп. З виходу відповідних елементів І 9 і 10 груп пара значень $(a_i^{'})*,(b_i^{'})*$ надходять до входів комутатора 17, з

виходу якого значення $[(a_i^{'})*\cdot(b_i^{'})*]\mathrm{mod}m_i$ в унітарному коді надходить до входу шифратора 20 з виходу якого значення $[(a_i^{'})*\cdot(b_i^{'})*]\mathrm{mod}m_i$ у двійковому коді надходить до перших (інформаційних) входів елементів І третьої 21 та четвертої 22 груп. Якщо $\gamma_{a_i^{'}}=\gamma_{b_i^{'}}$, тоді присутній вихідний сигнал нульового виходу суматора 16 за модулем два, який відкриває елементи І групи 21, і значення $[(a_i^{'})*\cdot(b_i^{'})*]\mathrm{mod}m_i$ надходить до входів елементів АБО 25 групи. Якщо $\gamma_{a_i^{'}}\neq\gamma_{b_i^{'}}$, тоді присутній вихідний сигнал одиничного виходу суматора 16 за модулем два, який відкриває елементи І групи 22, і значення $[(a_i^{'})*\cdot(b_i^{'})*]\mathrm{mod}m_i$ надходить до перших входів суматора 23, до других входів якого за шиною 24 надходить значення модуля m_i за яким працює пристрій. З виходу суматора 23 значення $m_i-[(a_i^{'})*\cdot(b_i^{'})*]\mathrm{mod}m_i$ надходить до входів елементів АБО 25 групи. З виходів елементів АБО 25 групи значення $(a_i^{'}\cdot b_i^{'})\mathrm{mod}m_i$ надходить до перших (інформаційних) входів ключових елементів 26 групи та елементів І п'ятої 27 групи. Якщо відсутній сигнал другої вихідної шини комутатора 17 (ознака того, що $(a_i\cdot b_i)'=a_i^{'}\cdot b_i^{'}$), тоді через відкриті ключові елементи 26 групи, елементи АБО групи 30 значення $(a_i^{'}\cdot b_i^{'})]\mathrm{mod}m_i$, надходить до входу вихідного регістра 18. Якщо присутній сигнал другої вихідної шини комутатора 17 (ознака того, що $(a_i\cdot b_i)'=a_i^{'}b_i^{'}+\frac{m_1-1}{2}$), тоді через відкриті елементи І групи 27 значення $(a_i^{'}\cdot b_i^{'})\mathrm{mod}m_i$ надходить до перших входів суматора 28, до других входів якого за шиною 29 надходить значення $\frac{m_i-1}{2}$. З виходу суматора 28 через елементи АБО групи 30 значення $(a_i^{'}b_i^{'})\mathrm{mod}m_i+\frac{m_i-1}{2}$ поступає до входу вихідного регістра 18.

Наведемо приклад роботи винаходу при реалізації операції множення лишків $a_i=1$ та $b_i=4$ числа за модулем $m_i=11$.

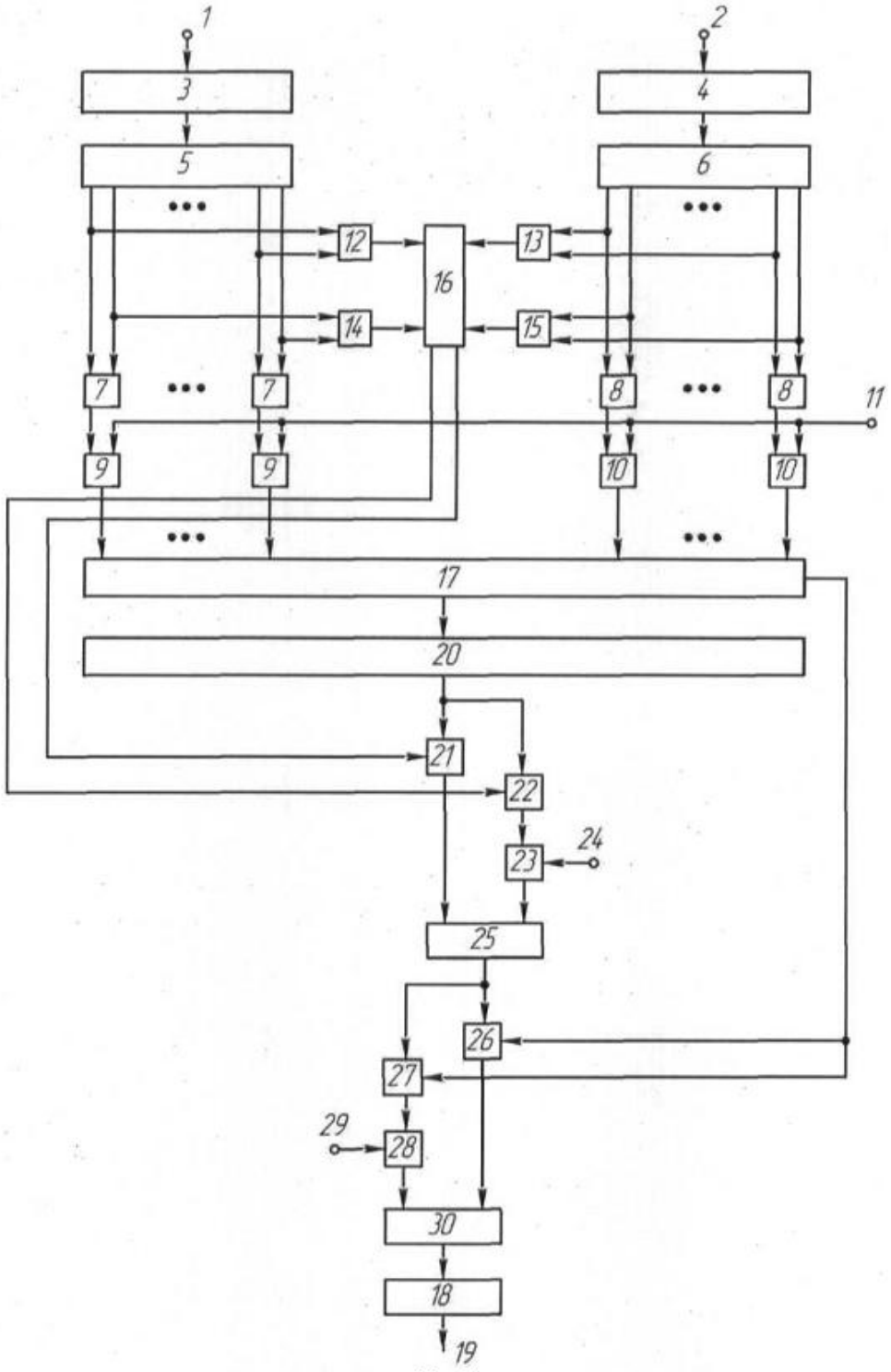
У відповідності з табл. 1 маємо, що $a_i^{'}=0110$ і $b_i^{'}=1001$. Значення чисел $a_i^{'}=0110$ і $b_i^{'}=1001$ за входами 1 і 2 надходять до пристрою. З виходів відповідних дешифраторів 5 і 6 значення $a_i^{'}=6$ і $b_i^{'}=9$ надходять до входів відповідних елементів АБО 7 і 8 груп та елементів АБО 12, 13, 14 і 15. Числа $a_i^{'}=0110$ і $b_i^{'}=1001$ у КТМ представляються у наступному вигляді $a_i^{'}=[\gamma_{a_i^{'}};(a_i^{'})*]=(1;101)$ та $b_i^{'}=[\gamma_{b_i^{'}};(b_i^{'})*]=(1;010)$ (табл. 3). До входів комутатора 17 в унітарному коді надходять значення $(a_i^{'})*=5$, та $(b_i^{'})*=2$. З виходу комутатора 17 значення $[(a_i^{'})*\cdot(b_i^{'})*]\mathrm{mod}m_i=(5\ 2)\mathrm{mod}11=10$ (табл. 6) надходить до входу шифратора 20. Так, як $\gamma_{a_i^{'}}=\gamma_{b_i^{'}}=1$, тоді присутній вихідний сигнал нульового виходу суматора 16 за модулем два, який відкриває елементи І групи 21, і з виходу шифратора 20 значення $(a_i^{'}\cdot b_i^{'})\mathrm{mod}m_i=1010$ у двійковому коді надходить до входів елементів АБО 25 групи. Для даних чисел $a_i^{'}=0110$ і $b_i^{'}=1001$ присутній сигнал другої вихідної шини комутатора 17 (ознака того, що $(a_i\cdot b_i)'=a_i^{'}b_i^{'}+\frac{m_i-1}{2}$). Тоді через відкриті елементи І групи 27 значення $(a_i^{'}\cdot b_i^{'})\mathrm{mod}m_i=1010$ надходить до перших входів суматора 28, до других входів якого за шиною 29 надходить значення $\frac{m_i-1}{2}=5$. З виходу суматора 28 через елементи АБО групи 30 значення $((a_i^{'}b_i^{'})\mathrm{mod}m_i+\frac{m_i-1}{2})\mathrm{mod}m_i=(1010+0101)=0100\ \mathrm{mod}11$ надходить до входу вихідного регістра 18.

Перевірка. З одного боку $(a_i\cdot b_i)'=a_i^{'}b_i^{'}+\frac{m_i-1}{2}=6\ 9+5=59=4\ \mathrm{mod}11$. З другого боку, у відповідності. з виразом (3) маємо, що $(a_i\cdot b_i)'=a_i^{'}\cdot b_i^{'}+\frac{m_i-1}{2}$, тобто $(1\cdot 4)'=1\cdot 4+5=9=4\mathrm{mod}5$. Це підтверджує достовірність отриманих результатів операції множення.

Представлений винахід дозволяє розширити функціональні можливості пристрою за рахунок представлення результату операції множення лишків a_i та b_i числа за довільним модулем m_i одночасно як в додатній, так і в від'ємній числових областях.

ФОРМУЛА ВИНАХОДУ

Пристрій для множення лишків a_i та b_i чисел за модулем m_i, що містить перший і другий вхідні регістри, вихідний регістр, перший і другий дешифратори, першу та другу групи елементів АБО, кожна з яких містить $\frac{m_i-1}{2}$ елементів АБО, першу та другу групи елементів І, кожна з яких містить $\frac{m_i-1}{2}$ елементів І, комутатор, суматор за модулем два, перший, другий, третій і четвертий елементи АБО, при цьому перший і другий входи пристрою підключено до входів відповідно першого та другого вхідних регістрів, виходи яких підключено до входів відповідно першого та другого дешифраторів, перший та (m_i-1)-й виходи першого та другого дешифраторів підключено до входів перших двох входових елементів АБО першої та другої груп елементів АБО, другий та (m_i-2)-й виходи першого та другого дешифраторів підключено до входів других елементів АБО першої та другої груп елементів АБО і т. д., а виходи $\left(\frac{m_i-1}{2}\right)$-го та $\left(\frac{m_i+1}{2}\right)$-го першого та другого дешифраторів підключено до входів $\left(\frac{m_i-1}{2}\right)$-х елементів АБО першої та другої груп, виходи елементів АБО першої та другої груп підключено до перших інформаційних входів елементів І відповідно першої та другої груп, до других керуючих входів яких підключена керуюча шина пристрою, виходи $1 \div \frac{m_i-1}{2}$ першого та другого дешифраторів підключено до входів відповідно першого та другого елементів АБО, а виходи $\frac{m_i+1}{2} \div m_i-1$ першого та другого дешифраторів підключені до входів відповідно третього та четвертого елементів АБО, а виходи першого та другого елементів АБО підключено до першого та другого нульових входів суматора за модулем два, а виходи третього та четвертого елементів АБО підключено до першого та другого одиничних входів суматора за модулем два, виходи елементів І першої та другої груп підключені відповідно до першої та другої груп входів комутатора, а вихід вихідного регістра є виходом пристрою, який **відрізняється** тим, що додатково введено шифратор, третю, четверту та п'яту групи елементів І, групу ключових елементів, суматор за модулем m_i, суматор за модулем $\frac{m_i-1}{2}$, третю та четверту групи елементів АБО, при цьому перші виходи комутатора підключені до входів шифратора, виходи якого підключено до перших інформаційних входів елементів І третьої та четвертої груп, до других керуючих входів яких підключено відповідно нульовий та одиничний виходи суматора за модулем два, виходи елементів І четвертої групи підключено до першої групи входів суматора за модулем m_i, до другої групи входів якого підключені шини подачі значення m_i виходи елементів І третьої групи та суматора за модулем m_i, через елементи АБО третьої групи підключені до перших інформаційних входів ключових елементів групи та елементів І п'ятої групи, виходи яких підключено до перших входів суматора за модулем $\frac{m_i-1}{2}$, до других входів якого підключені шини подачі значення $\frac{m_i-1}{2}$, другий вихід комутатора підключено до других заборонених входів ключових елементів групи та до других відкриваючих входів елементів І п'ятої групи, виходи ключових елементів групи та суматора за модулем $\frac{m_i-1}{2}$ через елементи АБО четвертої групи підключено до входу вихідного регістра.



Комп'ютерна верстка Д. Шеверун

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601