УКРАЇНА

ПАТЕНТ

НА ВИНАХІД

№ 110901

ПРИСТРІЙ ДЛЯ МНОЖЕННЯ ЛИШКІВ a_i ТА b_i ЧИСЛА ЗА ДОВІЛЬНИМ МОДУЛЕМ m_i СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

Видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі".

Зареєстровано в Державному реєстрі патентів України на винаходи **25.02.2016.**

В.о. Голови Державної служби
інтелектуальної власності України А.А.Малиш

Державна служба інтелектуальної власності України
Ідентифікаційний код 37552556
№1

(11) **110901**

(19) **UA**

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

(21) Номер заявки: **a 2015 01377**

(22) Дата подання заявки: **18.02.2015**

(24) Дата, з якої є чинними права на винахід: **25.02.2016**

(41) Дата публікації відомостей про заявку та номер бюлетеня: **10.06.2015, Бюл.№ 11**

(46) Дата публікації відомостей про видачу патенту та номер бюлетеня: **25.02.2016, Бюл. № 4**

(72) Винахідники:
Горбенко Іван Дмитрович, UA,
Краснобаєв Віктор Анатолійович, UA,
Янко Аліна Сергіївна, UA,
Кошман Сергій Олександрович, UA,
Горбенко Юрій Іванович, UA

(73) Власники:
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,
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

(54) Назва винаходу:

ПРИСТРІЙ ДЛЯ МНОЖЕННЯ ЛИШКІВ a_i ТА b_i ЧИСЛА ЗА ДОВІЛЬНИМ МОДУЛЕМ m_i СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

(57) Формула винаходу:

Пристрій для множення лишків a_i та b_i числа за довільним модулем m_i системи залишкових класів, 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, перший, другий, третій і четвертий елементи АБО, перший і другий елементи 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 $1 \div \frac{m_i-1}{2}$ 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 входів першого елемента І, а виходи третього та четвертого елементів АБО підключено до входів другого елемента І, 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 введено п'ятий і шостий елементи АБО, третю та четверту групи елементів І, групу ключових елементів, шифратор, суматор за модулем m_i, при цьому виходи комутатора підключено до входів шифратора, виходи якого підключено до перших інформаційних входів елементів І третьої групи та вентильних елементів групи, виходи елементів І третьої групи підключено до першої групи входів суматора за модулем m_i, до другої групи входів якого підключено виходи елементів І четвертої групи, до перших інформаційних входів елементів І четвертої групи підключено шини подачі сигналів, що визначають значення модуля m_i за яким працює пристрій, до других керуючих входів елементів І третьої та четвертої груп, а також до других заборонених входів ключових елементів підключено вихід п'ятого елемента АБО, до входу якого підключено виходи першого та другого елементів І, виходи суматора за модулем m_i і виходи ключових елементів через п'ятий елемент АБО підключено до входу вихідного регістра.

Пронумеровано, прошито металевими
люверсами та скріплено печаткою
3 арк.
25.02.2016

Уповноважена особа

Державна служба інтелектуальної власності України
Ідентифікаційний код 37552556
№1

(підпис)

УКРАЇНА

(19) **UA** (11) **110901** (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 01377**

(22) Дата подання заявки: **18.02.2015**

(24) Дата, з якої є чинними права на винахід: **25.02.2016**

(41) Публікація відомостей про заявку: **10.06.2015, Бюл.№ 11**

(46) Публікація відомостей про видачу патенту: **25.02.2016, Бюл.№ 4**

(72) Винахідник(и):
Горбенко Іван Дмитрович (UA),
Краснобаєв Віктор Анатолійович (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),
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

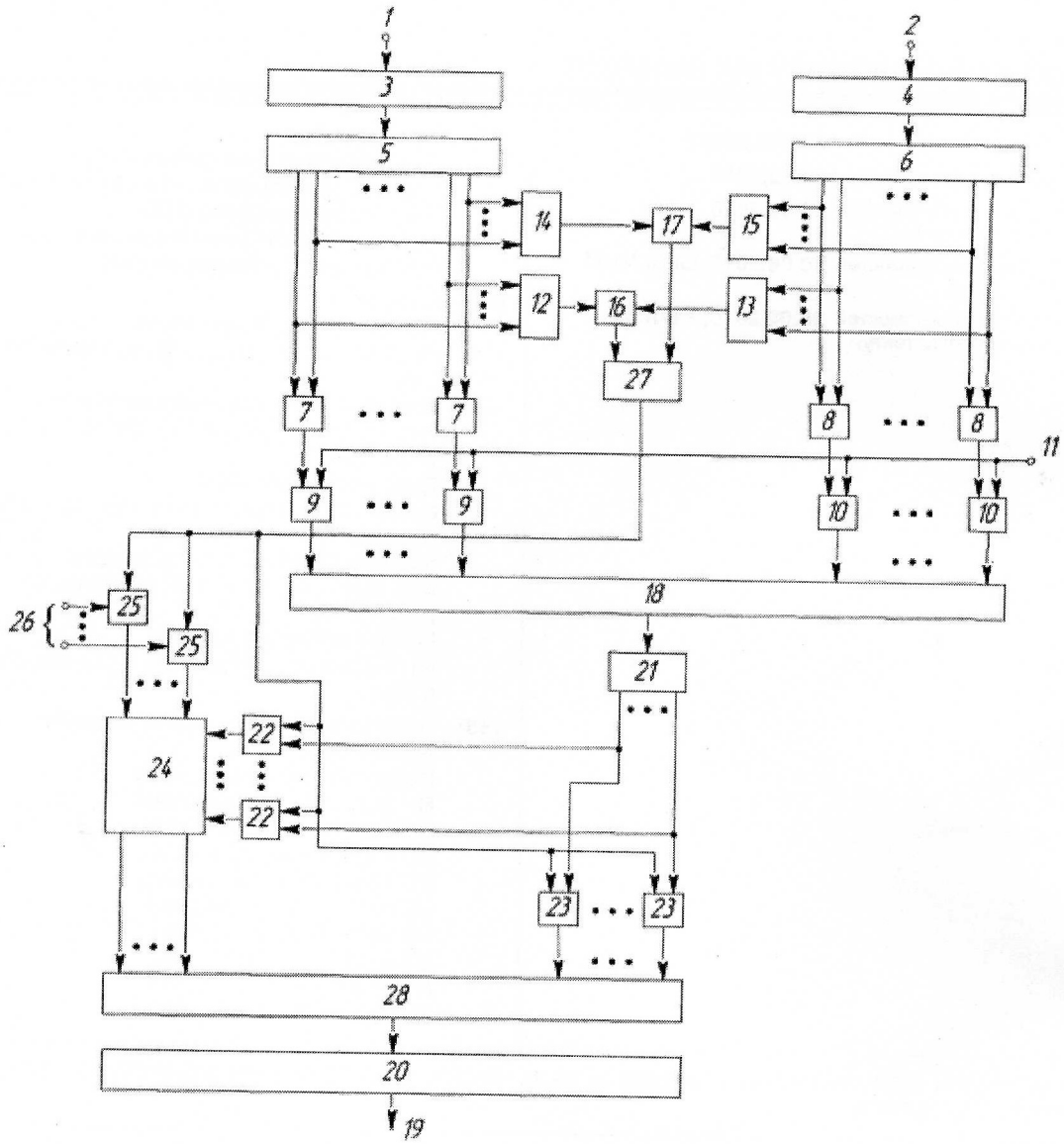
UA 110901 C2

(54) ПРИСТРІЙ ДЛЯ МНОЖЕННЯ ЛИШКІВ a_i ТА b_i ЧИСЛА ЗА ДОВІЛЬНИМ МОДУЛЕМ m_i СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

(57) Реферат:

Винахід належить до області обчислювальної техніки та автоматики і призначений 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 числа за довільним модулем m_i системи залишкових класів 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, перший, другий, третій і четвертий елементи АБО, перший і другий елементи І, введені п'ятий і шостий елементи АБО, третю та четверту групи елементів І, групу ключових елементів, шифратор, суматор за модулем m_i. Технічним результатом, що досягається даним винаходом, є розширення функціональних можливостей пристрою шляхом представлення результату операції множення безпосередньо у двійковому коді.



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 в тому, що результат операції множення лишків a_i та b_i числа за довільним модулем m_i СЗК представляється у коді табличного множення (КТМ). Дана обставина не дозволяє безпосередньо використовувати результат модульного множення у подальших загальних обчисленнях.

Відомий пристрій (аналог) для множення лишків a_i та b_i числа за довільним 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 в тому, що результат операції множення лишків a_i та b_i числа за довільним модулем m_i СЗК представляється у КТМ. Дана обставина не дозволяє безпосередньо використовувати результат модульного множення у подальших загальних обчисленнях.

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 $\frac{m_i-1}{2}$ елементів АБО, першу та другу групи елементів І, кожна з яких містить $\frac{m_i-1}{2}$ елементів І, комутатор, перший, другий, третій і четвертий елементи АБО, перший і другий елементи 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 входів першого елемента І, а виходи третього та четвертого елементів АБО підключено до входів другого елемента І. 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 в тому що результат операції множення лишків a_i та b_i числа за довільним модулем m_i СЗК представляється у КТМ. Дана обставина не дозволяє безпосередньо використовувати результат модульного множення у подальших загальних обчисленнях.

Поставлена задача: розширення функціональних можливостей винаходу за рахунок вдосконалення пристрою для множення лишків a_i та b_i числа за довільним модулем m_i СЗК шляхом представлення результату операції множення безпосередньо у двійковому коді.

Поставлена задача вирішується тим, що у пристрій для множення лишків a_i та b_i числа за довільним модулем m_i СЗК, 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, перший, другий, третій і четвертий елементи АБО, перший і другий елементи 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 $1\div\frac{m_i-1}{2}$ 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 входів першого елемента І, а виходи третього та четвертого елементів АБО підключено до входів другого елемента І, виходи елементів І першої та другої груп підключені відповідно до першої та другої груп входів комутатора, а вихід вихідного регістра є виходом пристрою, додатково введено п'ятий і шостий елементи АБО, третю та четверту групи елементів І, групу ключових елементів, шифратор, суматор за модулем m_i, при цьому виходи комутатора підключено до входів шифратора, виходи якого підключено до перших (інформаційних) входів елементів І третьої групи та ключових елементів групи, виходи елементів І третьої групи підключено до першої групи входів суматора за модулем m_i, до другої групи входів якого підключено виходи елементів І четвертої групи, до перших входів елементів І четвертої групи підключено шини подачі сигналів, що визначають значення модуля m_i за яким працює пристрій, до других (керуючих) входів елементів І третьої та четвертої груп, а також до других (заборонених) входів ключових елементів групи підключено вихід п'ятого елемента АБО, до входу якого підключено виходи першого та другого елементів І, виходи суматора за модулем m_i і виходи ключових елементів групи через п'ятий елемент АБО підключено до входу вихідного регістра.

Введення вказаних ознак дозволяє розширити функціональні можливості винаходу за рахунок представлення результату операції множення лишків a_i та b_i числа за довільним модулем m_i СЗК у двійковому коді. Що в свою чергу дозволяє безпосередньо використовувати результат операції модульного множення (який представлений у двійковому коді) у подальшій послідовності операцій.

У винаході 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 $\frac{(m_i+1)}{2}$, де m_i - модуль таблиці, а також відносно лівої діагоналі цієї таблиці. Використання цих властивостей дає змогу зменшити на 75 % кількість елементів І у повної арифметичної таблиці множення лишків a_i та b_i числа за модулем m_i комутатора пристрою. В таблиці 1 дана повна арифметична таблиця множення лишків a_i та b_i за модулем m_i=11, в таблиці 2 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.

Таблиця 1

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

a_i / b_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 представлені у КТМ $a_i = (\gamma_{a_i}; a_i')$ та $b_i = (\gamma_{b_i}; b_i')$, 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 1 (за другим квадрантом) визначається результат множення виду $(a_i' \cdot b_i') \bmod m_i = (\gamma_{c_i}; c_i')$, де $1 \geq a_i', b_i'$ та $c_i' \leq \frac{(m_i - 1)}{2}$. Після цього, якщо $\gamma_{a_i} = \gamma_{b_i}$, тоді індекс γ_{c_i} не треба інвертувати, а якщо $\gamma_{a_i} \neq \gamma_{b_i}$, тоді індекс γ_{c_i} треба інвертувати (0→1 або 1→0).

Таблиця 2

Представлення чисел у КТМ

Представлення чисел $a_i(b_i)$ у КТМ			
Представлення числа у десятковому коді	Представлення числа 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

В загальному випадку індекс КТМ визначається наступним чином

$$\gamma_{a_i}(\gamma_{b_i}, \gamma_{c_i}) = \begin{cases} 0, \text{ якщо } 1 \leq a_i(b_i, c_i) \leq (m_i - 1) \cdot 2, \\ 1, \text{ якщо } \frac{(m_i + 1)}{2} \leq a_i(b_i, c_i) \leq (m_i + 1) \cdot 2. \end{cases}$$

На кресленні представлена блок-схема пристрою множення лишків a_i та b_i числа за довільним модулем m_i, СЗК, 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 a_i та b_i 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, 17 - перший і другий елементи І; 18 - комутатор (табличний пристрій для визначення результату операції $(a_i' \cdot b_i')\mathrm{mod}m_i$); 19 - вихід пристрою; 20 - вихідний регістр; 21 - шифратор (пристрій для перетворення унітарного коду значення результату операції $(a_i' \cdot b_i')\mathrm{mod}m_i$ у двійковий код); 22 - третя група елементів І; 23 - група ключових елементів; 24 - суматор за модулем m_i (суматор призначений для інвертування значення $(a_i' \cdot b_i')\mathrm{mod}m_i$, тобто, на виході суматора отримуємо значення $m_i - (a_i' \cdot b_i')\mathrm{mod}m_i$); 25 - четверта група елементів І; 26 - шини подачі значення модуля m_i у двійковому коді; 27, 28 - п'ятий і шостий елементи 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 $(m_i\text{-}1)$-й виходи першого 5 та другого 6 дешифраторів підключено до входів перших елементів АБО першої 7 та другої 8 груп елементів АБО, другий та $(m_i\text{-}2)$-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 $\left(\frac{m_i-1}{2}\right)$-го та $\left(\frac{m_i+1}{2}\right)$-го першого 5 та другого 6 дешифраторів підключено до входів $\left(\frac{m_i-1}{2}\right)$-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 входів першого 16 елемента І, а виходи третього 14 та четвертого 15 елементів АБО підключено до входів другого 17 елемента І, виходи елементів І першої 9 та другої 10 груп підключені відповідно до першої та другої груп входів комутатора 18, а вихід 19 вихідного регістра 20 є виходом пристрою, при цьому виходи комутатора 18 підключено до входів шифратора 21, виходи якого підключено до перших (інформаційних) входів елементів І третьої 22 групи та вентильних елементів 23 групи, виходи елементів І третьої 22 групи підключено до першої групи входів суматора 24 за модулем m_i, до другої групи входів якого підключено виходи елементів І четвертої 25 групи, до перших (інформаційних) входів елементів І четвертої 25 групи підключено шини 26 подачі сигналів, що визначають значення модуля m_i за яким працює пристрій, до других (керуючих) входів елементів І третьої 22 і четвертої 25 груп, а також до других (заборонених) входів вентильних елементів 23 підключено вихід п'ятого 27 елемента АБО, до входу якого підключено виходи першого 16 та другого 17 елементів І, виходи суматора 24 за модулем m_i і виходи ключових елементів 23 групи через шостий 28 елемент АБО підключено до входу вихідного регістра 20.

Пристрій функціонує наступним чином. За входами 1 і 2 до пристрою у двійковому коді надходять значення першого a_i і другого b_i чисел. З виходів першого 5 і другого 6 дешифраторів значення першого a_i і 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 елементів І 9 і 10 груп значення a_i' та b' надходять до входів комутатора 18, з виходу якого значення $(a_i' \cdot b_i')\mathrm{mod}m_i$, в унітарному коді надходить до входу шифратора 21 з виходу якого значення $(a_i' \cdot b_i')\mathrm{mod}m_i$, у двійковому коді надходить до перших (інформаційних) входів елементів І третьої 22 групи, а також вентильних елементів групи 23. Якщо $\gamma_{a_i} = \gamma_{b_i}$, тоді відсутній вихідний сигнал елемента АБО 27 і значення $(a_i' \cdot b_i')\mathrm{mod}m_i$ через відкриті вентильні елементи 23, елемент АБО 28 надходить до входу вихідного регістра 20. Якщо $\gamma_{a_i} \neq \gamma_{b_i}$, тоді присутній

вихідний сигнал елемента АБО 27 і значення $(a_i' \cdot b_i')\mathrm{mod}m_i$ через відкриті елементи І групи 22 надходить до першої групи входів суматора 24 за модулем m_i, до другої групи входів якого за шинами 26, через відкриті елементи І 25 у двійковому коді, надходить значення m_i модуля. З виходу суматора 24 за модулем m_i, значення $m_i - (a_i' \cdot b_i')\mathrm{mod}m_i$ через елемент АБО 28 надходить до входу вихідного регістра 20.

Наведемо приклад роботи винаходу при реалізації множення лишків a_i та b_i числа за модулем m_i=11 (табл. 1, 2). Нехай a_i=1001 та b_i=0011.

Значення чисел a_i=1001 та b_i=0011 за входами 1 і 2 надходять до пристрою. З виходів відповідних дешифраторів 5 і 6 значення $a_i' = 010\left(a_i = (\gamma_{a_i}; a_i') = (1;010)\right)$ та $b_i' = 010\left(b_i = (\gamma_{b_i}; b_i') = (1;011)\right)$ (див. табл. 2), які через відповідні елементи АБО 7 і 8, елементи І 9 і 10 надходять до входу комутатора 18. Так, як $\gamma_{a_i} \neq \gamma_{b_i}$, тоді присутній сигнал на виході елемента АБО 27, який відкриває елементи І груп 22 і 25 і закриває ключові елементи 23. В цьому випадку з виходу комутатора 18 значення $a_i' \cdot b_i' = 2 \cdot 3 = 6$ (див. табл. 1) в унітарному коді надходить до входу шифратора 21 з виходу якого значення 0110 через відкриті елементи І 22 надходять до першої групи входів суматора 24, до другої групи входів якого по шинах 26 у двійковому надходить значення модуля m_i=1011 за яким працює пристрій. З виходу суматора значення 1011-0110=0101 через елемент АБО 28 надходить до входу регістра 20.

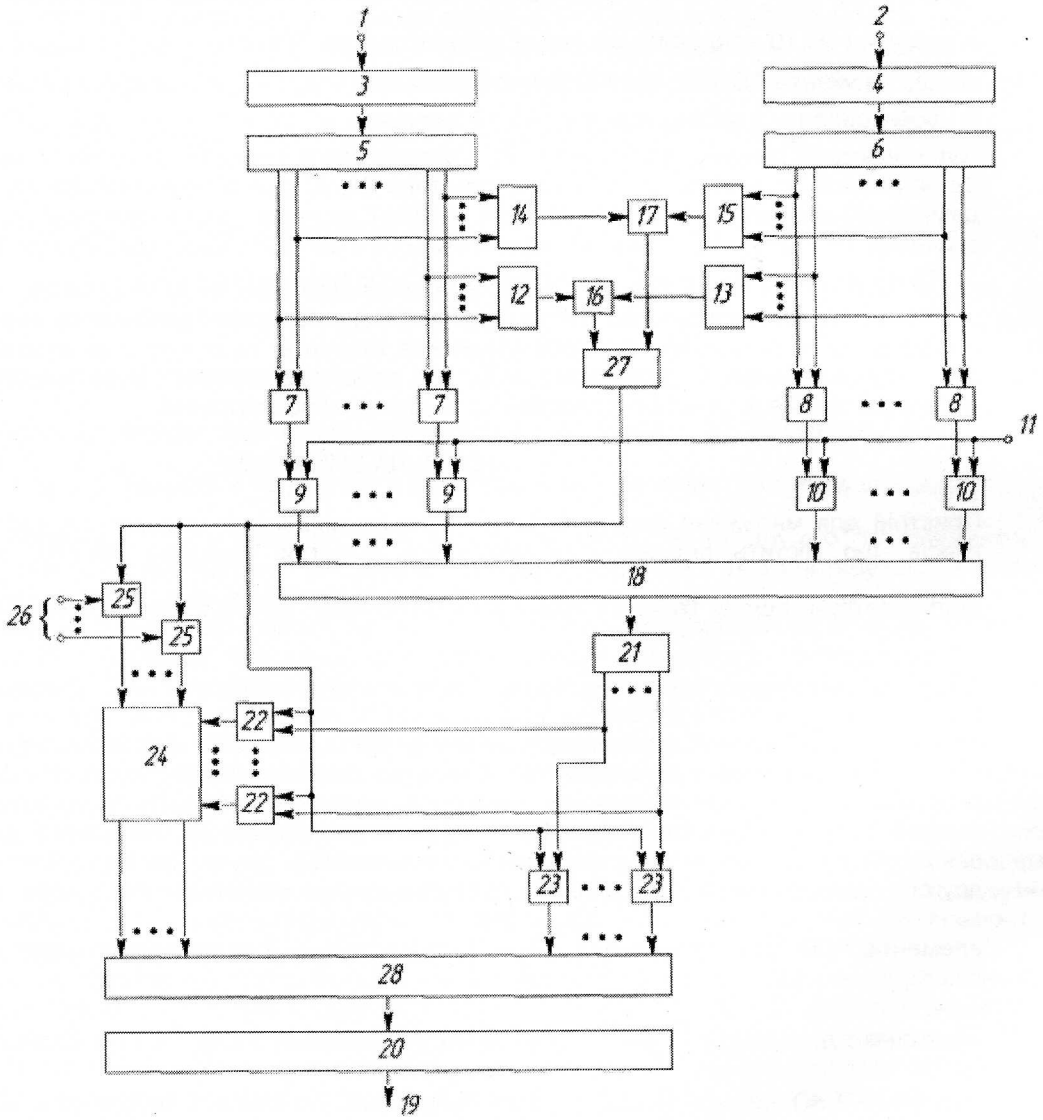
Перевірка: $(a_i \cdot b_i)\mathrm{mod}m_i = 1001 \cdot 0011 = 0101(\mathrm{mod}1011)$.

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 СЗК безпосередньо у двійковому коді. Це дозволяє використовувати результату операції множення лишків a_i та b_i безпосередньо у подальших обчисленнях.

ФОРМУЛА ВИНАХОДУ

Пристрій для множення лишків a_i та b_i числа за довільним модулем m_i системи залишкових класів, 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, перший, другий, третій і четвертий елементи АБО, перший і другий елементи 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 $1 \div \frac{m_i - 1}{2}$ 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 входів першого елемента І, а виходи третього та четвертого елементів АБО підключено до входів другого елемента І, 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 введено п'ятий і шостий елементи АБО, третю та четверту групи елементів І, групу ключових елементів, шифратор, суматор за модулем m_i, при цьому виходи комутатора підключено до входів шифратора, виходи якого підключено до перших інформаційних входів елементів І третьої групи та вентильних елементів групи, виходи елементів І третьої групи підключено до першої групи входів суматора за модулем m_i, до другої групи входів якого підключено виходи елементів І четвертої групи, до перших інформаційних входів елементів І четвертої групи підключено шини подачі сигналів, що визначають значення модуля m_i за яким працює пристрій, до других керуючих входів елементів І третьої та четвертої груп, а також до других заборонених входів ключових елементів підключено вихід п'ятого елемента АБО, до входу якого підключено виходи першого та другого елементів І, виходи суматора за модулем m_i і виходи ключових елементів через п'ятий елемент АБО підключено до входу вихідного регістра.



Комп'ютерна верстка Г. Паяльніков

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

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