УКРАЇНА

ПАТЕНТ

НА ВИНАХІД

№ 108828

ПРИСТРІЙ ДЛЯ РЕАЛІЗАЦІЇ ОПЕРАЦІЇ МОДУЛЬНОГО МНОЖЕННЯ ДВОХ ЧИСЕЛ, ЯКІ ПРЕДСТАВЛЕНІ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

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

Зареєстровано в Державному реєстрі патентів України на винаходи **10.06.2015.**

Голова Державної служби
інтелектуальної власності України А.Г. Жарінова

Державна служба інтелектуальної власності України
Ідентифікаційний код 37552556
№1

(11) **108828**

(19) **UA**

(51) **МПК** (2015.01)
G06F 7/52 (2006.01)
G06F 7/72 (2006.01)
H03M 7/00
H03M 7/18 (2006.01)

(21) Номер заявки: **a 2014 10608**

(22) Дата подання заявки: **29.09.2014**

(24) Дата, з якої є чинними права на винахід: **10.06.2015**

(41) Дата публікації відомостей про заявку та номер бюлетеня: **12.01.2015, Бюл.№ 1**

(46) Дата публікації відомостей про видачу патенту та номер бюлетеня: **10.06.2015, Бюл. № 11**

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

(73) Власники:
Краснобаєв Віктор Анатолійович,
вул. Астрономічна, 35-б, к. 24, м. Харків, 61085, UA,
Горбенко Іван Дмитрович,
пр. Л. Свободи, 50-а, к. 68, м. Харків, 61204, 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 РЕАЛІЗАЦІЇ ОПЕРАЦІЇ МОДУЛЬНОГО МНОЖЕННЯ ДВОХ ЧИСЕЛ, ЯКІ ПРЕДСТАВЛЕНІ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

(57) Формула винаходу:

Пристрій для модульного множення двох чисел, які представлені у системі залишкових класів (СЗК), який містить перший та другий вхідні прийомні регістри, вихідний прийомний регістр, регістр результату операції, суматор за модулем два, першу групу елементів АБО, групу з n пристроїв для множення $c' = (a_1' \cdot b_1') \bmod m_i$ двох лишків a_i' та b_i' чисел $A'_{СЗК}$ та $B'_{СЗК}$ за відповідними модулями m_i $(i = \overline{1,n}; n$ - кількість модулів СЗК), першу групу елементів І, групу вентилів, перший суматор за модулем $M = \prod_{i=1}^{n} m_i$, при цьому виходи і-х $(i = \overline{1,n})$

підрегістрів першого та другого вхідних прийомних регістрів підключено до входів і-го пристрою для множення лишків a_i' та b_i', відповідно чисел $A'_{СЗК}$ та $B'_{СЗК}$, за модулем m_i СЗК, виходи групи пристроїв множення лишків a_i' та b_i' за модулями m_i підключено до входів відповідних і-х підрегістрів вихідного прийомного регістру, вихід якого підключено до перших входів елементів І першої групи та до перших (інформаційних) входів вентильних елементів групи, виходи елементів І першої групи підключено до перших входів першого суматора за модулем $M = \prod_{i=1}^{n} m_i$, до других входів якого підключена шина подачі значення $\frac{M}{2}$, виходи першого суматора за модулем $M = \prod_{i=1}^{n} m_i$ і вентильних елементів групи через елементи АБО першої групи підключено до входу регістру результату операції, виходи перших (за модулем m_1 СЗК) підрегістрів вхідних прийомних регістрів підключено до входів суматора за модулем два, вихід якого підключено до других входів елементів І першої групи та до других входів вентильних елементів групи, який **відрізняється** тим, що в пристрій додатково введено перший та другий вхідні регістри, вихідний регістр, другу, третю, четверту та п'яту групи елементів І, другу та третю групи елементів АБО, другий, третій, четвертий, п'ятий та шостий суматори за модулем $M = \prod_{i=1}^{n} m_i$, при цьому, перший вхід пристрою підключено до входу першого вхідного регістру, вихід якого підключено до перших входів елементів І другої та третьої груп, виходи яких підключено до перших входів відповідно другого та третього суматорів за модулем $M = \prod_{i=1}^{n} m_i$, виходи яких через елементи АБО другої групи підключено до входу першого вхідного прийомного регістру, другий вхід пристрою підключено до входу другого вхідного регістру, вихід якого підключено до перших входів елементів І четвертої та п'ятої груп, виходи яких підключено до перших входів відповідно четвертого та п'ятого суматорів за модулем $M = \prod_{i=1}^{n} m_i$, виходи яких через елементи АБО третьої групи підключено до входу другого вхідного прийомного регістру, вихід регістру результату операції підключено до перших входів шостого суматора за модулем $M = \prod_{i=1}^{n} m_i$, вихід якого підключено до входу вихідного регістру, вихід якого є виходом пристрою, перша шина подачі сигналу ознаки "ДОДАВАННЯ 1" підключена до других входів елементів І другої групи, а друга шина подачі сигналу ознаки "ДОДАВАННЯ 2" підключена до других входів елементів І четвертої групи, перша шина подачі сигналу ознаки "ВІДНІМАННЯ 1" підключена до других входів елементів І третьої групи, а друга шина подачі сигналу ознаки "ВІДНІМАННЯ 2" підключена до других входів елементів І п'ятої групи, шина подачі значення $\frac{M}{2}$ підключена до других входів другого, третього, четвертого, п'ятого та шостого суматорів за модулем $M = \prod_{i=1}^{n} m_i$.

Пронумеровано, прошито металевими
люверсами та скріплено печаткою
3 арк.
10.06.2015

Уповноважена особа

Державна служба інтелектуальної власності України
Ідентифікаційний код 37552556
№1

(підпис)

УКРАЇНА

(19) **UA** (11) **108828** (13) **C2**

(51) МПК (2015.01)
G06F 7/52 (2006.01)
G06F 7/72 (2006.01)
H03M 7/00
H03M 7/18 (2006.01)

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки: **a 2014 10608**

(22) Дата подання заявки: **29.09.2014**

(24) Дата, з якої є чинними права на винахід: **10.06.2015**

(41) Публікація відомостей про заявку: **12.01.2015, Бюл.№ 1**

(46) Публікація відомостей про видачу патенту: **10.06.2015, Бюл.№ 11**

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

(73) Власник(и):
Краснобаєв Віктор Анатолійович,
вул. Астрономічна, 35-б, к. 24, м. Харків, 61085 (UA),
Горбенко Іван Дмитрович,
пр. Л. Свободи, 50-а, к. 68, м. Харків, 61204 (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:
SU 922731 A1, 23.04.1972
UA 70442 U, 11.06.2012
UA 91321 U, 25.06.2014
UA 68803 U, 10.04.2012
EP 1480119 A11, 24.11.2004
US 6341299 B1, 22.02.2002
US 4363106 A, 07.12.1982
JPS 6089246 A, 20.05.1985
RU 2509345 C1, 10.03.2014
US 2011231465 A1, 22.09.2011
US 2002120658 A1, 29.08.2009
US 6366940 B1, 02.04.2002
US 2006184600 A1, 17.08.2006

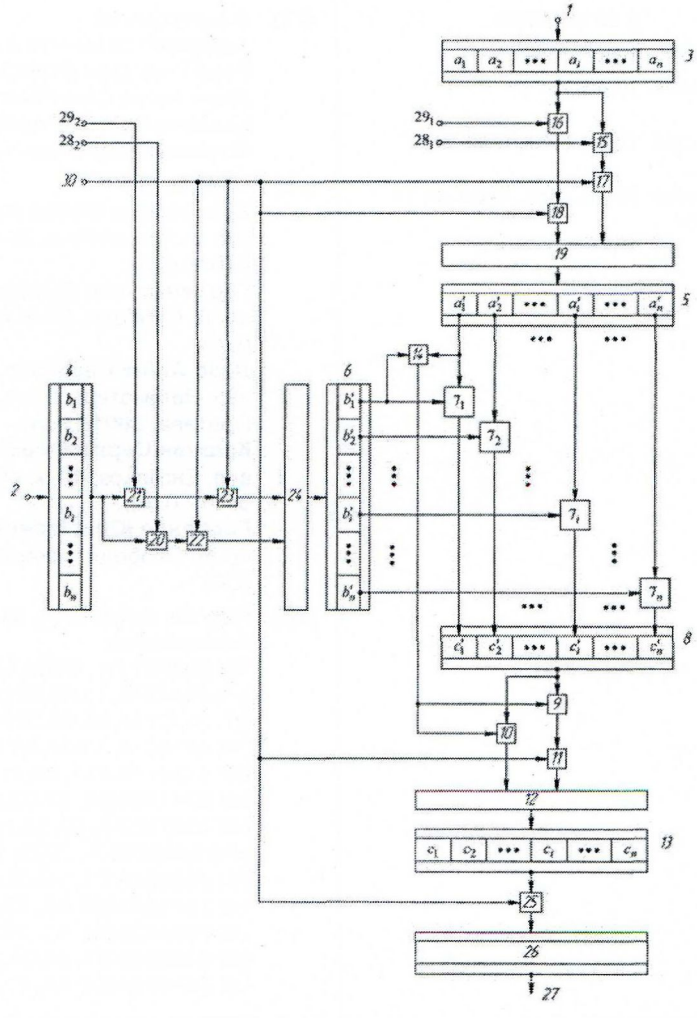
(54) ПРИСТРІЙ ДЛЯ РЕАЛІЗАЦІЇ ОПЕРАЦІЇ МОДУЛЬНОГО МНОЖЕННЯ ДВОХ ЧИСЕЛ, ЯКІ ПРЕДСТАВЛЕНІ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

(57) Реферат:

Винахід належить до області обчислювальної техніки і призначений для модульного множення двох чисел, як в додатному, так і у від'ємному числових діапазонах, які представлені у непозиційній системі числення залишкових класів. Пристрій для реалізації операції модульного

UA 108828 C2

множення двох чисел, які представлені у системі залишкових класів містить перший та другий вхідні прийомні регістри, вихідний прийомний регістр, регістр результату операції, суматор за модулем два, першу групу елементів АБО, групу з n пристроїв для множення двох лишків a_i' та b_i' чисел $A'_{СЗК}$ та $B'_{СЗК}$ за відповідними модулями, першу групу елементів І, групу вентилів, перший суматор за модулем $M=\prod_{i=1}^{n} m_i$, в який додатково введені перший та другий вхідні регістри, вихідний регістр, другу, третю, четверту та п'яту групи елементів І, другу та третю групи елементів АБО, другий, третій, четвертий, п'ятий та шостий суматори за модулем $M=\prod_{i=1}^{n} m_i$. Технічним результатом, що досягається даним винаходом є розширення функціональних можливостей пристрою множення за рахунок виконання додаткових операції перетворення чисел представлених безпосередньо у СЗК, у числа представлені у штучній формі СЗК.



Фіг. 1

Винахід (пристрій) належить до області обчислювальної техніки і призначено для модульного множення двох чисел, як в додатному, так і у від'ємному числових діапазонах, які представлені у непозиційній системі числення залишкових класів (СЗК).

Відомий пристрій (аналог) для множення по довільному модулю m_i КЛ (А.с. СРСР № 922731, кл. МПК G06F 7/39, Б В. № 15, 1982 р.), що містить вхідні регістри, дешифратори, групи елементів АБО, групи елементів І, суматор по модулю два, елементи І та АБО, комутатор та вихідний регістр.

Недоліком відомого пристрою є низькі функціональні можливості, які полягають в тому, що у даному пристрою неможливо реалізувати операцію перетворення чисел $A_{СЗК} = (a_1, a_2, ..., a_i, ..., a_n)$ і $B_{СЗК} = (b_1, b_2, ..., b_i, ..., b_n)$, представлених у СЗК, у числа $A'_{СЗК} = (a'_1, a'_2, ..., a'_i, ..., a'_n)$ і $B'_{СЗК} = (b'_1, b'_2, ..., b'_i, ..., b'_n)$, що представлені у штучній формі (ШФ) СЗК та навпаки.

Відомий пристрій (аналог) для множення по довільному модулю m_i КЛ є пристрій для множення по довільному модулю (Пат. № 60078, Україна, МПК (2011.01) G 06 F 7/00. Опубл. 10.06.2011., Б В. № 11). Він містить вхідні регістри, дешифратори, групи елементів АБО, групи елементів І, суматор по модулю два, елементи І та АБО, комутатор та вихідний регістр.

Недоліком відомого пристрою є низькі функціональні можливості, які полягають в тому, що у даному пристрою неможливо реалізувати операцію перетворення чисел $A_{СЗК} = (a_1, a_2, ..., a_i, ..., a_n)$ і $B_{СЗК} = (b_1, b_2, ..., b_i, ..., b_n)$, представлених у СЗК, у числа $A'_{СЗК} = (a'_1, a'_2, ..., a'_i, ..., a'_n)$ і $B'_{СЗК} = (b'_1, b'_2, ..., b'_i, ..., b'_n)$, що представлені у ШФ СЗК і навпаки.

Відомий пристрій (аналог) - табличний пристрій для множення двох чисел у КЛ (Пат. № 70442 Україна, МПК G06F 7/52. Б В № 11 від 11.06.2012 р. (2006.01)). Табличний пристрій для множення двох чисел у класі лишків, який містить перший та другий входи пристрою, перший та другий вхідні регістри, суматор за модулем два, групу елементів АБО, вихідний регістр, вихід пристрою, при цьому перший та другий входи пристрою підключено до входів відповідно першого та другого вхідних регістрів, а вихід вихідного регістру є виходом пристрою.

Недоліком аналогу є низькі функціональні можливості, які полягають в тому, що у даному пристрою неможливо реалізувати операцію перетворення чисел $A_{СЗК} = (a_1, a_2, ..., a_i, ..., a_n)$ і $B_{СЗК} = (b_1, b_2, ..., b_i, ..., b_n)$, представлених у СЗК, у числа $A'_{СЗК} = (a'_1, a'_2, ..., a'_i, ..., a'_n)$ і $B'_{СЗК} = (b'_1, b'_2, ..., b'_i, ..., b'_n)$, що представлені у ШФ СЗК і навпаки.

Найбільш близьким аналогом (прототипом) за технічною суттю і результатом, що досягається, є пристрій для реалізації операції множення двох чисел у класі лишків (Деклараційний патент на корисну модель № 91321 Україна, МПК G06F 7/52. БВ № 12 від 25.06.2014 р. (2006.01)). Пристрій містить перший та другий входи пристрою, перший та другий вхідні регістри, суматор за модулем два, групу елементів АБО, вихідний регістр, вихід пристрою, групу n пристроїв для множення двох лишків a'_i та b'_i чисел A' та B' за модулями m_i ($i = \overline{1,n}$; n - кількість модулів КЛ), прийомний регістр, групу елементів І, групу вентилів, суматор за модулем $M = \prod_{i=1}^{n} m_i$. При цьому перший та другий входи пристрою підключено до входів відповідно першого та другого вхідних регістрів, а вихід вихідного регістру є виходом пристрою. Виходи $i-x$ $\left(i = \overline{1,n}\right)$ підрегістрів першого та другого вхідних регістрів підключено до входів і-го пристрою для множення лишків a_i та b_i відповідно чисел А та В за модулем m_i КЛ, виходи групи пристроїв множення лишків a_i та b_i за модулями m_i підключено до входів відповідних і-х під регістрів прийомного регістру, вихід якого підключено до перших входів елементів І та вентильних елементів груп. Виходи елементів І групи підключено до перших входів суматора за модулем $M = \prod_{i=1}^{n} m_i$, до других входів якого підключена шина подачі значення $\frac{M}{2}$, виходи суматора за модулем М і вентильних елементів групи через елементи АБО групи підключено до входу вихідного регістру, виходи перших (за модулем m_1 КЛ) підрегістрів вхідних регістрів підключено до входів суматора за модулем два, вихід якого підключено до других входів елементів І групи та до других (заборонених) входів вентильних елементів групи.

Недоліком прототипу є низькі функціональні можливості, які полягають в тому, що у даному пристрою неможливо реалізувати операцію перетворення чисел $A_{СЗК} = (a_1, a_2, ..., a_i, ..., a_n)$ і

$B_{СЗК} = (b_1, b_2, ..., b_i, ..., b_n)$, представлених у СЗК, у числа $A' = (a_1', a_2', ..., a_i', ..., a_n')$ і $B' = (b_1', b_2', ..., b_i', ..., b_n')$, що представлені у ШФ СЗК і навпаки. Дана обставина не дозволяє, коли є необхідність, безпосередньо контролювати та коректувати дані, що представлено у вигляді чисел $A'_{СЗК} = (a_1', a_2', ..., a_i', ..., a_n')$ і $B'_{СЗК} = (b_1', b_2', ..., b_i', ..., b_n')$, а також результат $C'_{СЗК} = (c_1', c_2', ..., c_i', ..., c_n')$ операції модульного множення цих двох чисел $A'_{СЗК} = (a_1', a_2', ..., a_i', ..., a_n')$ і $B'_{СЗК} = (b_1', b_2', ..., b_i', ..., b_n')$.

В основу винаходу поставлено задачу розширення функціональних можливостей пристрою-прототипу за рахунок виконання додаткової операції перетворення чисел $A_{СЗК} = (a_1, a_2, ..., a_i, ..., a_n)$ і $B_{СЗК} = (b_1, b_2, ..., b_i, ..., b_n)$, представлених безпосередньо у СЗК, у числа $A'_{СЗК} = (a_1', a_2', ..., a_i', ..., a_n')$ і $B'_{СЗК} = (b_1', b_2', ..., b_i', ..., b_n')$, що представлені у ШФ СЗК і навпаки. Це дає можливість, при необхідності, безпосередньо контролювати та коректувати дані, що представлено у вигляді чисел $A_{СЗК} = (a_1, a_2, ..., a_i, ..., a_n)$, $B_{СЗК} = (b_1, b_2, ..., b_i, ..., b_n)$, $A'_{СЗК} = (a_1', a_2', ..., a_i', ..., a_n')$, $B'_{СЗК} = (b_1', b_2', ..., b_i', ..., b_n')$ і $C'_{СЗК} = (c_1', c_2', ..., c_i', ..., c_n')$.

Поставлена задача вирішується тим, що пристрій для реалізації операції модульного множення двох чисел, які представлені у системі залишкових класів, містить перший та другий вхідні прийомні регістри, вихідний прийомний регістр, регістр результату операції, суматор за модулем два, першу групу елементів АБО, групу з n пристроїв для множення $c_i' = (a_i' \cdot b_i') \bmod m_i$ двох лишків a_i' та b_i' чисел $A'_{СЗК}$ та $B'_{СЗК}$ за модулями m_i ($i = \overline{1,n}$; n - кількість модулів СЗК), першу групу елементів І, першу групу вентилів, перший суматор за модулем $M = \prod_{i=1}^{n} m_i$. При цьому виходи і-х $(i = \overline{1,n})$ підрегістрів першого та другого вхідних прийомних регістрів підключено до входів і-го пристрою для множення лишків a_i' та b_i', відповідно чисел $A'_{СЗК}$ та $B'_{СЗК}$, за модулем m_i СЗК, виходи групи пристроїв множення лишків a_i' та b_i' за модулями m_i підключено до входів відповідних і-х підрегістрів вихідного прийомного регістру, вихід якого підключено до перших входів елементів І першої групи та вентильних елементів першої групи, виходи елементів І першої групи підключено до перших входів суматора за модулем $M = \prod_{i=1}^{n} m_i$, до других входів якого підключена шина подачі значення $\frac{M}{2}$. Виходи суматора за модулем $M = \prod_{i=1}^{n} m_i$ і вентильних елементів першої групи через елементи АБО першої групи підключено до входу регістру результату операції, виходи перших (за модулем m_1 КЛ) підрегістрів вхідних прийомних регістрів підключено до входів суматора за модулем два, вихід якого підключено до других входів елементів І першої групи та до других (заборонених) входів вентильних елементів першої групи. При цьому пристрій додатково містить перший та другий вхідні регістри, вихідний регістр, другу, третю, четверту та п'яту групи елементів І, другу та третю групи елементів АБО, другий, третій, четвертий, п'ятий та шостий суматори за модулем $M = \prod_{i=1}^{n} m_i$. Перший вхід пристрою підключено до входу першого вхідного регістру, вихід якого підключено до перших входів елементів І другої та третьої груп, виходи яких підключено до перших входів відповідно другого та третього суматорів за модулем $M = \prod_{i=1}^{n} m_i$, виходи яких через елементи АБО другої групи підключено до входу першого вхідного прийомного регістру, другий вхід пристрою підключено до входу другого вхідного регістру, вихід якого підключено до перших входів елементів І четвертої та п'ятої груп, виходи яких підключено до перших входів відповідно четвертого та п'ятого суматорів за модулем $M = \prod_{i=1}^{n} m_i$, виходи яких через елементи АБО третьої групи підключено до входу другого вхідного прийомного регістру. Вихід регістру результату

операції підключено до перших входів шостого суматора за модулем $M=\prod_{i=1}^{n} m_i$, вихід якого підключено до входу вихідного регістру, вихід якого є виходом пристрою, перша шина подачі сигналу ознаки "ДОДАВАННЯ 1" підключена до других входів елементів І другої групи, а друга шина подачі сигналу ознаки "ДОДАВАННЯ 2" підключена до других входів елементів І четвертої групи, перша шина подачі сигналу ознаки "ВІДНІМАННЯ 1" підключена до других входів елементів І третьої групи, а друга шина подачі сигналу ознаки "ВІДНІМАННЯ 2" підключена до других входів елементів І п'ятої групи, шина подачі значення $\frac{M}{2}$ підключена до других входів другого, третього, четвертого, п'ятого та шостого суматорів за модулем $M=\prod_{i=1}^{n} m_i$.

Введення вказаних ознак дозволяє розширити функціональні можливості пристрою-прототипу за рахунок виконання додаткової операції перетворення чисел $A_{СЗК}=(a_1,a_2,...,a_i,...,a_n)$ і $B_{СЗК}=(b_1,b_2,...,b_i,...,b_n)$, представлених безпосередньо у СЗК, у числа $A'_{СЗК}=(a'_1,a'_2,...,a'_i,...,a'_n)$ і $B'_{СЗК}=(b'_1,b'_2,...,b'_i,...,b'_n)$, що представлені у ШФ СЗК. Це дає можливість, при необхідності, безпосередньо контролювати та коректувати дані, що представлено у вигляді чисел $A'_{СЗК}=(a'_1,a'_2,...,a'_i,...,a'_n)$ і $B'_{СЗК}=(b'_1,b'_2,...,b'_i,...,b'_n)$ і $C'_{СЗК}=(c'_1,c'_2,...,c'_i,...,c'_n)$.

У запропонованому пристрою процес виконання операції множення у СЗК, як у додатному, так і у від'ємному числових діапазонах, здійснюється над вхідними числами $A_{СЗК}=(a_1,a_2,...,a_i,...,a_n)$ і $B_{СЗК}=(b_1,b_2,...,b_i,...,b_n)$, що представлені у ШФ, тобто у вигляді $A'_{СЗК}=(a'_1,a'_2,...,a'_i,...,a'_n)$ і $B'_{СЗК}=(b'_1,b'_2,...,b'_i,...,b'_n)$. Штучна форма чисел $A_{СЗК}$ та $B_{СЗК}$, що представлені у СЗК, визначається наступним чином

$$\begin{cases} A'_{СЗК}(B'_{СЗК})=\frac{M}{2}+|A_{СЗК}|(|B_{СЗК}|), \text{если } A_{СЗК}(B_{СЗК})\geq 0, \\ A'_{СЗК}(B'_{СЗК})=\frac{M}{2}-|A_{СЗК}|(|B_{СЗК}|), \text{если } A_{СЗК}(B_{СЗК})<0, \end{cases} \quad (1)$$

тобто, для додатних чисел $A'_{СЗК}=\frac{M}{2}+|A_{СЗК}|$, а для від'ємних - $A'_{СЗК}=\frac{M}{2}-|A_{СЗК}|$, де $M=\prod_{i=1}^{n} m_i$.

У цьому випадку, для $m_1=2$, алгоритм виконання операції множення у СЗК як у додатному, так і у від'ємному числових діапазонах, представлено у вигляді

$$(A_{СЗК}\cdot B_{СЗК})'=f(A'_{СЗК},B'_{СЗК})=\begin{cases} A'_{СЗК}\cdot B'_{СЗК}, \text{якщо } A'_{СЗК} \text{ і } B'_{СЗК} \text{ однакової парності}, \\ A'_{СЗК}\cdot B'_{СЗК}+\frac{M}{2}, \text{якщо } A'_{СЗК} \text{ і } B'_{СЗК} \text{ різної парності}. \end{cases} \quad (2)$$

На малюнку (фіг. 1) представлена блок-схема пристрою для реалізації операції модульного множення двох чисел, які представлені у системі залишкових класів.

На малюнку (фіг. 2) представлена блок-схема пристрою для реалізації операції модульного множення двох чисел, які представлені у системі залишкових класів, що задана основами $m_1=2$, $m_2=3$, $m_3=5$.

В таблиці 1 представлено кодові слова для СЗК, що задана основами $m_1=2$, $m_2=3$, $m_3=5$.

На фіг. 1 представлена блок-схема пристрою для реалізації операції модульного множення двох чисел, які представлені у системі залишкових класів, де: 1, 2 - перший та другий входи пристрою; 3, 4 - перший та другий вхідні регістри; 5, 6 - перший та другий вхідні прийомні регістри; 7_1-7_n група пристроїв множення $c'_i=(a'_i\cdot b'_i)\bmod m_i$ лишків a'_i та b'_i за модулями m_i $i=\overline{1,n}$; 8 - вихідний прийомний регістр; 9 - перша група елементів І; 10 - група вентильних елементів; 11 - перший суматор за модулем $M=\prod_{i=1}^{n} m_i$, 12 - перша група елементів АБО; 13 - регістр результату операції; 14 - суматор за модулем два; 15, 16 - друга та третя групи

елементів І; 17, 18 - другий та третій суматори за модулем $M = \prod_{i=1}^{n} m_i$; 19 - друга група елементів АБО; 20, 21 - четверта та п'ята групи елементів І; 22, 23 - четвертий та п'ятий суматори за модулем $M = \prod_{i=1}^{n} m_i$; 24 - третя група елементів АБО; 25 - шостий суматор за модулем $M = \prod_{i=1}^{n} m_i$; 26 - вихідний регістр;

Таблиця 1

Кодові слова у СЗК

А (В) у ПСЧ	A' (B') у ПСЧ	$A'_{СЗК}$ $(B'_{СЗК})$ у СЗК		
		$m_1 = 2$	$m_2 = 3$	$m_3 = 5$
-15	0	0	0	0
-14	1	1	1	1
-13	2	0	2	2
-12	3	1	0	3
-11	4	0	1	4
-10	5	1	2	0
-9	6	0	0	1
-8	7	1	1	2
-7	8	0	2	3
-6	9	1	0	4
-5	10	0	1	0
-4	11	1	2	1
-3	12	0	0	2
-2	13	1	1	3
-1	14	0	2	4
0	15	1	0	0
1	16	0	1	1
2	17	1	2	2
3	18	0	0	3
4	19	1	1	4
5	20	0	2	0
6	21	1	0	1
7	22	0	1	2
8	23	1	2	3
9	24	0	0	4
10	25	1	1	0
11	26	0	2	1
12	27	1	0	2
13	28	0	1	3
14	29	1	2	4

В таблиці 2 представлено алгоритм функціонування суматора за модулем два

Таблиця 2

Алгоритм функціонування суматора 14

Входи суматора 14		Виходи суматора 14
a'_1	b'_1	$(a'_1 + b'_1) \bmod 2$
0	0	0
0	1	1
1	0	1
1	1	0

27 - вихід регістра; 28_1, 28_2 - шини подачі сигналу ознаки відповідно "ДОДАВАННЯ 1" та "ДОДАВАННЯ 2"; 29_1, 29_2 - шини подачі сигналу ознаки відповідно "ВІДНІМАННЯ 1" та "ВІДНІМАННЯ 2"; 30 - шина подачі значення $\frac{M}{2}$.

Перший 1 та другий 2 входи пристрою підключено до входів відповідно першого 3 та другого 4 вхідних регістрів. Виходи і-х $\left(i=\overline{1,n}\right)$ підрегістрів першого 5 та другого 6 вхідних прийомних регістрів підключено до входів і-го пристрою 7_1-7_n для множення лишків a_i' та b_i'. Виходи групи 7_1-7_n пристроїв множення лишків a_i' та b_i' за модулями m_i підключено до входів відповідних і-х підрегістрів вихідного прийомного регістру 8, вихід якого підключено до перших входів елементів І першої 9 групи та до перших (інформаційних) входів вентильних елементів групи 10. Виходи елементів І першої 9 групи підключено до перших входів першого 11 суматора за модулем $M=\prod_{i=1}^{n}m_i$, а виходи першого 11 суматора за модулем $M=\prod_{i=1}^{n}m_i$ і вентильних елементів групи 10 через елементи АБО першої 12 групи підключено до входу регістру 13 результату операції. Виходи перших (за модулем m_1 СЗК) підрегістрів вхідних прийомних регістрів 5 і 6 підключено до входів суматора 14 за модулем два, вихід якого підключено до других входів елементів І першої 9 групи та до других (заборонених) входів вентильних елементів групи 10. Вихід першого 3 вхідного регістру підключено до перших входів елементів І другої 15 та третьої 16 груп, виходи яких підключено до перших входів відповідно другого 17 та третього 18 суматорів за модулем $M=\prod_{i=1}^{n}m_i$, виходи яких, через елементи АБО другої 19 групи підключено до входу першого 5 вхідного прийомного регістру. Вихід другого 4 вхідного регістру підключено до перших входів елементів І четвертої 20 та п'ятої 21 груп, виходи яких підключено до перших входів відповідно четвертого 22 та п'ятого 23 суматорів за модулем $M=\prod_{i=1}^{n}m_i$, виходи яких через елементи АБО третьої 24 групи підключено до входу другого 6 вхідного прийомного регістру. Вихід регістру 13 результату операції підключено до перших входів шостого 25 суматора за модулем $M=\prod_{i=1}^{n}m_i$, вихід якого підключено до входу вихідного 26 регістру, вихід 27 якого є виходом пристрою. Перша 28_1 шина подачі сигналу ознаки "ДОДАВАННЯ 1" підключена до других входів елементів І другої 15 групи, а друга 28_2 шина подачі сигналу ознаки "ДОДАВАННЯ 2" підключена до других входів елементів І четвертої 20 групи. Перша 29_1 шина подачі сигналу ознаки "ВІДНІМАННЯ 1" підключена до других входів елементів І третьої 16 групи, а друга 29_2 шина подачі сигналу ознаки "ВІДНІМАННЯ 2" підключена до других входів елементів І, а п'ятої 21 групи. Шина 30 подачі значення $\frac{M}{2}$ підключена до других входів першого 11, другого 17, третього 18, четвертого 22, п'ятого 23 та шостого 25 суматорів за модулем $M=\prod_{i=1}^{n}m_i$.

Пристрій функціонує наступним чином (фіг. 1). За першим 1 та другим 2 входами пристрою до першого 3 та другого 4 вхідних регістрів поступають значення чисел $A_{СЗК}=(a_1,a_2,...,a_i,...,a_n)$ і $B_{СЗК}=(b_1,b_2,...,b_i,...,b_n)$ у КЛ. У відповідності зі співвідношенням (1) маємо, що коли $A_{СЗК}(B_{СЗК})\geq 0$, тоді відкриті елементи І груп 15 і 20 (присутній сигнал шин 28_1 і 28_2). На виході суматорів 17 і 22 маємо $A'_{СЗК}\left(B'_{СЗК}\right)=\frac{M}{2}+|A_{СЗК}|(|B_{СЗК}|)$ (присутній сигнал шини 30). Якщо $A_{СЗК}(B_{СЗК})<0$ тоді відкриті елементи І груп 16 і 21 (присутній сигнал шин 29_1 і 29_2). На виході суматорів 18 і 21 маємо, що $A'_{СЗК}\left(B'_{СЗК}\right)=\frac{M}{2}-|A_{СЗК}|(|B_{СЗК}|)$ (присутній сигнал шини 30). В цьому випадку до регістрів 5 і 6, через відповідні групи 19 і 24, поступає значення $A'_{СЗК}=\left(a_1',a_2',...,a_i',...,a_n'\right)$ і $B'_{СЗК}=\left(b_1',b_2',...,b_i',...,b_n'\right)$. З виходу регістрів 5 і 6 пара лишків a_i' та b_i' поступає до входів відповідного і-го пристрою 7_i для множення $c'=\left(a_1'\cdot b_1'\right)\mathrm{mod}m_i$, лишків a_i та b_i, відповідно чисел $A'_{СЗК}=\left(a_1',a_2',...,a_i',...,a_n'\right)$ і $B'_{СЗК}=\left(b_1',b_2',...,b_i',...,b_n'\right)$, за модулем m_i КЛ. 3

виходу пристрою 7_i для множення лишків $a_i^{'}$ та $b_i^{'}$ значення $c^{'}=(a_1^{'}\cdot b_1^{'})\mathrm{mod}m_i$, поступає до входу і-го підрегістру прийомного регістру 8, з виходу якого значення $C_{СЗК}^{'}=A_{СЗК}^{'}\cdot B_{СЗК}^{'}$, тобто $C_{СЗК}^{'}=(c_1^{'},c_2^{'},...,c_i^{'},...,c_n^{'})=(a_1^{'},a_2^{'},...,a_i^{'},...,a_n^{'})\cdot(b_1^{'},b_2^{'},...,b_i^{'},...,b_n^{'})$, поступає до перших входів елементів І 9 та вентильних елементів 10 груп, до других входів яких, з виходу суматора 14 за модулем два, поступає значення $(a_1^{'}+b_1^{'})\mathrm{mod}2$ (табл. 2). Якщо $(a_1^{'}+b_1^{'})\mathrm{mod}2=1$ (присутній вихідний сигнал суматора 14), тоді через відкриті елементи І 9 першої групи значення $C_{СЗК}^{'}=(c_1^{'},c_2^{'},...,c_i^{'},...,c_n^{'})$ поступає до перших входів першого суматора 11 за модулем $M=\prod_{i=1}^{n}m_i$, на другі входи якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу суматору 11 значення $C_{РСЗК}^{'}=\left(C_{СЗК}^{'}+\frac{M}{2}\right)\mathrm{mod}M$ через елементи АБО першої групи 12 поступає до входу регістру 13 результату операції. Якщо $(a_1^{'}+b_1^{'})\mathrm{mod}2=0$ (відсутній вихідний сигнал суматора 14), тоді через відкриті вентильні елементи групи 10 (відсутній сигнал заборони) значення $C_{СЗК}^{'}=(c_1^{'},c_2^{'},...,c_i^{'},...,c_n^{'})$ через елементи АБО першої групи 12 поступає до входу регістру 13 результату операції (див. співвідношення (2)). З виходу регістру 13 результату операції поступає до перших входів шостого 25 суматора за модулем $M=\prod_{i=1}^{n}m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу шостого 25 суматора за модулем $M=\prod_{i=1}^{n}m_i$, до входу вихідного регістру 26 поступає М результат $C_{РСЗК}=\left(C_{РСЗК}^{'}+\frac{M}{2}\right)\mathrm{mod}M$ операції множення двох чисел $A_{СЗК}=(a_1,a_2,...,a_i,...,a_n)$ і $B_{СЗК}=(b_1,b_2,...,b_i,...,b_n)$ у СЗК.

Розглянемо процес функціонування запропонованого винаходу для СЗК, що задана основами $m_1=2$, $m_2=3$, $m_3=5$ (див. фіг. 2, табл. 1, 2). При цьому: М = 30; $\frac{M}{2}=15$; у даній СЗК значення $\frac{M}{2}=15$ дорівнює $(1\|0\|0)$.

Приклад 1. Треба провести операцію модульного множення двох чисел $A_{ПСЧ}=3$, $B_{ПСЧ}=4$, що задано у СЗК у наступному вигляді $A_{СЗК}=(1\|0\|3)$ і $B_{СЗК}=(0\|1\|4)$. В цьому випадку присутні сигнали шин 28_1 і 28_2. За входами 1 і 2 пристрою в регістри 3 і 4 відповідно поступають числа $A_{СЗК}=(1\|0\|3)$ і $B_{СЗК}=(0\|1\|4)$. Значення $A_{СЗК}=(1\|0\|3)$ через відкриті елементи І другої групи поступає до перших входів другого 17 суматора за модулем $M=\prod_{i=1}^{n}m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу суматора 17, через елементи АБО другої 19 групи, значення $A_{СЗК}^{'}=\frac{M}{2}+A_{СЗК}=(1\|0\|0)+(1\|0\|3)=(0\|0\|3)$ поступає до входу регістру 5. Значення $B_{СЗК}=(0\|1\|4)$ через відкриті елементи І четвертої 20 групи поступає до перших входів четвертого 22 суматора за модулем $M=\prod_{i=1}^{n}m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу суматора 22, через елементи АБО третьої 24 групи, значення $B_{СЗК}^{'}=\frac{M}{2}+B_{СЗК}=(1\|0\|0)+(0\|1\|4)=(1\|1\|4)$ поступає до входу регістру 6. Значення підрегістрів регістрів 5 і 6 поступають на відповідні пристрої $7_1\div7_3$ для множення двох лишків $a_i^{'}$ та $b_i^{'}$. На виходах групи $7_1\div7_3$ пристроїв множення отримуємо наступні значення: $7_1-(0\cdot1)\mathrm{mod}2=0$; $7_2-(0\cdot1)\mathrm{mod}3=0$ і $7_3-(3\cdot4)\mathrm{mod}5=2$. Таким чином до входу регістру 8 поступає значення

$C'_{СЗК}=(0\|0\|2)$ результату множення двох чисел $A'_{СЗК}=(0\|0\|3)$ і $B'_{СЗК}=(1\|1\|4)$, що представлено у ШФ СЗК. Так як $(a'_1+b'_1)\bmod 2=(0+1)\bmod 2=1$ (табл. 2), тоді вихідний сигнал суматора 14 відкриває елементи І групи 9 (вентильні елементи групи 10 закриті). У цьому випадку з регістру 8 значення $C'_{СЗК}=(0\|0\|2)$ через відкриті елементи І першої групи 9 поступає до перших входів першого суматора 11 за модулем $M=\prod_{i=1}^{n}m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}=(1\|0\|0)$. З виходу суматора 11 результат множення двох чисел $A'_{СЗК}=(0\|0\|3)$ і $B'_{СЗК}=(1\|1\|4)$, представлений у вигляді $C'_{РСЗК}=\left(C'_{СЗК}+\frac{M}{2}\right)=(0\|0\|2)+(1\|0\|0)=(1\|0\|2)$, через елементи АБО першої 12 групи поступає до входу регістра 13, з виходу якого він поступає до перших входів шостого 25 суматора за модулем $M=\prod_{i=1}^{n}m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу суматора 25 результат $C_{РСЗК}=\left(C'_{РСЗК}+\frac{M}{2}\right)=(1\|0\|2)+(1\|0\|0)=(0\|0\|2)$ модульного множення двох чисел у СЗК $A_{СЗК}=(1\|0\|3)$ і $B_{СЗК}=(0\|1\|4)$ поступає до входу вихідного 26 регістру. У ПСЧ значення $(0\|0\|2)$ дорівнює 12.

Перевірка. Зробимо перевірку правильності отриманого результату $C'_{РСЗК}=(1\|0\|2)$ множення двох чисел $A'_{СЗК}=(0\|0\|3)$ (у ПСЧ $A'_{ПСЧ}=18$ і $A_{ПСЧ}=3$) та $B'_{СЗК}=(1\|1\|4)$ (у ПСЧ $B'_{ПСЧ}=19$ і $B_{ПСЧ}=4$) у ШФ СЗК. Результат $C_{РСЗК}=(0\|0\|2)$ множення у СЗК двох чисел $A_{СЗК}=(1\|0\|3)$ і $B_{СЗК}=(0\|1\|4)$ у ПСЧ дорівнює значенню 12. У відповідності з ознакою ШФ чисел у КЛ для перевірки отриманого результату маємо наступну умову, що представлена рівнянням:

$$(A_{ПСЧ}\cdot B_{ПСЧ})'=\left[\frac{M}{2}+(A_{ПСЧ}\cdot B_{ПСЧ})\right]\bmod M=C'_{РСЗК}\ \text{або}$$

$$(A_{ПСЧ}\cdot B_{ПСЧ})'=[15+(A_{ПСЧ}\cdot B_{ПСЧ})]\bmod 30=C'_{РСЗК}.$$

Таким чином маємо $(3\cdot 4)'=15+(3\cdot 4)=27=C'_{РСЗК}$. Значення добутку чисел $A_{ПСЧ}=3$ і $B_{ПСЧ}=4$ дорівнює 12, що відповідає значенню 27 у ШФ СЗК (див. табл. 1).

Приклад 2. Треба провести операцію модульного множення двох чисел $A_{ПСЧ}=-3$, $B_{ПСЧ}=-4$, (у СЗК $A_{СЗК}=(1\|0\|3)$ і $B_{СЗК}=(0\|1\|4)$). В цьому випадку присутні сигнали шин 29_1 і 29_2. За входами 1 і 2 пристрою в регістри 3 і 4 відповідно поступають числа $A_{СЗК}=(1\|0\|3))$ і $B_{СЗК}=(0\|1\|4)$. Значення $A_{СЗК}=(1\|0\|3)$ через відкриті елементи І третьої 16 групи поступає до перших входів третього 18 суматора за модулем $M=\prod_{i=1}^{n}m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу суматора 18, через елементи АБО другої 19 групи, значення $A'_{СЗК}=\frac{M}{2}-A_{СЗК}=(1\|0\|0)-(1\|0\|3)=(0\|0\|2)$ поступає до входу регістру 5. Значення $B_{СЗК}=(0\|1\|4)$ через відкриті елементи І п'ятої 21 групи поступає до перших входів п'ятого 23 суматора за модулем $M=\prod_{i=1}^{n}m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу п'ятого 23 суматора, через елементи АБО третьої 24 групи, значення $B'_{СЗК}=\frac{M}{2}-B_{СЗК}=(1\|0\|0)-(0\|1\|4)=(1\|2\|1)$ поступає до входу регістру 6. Значення підрегістрів регістрів 5 і 6 поступають на відповідні пристрої $7_1\div 7_3$ для множення двох лишків a'_i та b'_i. З

виходів групи $7_1 \div 7_3$ пристроїв множення отримуємо наступні значення: $7_1 - (0 \cdot 1) \bmod 2 = 0$; $7_2 - (0 \cdot 2) \bmod 3 = 0$ і $7_3 - (2 \cdot 1) \bmod 5 = 2$. Таким чином до входу регістру 8 поступає значення $C'_{СЗК} = (0 \| 0 \| 2)$. Так, як $(a'_1 + b'_1) \bmod 2 = (0+1) \bmod 2 = 1$, тоді вихідний сигнал суматора 14 присутній. Він відкриває елементи І першої 9 групи, через які значення $C'_{СЗК} = (0 \| 0 \| 2)$ поступає до перших входів суматора 11, до других входів якого за шиною 30 поступає значення $\frac{M}{2} = (1 \| 0 \| 0)$. З виходу суматора 11 значення $C'_{РСЗК} = \left(C'_{СЗК} + \frac{M}{2} \right) = (0 \| 0 \| 2) + (1 \| 0 \| 0) = (1 \| 0 \| 2)$ через елементи АБО першої 12 групи поступає до входу регістра 13, з виходу якого він поступає до перших входів шостого 25 суматора за модулем $M = \prod_{i=1}^{n} m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу суматора 25 результат $C_{РСЗК} = \left(C'_{РСЗК} + \frac{M}{2} \right) = (1 \| 0 \| 2) + (1 \| 0 \| 0) = (0 \| 0 \| 2)$ модульного множення двох чисел у СЗК поступає до входу вихідного 26 регістру. (Результат значення $C'_{РСЗК} = (1 \| 0 \| 2)$ у ПСЧ дорівнює 27).

Перевірка. $[(-3) \cdot (-4)]' = 15 + (-3) \cdot (-4) = 15 + 12 = 27 = C'_{РСЗК}$. Значення добутку чисел $A_{ПСЧ} = -3$ і $B_{ПСЧ} = -4$ дорівнює 12, що відповідає значенню 27 у ШФ СЗК (див. табл. 1).

Приклад 3. Треба провести операцію модульного множення двох чисел $A_{ПСЧ} = 3$, $B_{ПСЧ} = -4$ (у СЗК $A_{СЗК} = (1 \| 0 \| 3)$ і $B_{СЗК} = (0 \| 1 \| 4)$). В цьому випадку присутні сигнали шин 28_1 і 29_2. За входами 1 і 2 пристрою в регістри 3 і 4 відповідно поступають числа $A_{СЗК} = (1 \| 0 \| 3)$ і $B_{СЗК} = (0 \| 1 \| 4)$. Значення $A_{СЗК} = (1 \| 0 \| 3)$ через відкриті елементи І другої 15 групи поступає до перших входів другого 17 суматора за модулем $M = \prod_{i=1}^{n} m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу суматора 17, через елементи АБО другої 19 групи, значення $A'_{СЗК} = \frac{M}{2} + A_{СЗК} = (1 \| 0 \| 0) - (1 \| 0 \| 3) = (0 \| 0 \| 3)$ поступає до входу регістру 5. Значення $B_{СЗК} = (0 \| 1 \| 4)$ через відкриті елементи І п'ятої 21 групи поступає до перших входів п'ятого 23 суматора за модулем $M = \prod_{i=1}^{n} m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу п'ятого суматора 23, через елементи АБО третьої 24 групи, значення $B'_{СЗК} = \frac{M}{2} - B_{СЗК} = (1 \| 0 \| 0) - (0 \| 1 \| 4) = (1 \| 2 \| 1)$ поступає до входу регістру 6. Значення підрегістрів регістрів 5 і 6 поступають на відповідні пристрої $7_1 \div 7_3$ для множення двох лишків a'_i та b'_i. З виходів групи $7_1 \div 7_3$ пристроїв множення отримуємо наступні значення: $7_1 - (0 \cdot 1) \bmod 2 = 0$; $7_2 - (0 \cdot 2) \bmod 3 = 0$ і $7_3 - (3 \cdot 1) \bmod 5 = 2$. Таким чином до входу регістру 8 поступає значення $C'_{СЗК} = (0 \| 0 \| 3)$. Так, як $(a'_1 + b'_1) \bmod 2 = (0+1) \bmod 2 = 1$, тоді вихідний сигнал суматора 14 присутній. Він відкриває елементи І першої 9 групи, через які значення $C'_{СЗК} = (0 \| 0 \| 3)$ поступає до перших входів першого суматора 11, до других входів якого за шиною 30 поступає значення $\frac{M}{2} = (1 \| 0 \| 0)$. З виходу суматора 11 значення $C'_{РСЗК} = \left(C'_{СЗК} + \frac{M}{2} \right) = (0 \| 0 \| 3) + (1 \| 0 \| 0) = (1 \| 0 \| 3)$ через елементи АБО першої 12 групи поступає до входу регістра 13, з виходу якого воно поступає до перших входів шостого 25 суматора за модулем $M = \prod_{i=1}^{n} m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу суматора 25 результат

$C_{РСЗК} = \left(C'_{РСЗК} + \frac{M}{2} \right) = (1\|0\|3) + (1\|0\|0) = (0\|0\|3)$ операції модульного множення двох чисел у СЗК поступає до входу вихідного 26 регістру (значення $C'_{РСЗК} = (1\|0\|3)$ у ПСЧ дорівнює 3).

Перевірка. $[3 \cdot (-4)]' = 15 + 3 \cdot (-4) = 15 - 12 = 3 = C'_{РСЗК}$. Значення добутку чисел $A_{ПСЧ} = 3$ і $B_{ПСЧ} = -4$ дорівнює -12, що відповідає значенню 3 у ПІФ СЗК (див. табл. 1).

Приклад 4. Треба провести операцію модульного множення двох чисел $A_{ПСЧ} = -3$, $B_{ПСЧ} = 4$ (у СЗК $A_{СЗК} = (1\|0\|3)$ і $B_{СЗК} = (0\|1\|4)$). В цьому випадку присутні сигнали шин 29_1 і 28_2. За входами 1 і 2 пристрою в регістри 3 і 4 відповідно поступають числа $A_{СЗК} = (1\|0\|3)$ і $B_{СЗК} = (0\|1\|4)$. Значення $A_{СЗК} = (1\|0\|3)$ через відкриті елементи І третьої 16 групи поступає до перших входів третього 18 суматора за модулем $M = \prod_{i=1}^{n} m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу суматора 18, через елементи АБО другої 19 групи, значення $A'_{КЛ} = \frac{M}{2} - A_{КЛ} = (1\|0\|0) - (1\|0\|3) = (0\|0\|2)$ поступає до входу регістру 5. Значення $B_{СЗК} = (0\|1\|4)$ через відкриті елементи І четвертої 20 групи поступає до перших входів четвертого 22 суматора за модулем $M = \prod_{i=1}^{n} m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу суматора 22, через елементи АБО третьої 24 групи, значення $B'_{СЗК} = \frac{M}{2} + B_{СЗК} = (1\|0\|0) - (0\|1\|4) = (1\|1\|4)$ поступає до входу регістру 6. Значення підрегістрів регістрів 5 і 6 поступають на відповідні пристрої $7_1 \div 7_3$ для множення двох лишків a'_i та b'_i. З виходів групи $7_1 \div 7_3$ пристроїв множення отримуємо наступні значення: $7_1 - (0 \cdot 1) \bmod 2 = 0$; $7_2 - (0 \cdot 1) \bmod 3 = 0$ і $7_3 - (2 \cdot 4) \bmod 5 = 2$. Таким чином до входу регістру 8 поступає значення $C'_{СЗК} = (0\|0\|3)$. Так, як $(a'_1 + b'_1) \bmod 2 = (0+1) \bmod 2 = 1$, тоді вихідний сигнал суматора 14 присутній. Він відкриває елементи І першої 9 групи, через які значення $C'_{СЗК} = (0\|0\|3)$ поступає до перших входів суматора 11, до других входів якого за шиною 30 поступає значення $\frac{M}{2} = (1\|0\|0)$. З виходу суматора 11 значення $C'_{РСЗК} = \left(C'_{СЗК} + \frac{M}{2} \right) = (0\|0\|3) + (1\|0\|0) = (1\|0\|3)$ через елементи АБО першої 12 групи поступає до перших входів шостого 25 суматора за модулем $M = \prod_{i=1}^{n} m_i$, до других входів якого за шиною 30 поступає значення $\frac{M}{2}$. З виходу суматора 25 результат $C_{РСЗК} = \left(C'_{РСЗК} + \frac{M}{2} \right) = (1\|0\|3) + (1\|0\|0) = (0\|0\|3)$ модульного множення двох чисел у СЗК поступає до входу вихідного 26 регістру.

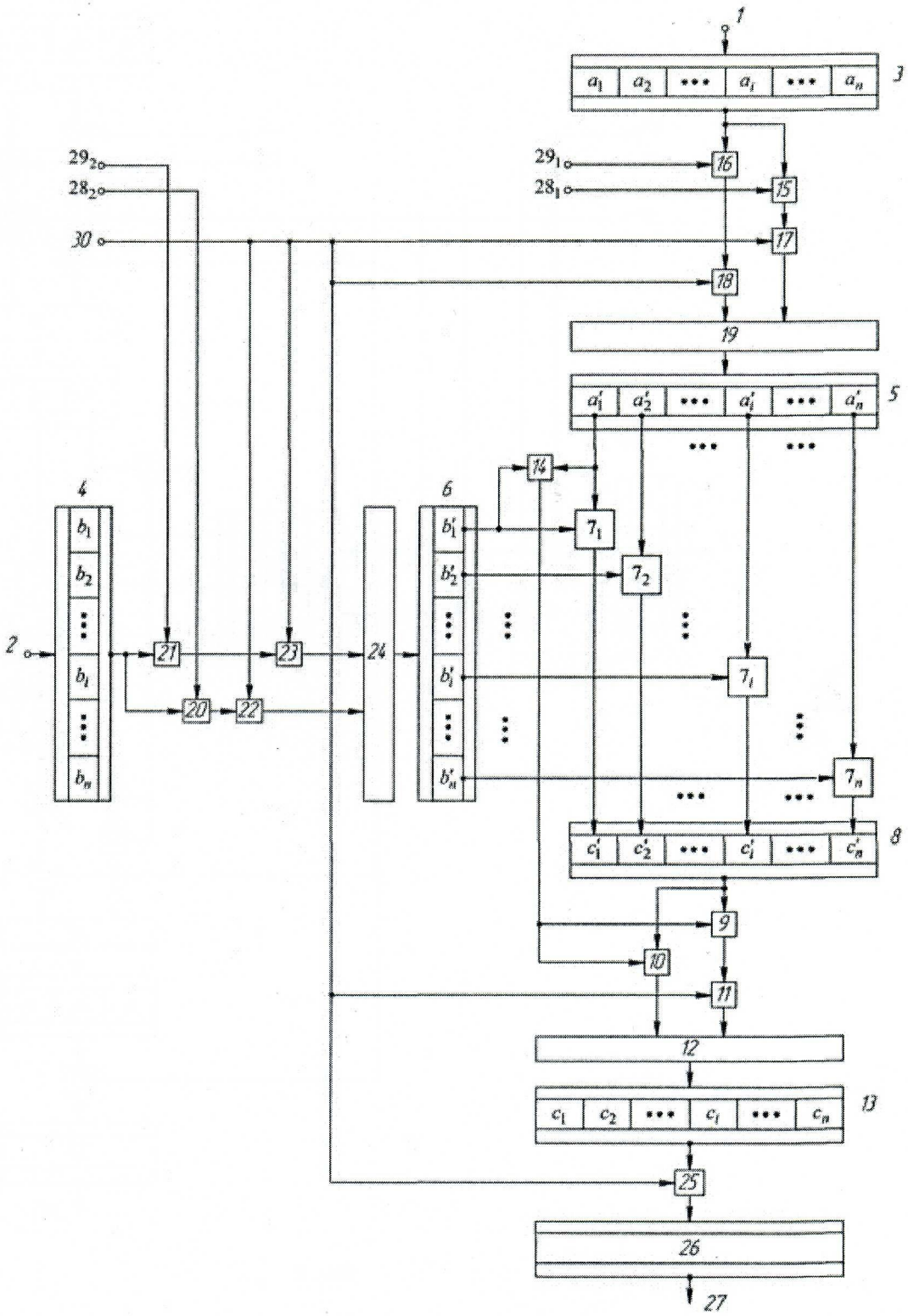
Перевірка. $[(-3) \cdot 4]' = 15 + (-3) \cdot 4 = 15 - 12 = 3 = C'_{РСЗК}$. Значення добутку чисел $A_{ПСЧ} = -3$ і $B_{ПСЧ} = 4$ дорівнює -12, що відповідає значенню 3 у ШФ СЗК (див. табл. 1).

Таким чином запропонований винахід дозволяє суттєво розширити функціональні можливості пристрою-прототипу за рахунок виконання додаткової операції перетворення чисел $A_{СЗК} = (a_1, a_2, ..., a_i, ..., a_n)$ і $B_{СЗК} = (b_1, b_2, ..., b_i, ..., b_n)$, представлених безпосередньо у СЗК, у числа $A'_{СЗК} = (a'_1, a'_2, ..., a'_i, ..., a'_n)$ і $B'_{СЗК} = (b'_1, b'_2, ..., b'_i, ..., b'_n)$, що представлені у ШФ СЗК та навпаки, перетворення результату $C'_{СЗК} = (c'_1, c'_2, ..., c'_i, ..., c'_n)$ операції модульного множення двох чисел $A'_{СЗК} = (a'_1, a'_2, ..., a'_i, ..., a'_n)$ і $B'_{СЗК} = (b'_1, b'_2, ..., b'_i, ..., b'_n)$, що представлені у ШФ СЗК, безпосередньо у СЗК $C_{СЗК} = (c_1, c_2, ..., c_i, ..., c_n)$. Це дає можливість, при необхідності у подальшому, безпосередньо контролювати та коректувати дані, що представлено у вигляді

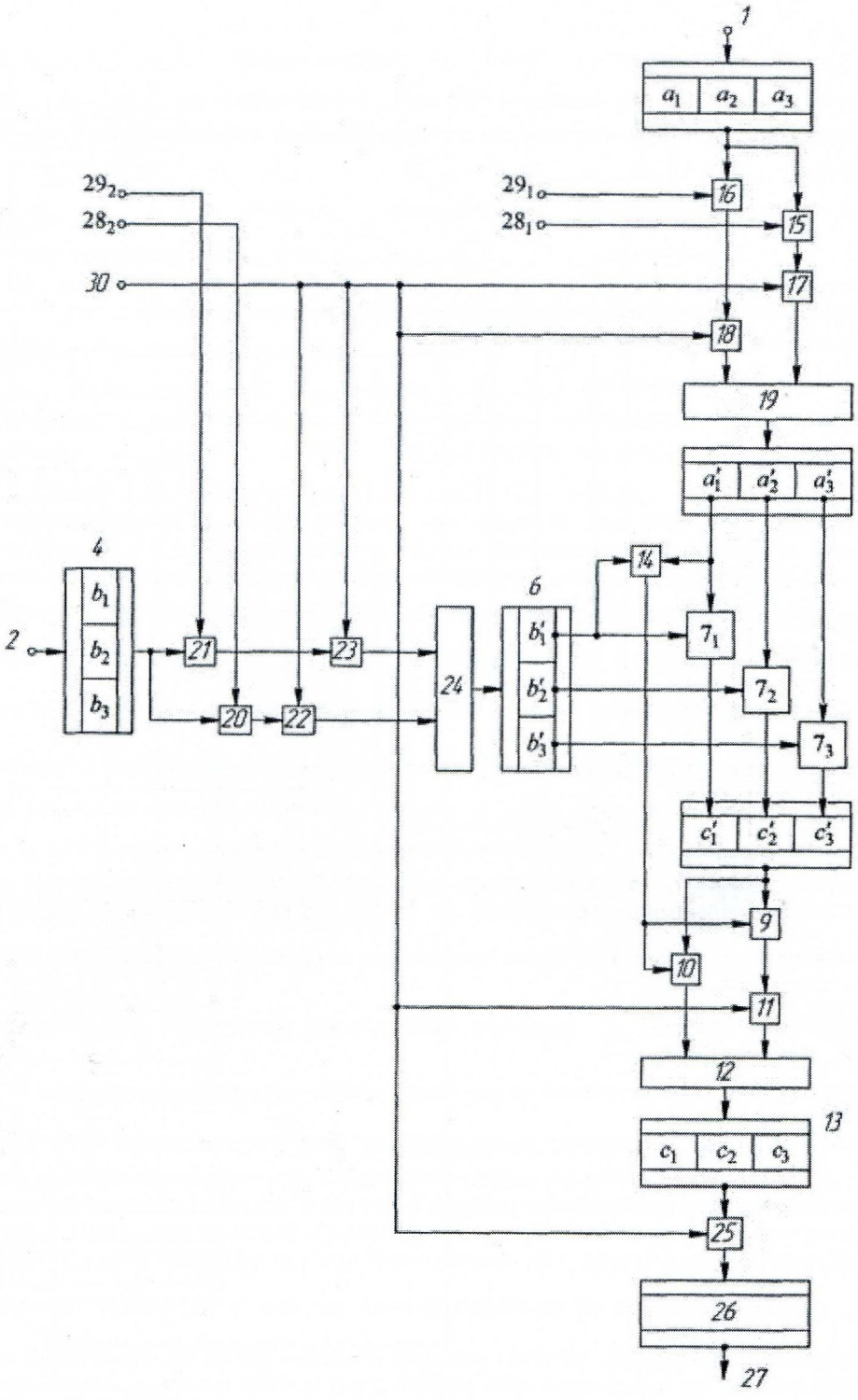
чисел $A_{СЗК} = (a_1, a_2, ..., a_i, ..., a_n)$, $B_{СЗК} = (b_1, b_2, ..., b_i, ..., b_n)$ і $C_{СЗК} = (c_1, c_2, ..., c_i, ..., c_n)$. Наведені приклади застосування представленого винаходу для конкретної СЗК підтверджують достовірність і практичну цінність отриманих результатів.

ФОРМУЛА ВИНАХОДУ

Пристрій для модульного множення двох чисел, які представлені у системі залишкових класів (СЗК), який містить перший та другий вхідні прийомні регістри, вихідний прийомний регістр, регістр результату операції, суматор за модулем два, першу групу елементів АБО, групу з n пристроїв для множення $c_i' = (a_i' \cdot b_i') \bmod m_i$ двох лишків a_i' та b_i' чисел $A'_{СЗК}$ та $B'_{СЗК}$ за відповідними модулями m_i ($i = \overline{1,n}$; n - кількість модулів СЗК), першу групу елементів І, групу вентилів, перший суматор за модулем $M = \prod_{i=1}^{n} m_i$, при цьому виходи і-х $(i = \overline{1,n})$ підрегістрів першого та другого вхідних прийомних регістрів підключено до входів і-го пристрою для множення лишків a_i' та b_i', відповідно чисел $A'_{СЗК}$ та $B'_{СЗК}$, за модулем m_i СЗК, виходи групи пристроїв множення лишків a_i' та b_i' за модулями m_i підключено до входів відповідних і-х підрегістрів вихідного прийомного регістру, вихід якого підключено до перших входів елементів І першої групи та до перших (інформаційних) входів вентильних елементів групи, виходи елементів І першої групи підключено до перших входів першого суматора за модулем $M = \prod_{i=1}^{n} m_i$, до других входів якого підключена шина подачі значення $\frac{M}{2}$, виходи першого суматора за модулем $M = \prod_{i=1}^{n} m_i$ і вентильних елементів групи через елементи АБО першої групи підключено до входу регістру результату операції, виходи перших (за модулем m_1 СЗК) підрегістрів вхідних прийомних регістрів підключено до входів суматора за модулем два, вихід якого підключено до других входів елементів І першої групи та до других входів вентильних елементів групи, який **відрізняється** тим, що в пристрій додатково введено перший та другий вхідні регістри, вихідний регістр, другу, третю, четверту та п'яту групи елементів І, другу та третю групи елементів АБО, другий, третій, четвертий, п'ятий та шостий суматори за модулем $M = \prod_{i=1}^{n} m_i$, при цьому, перший вхід пристрою підключено до входу першого вхідного регістру, вихід якого підключено до перших входів елементів І другої та третьої груп, виходи яких підключено до перших входів відповідно другого та третього суматорів за модулем $M = \prod_{i=1}^{n} m_i$, виходи яких через елементи АБО другої групи підключено до входу першого вхідного прийомного регістру, другий вхід пристрою підключено до входу другого вхідного регістру, вихід якого підключено до перших входів елементів І четвертої та п'ятої груп, виходи яких підключено до перших входів відповідно четвертого та п'ятого суматорів за модулем $M = \prod_{i=1}^{n} m_i$, виходи яких через елементи АБО третьої групи підключено до входу другого вхідного прийомного регістру, вихід регістру результату операції підключено до перших входів шостого суматора за модулем $M = \prod_{i=1}^{n} m_i$, вихід якого підключено до входу вихідного регістру, вихід якого є виходом пристрою, перша шина подачі сигналу ознаки "ДОДАВАННЯ 1" підключена до других входів елементів І другої групи, а друга шина подачі сигналу ознаки "ДОДАВАННЯ 2" підключена до других входів елементів І четвертої групи, перша шина подачі сигналу ознаки "ВІДНІМАННЯ 1" підключена до других входів елементів І третьої групи, а друга шина подачі сигналу ознаки "ВІДНІМАННЯ 2" підключена до других входів елементів І п'ятої групи, шина подачі значення $\frac{M}{2}$ підключена до других входів другого, третього, четвертого, п'ятого та шостого суматорів за модулем $M = \prod_{i=1}^{n} m_i$.


1
3
a_1 a_2 ••• a_i ••• a_n
29_2
28_2
30
29_1
28_1
16
15
17
18
19
5
a'_1 a'_2 ••• a'_i ••• a'_n
14
4
6
b_1 b_2 b_i b_n
b'_1 b'_2 b'_i b'_n
7_1 7_2 7_i 7_n
2
21
23
24
20
22
8
c'_1 c'_2 ••• c'_i ••• c'_n
9
10
11
12
13
c_1 c_2 ••• c_i ••• c_n
25
26
27

Фіг. 1



Фіг. 2

Комп'ютерна верстка А. Крулевський

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