



УКРАЇНА

(19) **UA** (11) **115182** (13) **C2**  
(51) МПК (2017.01)  
**G06F 7/00**  
**G06F 7/38** (2006.01)

МІНІСТЕРСТВО  
ЕКОНОМІЧНОГО  
РОЗВИТКУ І ТОРГІВЛІ  
УКРАЇНИ

**(12) ОПИС ДО ПАТЕНТУ НА ВІНАХІД**

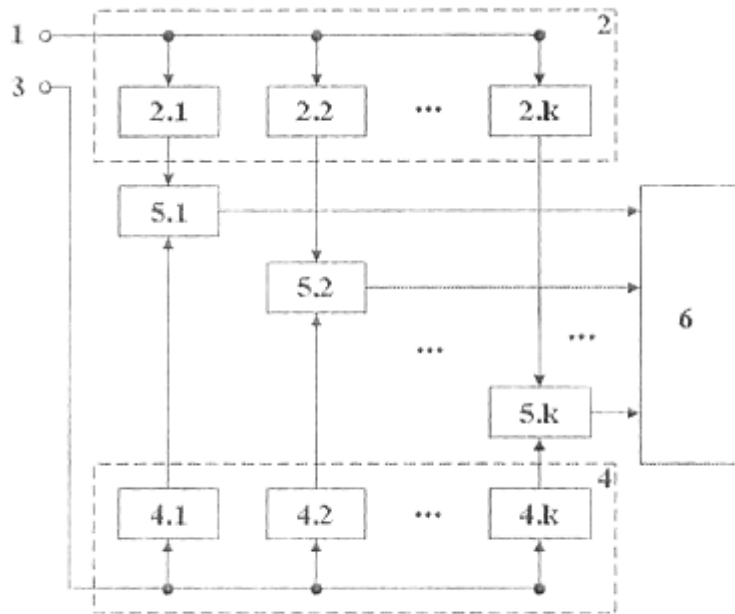
<p>(21) Номер заявки: <b>а 2015 12081</b></p> <p>(22) Дата подання заявки: <b>07.12.2015</b></p> <p>(24) Дата, з якої є чинними права на винахід: <b>25.09.2017</b></p> <p>(41) Публікація відомостей про заяву: <b>12.06.2017, Бюл.№ 11</b></p> <p>(46) Публікація відомостей про видачу патенту: <b>25.09.2017, Бюл.№ 18</b></p>	<p>(72) Винахідник(и): <b>Давлетова Аліна Ярославівна (UA), Круліковський Борис Борисович (UA), Николайчук Ярослав Миколайович (UA), Возна Наталія Ярославівна (UA)</b></p> <p>(73) Власник(и): <b>Давлетова Аліна Ярославівна, вул. Броварна, 12, кв. 7, м. Тернопіль, 46003 (UA), Круліковський Борис Борисович, вул. Соборна, 11, м. Рівне, 33028 (UA), Николайчук Ярослав Миколайович, вул. В. Великого, 14-а, м. Надвірна, Івано- Франківська обл., 78400 (UA), Возна Наталія Ярославівна, вул. Київська, 11-б, кв. 21, м. Тернопіль, 46016 (UA)</b></p> <p>(56) Перелік документів, взятих до уваги експертизою: SU 754414, 07.08.0980 GB 955330 A, 15.04.1964 UA 27631 U, 12.11.2007 UA 53731 C2, 17.02.2003 SU 190658, 01.03.1967 US 7257609 B1, 14.08.2007 JP 6246370 A, 28.02.1987 RU 2143723 C1, 27.12.1999</p>
--	--

**(54) ЧИСЛОІМПУЛЬСНИЙ ПРИСТРІЙ ДЛЯ МНОЖЕННЯ**

**(57) Реферат:**

Числоімпульсний пристрій для множення належить до засобів обчислювальної техніки і систем статистичної обробки інформації, цифрових взаємкореляторів та засобів паралельного розпізнавання образів на основі матриць великого числа пікселів оцифрованих зображень. Пристрій ґрунтується на обчисленні добутку двох чисел шляхом додаткового введення модульних лічильників у базисі Хаара-Крестенсона, входи яких з'єднані з вхідними шинами додатково введених матричних модульних перемножувачів та цифрового шифратора. Пристрій забезпечує отримання на виході двійкового цифрового значення добутку двох чисел, представлених унітарними кодами, та за допомогою запропонованого пристрою досягається підвищення швидкодії та регулярності структури для обчислення добутку двох чисел.

UA 115182 C2



Фиг. 1

Числоімпульсний пристрій для множення належить до засобів обчислювальної техніки і може бути використаний для множення чисел, представлених унітарним кодом у пристроях статистичної обробки інформації, цифрових взаємкореляторах та засобах паралельного розпізнавання образів шляхом опрацювання матриці великого числа пікселів оцифрованих зображень.

Відомий аналог - пристрій множення [Грибок Н.И. Обуханич Р.-А.В. Квадратор, // А.С. СССР № 475619. - Бюллетень № 24. - 1975], який містить вхідну шину, лічильник, накопичувач, який дозволяє шляхом перемноження однакових чисел отримувати код їх квадрата.

Недоліком такого пристрою є обмежені функціональні можливості та низька швидкодія, обумовлені тим, що даний пристрій визначає тільки квадрат одного числа, заданого унітарним кодом, що дозволяє у взаємкореляторах вичислити тільки одну точку  $x_i x_{i+0} = x^2$ . Недоліком відомого пристрою також є низька швидкодія, обумовлена тим, що представлення інформації у лічильнику та накопичуючому суматорі відбувається у двійковій системі числення теоретико-числового базису Радемахера, що передбачає наявність наскрізних переносів у накопичуючому суматорі, які відбуваються після кожного імпульсу вхідного унітарного коду.

Відомий прототип - числоімпульсний пристрій для множення [Николайчук Я.М. Числоимпульсное множительное устройство // А.С. СССР № 754414. - Бюллетень № 29). - 1980], який містить лічильник, логічні елементи, перемножувач, накопичувач, який дозволяє тримати двійковий код добутку у базисі Радемахера шляхом перемноження двох нерівних чисел заданих унітарним кодом.

Недоліком числоімпульсного множильного пристрою є низька швидкодія та значна структурна складність, які обумовлені тим, що даний пристрій містить двійковий лічильник та двійковий накопичуючий суматор, причому швидкодіюча реалізація двійкового синхронного лічильника з вхідними логічними елементами прискорення переносів та реалізація накопичувача на основі повних однорозрядних двійкових суматорів, які містять від 4 до 6 послідовно включених логічних елементів, характеризується низькою швидкістю та значною структурною складністю, що обмежує можливість реалізації їх великого числа в мікроелектронному кристалі матриці пікселів цифрової відеокамери.

В основу винаходу поставлена задача вдосконалення числоімпульсного множильного пристрою шляхом додаткового введення модульних лічильників теоретико-числового базису Хаара-Крестенсона, входи яких з'єднані з вхідними шинами додатково введених матричних модульних перемножувачів та цифрового шифратора, що дозволяє отримати підвищення на 1-2 порядки швидкодії, по відношенню до відомого прототипу, а також більш високу регулярність структури за рахунок реалізації модульних лічильників на регістрах зсуву та матричних модульних перемножувачів на елементах І-НІ.

Поставлена задача вирішується завдяки тому, що числоімпульсний пристрій для множення містить першу і другу вхідні шини, лічильник і помножувач, згідно з винаходом, додатково введених перша і друга групи К модульних лічильників у базисі Хаара-Крестенсона, група К модульних матричних перемножувачів, перша вхідна шина з'єднана з входами першої групи модульних лічильників, друга шина з'єднана з входами другої групи модульних лічильників, виходи яких підключені до відповідних входів додатково введених матричних перемножувачів, другі входи яких підключені до виходів відповідних модульних лічильників першої групи, а виходи підключені до входів додатково введеного шифратора, виходи якого є виходами пристрою.

Винахід ілюструється кресленням, де на фіг. 1 показана структурна схема пристрою: 1 - перша вхідна шина; 2 - перша група модульних лічильників; 3 - друга вихідна шина; 4 - друга група модульних лічильників; 5 - група матричних модульних перемножувачів; 6 - шифратор.

На фіг. 2 показана структурна схема модульного лічильника, на фіг. 3 - структурна схема модульного матричного перемножувача у базисі Хаара-Крестенсона по модулю P, а на фіг. 4 - приклад реалізації модульного матричного перемножувача для P=7.

Пристрій працює наступним чином:

Перед початком кожного циклу множення всі Д-тригери модульних лічильників пристрою окремою мікрокомандою скидаються в "0", крім нульового тригера, який встановлюється в стан "1" (на структурній схемі не показано). При синхронному надходженні кожної пари імпульсів унітарних кодів чисел, що перемножуються, на вхідні шини (1, 3) у модульних лічильниках першої (2) і другої (4) групи накопичуються коди залишків системи залишкових класів базису Хаара-Крестенсона, які одночасно надходять на входи відповідних модульних матричних перемножувачів (5), на виходах яких формуються добутки у вигляді кодів Хаара-Крестенсона, згідно з виразом  $(a_i \cdot b_i) \bmod P_i = d_i$ ;  $i \in \overline{1, k}$ , де  $a_i$  та  $b_i$  поточні залишки чисел X та Y згідно з виразами  $a_i = \text{res}X(\bmod P_i)$ ;  $b_i = \text{res}Y(\bmod P_i)$ .

Після закінчення циклу перемноження на виході матричних модульних перемножувачів (5) формується код добутку  $d_1, d_2, \dots, d_i, \dots, d_k$  у системі числення залишкових класів базису Крестенсона, який шифратором (6) перетворюється у двійковий код базису Радемахера,

Принцип роботи пристрою полягає у тому, що в числоімпульсному множилному пристрої  
 5 унітарні коди паралельно записуються у модульні лічильники системи залишкових класів теоретико-числового базису Хаара-Крестенсона, паралельно перемножуються у матричних модульних перемножувачах, а результати дешифруються з системи залишкових класів в двійкову систему числення. При цьому, як показано на фіг. 2 модульний лічильник базису Хаара-Крестенсона реалізується на основі регістра зсуву на Д-тригерах зі зворотним зв'язком  
 10  $T_{P-1} - T_0$ .

На початку циклу перемноження макрокомандою  $y_0$  всі Д-тригери  $T_1 - T_{P-1}$  по R-входах встановлені в стан "0", а тригер  $T_0$  по S-входу в стан "1". У процесі надходження імпульсів унітарного коду на вхідну шину, яка з'єднана з С-входами синхронізації всіх Д-тригерів, на прямих виходах тригерів формуються модульні коди залишків  $a_i, b_i$  Хаара-Крестенсона з  
 15 розрядністю  $p_i$ . Таким чином у процесі надходження вхідних імпульсів унітарного коду на модульні лічильники на їх виходах з часовою затримкою  $2\upsilon$ , де  $\upsilon$  - тактова частота переключення логічних елементів кристала, на якому реалізується пристрій.

Структура модульного матричного перемножувача, на входи якого надходять коди Хаара-Крестенсона з першої і другої груп модульних лічильників, забезпечує виконання операції  
 20 модульного множення також за інтервал часу  $2\upsilon$  згідно з таблицею та структурою, показаної на фіг. 4 для  $P = 7$ .

$P = 7$

$a_i$ $b_i$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Приклад реалізації модульного матричного перемножувача для  $P = 7$ , показаний на фіг. 4, швидкодія якого визначається двома послідовно включеними логічними інвенторами, що  
 25 складає  $2\upsilon$ .

Таким чином швидкодія числоімпульсного множилного пристрою згідно з винаходу визначається затримкою сигналів внаслідок переключення елементів матричного модульного лічильника  $\tau_{л}$ , модульного матричного перемножувача  $\tau_{п}$  та шифратора ( $\tau_{\partial}$ )

30  $\tau = \tau_{л} + \tau_{п} + \tau_{\partial} = 2\upsilon + 2\upsilon + 2\upsilon = 6\upsilon$ .

Швидкодія відомого пристрою прототипу визначається сумарною швидкодією переключення JK-тригерів двійкового лічильника, мультиплексора та накопичуючого суматора, який складається з двійкового багаторозрядного суматора на основі повних тривходових  
 35 однорозрядних суматорів з часом переключення  $4 - 6\upsilon$  [Круліковський Б.Б. Архітектура високопродуктивних матричних прискорювачів операції множення у базисах Радемахера та Хаара / Б.Б. Круліковський, А.Я. Давлетова, В.Л. Кімак, І.Б. Албанський / Праці міжнародної наукової школи-семінару "Питання оптимізації обчислень (ПОО-ХЛІІ)" Київ: Інститут кібернетики імені В.М. Глушкова НАН України. 2015. - С. 47-49], а також  $2\upsilon$ , наскрізних переносів при  $2^n$ -розрядних унітарних кодів перемножуваних чисел. Тобто  $\tau = \tau_{л} + \tau_{м} + \tau_{р} + 2n\tau_{с}$ .

Наприклад, при діапазоні кодування вхідних чисел унітарним кодом  $2^8$  швидкодія відомого пристрою буде визначатися наступним чином  $\tau = 4\upsilon + 2\upsilon + 2\upsilon + 2 \cdot 8 \cdot 4\upsilon = 72\upsilon$ , в той час як у пристрої згідно з винаходом швидкодія складає  $6\upsilon$ , не залежно від розрядності вхідних унітарних кодів перемножуваних чисел.

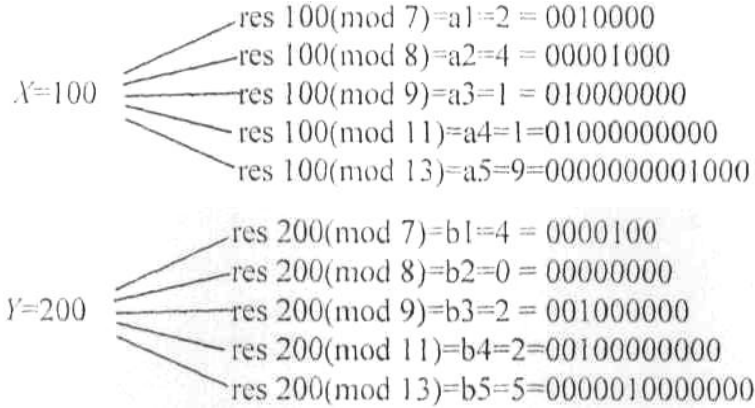
Розрахунок системи взаємно простих модулів  $P_1, P_2, \dots, P_i, \dots, P_k$  для числоімпульсного множилного пристрою при  $k = 8$  виконується, виходячи з умови, що добуток модулів  
 45

$P_1, P_2, \dots, P_i, \dots, P_k$  повинен перевищувати числове значення  $2^{16}$ . Цій умові відповідає наступний набір модулів системи залишкових класів базису Крестенсона 7, 8, 9, 11, 13 = 72072 >  $2^{16} = 65536$ . Таким чином на виходах матричних модульних перемножувачів, після завершення процесу множення, формується код Хаара-Крестенсона  $d_1, d_2, \dots, d_5$ , який дешифрується у 16-розрядний двійковий код базису Радемахера,

5

Приклад: Нехай перемножуються числа  $X = 100$ ,  $Y = 200$ ;  $X \cdot Y = 20000$ .

Числа  $X$  та  $Y$  представляються у базисі Хаара-Крестенсона наступним кодом:



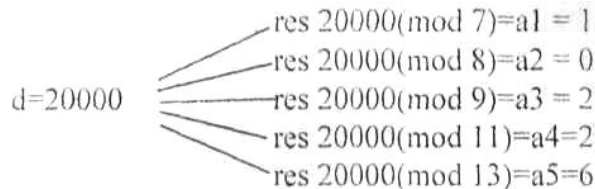
10

Сформовані таким чином коди надходять на входи  $i$ -тих матричних модульних перемножувачів, на виходах яких формується код Хаара-Крестенсона результатів перемноження  $d_1, d_2, \dots, d_k$  згідно з виразом:  $(a_i b_i) \bmod P_i = d_i$ .

15

$P_i$		7	8	9	11	13
$a_i =$	$x$	(2	4	1	1	9)
$b_i =$		(4	0	2	2	5)
$d_i =$		(1	0	2	2	6);

що відповідає дешифрованому значенню 20 000 у двійковій системі числення базису Радемахера 100111000100000.



20

Для спрощення структури шифратора (6) він реалізується по двокаскадній схемі, де в першому каскаді коди Хаара-Крестенсона по кожному модулю перетворюються в двійкові коди Радемахера, які в другому каскаді перетворюються в позиційний код двійкової системи числення, тобто 48-бітний код Хаара-Крестенсона дешифрується у 18-бітний код Радемахера-Крестенсона та 16-бітний код Радемахера. При цьому в шифраторі (6) затримка сигналів складає  $4\tau$  і загальна швидкодія пристрою буде складати  $6 + 2 = 8\tau$ .

25

Технічний результат: пристрій згідно з винаходом характеризується підвищеною на 1-2 порядки швидкістю по відношенню до відомого прототипу, а також більш високою регулярністю структури за рахунок реалізації модульних лічильників на регістрах зсуву, та матричних модульних перемножувачів на елементах І-НІ.

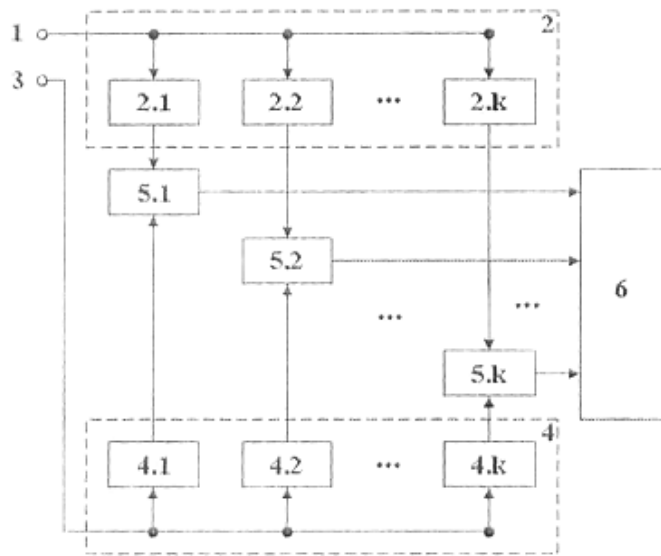
30

### ФОРМУЛА ВИНАХОДУ

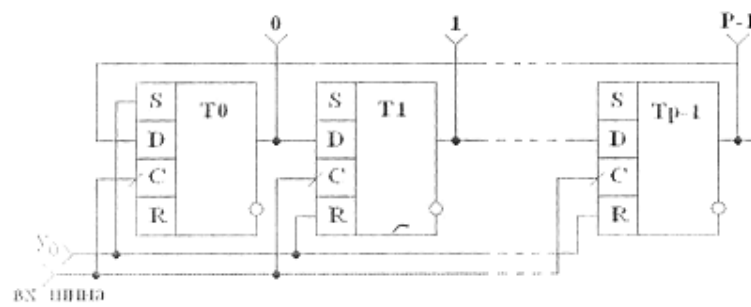
35

Числоімпульсний пристрій для множення, що містить першу і другу вхідні шини, першу і другу групи  $K$  модульних лічильників у базисі Хаара-Крестенсона, групу  $K$  модульних матричних помножувачів, перша вхідна шина з'єднана з входами першої групи модульних лічильників, друга вхідна шина з'єднана з входами другої групи модульних лічильників, виходи яких

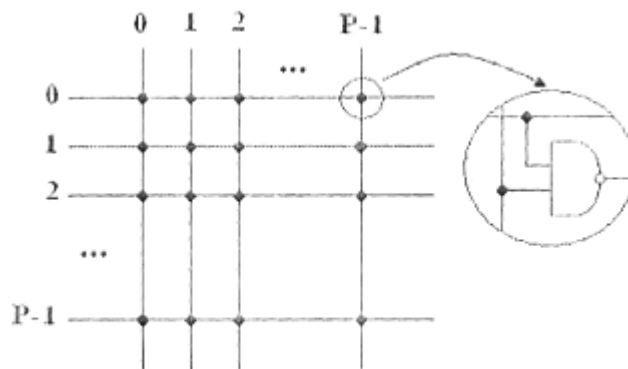
підключені до відповідних перших входів матричних помножувачів, другі входи яких підключені до виходів відповідних модульних лічильників першої групи, а виходи підключені до входів шифратора, виходи якого є виходами пристрою.



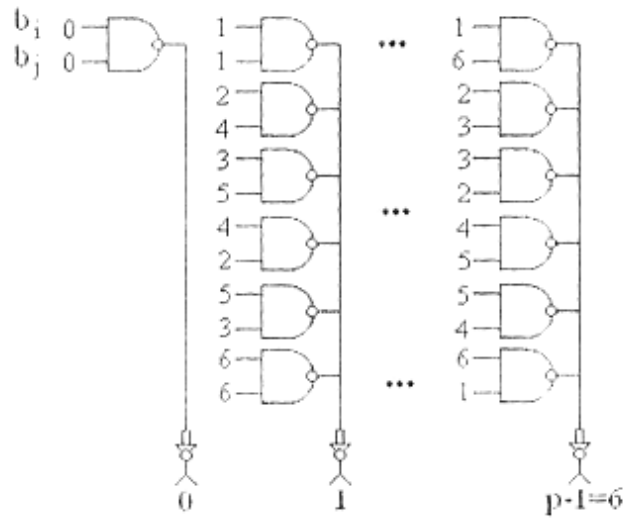
Фиг. 1



Фиг. 2



Фиг. 3



Фиг. 4