



УКРАЇНА

(19) **UA** (11) **107811** (13) **U**
(51) МПК
G06F 7/38 (2006.01)

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

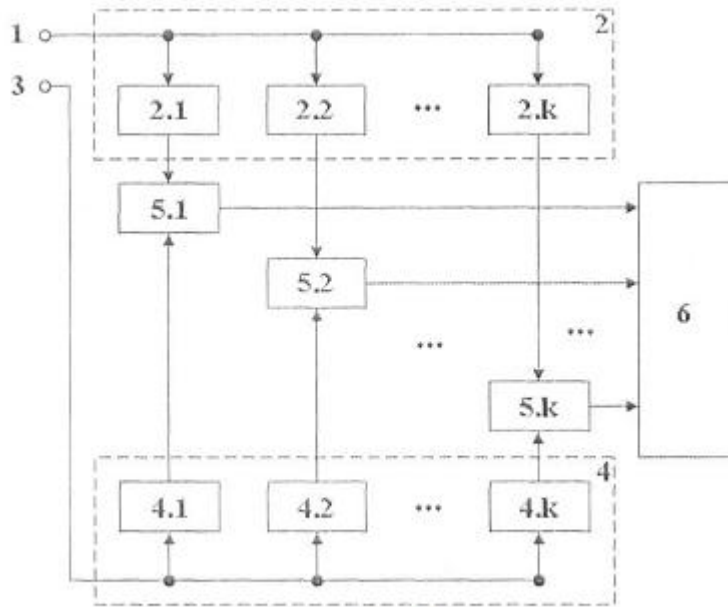
<p>(21) Номер заявки: u 2015 12080</p> <p>(22) Дата подання заявки: 07.12.2015</p> <p>(24) Дата, з якої є чинними права на корисну модель: 24.06.2016</p> <p>(46) Публікація відомостей про видачу патенту: 24.06.2016, Бюл.№ 12</p>	<p>(72) Винахідник(и): Давлетова Аліна Ярославівна (UA), Круліковський Борис Борисович (UA), Николайчук Ярослав Миколайович (UA), Возна Наталія Ярославівна (UA)</p> <p>(73) Власник(и): 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)</p>
--	---

(54) ЧИСЛОІМПУЛЬСНИЙ МНОЖИЛЬНИЙ ПРИСТРІЙ

(57) Реферат:

Числоімпульсний множильний пристрій містить першу і другу вхідні шини, лічильник і помножувач. Додатково введені 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 вхідна шипа 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.

UA 107811 U



Фиг. 1

Числоімпульсний множильний пристрій 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 квадрату.

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 накопичувальному суматорі відбувається у двійковій системі числення теоретико-числового базису Радемахера, що передбачає наявність наскрізних переносів у накопичувальному суматорі, які відбуваються після кожного імпульсу вхідного унітарного коду.

Відомий прототип - числоімпульсний множильний пристрій [Николайчук Я.М. Числоимпульсное множительное устройство // А.С. СССР № 754414, - Бюллетень № 29. - 1980], який містить лічильник, логічні елементи, перемножувач, накопичувач, який дозволяє отримати 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 накопичувальний 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 швидкодією та значною структурною складністю, що обмежує можливість реалізації їх великого числа в мікроелектронному кристалі матриці пікселів цифрової відеокамери.

В основу корисної моделі 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 па регістрах зсуву та матричних модульних перемножувачів на елементах І-НЕ.

Поставлена задача вирішується завдяки тому, що числоімпульсний множильний пристрій містить першу і другу вхідні шини, лічильник і помножувач, згідно з корисною моделлю, додатково введені 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.

Корисна модель 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 Р, а на фіг. 4 - приклад реалізації модульного матричного перемножувача для Р=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 виразу $(a_i \cdot b_i) \bmod P_i = d_i$; $i \in \overline{1, k}$, де a_i та b_i поточні залишки чисел X та Y згідно виразів $a_i = \text{res } X(\bmod P_i)$; $b_i = \text{res } Y(\bmod P_i)$.

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 множильному пристрої 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 D -тригерах зі зворотним зв'язком $T_{P-1} - T_0$.

На початку циклу перемноження мікрокомандою y_0 всі D -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 S -входами синхронізації всіх D -тригерів на прямих виходах тригерів формуються модульні коди залишків a_i, b_i Хаара-Крестенсона з розрядністю P_i . Таким чином у процесі надходження вхідних імпульсів унітарного коду на модульні лічильники на їх виходах з часовою затримкою 2υ , де υ - 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 модульного множення також за інтервал часу 2υ згідно таблиці та структури показаної на фіг. 4 для $P=7$.

$P = 7$

a_i	0	1	2	3	4	5	6
b_i	0	0	0	0	0	0	0
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 складає 2υ .

Таким чином швидкодія числоімпульсного множильного пристрою згідно корисної моделі визначається затримкою сигналів внаслідок переключення елементів матричного модульного лічильника (τ_n), модульного матричного перемножувача (τ_m) та шифратора (τ_σ)

$$\tau = \tau_n + \tau_m + \tau_\sigma = 2\upsilon + 2\upsilon + 2\upsilon = 6\upsilon.$$

Швидкодія відомого пристрою-прототипу визначається сумарною швидкодією переключення J -тригерів двійкового лічильника, мультиплексора та накоплюючого суматора, який складається з двійкового багаторозрядного суматора на основі повних трьохвходових однорозрядних суматорів з часом переключення $4 \cdot 6\upsilon$ [Круліковський Б.Б. Архітектура високопродуктисних 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 ПАН України, 2015. - С.47-49]. а таке 2_n наскрізних переносів при 2^n -розрядних унітарних кодів перемножуваних чисел. Тобто $\tau = \tau_n + \tau_m + \tau_p + 2n\tau_c$.

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 пристрою згідно корисної моделі швидкодія складає 6υ не залежно від розрядності вхідних унітарних кодів перемножуваних чисел.

Розрахунок системи взаємнопростих модулів $P_1, P_2, \dots, P_i, \dots, P_k$ для числоімпульсного множильного пристрою при $k=8$ виконується виходячи з умови, що добуток модулів $P_1, P_2, \dots, P_i, \dots, P_k$ повинен перевищувати числове значення 2^{16} . Цій умові відповідає наступний набір модулів системи залишкових класів базису Крестенсона

5

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.

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

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

$$X=100 \begin{cases} \text{res } 100(\text{mod } 7)=a_1=2 = 0010000 \\ \text{res } 100(\text{mod } 8)=a_2=4 = 00001000 \\ \text{res } 100(\text{mod } 9)=a_3=1 = 010000000 \\ \text{res } 100(\text{mod } 11)=a_4=1=0100000000 \\ \text{res } 100(\text{mod } 13)=a_5=9=0000000001000 \end{cases}$$

$$Y=200 \begin{cases} \text{res } 200(\text{mod } 7)=b_1=4 = 0000100 \\ \text{res } 200(\text{mod } 8)=b_2=0 = 00000000 \\ \text{res } 200(\text{mod } 9)=b_3=2 = 001000000 \\ \text{res } 200(\text{mod } 11)=b_4=2=0010000000 \\ \text{res } 200(\text{mod } 13)=b_5=5=0000010000000 \end{cases}$$

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 виразу: $(a_i \cdot b_i) \text{mod } P_i = d_i$.

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

15

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

$$d=20000 \begin{cases} \text{res } 20000(\text{mod } 7)=a_1 = 1 \\ \text{res } 20000(\text{mod } 8)=a_2 = 0 \\ \text{res } 20000(\text{mod } 9)=a_3 = 2 \\ \text{res } 20000(\text{mod } 11)=a_4=2 \\ \text{res } 20000(\text{mod } 13)=a_5=6 \end{cases}$$

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 4υ і загальна швидкодія пристрою буде складати $6+2=8\upsilon$.

25

Технічний результат: пристрій згідно корисної моделі характеризується підвищеною на 1-2 порядки швидкістю відносно відомого прототипу, а також більш високою регулярністю структури за рахунок реалізації модульних лічильників на регістрах зсуву, та матричних модульних перемножувачів на елементах І-НЕ.

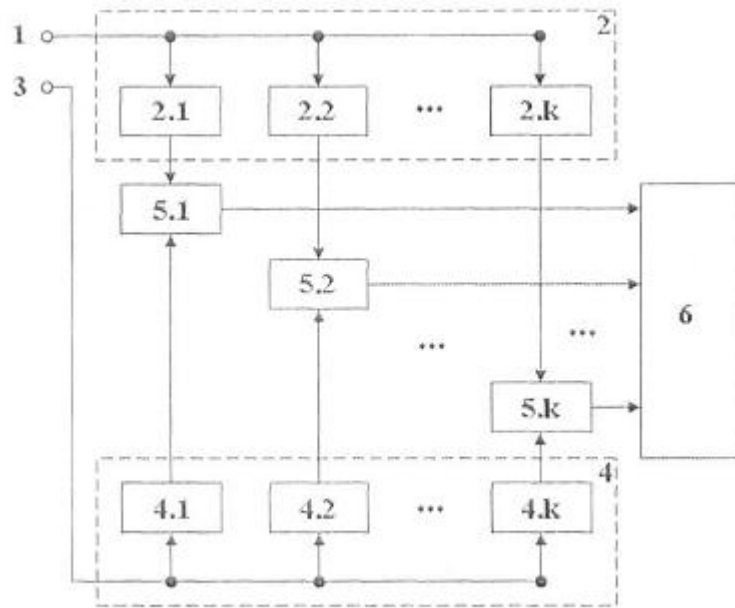
ФОРМУЛА КОРИСНОЇ МОДЕЛІ

30

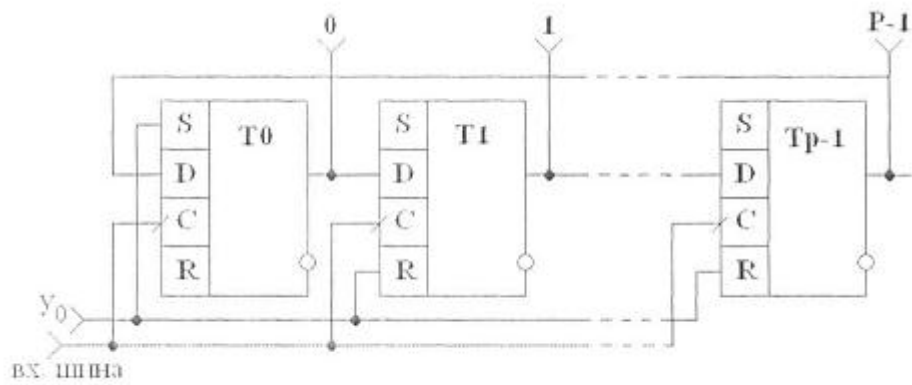
Числоімпульсний множильний пристрій, що містить першу і другу вхідні шини, лічильник і помножувач, який **відрізняється** тим, що додатково введені перша і друга групи K модульних лічильників у базисі Хаара-Крестенсона, група K модульних матричних перемножувачів, перша вхідна шина з'єднана з входами першої групи модульних лічильників, друга вхідна шипа з'єднана з входами другої групи модульних лічильників, виходи яких підключені до відповідних входів додатково введених матричних перемножувачів, другі входи яких підключені до виходів

35

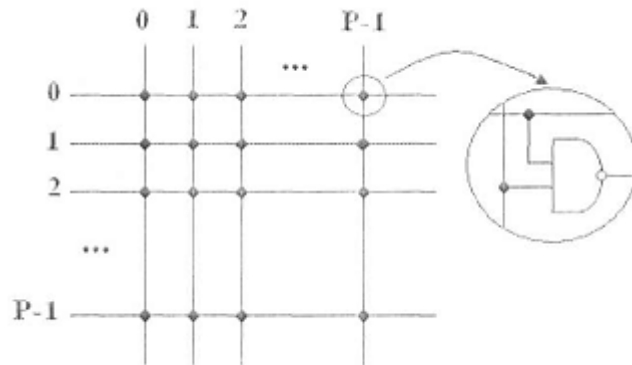
відповідних модульних лічильників першої групи, а виходи підключені до входів додатково введеного шифратора, виходи якого є виходами пристрою.



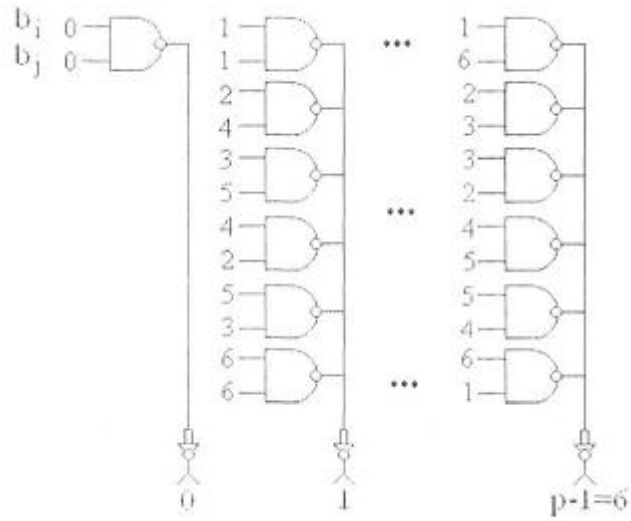
Фиг. 1



Фиг. 2



Фиг. 3



Фіг. 4