УКРАЇНА

(19) UA **(11) 142006** **(13) U**

(51) МПК
G06F 7/52 (2006.01)

МІНІСТЕРСТВО РОЗВИТКУ ЕКОНОМІКИ, ТОРГІВЛІ ТА СІЛЬСЬКОГО ГОСПОДАРСТВА УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2019 10087**

(22) Дата подання заявки: **30.09.2019**

(24) Дата, з якої є чинними права на корисну модель: **12.05.2020**

(46) Публікація відомостей про видачу патенту: **12.05.2020, Бюл.№ 9**

(72) Винахідник(и):
Грига Володимир Михайлович (UA),
Круліковський Борис Борисович (UA),
Возна Наталя Ярославівна (UA),
Николайчук Любов Михайлівна (UA),
Давлетова Аліна Ярославівна (UA)

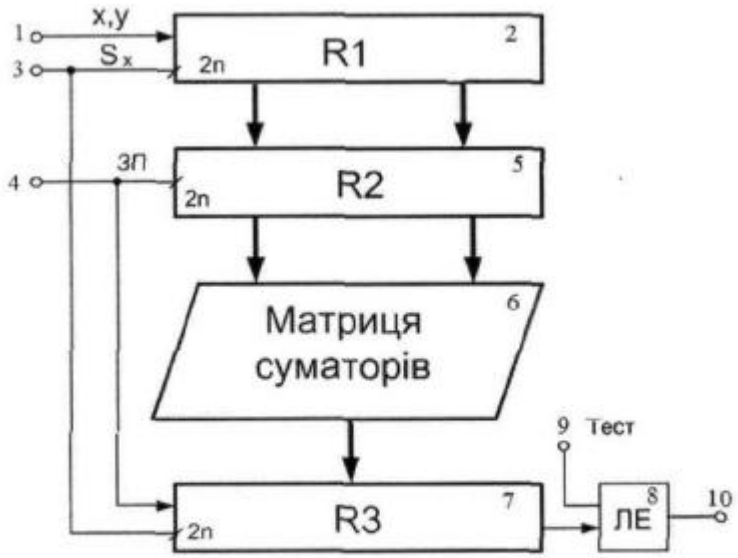
(73) Власник(и):
Грига Володимир Михайлович,
пров. І. Богуна, 12, м. Надвірна, Івано-Франківська обл., 78400 (UA),
Круліковський Борис Борисович,
вул. Соборна, 11, м. Рівне, Рівненська обл., 33028 (UA),
Возна Наталя Ярославівна,
вул. Київська, 11-б, кв. 21, м. Тернопіль, 46016 (UA),
Николайчук Любов Михайлівна,
вул. В. Великого, 14-а, м. Надвірна, Івано-Франківська обл., 78400 (UA),
Давлетова Аліна Ярославівна,
вул. Броварна, 12, кв. 7, м. Тернопіль, 46003 (UA)

(54) ПЕРЕМНОЖУВАЧ ПОТОКІВ БАГАТОРОЗРЯДНИХ ДАНИХ

(57) Реферат:

Перемножувач потоків багаторозрядних даних містить перший регістр пам'яті на D-тригерах з прямими виходами, перші входи якого є вхідною шиною двійкових кодів перемножуваних чисел, другий вхід з'єднаний з другим входом пристрою, виходи з'єднані з відповідними прямими входами матриці однорозрядних повних двійкових суматорів, виходи якої з'єднані з відповідними першими входами другого регістра пам'яті, другий вхід якого з'єднаний з другим входом першого регістра пам'яті. Перемножувач одатково містить перший 2n-розрядний регістр зсуву на D-тригерах, перший вхід якого є першим входом пристрою, другий вхід якого є другим входом синхронізації пристрою, виходи якого додатково з'єднані з відповідними першими входами першого регістра пам'яті, виходи матриці перемноження додатково з'єднані з відповідними першими входами додатково введеного регістра пам'яті та зсуву, другий вхід якого з'єднаний з другим входом першого регістра пам'яті і другим входом пристрою, третій вхід з'єднаний з третім входом синхронізації пристрою, вихід регістра пам'яті та зсуву додатково з'єднаний з першим входом додатково введеного логічного елемента "Виключаюче АБО", другий вхід якого з'єднаний з додатково введеним четвертим входом пристрою а вихід є вихідним каналом пристрою.

UA 142006 U


1
x,y
3
Sx
2n
R1
2
4
ЗП
2n
R2
5
Матриця
суматорів
6
9
Тест
2n
R3
7
ЛЕ
8
10

Фіг. 1

Перемножувач потокових багаторозрядних даних належить до засобів обчислювальної техніки і може бути використаний як компонент швидкодіючих спеціалізованих процесорів цифрового опрацювання та шифрування даних.

Відомий аналог - матричний перемножувач [Шатилло В.В., Прохоров С.Н., Явиц А.С. Матричный умножитель //АС № 1615704 SU, Бюллетень № 47, 1990], який містить матрицю елементів nx.ni, які з'єднані між собою відповідними горизонтальними та вертикальними інформаційними зв'язками переносів.

Недоліком такого матричного перемножувача є велика структурна складність, обумовлена тим, що такий пристрій містить 2(n+m) входо/виходів, що при великій розрядності кодів, наприклад, у алгоритмах шифрування RSA n=m=(512, 1024, 2048), відповідно збільшується кількість внутрішніх та зовнішніх виводів, а також зростають габарити корпусів мікроелектронних кристалів та зменшується надійність.

Відомий найближчий аналог - матричний перемножувач [Давлетова А.Я., Грига В.М., Николайчук Я.М. /Матричний перемножувач. Патент на корисну модель UA№ 132520, Бюл. № 4, 2019. - Фіг. 2, Фіг. 3], який містить вхідну шину двійкових кодів перемножуваних чисел виходи якої з'єднані з першими входами першого регістра пам'яті, прямі виходи якого з'єднані з відповідними прямими входами матриці повних однорозрядних суматорів з прямими входами та прямими виходами сум, біти яких попарно з'єднані з входами логічних елементів "І", виходи яких підключені до відповідних входів матриці повних однорозрядних суматорів з прямими входами та виходами, який містить перший регістр пам'яті на D-тригерах з прямими виходами, перші входи якого є вхідною шиною двійкових кодів перемножуваних чисел, другий вхід з'єднаний з другим входом пристрою, виходи з'єднані з відповідними прямими входами матриці однорозрядних повних двійкових суматорів з прямими входами та виходами сум та інверсними виходами переносів, прямі виходи якої з'єднані з відповідними першими входами другого регістра пам'яті на D-тригерах, другий вхід якого з'єднаний з третім входом пристрою.

Недоліком такого пристрою є обмежені функціональні можливості, які обумовлені відсутністю можливості тестування і контролю правильності результатів множень у процесі зчитування а також шифрування вихідних кодів шляхом логічно-модульного додавання рекурентних біт-орієнтованих послідовностей.

Іншим недоліком такого перемножувача є неможливість паралельного біт-орієнтованого вводу/виводу та перемноження двійкових кодів у матриці суматорів.

В основу корисної моделі поставлена задача зменшення структурної та апаратної складності та розширення функціональних можливостей пристрою шляхом додаткового застосування вхідної та вихідної однобітових шин на основі регістрів зсуву на D-тригерах, у якості компонентів застосовуються у молодших розрядах неповні однорозрядні суматори [Давлетова А.Я., Николайчук Я.М. /Однорозрядний напівсуматор. Патент на корисну модель UA № 115861, Бюл. № 8, 2017. - Фіг. 2] (Фіг. 3) з прямими входами та виходами, у другому розряді повні однорозрядні суматори з прямими входами та виходами суми та інверсними виходами переносів (Фіг. 4) в наступних (n-2) розрядах повні однорозрядні суматори з прямими входами та виходами сум та інверсними входами та виходами переносів [Николайчук Я.М., Грига В.М., Возна Н.Я., Давлетова А.Я. /Повний однорозрядний суматор. Патент на корисну модель UA № 124563, Бюл. № 7, 2018] (Фіг. 5) та додаткового інвертора на виході старшого розряду лінійки суматорів матриці перемноження, які послідовно з'єднані входами/виходами між собою (Фіг. 6) та додаткового уведення на вихідній шині логічного елемента "Виключаюче АБО" реалізованого на елементах "І-НІ", які є компонентом неповного двійкового однорозрядного суматора на елементах "Виключаюче І" [Давлетова А.Я., Николайчук Я.М. /Однорозрядний напівсуматор. Патент на корисну модель UA № 115861, Бюл. № 8, 2017. - Фіг. 1, Фіг. 2] на другий вхід якого подається код контролю правильності виконання операції множення багаторозрядних двійкових чисел чи псевдовипадковий код криптозахисту вихідних даних.

Поставлена задача вирішується завдяки тому, що у першому розряді матриці суматорів матричного перемножувача додатково містяться однорозрядні неповні суматори з прямими виходами переносів, у другому ряді матриці суматорів додатково містяться повні однорозрядні суматори з прямими входами та інверсними виходами переносів, а у старшому розряді матриці додатково містяться однорозрядні повні суматори з прямими виходами переносів.

Корисна модель ілюструється кресленням, де на Фіг. 1 показана структурна схема пристрою, який містить 1 - перший інформаційний вхід потокових даних x, y; 2 - перший 2n-розрядний регістр зсуву R1; 3 - другий вхід пристрою синхронізації; 4 - третій вхід пристрою (тестовий); 5 - перший 2n-розрядний регістр пам'яті R2; 6 - матриця суматорів (перемноження); 7 - другий 2n-розрядний регістр пам'яті та зсуву R3; 8 - логічний елемент "Виключаюче АБО"; 9 -

четвертій вхід пристрою (контрольний код); 10 - вихідний канал пристрою. На Фіг. 2 показано структуру перемноження чисел на матриці однорозрядних суматорів.

Виходи першого регістра зсуву з'єднані з відповідними входами матриці перемноження, другий вхід якого з'єднаний з другим входом пристрою, прямі однофазні виходи матриці перемноження з'єднані з відповідними першими входами другого регістра пам'яті та зсуву вихід якого з'єднаний з першим входом логічного елемента "Виключаюче АБО" другий вхід якого з'єднаний з четвертим входом пристрою, а вихід з'єднаний з вихідним каналом пристрою.

Пристрій працює наступним чином.

В потоковому перемножувачі багаторозрядних двійкових чисел регістр R1 виконує операцію перетворення n - розрядних біт-орієнтованих кодів множників x та y у паралельний 2n - розрядний двійковий код. Часова складність $T_{трг}=2$ мікротакти, тобто занесення кодів (x, y) в регістр R1 здійснюється за 4n мікротактів. Регістр пам'яті R2 призначений для запису та зберігання кодів множників на часовий інтервал занесення вхідних кодів (x, y) у регістр зсуву R1. Матриця однорозрядних суматорів виконує операцію перемноження кодів (x, y), на виході якої формується 2n - розрядний вихідний код добутку на інтервалі часу $(k_1\times n)+(k_1\times n)$, де k_1 - затримка сигналів формування наскрізних переносів; а k_2 - відповідно затримка сигналів на виходах сум. Регістр R3 виконує операції запису коду добутку та його зсув на вихід пристрою на інтервалі 2n мікротактів. Логічний елемент "Виключаюче АБО" реалізує операції тестування безпомилковості роботи перемножувача чи шифрування вихідних даних псевдовипадковим кодом. З метою контролю надійності роботи перемножувача на початку певного числа циклів здійснюється тестування правильності його роботи шляхом порівняння добутку заданих перемножувачів (x, y) з тестовим кодом добутку, який надходить на вхід 5 перемножувача. При цьому на виході 6 логічного елемента "Виключаюче АБО" формується 2n - розрядний потік нулів, що означає про безпомилковість виконання операції множення. На початку кожного циклу перемноження сигналом входу 4 здійснюється запис прямих кодів регістра R1 у регістр R2 та прямих кодів добутків у регістр R3. У наступному циклі роботи перемножувача сигналами синхронізації Sx входу 3 тактується занесенням біт-орієнтованих кодів множників x та y в регістр R1. Одночасно цими сигналами тактується зчитування біт-орієнтованих кодів добутків на виході 6 пристрою. Одночасно з виконанням операцій вводу та виводу даних у матричній структурі суматорів МС здійснюється перемноження двійкових кодів x та y за (n+2n) мікротактів. Регістри зсуву побудовані на основі D-тригерів.

Технічний результат: пристрій характеризується зменшеною структурною складністю за рахунок зменшення кількості інформаційних входо-виходів $4n/2$, що при розрядності вхідних чисел 512, 1024, 2048 зменшення структурної складності входів/виходів згідно критерію Квайна складає: 1024, 2048 та 4096 разів.

Апаратна складність відомого пристрою розраховується згідно виразу:

$A_1=4n\times A_{трг}, +n^2\times A_{ЛЕ}+(n-1)^2\times A_{сум.}$, де $A_{трг}=2$ (вентилі), $A_{ЛЕ}=1$ (вентиль), $A_{сум}=20$ (вентилів), при n=512 апаратна складність відомого пристрою буде рівна:

$A_1=4\times 512\times 2+512^2\times 1+511^2\times 20=4096+5484564=5488660$(вентилів).

Апаратна складність запропонованого пристрою розраховується згідно виразу:

$A_2=3n\times 2\times A_{трг.}+n^2\times A_{ЛЕ}+n\times(A_{НС}+A_{ПС1}+(n-2)\times A_{ПС2}+A_{інв.})$, де

$A_{трг}=$ (вентилі), $A_{ЛЕ}=1$ (вентиль), $A_{НС}=3$ (вентилі), $A_{ПС1}=6$ (вентилів), $A_{ПС2}=8$ (вентилів) при n=512 апаратна складність запропонованого пристрою буде рівна:

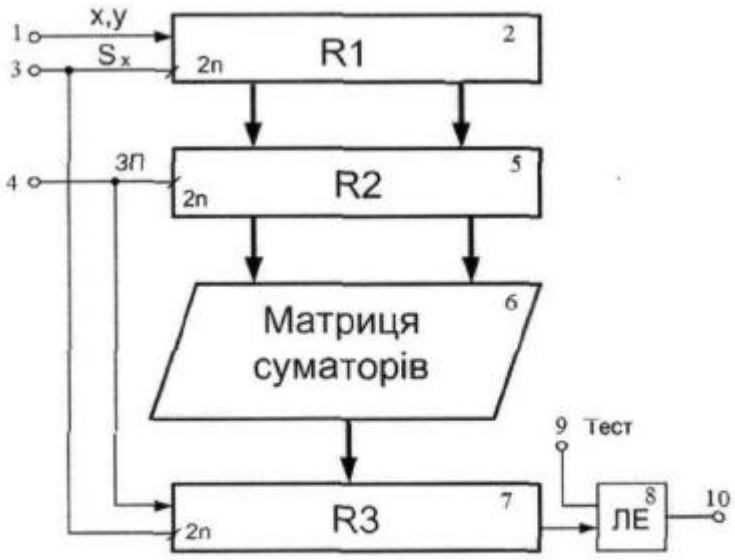
$A_2=3\times 512\times 2\times 2+512^2+512\times(3+6+(510\times 8)+1)=6144+2356225=2362369$ (вент.).

В результаті, апаратна складність запропонованого пристрою у 2,3 разів менша ніж у відомого пристрою.

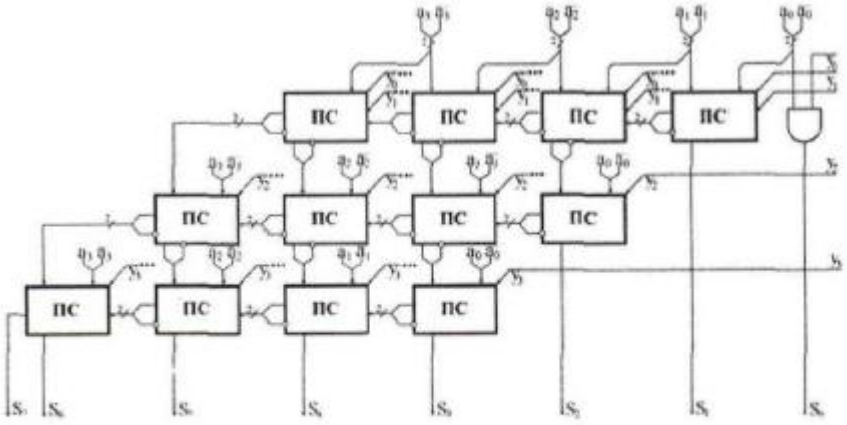
ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Перемножувач потоків багаторозрядних даних, що містить перший регістр пам'яті на D-тригерах з прямими виходами, перші входи якого є вхідною шиною двійкових кодів перемножуваних чисел, другий вхід з'єднаний з другим входом пристрою, виходи з'єднані з відповідними прямими входами матриці однорозрядних повних двійкових суматорів, виходи якої з'єднані з відповідними першими входами другого регістра пам'яті, другий вхід якого з'єднаний з другим входом першого регістра пам'яті, який **відрізняється** тим, що додатково містить перший 2n-розрядний регістр зсуву на D-тригерах, перший вхід якого є першим входом пристрою, другий вхід якого є другим входом синхронізації пристрою, виходи якого додатково з'єднані з відповідними першими входами першого регістра пам'яті, виходи матриці перемноження додатково з'єднані з відповідними першими входами додатково введеного регістра пам'яті та зсуву, другий вхід якого з'єднаний з другим входом першого регістра пам'яті і другим входом

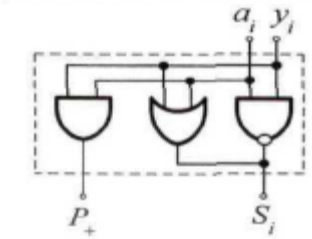
пристрою, третій вхід з'єднаний з третім входом синхронізації пристрою, вихід регістра пам'яті та зсуву додатково з'єднаний з першим входом додатково введеного логічного елемента "Виключаюче АБО", другий вхід якого з'єднаний з додатково введеним четвертим входом пристрою а вихід є вихідним каналом пристрою.



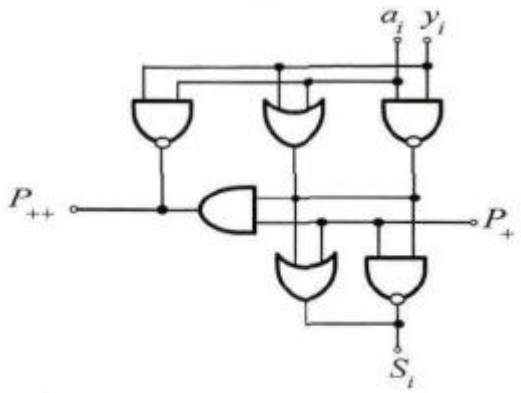
Фіг. 1



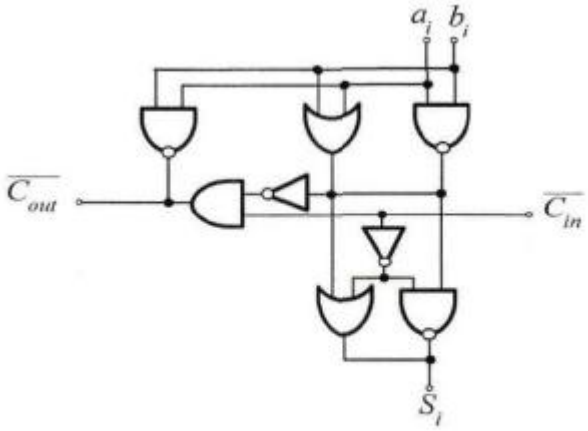
Фіг. 2



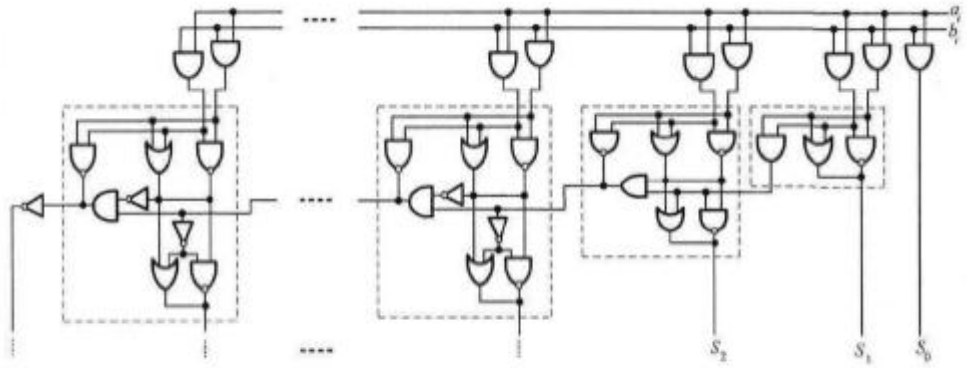
Фіг. 3



Фіг. 4



Фіг. 5



Фіг. 6

Комп'ютерна верстка М. Мацело

Міністерство розвитку економіки, торгівлі та сільського господарства України,
вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

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