УКРАЇНА

(19) UA (11) 132145 (13) U

(51) МПК (2018.01)
G06F 7/00
G06F 7/40 (2006.01)

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2018 09550**

(22) Дата подання заявки: **24.09.2018**

(24) Дата, з якої є чинними права на корисну модель: **11.02.2019**

(46) Публікація відомостей про видачу патенту: **11.02.2019, Бюл.№ 3**

(72) Винахідник(и):
Сидор Андрій Іванович (UA),
Николайчук Ярослав Миколайович (UA),
Возна Наталія Ярославівна (UA)

(73) Власник(и):
Сидор Андрій Іванович,
вул. Польова, 17, с. Дідичі, Ківерцівський р-н, Волинська обл., 45261 (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)

(54) РІЗНИЦЕВО-МОДУЛЬНИЙ КВАДРАТОР

(57) Реферат:

Різницево-модульний квадратор містить першу вхідну шину, логічні модулі рандомізації та вихідну шину, яка з'єднана з виходами логічних модулів рандомізації, крім того, перша вхідна шина додатково з'єднана з першими входами першого та другого додатково введених модульних регістрів пам'яті, додатково введена друга вхідна шина з'єднана з другим входом першого модульного регістра пам'яті, третя додатково введена вхідна шина з'єднана з другим входом другого модульного регістра пам'яті, виходи другого модульного регістра пам'яті з'єднані з відповідними першими входами відповідних додатково введених різницево-модульних матриць, другі входи яких додатково з'єднані з відповідними виходами першого модульного регістра пам'яті, а виходи різницевих матриць додатково з'єднані з входами відповідних логічних модулів рандомізації.

UA 132145 U

Різницево-модульний квадратор належить до засобів обчислювальної техніки і може бути використаний в якості швидкодіючого компонента при розробці дискретних пристроїв для задач статистичного аналізу та високопродуктивних компонентів спецпроцесорів визначення Хеммінгової віддалі згідно квадратичної оцінки Евклідової відстані.

Відомий аналог - числоімпульсний множильний пристрій [Николайчук Я.М. Числоимпульсное множительное устройство // А.С. СССР № 754414. - Бюлетень № 29. - 1980], який містить вхідну шину, лічильник, виходи якого порозрядно, через логічні ключі, підключені до накопичувача.

Недоліком такого пристрою, який при однаковому числі імпульсів на вхідних шинах, виконує обчислення їх квадрату, є низька швидкодія, яка обумовлена тим, що обчислювальні операції у пристрої виконуються у двійковій системі числення теоретико-числового базису Радемахера, що приводить до багаторазового виконання наскрізних переносів у суматорі накопичувача.

Крім того недоліком такого пристрою є обмежені функціональні можливості обумовлені тим, що пристрій не дозволяє реалізувати визначення квадрату різниці між двома числами.

Відомий найближчий аналог квадратор [Круліковський Б.Б., Давлетова А.Я., Николайчук Я.М., Івасьєв С.В. Квадратор, патент України на корисну модель №108333, Бюл. №13, 2016], який містить вхідну шину, розрядно-позиційні лічильники теоретико-числового базису Хаара-Крестенсона, входи яких з'єднані з вхідною шиною, а виходи з'єднані з входами логічного модуля рандомізації, виходи якого з'єднані з виходами пристрою кодів квадратів у теоретико-числовому базисі Хаара-Крестенсона.

Недоліком такого пристрою є низька швидкодія, обумовлена тим що на вхідну шину пачкою імпульсів на протязі 2^k подається унітарний код числа, яке підноситься до квадрату. Таким чином, часова складність такого пристрою визначається згідно виразу: $\tau_к = 2^k \cdot (\tau_т + \tau_{кв})$, 2^k - діапазон квантування вхідного числа, $\tau_т = 2$ мікротакти - затримка сигналів при переключенні D-тригера; $\tau_{кв} = 1$ мікротакт - затримка сигналів в логічному модулі рандомізації. При k=4 $\tau_к = 2^4 \cdot (2+1) = 48$ мікротактів, відповідно при k=7,8,10,11 отримаємо: $\tau_к = 384$, $\tau_к = 768$, $\tau_к = 3072$, $\tau_к = 6144$ мікротакти.

Іншим недоліком відомого пристрою є обмежені функціональні можливості обумовлені тим, що пристрій не дозволяє реалізувати визначення квадрату різниці між двома числами представленими в кодах Хаара-Крестенсона.

В основу винаходу поставлена задача вдосконалення, підвищення швидкодії та розширення функціональних можливостей пристрою шляхом визначення квадрату модульної різниці двох чисел x_i та y_i, представлених у системі числення залишкових класів теоретико-числового базису Хаара-Крестенсона згідно виразу:

$$Z = (x_i - y_i)^2.$$

Такі коди за 4 мікротакти отримуються на виходах АЦП паралельного типу з вихідними кодами Хаара-Крестенсона [Возна Н.Я., Круліковський Б.Б., Николайчук Я.М., Грига В.М., Піх В.Я. Аналого-цифровий перетворювач, патент України на корисну модель №116176, Бюл. №3, 2018]. Вдосконалення пристрою здійснюється додатковим поданням на другу та третю додатково введені вхідні шини паралельних кодів x_i та y_i, у базисі Хаара-Крестенсона, які з'єднані з входами відповідних додатково введених першого та другого регістрів пам'яті, другі входи яких з'єднані з вхідною шиною синхронізації, а виходи з'єднані з першими та другими входами відповідних додатково введених різнецево-модульних матриць, виходи яких з'єднані з входами відповідних логічних модулів рандомізації, які містять додатково введені логічні елементи І-НІ, виходи яких є виходами пристрою у коді Хаара-Крестенсона системи залишкових класів.

Поставлена задача вирішується тим, що різницево-модульний квадратор містить першу вхідну шину, логічні модулі рандомізації, регістри пам'яті та вихідну шину, яка з'єднана з відповідними виходами рандомізаторів, згідно з винаходом, перша вхідна шина додатково з'єднана з першими входами додатково введених першого та другого модульних регістрів пам'яті, додатково введені друга та третя вхідні шини паралельних кодів Хаара-Крестенсона чисел x_i та y_i, які додатково з'єднані з другими входами відповідних першого та другого модульних регістрів пам'яті, виходи першого регістра пам'яті з'єднані з відповідними першими входами відповідних додатково введених різницево-модульних матриць, другі входи яких додатково з'єднані з відповідними виходами другого модульного регістра пам'яті, а виходи додатково з'єднані з входами відповідних логічних модулів рандомізації.

Корисна модель ілюструється кресленнями: на фіг. 1 показана структурна схема пристрою, де: 1 - перша вхідна шина синхронізації; 2 - друга вхідна шина числа x_i; 3 - третя вхідна шина

числа y_i; 4.1, 4.2 - перший та другий модульні регістри пам'яті; 5 - різницево-модульні матриці; 6 - логічні модулі рандомізації; 7 - вихідна шина; на фіг.2 показана структурна схема компонента пристрою - модульного регістра пам'яті 4; на фіг.3 - приклад реалізації та структура з'єднання вентилів входів та виходів різницево-модульної матриці на елементах I-HI (P=11); на фіг.4 - приклад реалізації формування коду квадрата залишку по модулю P_I на виходах логічного модуля рандомізації у базисі Хаара-Крестенсона на логічних елементах I-HI (P=11);

Пристрій працює наступним чином: на початку циклу роботи пристрою на першій вхідній шині (1) формується сигнал синхронізації, по фронту наростання якого у відповідні модульні регістри 4.1, 4.2 записуються коди Хаара-Крестенсона вхідних чисел x_i, y_i. При цьому, на перші та другі входи різницево-модульних матриць 5 поступають коди залишків по модулю P_i у базисі Хаара. Отримані вихідні коди прямих або доповнюючих залишків модульних різниць поступають на входи відповідних логічних модулів рандомізації 6, на виходах яких формуються коди модульних квадратів, які поступають на вихідну шину пристрою 7.

Згідно із системою числення залишкових класів для однозначного представлення квадрату різниці двох чисел $(x_i - y_i)^2$ повинна виконуватися умова: добуток P_0 взаємопростих модулів P_i повинен бути рівний або більший $N = [(x_i - y_i)max]$, що відповідає умові: сума двійкових розрядностей модулів P_i, повинна бути на 1-2 розряди більша відносно кількості розрядів двійкового представлення максимального квадрату різниці між числами x_i, та y_i тобто: $n \geq E[\log_2 N^2]$, де E - цілочисельна функція з округленням до більшого цілого. Наприклад, при числі модулів P_i, k = 4 і максимальних значеннях квадратів N, розрахунки для різних N показано в таблиці:

Таблиця

		P_1	P_2	P_3	P_4	2n + 1	N^2	P_0
N	15	2	3	5	11	11	225	330
n	4	1	3	3	4			
N	99	8	9	11	13	15	9801	10296
n	7	3	4	4	4			
N	255	13	16	17	19	18	65025	67194
n	8	4	4	5	5			
N	1023	29	32	33	37	22	1046529	1133088
n	10	5	5	6	6			
N	2047	43	45	47	49	24	4190209	4456305
n	12	6	6	6	6			

Особливістю роботи пристрою є незалежність формування прямого коду квадрату на виходах логічних модулів рандомізації 6, незалежно від того прямі чи інвертовані коди по модулю формуються на виходах різницево-модульних матриць 5.

Наприклад: необхідно визначити квадрат різниці між двома числами, які можуть бути представлені у діапазоні: $0 \leq x_i \leq 99, 0 \leq y_i \leq 99,$ максимальне значення квадрату їх різниць рівне $99^2=9801$.

Представимо за дані числа $x_i = 29, y_i = 17,$ у базисах Радемахера-Крестенсона (RC) та Хаара-Крестенсона (HC) у системі числення залишкових класів з набором модулів: P_1 =8, P_2=9, P_3 =11, P_4 =13, добуток яких P_i рівний $8 \cdot 9 \cdot 11 \cdot 13 = 10296 > 9801$, тобто у кодах (RC) $x_i = 29_{10} = (5\,2\,7\,3)_{(8,9,11,13)}$, $y_i = 17_{10} = (1\,8\,6\,4)_{(8,9,11,13)}$, 4 виконаємо віднімання цих чисел двома варіантами в системі залишкових класів із піднесенням до квадрату отриманих різниць:

x_i	5	2	7	3		x_i	5	2	7	3
y_i	1	8	6	4		y_i	1	8	6	4
$(x_i - y_i)$	4	3	1	12		$(x_i - y_i)$	4	6	10	1
	4	3	1	12			4	6	10	1
$(x_i - y_i)^2$	0	0	1	1	=	$(x_i - y_i)^2$	0	0	1	1

.

Тобто отримані результати квадратів рівні між собою і представляють число 144. В кодах (НС) по кожному модулю Р, дані операції виконуються на різницево-модульних матрицях 5 та логічних модулях рандомізації 6. У результаті отримується наступний код (НС): 0 0 1 1.

Така властивість квадратів НС-кодів дозволяє спростити реалізацію двох послідовно з'єднаних компонентів спецпроцесора Хаара-Крестенсона шляхом безпосереднього використання вихідних прямих та доповнюючих кодів різницево-модульних матриць 5 та заміни логічних елементів АБО відповідними логічними елементами І-НІ у модульних квадраторах на основі логічних схем рандомізації 6.

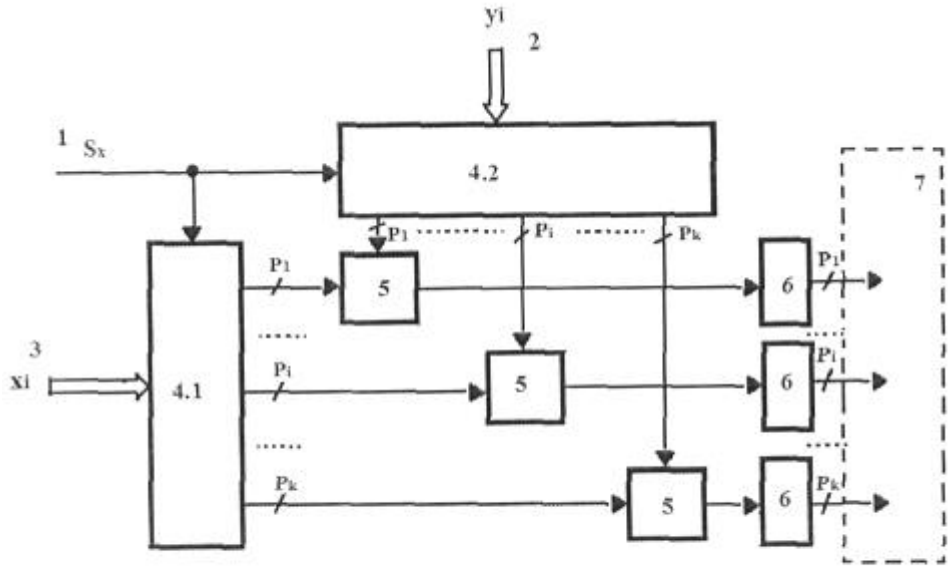
Часова складність, яка визначає швидкодію запропонованого пристрою розраховується згідно виразу $\tau_{кв} = \tau_т + \tau_м + \tau_р, \tau_т = 2\upsilon$ - затримка сигналів на 2 мікротакти при переключенні D-тригерів регістрів 4; $\tau_м = 1\upsilon$ - затримка сигналів на 1 мікротакт у різницево-модульних матрицях 5; $\tau_р = 1\upsilon$ - затримка сигналів на 1 мікротакт у логічних модулях рандомізації 6.

Отже, загальна затримка сигналів у пристрої, незалежно від розрядності вхідних чисел, складає: $\tau_{кв} = 2+1+1 = 4\upsilon$. Тобто при тактовій частоті роботи вентилів ПЛІС 500 МГц формування вихідних кодів різницевих квадратів буде здійснюватися з частотою 125 МГц, що в порівняні з аналогом, при кодуванні вхідних чисел в діапазонах 16, 128, 256, 1024, 2048 підвищення швидкодії складає 12, 125, 179, 625, 1536 разів, що відповідно 1-3 порядки.

В частковому випадку, коли одне з чисел x_i, або y_i, є нульовим, пристрій реалізує функцію відомого пристрою шляхом піднесення до квадрату одного числа у базисі Хаара-Крестенсона.

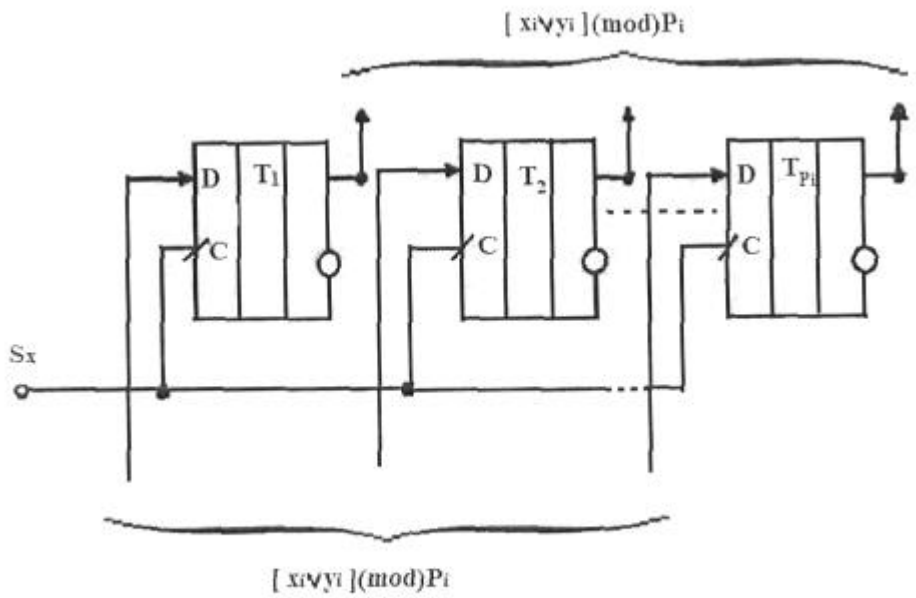
ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Різницево-модульний квадратор, який містить першу вхідну шину, логічні модулі рандомізації та вихідну шину, яка з'єднана з виходами логічних модулів рандомізації, який **відрізняється** тим, що згідно з винаходом перша вхідна шина додатково з'єднана з першими входами першого та другого додатково введених модульних регістрів пам'яті, додатково введена друга вхідна шина з'єднана з другим входом першого модульного регістра пам'яті, третя додатково введена вхідна шина з'єднана з другим входом другого модульного регістра пам'яті, виходи другого модульного регістра пам'яті з'єднані з відповідними першими входами відповідних додатково введених різницево-модульних матриць, другі входи яких додатково з'єднані з відповідними виходами першого модульного регістра пам'яті, а виходи різницевих матриць додатково з'єднані з входами відповідних логічних модулів рандомізації.



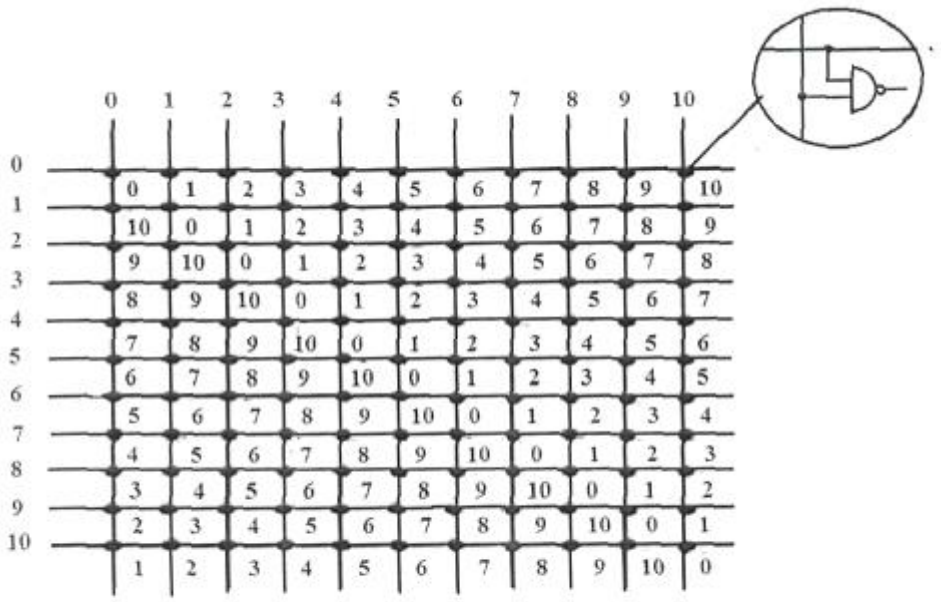
Структурна схема різницево-модульного квадратора

Фіг. 1



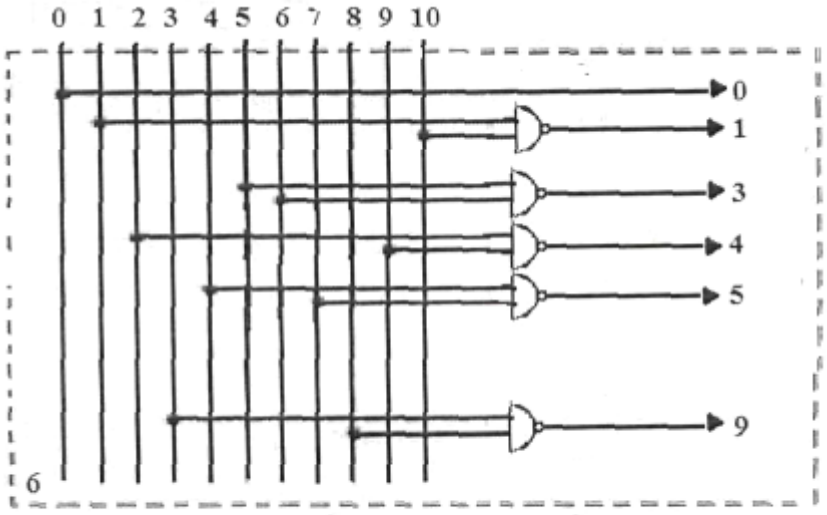
Структура модульного регістра пам'яті.

Фіг. 2



Різницево-модульна матриця на елементах І-НІ.

Фіг. 3



Реалізації формування коду квадрата залишку по модулю P_i

Фіг. 4

Комп'ютерна верстка А. Крулевський

Міністерство економічного розвитку і торгівлі України, вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

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