ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

**УКРАЇНА** **(19) UA** **(11) 74576** **(13) U**

**(51)** МПК (2012.01)
**G06F 5/00**

## (12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

**(21)** Номер заявки: **u 2012 00611**

**(22)** Дата подання заявки: **19.01.2012**

**(24)** Дата, з якої є чинними права на корисну модель: **12.11.2012**

**(46)** Публікація відомостей про видачу патенту: **12.11.2012, Бюл.№ 21**

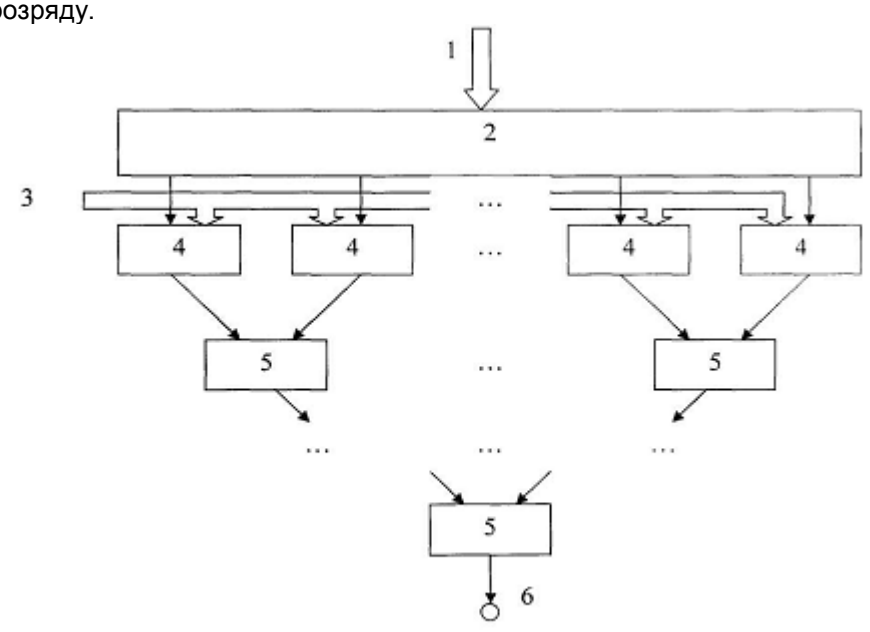
**(72)** Винахідник(и):
**Николайчук Ярослав Миколайович (UA),**
**Волинський Орест Ігорович (UA)**

**(73)** Власник(и):
**Николайчук Ярослав Миколайович**,
вул. В. Великого, 14-а, м. Надвірна, Івано-Франківська обл., 78400 (UA),
**Волинський Орест Ігорович**,
вул. Вагилевича, 6/2, м. Надвірна, Івано-Франківська обл., 78400 (UA)

### (54) СПОСІБ ВИЗНАЧЕННЯ ЗАЛИШКУ ДВІЙКОВОГО ЧИСЛА

**(57)** Реферат:

Спосіб визначення залишку двійкового числа по модулю, в якому n-розрядне двійкове число з вхідної шини записують в регістр пам'яті, а з вихідної шини знімають m-розрядний кінцевий код залишку цього числа по m-розрядному модулю, при якому двійковий код порозрядно зчитують починаючи зі старших розрядів, підсумовують його з подвоєним кодом попереднього залишку, починаючи з його нульового значення та формують новий код залишку по модулю з постійної пам'яті, який після n повторень таких операцій зчитується як кінцевий код залишку, починаючи зі старшого розряду.




Фіг. 1

UA 74576 U

Спосіб визначення залишку двійкового числа належить до систем перетворення інформації, які можуть бути використані для перетворення великорозрядних двійкових чисел по великорозрядним модулям у системах передавання та захисту інформації від несанкціонованого доступу, а також, побудови спецпроцесорів в системі залишкових класів теоретико-числового базису Крестенсона.

Відомий спосіб визначення залишку двійкового числа, що ґрунтується на виконанні операції ділення двійкового числа на заданий модуль і отримання найменшого невід'ємного залишку згідно з алгоритмом ділення по модулю двійкових чисел в доповнюючих кодах [Майоров С.А., Новиков Г.И. Принципы организации цифровых машин. - Л.: Машиностроение, 1974.-306 с., рис. 8.12].

Недоліком такого способу є велика алгоритмічна складність визначення залишку, оскільки його реалізація потребує багаторазового виконання операцій додавання доповнюючих кодів та операції порівняння чисел, що приводить до низької швидкодії обчислень, оскільки операція ділення потребує (n+1-m)·m-тактів виконання операцій сумування, (n+1-m) - операцій порівняння та (n-m) - операцій зсуву процесора при n-розрядності ділимого та m-розрядного дільника.

Найбільш близьким за суттю до корисної моделі, що заявляється, є спосіб отримання залишків двійкових чисел по заданому модулю, в якому n-розрядне двійкове число з вхідної шини записують в регістр пам'яті, а з вихідної шини знімають m-розрядний кінцевий код залишку цього числа по m-розрядному модулю, що ґрунтується на використанні розмежованої системи числення залишкових класів шляхом отримання сукупності залишків кожного одиничного розряду двійкового числа та їх лінійного підсумовування по заданому модулю, який потребує n операцій сумування залишків для n-розрядного двійкового числа та наявності n-суматорів по модулю [Волинський О.І., "Методи міжбазисних перетворень на основі розмежованої системи числення залишкових класів", Вісник національного університету "Львівська політехніка", "Комп'ютерні системи та мережі". - Львів: Видавництво львівська політехніка, 2010. - № 688.-58 с., рис. 6].

Проте такий спосіб характеризується великою часовою складністю та апаратною складністю, оскільки для отримання залишку n-розрядного числа необхідне знаходження n окремих залишків для кожною окремого і-того розряду двійкового числа з наступним n-разовим їх підсумовуванням по модулю.

В основу корисної моделі поставлена задача розробки нового способу визначення залишку двійкового числа шляхом послідовного зчитування n-розрядного двійкового числа, починаючи зі старших розрядів та послідовного отримання m-розрядних кодів залишків по модулю з постійної пам'яті, що дозволяє підвищити швидкодію отримання текучих та кінцевого залишку двійкового числа по модулю за n операцій зсуву та вибірки з пам'яті, в яких відсутні операції наскрізних переносів.

Поставлена задача вирішується завдяки тому, що спосіб визначення залишку двійкового числа по модулю, в якому n-розрядне двійкове число з вхідної шини записують в регістр пам'яті, а з вихідної шини знімають m-розрядний кінцевий код залишку цього числа по m-розрядному модулю, згідно з корисною моделлю, вводиться те, що двійковий код порозрядно зчитують, починаючи зі старших розрядів, підсумовують його з подвоєним кодом попереднього залишку, починаючи з його нульового та формують повний код залишку по модулю з постійної пам'яті, який після n повторень таких операцій зчитується як кінцевий код залишку, починаючи зі старшого розряду.

Суть корисної моделі полягає у тому, що в способі отримання залишку, відносно до прототипу, відсутня операція порівняння, яка потребує використання суматорів, що у свою чергу приводить до виникнення наскрізних переносів, які знижують швидкодію визначення залишку. У запропонованому способі, замість вказаних операцій, здійснюється проста вибірка з постійної пам'яті з врахуванням модульної операції.

На фіг. 1 показана формалізована функціональна структура пристрою, який реалізує відомий спосіб визначення залишку двійкового числа де: 1 - вхідна шина двійкового числа X; 2-n-розрядний регістр пам'яті; 3 - вхідна шина m-розрядного коду модуля P; 4 - дешифратори $2^i$ значень бітів числа X в коди залишків $b_i$ по модулю P; 5 - m-розрядні суматори кодів залишків $b_i$, та $b_i$, по модулю P; 6 - вихідна шина коду залишку $b_0$.

Корисна модель ілюструється кресленням на фіг. 2, де зображена функціональна структура пристрою, який реалізує запропонований спосіб визначення залишку двійкового числа по модулю P, що складається: 1 - вхідна шина двійкового числа X та залишку $b_0=0$; 2-n+m-розрядний регістр пам'яті та зсуву; 3 - вхідна шина m-розрядного коду модуля P; 4 - постійний запам'ятовуючий пристрій; 5 - вихідна шина проміжних та кінцевого залишку $b_0$ по модулю P.

На фіг. 3 показано приклад вибірки кодів залишків $b_i$, згідно адресних входів $b_{i-1}$ по модулю $P_{(10)}=11$.

Спосіб здійснюють таким чином.

У регістр пам'яті та зсуву - 2 з вхідної шини - 1 заноситься n-розрядний код числа X, молодші розряди якого записуються у відповідні розряди регістра 2, починаючи зліва, а в інші m-розряди записуються нулі. Одночасно з вхідної шини - 3 в постійний запам'ятовуючий пристрій - 4 подається m-розрядний двійковий код модуля P. Після n зсувів з вихідної шини - 5 зчитують код кінцевого залишку $b_0$ числа X по модулю P, починаючи зі старшого розряду з права.

Наприклад, потрібно обчислити залишок числа $X=100_{(10)}=1100100_{(2)}$, по модулю $P=11_{(10)}=1011_{(2)}$.

У регістр пам'яті та зсуву в n-розрядів записуємо X=1100100, а в інші m-розряди $b_{i-1}$=00000.

(Зсув 1) Зсуваємо код числа X починаючи з старшого розряду вправо, при цьому, старший розряд числа X потрапляє в перший розряд m-розрядного регістра пам'яті та зсуву, де отримаємо $b_{i-1}$=10000 код, відповідно фіг. 3. $b_i$=00001, який порозрядно записується в m-розряди регістра пам'яті та зсуву.

Аналогічно здійснюються наступні зсуви при яких $b_{i-1}$ та $b_i$, будуть набувати значень (фіг. 3):

(Зсув 2) $b_{i-1}$=11000, $b_i$=11000;

(Зсув 3) $b_{i-1}$=01100, $b_i$=01100;

(Зсув 4) $b_{i-1}$=00110, $b_i$=10000;

(Зсув 5) $b_{i-1}$=11000, $b_i$=11000;

(Зсув 6) $b_{i-1}$=01100, $b_i$=01100;

(Зсув 7) $b_{i-1}$=00110, $b_i$=10000.

Після n=7 зсувів отримаємо кінцеве значення залишку $b_0$=10000, що зчитується вихідною шиною, в якому старший розряд справа.

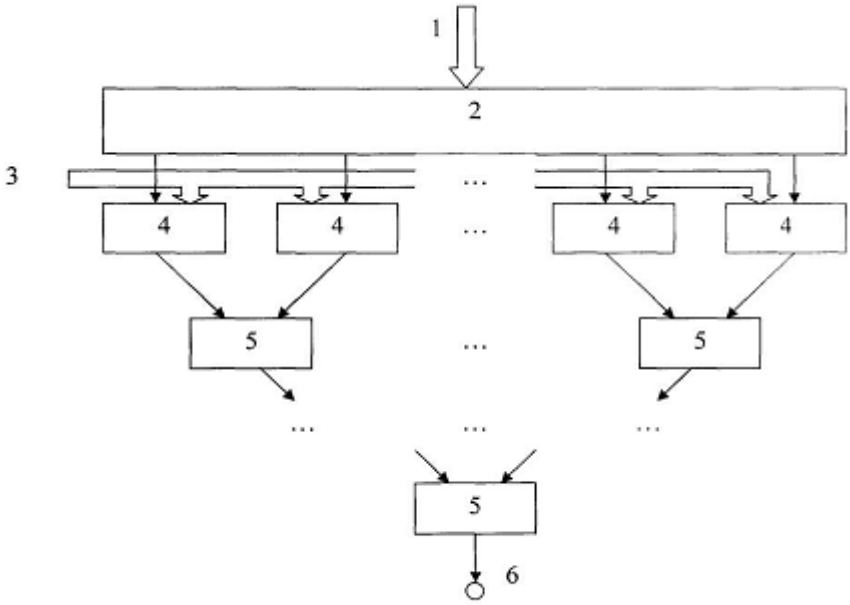
Для реалізації запропонованого способу регістр пам'яті та зсуву - 2 виконується відомою мікроелектронною схемою на D-тригерах з мультиплексорами на D входах, а постійний запам'ятовуючий пристрій на основі групи k m-адресних кристалів флеш пам'яті.

Наприклад, для використовуваних сучасних способів захисту інформації RSA та Ель-Гамаля з розрядністю модулів 512-1024 біти потрібно 4 кристали флеш пам'яті 16 ГБ. При тактовій частоті регістра пам'яті та зсуву - 2100 МГц затримка часу визначення одного залишку 1024-х бітного числа X складає близько 1 млс.

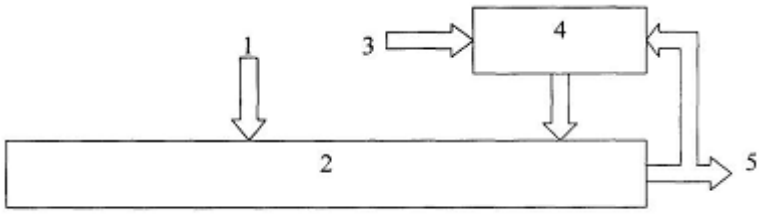
Операція обчислення залишку заявленим способом потребує n тактів в регістрі пам'яті та зсуву - 2 та n тактів вибірки коду залишку з постійного запам'ятовуючого пристрою - 4, тобто рівне 2n, у випадку якщо двійкове число буде займати 512 біт, а модуль, за яким обчислюють залишок, буде від 2 біт до 128 то швидкодія, в порівнянні з відомим способом, зросте від 2-х до 48-и разів.

## ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб визначення залишку двійкового числа по модулю, в якому n-розрядне двійкове число з вхідної шини записують в регістр пам'яті, а з вихідної шини знімають m-розрядний кінцевий код залишку цього числа по m-розрядному модулю, який **відрізняється** тим, що двійковий код порозрядно зчитують, починаючи зі старших розрядів, підсумовують його з подвоєним кодом попереднього залишку, починаючи з його нульового значення та формують новий код залишку по модулю з постійної пам'яті, який після n повторень таких операцій зчитується як кінцевий код залишку, починаючи зі старшого розряду.




**Фіг. 1**




**Фіг. 2**

| | |
|---|---|
| 10 | 01010 |
| 9 | 10010 |
| 8 | 00010 |
| 7 | 11100 |
| 6 | 01100 |
| 5 | 10100 |
| 4 | 00100 |
| 3 | 11000 |
| 2 | 01000 |
| 1 | 10000 |
| 0 | 00000 |
| 10 | 01010 |
| 9 | 10010 |
| 8 | 00010 |
| 7 | 11100 |
| 6 | 01100 |
| 5 | 10100 |
| 4 | 00100 |
| 3 | 11000 |
| 2 | 01000 |
| 1 | 10000 |
| 0 | 00000 |

$b_i$

| | |
|---|---|
| 10101 | 21 |
| 00101 | 20 |
| 11001 | 19 |
| 01001 | 18 |
| 10001 | 17 |
| 00001 | 16 |
| 11110 | 15 |
| 01110 | 14 |
| 10110 | 13 |
| 00110 | 12 |
| 11010 | 11 |
| 01010 | 10 |
| 10010 | 9 |
| 00010 | 8 |
| 11100 | 7 |
| 01100 | 6 |
| 10100 | 5 |
| 00100 | 4 |
| 11000 | 3 |
| 01000 | 2 |
| 10000 | 1 |
| 00000 | 0 |

$b_{i-1}$

**Фіг. 3**

Комп'ютерна верстка А. Крижанівський

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

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