УКРАЇНА

ПАТЕНТ

НА КОРИСНУ МОДЕЛЬ

№ 118065

СПОСІБ ПІДНЕСЕННЯ ДО КВАДРАТА ЦІЛИХ ЧИСЕЛ

Видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі".

Зареєстровано в Державному реєстрі патентів України на корисні моделі **25.07.2017.**

Директор департаменту інтелектуальної власності Міністерства економічного розвитку і торгівлі України В.О. Жалдак

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ * ІДЕНТИФІКАЦІЙНИЙ КОД 37508596 *

(11) **118065**

(19) **UA**

(51) **МПК**
G06F 7/523 **(2006.01)**

(21) Номер заявки: **u 2016 13439**

(22) Дата подання заявки: **27.12.2016**

(24) Дата, з якої є чинними права на корисну модель: **25.07.2017**

(46) Дата публікації відомостей про видачу патенту та номер бюлетеня: **25.07.2017, Бюл. № 14**

(72) Винахідники:
Охріменко Андрій Олександрович, UA,
Ковтун Владислав Юрійович, UA,
Ковтун Марія Григорівна, UA,
Євсеєв Сергій Петрович, UA,
Король Ольга Григорівна, UA,
Грищук Руслан Валентинович, UA,
Коц Григорій Павлович, UA

(73) Власники:
Охріменко Андрій Олександрович,
вул. Покровська, 8, кв. 6, м. Васильків, Київська обл., 08600, UA,
Ковтун Владислав Юрійович,
вул. Олени Пчілки, 4, кв. 508, м. Київ, 02081, UA,
Ковтун Марія Григорівна,
вул. Олени Пчілки, 4, кв. 508, м. Київ, 02081, UA,
Євсеєв Сергій Петрович,
вул. Героїв Праці, 21-а, кв. 26, м. Харків, 61144, UA,
Король Ольга Григорівна,
вул. Героїв Праці, 21-а, кв. 26, м. Харків, 61144, UA,
Грищук Руслан Валентинович,
вул. Чуднівська, 108-в, кв. 3, м. Житомир, 10005, UA,
Коц Григорій Павлович,
вул. 8-го Березня, 9-а, смт Хорошево, Харківська обл., 62466, UA

(54) Назва корисної моделі:

СПОСІБ ПІДНЕСЕННЯ ДО КВАДРАТА ЦІЛИХ ЧИСЕЛ

(57) Формула корисної моделі:

Спосіб піднесення до квадрата цілих чисел, що включає виконання піднесення до квадрата цілого числа, за допомогою використання послідовної дії пристроїв "МНОЖЕННЯ", "РЕЄСТР ЗСУВУ" та "ДОДАВАННЯ" у двох

каналах згідно з алгоритмом піднесення до квадрата цілого числа, який **відрізняється** тим, що додатково включено тимчасові змінні, які зберігаються у відповідних пристроях циклів "РЕЄСТР ЗСУВУ", та виконання над ними послідовної дії пристроїв "МНОЖЕННЯ" та "ДОДАВАННЯ" з виключенням повторень, що дозволяє зменшити кількість виконуваних операцій та зменшити час отримання результату обчислення піднесення до квадрата цілого числа довільної довжини.

Державне підприємство
«Український інститут інтелектуальної власності»
(Укрпатент)

Оригіналом цього документа є електронний документ з відповідними реквізитами, у тому числі з накладеним електронним цифровим підписом уповноваженої особи Міністерства економічного розвитку і торгівлі України та сформованою позначкою часу.

Ідентифікатор електронного документа 2431010817.

Для отримання оригіналу документа необхідно:

1. Зайти до ІДС «Стан діловодства за заявками на винаходи та корисні моделі», яка розташована на сторінці http://base.uipv.org/searchInvStat/.

2. Виконати пошук за номером заявки.

3. У розділі «Документи Укрпатенту» поруч з реєстраційним номером документа натиснути кнопку «Завантажити оригінал» та ввести ідентифікатор електронного документа.

Ідентичний за документарною інформацією та реквізитами паперовий примірник цього документа містить 3 арк., які пронумеровані та прошиті металевими люверсами.

Уповноважена особа Укрпатенту І.Є. Матусевич

25.07.2017

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

УКРАЇНА **(19) UA** **(11) 118065** **(13) U**

(51) МПК
G06F 7/523 (2006.01)

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2016 13439**

(22) Дата подання заявки: **27.12.2016**

(24) Дата, з якої є чинними права на корисну модель: **25.07.2017**

(46) Публікація відомостей про видачу патенту: **25.07.2017, Бюл.№ 14**

(72) Винахідник(и):
Охріменко Андрій Олександрович (UA),
Ковтун Владислав Юрійович (UA),
Ковтун Марія Григорівна (UA),
Євсеєв Сергій Петрович (UA),
Король Ольга Григорівна (UA),
Грищук Руслан Валентинович (UA),
Коц Григорій Павлович (UA)

(73) Власник(и):
Охріменко Андрій Олександрович,
вул. Покровська, 8, кв. 6, м. Васильків, Київська обл., 08600 (UA),
Ковтун Владислав Юрійович,
вул. Олени Пчілки, 4, кв. 508, м. Київ, 02081 (UA),
Ковтун Марія Григорівна,
вул. Олени Пчілки, 4, кв. 508, м. Київ, 02081 (UA),
Євсеєв Сергій Петрович,
вул. Героїв Праці, 21-а, кв. 26, м. Харків, 61144 (UA),
Король Ольга Григорівна,
вул. Героїв Праці, 21-а, кв. 26, м. Харків, 61144 (UA),
Грищук Руслан Валентинович,
вул. Чуднівська, 108-в, кв. 3, м. Житомир, 10005 (UA),
Коц Григорій Павлович,
вул. 8-го Березня, 9-а, смт Хорошево, Харківська обл., 62466 (UA)

UA 118065 U

(54) СПОСІБ ПІДНЕСЕННЯ ДО КВАДРАТА ЦІЛИХ ЧИСЕЛ

(57) Реферат:

Спосіб піднесення до квадрата цілих чисел включає виконання піднесення до квадрата цілого числа, за допомогою використання послідовної дії пристроїв "МНОЖЕННЯ", "РЕЄСТР ЗСУВУ" та "ДОДАВАННЯ" у двох каналах згідно з алгоритмом піднесення до квадрата цілого числа. В якому додатково включено тимчасові змінні, які зберігаються у відповідних пристроях циклів "РЕЄСТР ЗСУВУ", та виконання над ними послідовної дії пристроїв "МНОЖЕННЯ" та "ДОДАВАННЯ" з виключенням повторень.

Запропонована корисна модель належить до автоматики й обчислювальної техніки і може бути використана в системах криптографічного захисту інформації для розширення їх можливостей.

Відомий спосіб піднесення до квадрата двох цілих чисел, який використовує послідовну дію пристроїв "МНОЖЕННЯ" згідно з алгоритмом множення в стовпчик [1]. Піднесення до квадрата є окремим випадком множення, при якому обидва множники однакові. Він може бути використаний для піднесення до квадрата двох чисел довільного розміру. На вхід двох пристроїв "МНОЖЕННЯ" подаються два машинних слова: $a=(a_n, \ldots, a_i, \ldots, a_1, a_0)$ та $b=(b_n, \ldots, b_i, \ldots, b_1, b_0)$, де a_i і b_i - машинні слова чисел a і b, n - кількість машинних слів, необхідних для представлення числа $(\log_{2^w} a)$, w - розмір машинного слова в бітах. Далі у першому пристрої "МНОЖЕННЯ" частина машинних слів a_i $(I = \overline{0,n})$ послідовно, рядками, перемножується на всі частини другого множника b_j $(j = \overline{1,n})$. Проміжний результат множення a_i і b_j формується з урахуванням всіх переносів. Кожен проміжний результат зміщується вліво на w-біт в пристрої "РЕЄСТР ЗСУВУ", а потім всі проміжні результати послідовно додаються в пристрої "ДОДАВАННЯ". На фіг. 1 зображене множення двох чисел у стовпчик, для n=3. Недоліком цього способу є те, що множення двох цілих чисел, що базується на основі множення в стовпчик, вимагає великої кількості операцій множення в стовпчик, що виконуються за допомогою послідовної дії пристроїв "МНОЖЕННЯ", тому при множенні великих чисел він буде повільним у часі.

Найближчим аналогом до запропонованої корисної моделі вибрано спосіб множення цілих чисел Comba [2], який ґрунтується на виконанні процедури множення в стовпчик, за допомогою послідовної дії пристроїв "МНОЖЕННЯ", "РЕЄСТРА ЗСУВУ" та "ДОДАВАННЯ".

На вхід пристроїв "МНОЖЕННЯ" подаються два числа a і b, які наведені як набір машинних слів $a=(a_n, \ldots, a_{i,\ldots}, a_1, a_0)$ та $b=(b_n, \ldots, b_i, \ldots, b_1, b_0)$, де n - кількість машинних слів, необхідних для представлення числа $(\log_{2^w} a)$, w - розмір машинного слова в бітах. На виході пристрою "МНОЖЕННЯ" отримується результат $c=a\times b$ розміром 2n машинних слів. Даний спосіб реалізує алгоритм множення в стовпчик з невеликою різницею: перемножується частина множника a_i $(I = \overline{0,n})$ на всі частини іншого множника b_j $(j = \overline{1,n})$, в порядку виконання умови (I+j=k) у стовпчиках, а не послідовно по рядках. Основу "МНОЖЕННЯ" складають два канали пристроїв "МНОЖЕННЯ", "РЕЄСТРА ЗСУВУ" та "ДОДАВАННЯ", які реалізують два цикли формування результату множення. Перший пристрій формує результат в інтервалі $k = \left[\overline{1,n}\right)$ та містить реалізацію вкладеного циклу множення в інтервалах $I = \left[\overline{0,k}\right]$ та $j = \left[\overline{k,0}\right]$. Другий пристрій формує результат в інтервалі $k = \left[\overline{n2,n-1}\right)$ з використанням допоміжного інтервалу $I = \left(\overline{1,n-1}\right]$ та містить реалізацію вкладеного циклу множення в інтервалах $i = \left(\overline{l,n}\right]$ та $j = \left[\overline{k-l,n-l}\right)$. У вкладених пристроях за допомогою пристрою "ДОБУТКУ" обчислюється добуток $(uv)^{(2w)}=a_i^{(w)}\times b_i^{(w)}$, результатом якого є 2w-розрядне ціле число, яке потім розділяється на два w-розрядних $u^{(w)}$ і $v^{(w)}$ числа. Накопичення суми відбувається в пристроях "ДОДАВАННЯ" та "РЕЄСТРІ ЗСУВУ" w-розрядних тимчасових змінних r_0, r_1 і r_2 на кожній ітерації:

$r_0^{(w)} \leftarrow r_0^{(w)} + v^{(w)}$,
$r_1^{(w)} \leftarrow r_1^{(w)} + u^{(w)} + carry$, $carry \leftarrow 0$,
$r_2^{(w)} \leftarrow r_2^{(w)} + carry$, $carry \leftarrow 0$.

Присвоєння кінцевого результату, а також зміна акумуляторів суми r_0, r_1 і r_2 відбувається в пристрої "ДОДАВАННЯ" на кожній ітерації циклу формування результату:

$c_k^{(w)} \leftarrow r_0^{(w)}$,
$r_0^{(w)} \leftarrow r_1^{(w)}$,
$r_1^{(w)} \leftarrow r_2^{(w)}$
$r_2^{(w)} \leftarrow 0$.

Після завершення циклів формування результату в пристрої "ДОДАВАННЯ" відбувається обчислення $c^{(w)}_{2n-1} \leftarrow r_0^{(w)}$.

На виході пристрою "МНОЖЕННЯ" формується ціле число $c=(c_{2n-1},\ldots, c_k, \ldots, c_1, c_0)$. На фіг. 2 зображене множення двох чисел способом Comba, для n=3.

Недоліками даного способу є те, що множення цілих чисел вимагає великої кількості операцій в пристроях "МНОЖЕННЯ" й "ДОДАВАННЯ" з накопиченням суми з переносом в w-бітних тимчасових змінних r_0, r_1 і r_2 в пристрої "РЕЄСТР ЗСУВУ"; його висока внутрішня зв'язність з урахуванням переносів між r_0, r_1 і r_2, що не дозволяє виконувати спарювання таких операцій на сучасних суперскалярних процесорах.

В основу корисної моделі поставлена задача створення способу піднесення до квадрата цілих чисел, який дозволить виконувати меншу кількість операцій, що забезпечує зменшення часу на отримання результату обчислення за допомогою послідовної дії пристроїв "МНОЖЕННЯ", "РЕЄСТРА ЗСУВУ" та "ДОДАВАННЯ" цілих чисел, згідно з алгоритмом піднесення до квадрата цілих чисел з використанням відкладеного переносу.

Технічний результат, що досягається при здійсненні корисної моделі полягає в отриманні можливості зниження обчислювальної складності та зменшення часу на отримання результату піднесення до квадрата цілих чисел завдяки позбуття необхідності враховувати перенос після кожної арифметичної операції за допомогою послідовної дії пристроїв "МНОЖЕННЯ", "РЕЄСТРУ ЗСУВУ" та "ДОДАВАННЯ" цілих чисел, згідно з алгоритмом множення цілих чисел.

Суть запропонованого способу піднесення до квадрата цілих чисел полягає в виконанні процедури множення, за допомогою послідовної дії пристроїв "МНОЖЕННЯ", "РЕЄСТРУ ЗСУВУ" та "ДОДАВАННЯ" згідно з алгоритмом піднесення до квадрата, який відповідно корисної моделі додатково включає тимчасові змінні, що зберігаються у відповідних пристроях "РЕЄСТРАХ ЗСУВУ", та виконанням над ними послідовної дії пристроїв "МНОЖЕННЯ" та "ДОДАВАННЯ".

В пристроях "РЕЄСТР ЗСУВУ" та "ДОДАВАННЯ" запропонована реалізація відкладеного переносу, яка дозволяє незалежно проводити складання результатів відповідних добутків у стовпчиках, що дає можливість накопичувати суми старших і молодших розрядів окремо. Після завершення накопичення суми на кожній ітерації циклу, для формування результату необхідно виконати корегування (врахувати перенос) за допомогою пристрою "ДОДАВАННЯ":

$r_1=r_1+Hi(r_0)$;

$r_2=r_2+Hi(r_1)$;

і сформувати результат $c_i=low(r_0)$.

На фіг. 1 наведено множення двох чисел в стовпчик, для n=3. На фіг. 2 наведено множення двох чисел способом Comba, для n=3. На фіг. 3 показана реалізація відкладеного переносу.

На вхід пристрою "МНОЖЕННЯ" подається велике число a, яке представляється у вигляді машинних слів $a=(a_n, \ldots, a_i, \ldots, a_1, a_0)$ розміром w-біт, n-кількість машинних слів необхідних для представлення чисел a. На виході отримуємо результат $c=a^2$ розміром 2n машинних слів.

Основу вказаного способу піднесення до квадрата складають пристрої "МНОЖЕННЯ", "РЕЄСТРУ ЗСУВУ" та "ДОДАВАННЯ", які реалізують цикли формування результату множення. Пристрої першого циклу формують результат в інтервалі $k=\left[\overline{0,n}\right)$ та містять вкладений цикл множення в інтервалах $i=\left\lfloor\overline{0,k/2}\right\rfloor$ та $j=\left|\overline{k,k/2}\right|$. Пристрої другого циклу формують результат в інтервалі $k=\left[\overline{n,2n-1}\right)$ з використанням допоміжного інтервалу $l=\left[\overline{1,n-1}\right)$ та містять вкладений цикл множення в інтервалах $i=\left\lfloor\overline{l,k/2-l}\right\rfloor$ та $j=\left|\overline{k-l,k/2-l}\right|$. У вкладених пристроях за допомогою пристрою "МНОЖЕННЯ" обчислюється добуток $(uv)^{(2w)}=a_i^{(w)}\times a_i^{(w)}$ результатом якого є 2w-розрядне ціле число, яке потім розділяється на два w-розрядних $u^{(w)}$ і $v^{(w)}$ числа. Накопичення суми відкладеного переносу відбувається в пристрої "ДОДАВАННЯ" 2w-розрядних заздалегідь проініціалізованих тимчасових змінних r_0, r_1 на кожній ітерації. При цьому, при i<j, для виключення повторень при накопиченні суми:

$r_0^{(2w)} \leftarrow r_0^{(2w)} + (v^{(w)}<<1)$,

$r_1^{(2w)} \leftarrow r_1^{(2w)} + ((u^{(w)}<<1)\ or\ (u^{(w)}>>(w-1)))$,

а при i=j:

$r_0^{(2w)} \leftarrow r_0^{(2w)} + v^{(w)}$,

$r_1^{(2w)} \leftarrow r_1^{(2w)} + u^{(w)}$.

В пристрої "РЕЄСТР ЗСУВУ" на кожній ітерації циклу формування результату виконується корегування (врахування переносу) з використанням 2w-розрядних тимчасових змінних r_1 та r_2 (r_2 заздалегідь проініціалізована):

$r_1^{(2w)} \leftarrow r_1^{(2w)} + h_{i(w)}(r_0^{(2w)})$,

$r_2^{(2w)} \leftarrow r_2^{(2w)} + h_{i(w)}(r_1^{(2w)})$

та відбувається присвоєння кінцевого результату і зміна тимчасових змінних

r_0, r_1 і r_2

$c_k^{(w)} \leftarrow low_{(w)}(r_0^{(2w)})$,

$r_0^{(2w)} \leftarrow low_{(w)}(r_1^{(2w)})$,

$r_1^{(2w)} \leftarrow low_{(w)}(r_2^{(2w)})$,

$r_2^{(2w)} \leftarrow 0$.

Наприкінці в пристрої "ДОДАВАННЯ" відбувається формування результату $c^{(w)}_{2n-1} \leftarrow low_{(w)}(r_0^{(2w)})$.

Результатом піднесення до квадрата є ціле число $c=(c_{2n-1},\ldots, c_k, \ldots, c_1, c_0)$.

Таким чином, за рахунок додаткового включення тимчасових змінних, які зберігаються у відповідних пристроях, та виконанням над ними послідовної дії пристроїв "МНОЖЕННЯ" та "ДОДАВАННЯ" цілих чисел вдається зменшити кількість виконуваних операцій та зменшити час отримання результату обчислення піднесення до квадрата цілого числа довільної довжини.

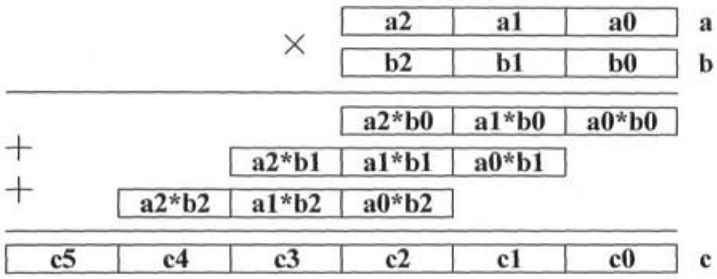
Джерела інформації:

1. Handbook of Elliptic and Hyperelliptic Curve Cryptography / Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. - Chapman & Hall/CRC. - 2005. - P. 848.

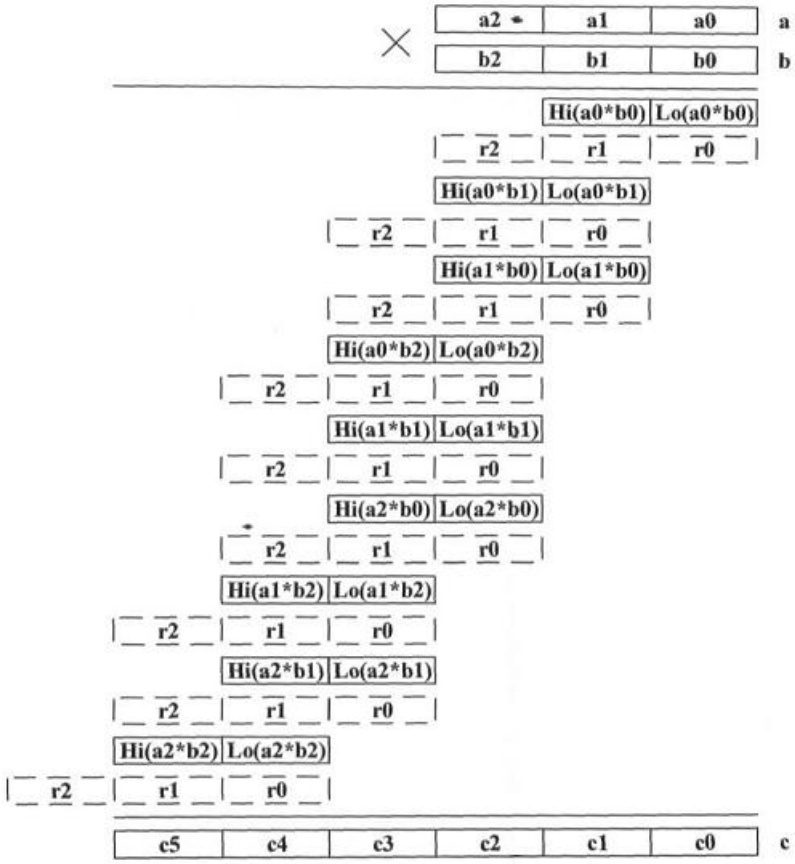
2. Comba, P.G. Exponentiation cryptosystems on the IBM PC // IBM Systems Journal. - 1990. - Vol. 29. - No. 4, December 1990.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

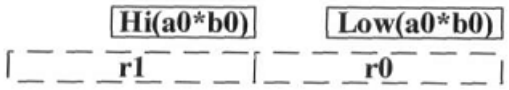
Спосіб піднесення до квадрата цілих чисел, що включає виконання піднесення до квадрата цілого числа, за допомогою використання послідовної дії пристроїв "МНОЖЕННЯ", "РЕЄСТР ЗСУВУ" та "ДОДАВАННЯ" у двох каналах згідно з алгоритмом піднесення до квадрата цілого числа, який **відрізняється** тим, що додатково включено тимчасові змінні, які зберігаються у відповідних пристроях циклів "РЕЄСТР ЗСУВУ", та виконання над ними послідовної дії пристроїв "МНОЖЕННЯ" та "ДОДАВАННЯ" з виключенням повторень, що дозволяє зменшити кількість виконуваних операцій та зменшити час отримання результату обчислення піднесення до квадрата цілого числа довільної довжини.



Фіг. 1



Фіг. 2



Фіг. 3

Комп'ютерна верстка Г. Паяльніков

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

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