ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

УКРАЇНА **(19) UA** **(11) 90144** **(13) U**

(51) МПК (2014.01)
G06F 7/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2013 15351**

(22) Дата подання заявки: **27.12.2013**

(24) Дата, з якої є чинними права на корисну модель: **12.05.2014**

(46) Публікація відомостей про видачу патенту: **12.05.2014, Бюл.№ 9**

(72) Винахідник(и):
Николайчук Ярослав Миколайович (UA),
Кімак Володимир Любомирович (UA),
Волинський Орест Ігорович (UA),
Круліковський Борис Борисович (UA)

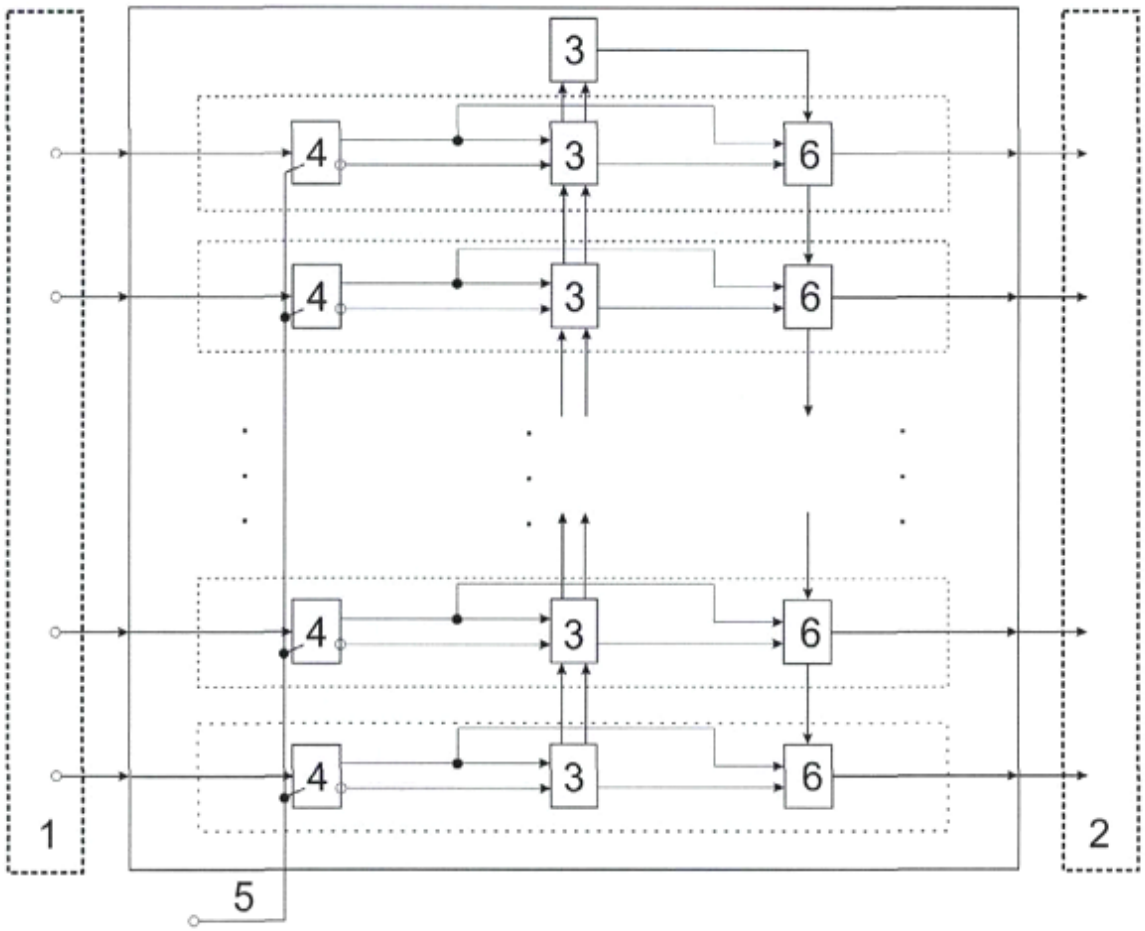
(73) Власник(и):
ІВАНО-ФРАНКІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ НАФТИ І ГАЗУ, вул. Карпатська, 15, м. Івано-Франківськ, 76019 (UA)

(54) ПРИСТРІЙ ВИЗНАЧЕННЯ ЗАЛИШКУ ПО МОДУЛЮ БАГАТОРОЗРЯДНОГО ЧИСЛА

(57) Реферат:

Пристрій визначення залишку по модулю багаторозрядного числа містить вхідну і вихідну шини, які є відповідно n-розрядними входами і n-розрядними виходами пристрою, в кожному розряді пристрою міститься спеціальний однорозрядний суматор, в кожний розряд пристрою додатково введено D-тригер, вхід якого з'єднаний з відповідним розрядом вхідної шини, входи синхронізації об'єднані між собою і є другим входом пристрою. Кожен розряд суматора додатково містить інверсний вихід переносу, який підключений до інверсного входу переносу наступного старшого розряду суматора, вихід суми найстаршого розряду суматора з'єднаний з третіми входами мультиплексорів всіх розрядів, виходи яких підключені до відповідних виходів пристрою.

UA 90144 U



Фіг. 1

Пристрій належить до перетворювачів форми інформації, які можуть бути використані для перетворення багаторозрядних двійкових чисел у залишки по модулю у системах передавання та захисту інформації від несанкціонованого доступу, а також побудови спецпроцесорів в системі залишкових класів теоретико-числового базису Крестенсона.

Відомий аналог - пристрій визначення залишку багаторозрядного числа [Николайчук Я.М. Пристрій визначення залишку багаторозрядного числа № 68872, Бюл. № 7-20121, який містить n-розрядний регістр зсуву, вхід якого підключений до шини запису кодового представлення числа, шину запису кодового представлення модуля P, яка підключена до першого входу k+1-розрядного регістра зсуву, другий адресний вхід, якого підключений до першого виходу блока управління. Недоліком такого аналога є низька швидкодія та обмежені функціональні особливості, обумовлені тим, що схема характеризується універсальністю, щодо модуля P, який задається зовнішньою шиною і не може бути таємним, що обмежує застосування цієї схеми у системах шифрування інформації.

Відомий аналог-спосіб та пристрій визначення залишку двійкового числа [Николайчук Я.М. Спосіб визначення залишку двійкового числа № 74576, Бюл. № 21-2012], який містить регістр, ПЗП і характеризується високою апаратною складністю та обмеженими функціональними можливостями, апаратна складність якого обумовлена експоненціальною складністю ПЗП при зростанні розрядності модуля (більше 1024 біт), а також відсутністю криптозахисту багаторозрядного коду модуля $P=P_1 \cdot P_2$, де P_1, P_2 - секретні багаторозрядні прості числа у галузі криптозахисту.

Відомий прототип - універсальний багаторозрядний двійковий суматор на основі повних суматорів. Недоліком прототипу є низька швидкодія, яка обумовлена наявністю реалізації окремих розрядів суматора на основі типових схем XOR, які мають не менше 2-5 послідовно з'єднаних логічних елементи і їх час затримки в одному розряді не менше 2-5 мікротактів, що для суматорів більше 1024 розрядів, що використовуються в схемах шифрування з урахуванням наскрізних переносів потребує не менше 2000-5000 мікротактів на виконання операції модульного підсумовування. Іншим недоліком прототипу є обмежені функціональні можливості, оскільки код модуля, який може бути секретним в системі шифрування задається вхідною шиною, що обмежує його застосування в системах криптозахисту даних.

Суть пристрою пояснюється тим, що в основу роботи пристрою поставлено різне схемотехнічне виконання однорозрядних спеціалізованих суматорів для нульових та одиничних біт доповнюючого коду модуля, а також секретність цього коду внаслідок відсутності зовнішньої шини його запису.

Метою пристрою є підвищення швидкодії, зменшення апаратної складності та розширення функціональних можливостей. Ця мета досягається, тим що пристрій містить додатково мультиплексори, D-тригери та має різну реалізацію однорозрядних спеціалізованих суматорів для одиничних та нульових біт доповнюючого секретного коду модуля, шина якого не виведена назовні, а також наскрізні переноси реалізуються паралельно прямим та інверсним бітом переносу. Даний пристрій використовується для виконання операції $(a+P_д) \bmod P$, де $P_д$ - доповнюючий код числа P ($P_д = \vec{P} + 1$), який використовується в асиметричних системах шифрування даних. Для отримання доповнюючого коду спочатку записують зворотний код початкового числа, для чого всі його розряди інвертують, а потім до отриманого після інвертування коду додають одиницю і на основі даного коду проектується однокристальна мікроелектронна реалізація багаторозрядного модульного суматора. Для можливості шифрування і розшифрування інформації такі кристали використовуються як апаратні засоби шифрування інформації.

Пристрій ілюструється кресленнями, де на фіг. 1 зображена структурна схема пристрою: 1 - вхідна шина, 2 - вихідна шина, 3 - спеціалізований однорозрядний суматор, 4-D-тригер, 5 - вхід синхронізації, 6 - мультиплексор.

На фіг. 2 і фіг. 3 показані структури одиничного та нульового спеціалізованих однорозрядних суматорів.

Нульовий спеціалізований однорозрядний суматор - це однорозрядний суматор, який працює тільки для $P_{Д_i} = 0$. Виходи суматора відповідають логічним виразам:

$$\overrightarrow{S = \vec{P}_+ \cap \vec{a} \cup P_+ \cap a};$$

$$P_{++} = P_+ \cap a;$$

$$\overrightarrow{P_{++}} = \overrightarrow{P_+ \cap a};$$

Де, P_+ - перенос з суматора попереднього розряду пристрою, S - сума суматора, P_{++} -

перенос у суматор наступного розряду пристрою.

Одиничний спеціалізований однорозрядний суматор - це однорозрядний суматор, який працює тільки для $P_{д_i} = 1$. Виходи суматора відповідають логічним виразам:

$$S = \overrightarrow{P_+} \cap a \cup P_+ \cap \bar{a};$$

$$P_{++} = \overrightarrow{P_+} \cap \bar{a};$$

$$\overrightarrow{P_{++}} = \overrightarrow{P_+} \cap \bar{a}.$$

Пристрій працює наступним чином.

На початку роботи пристрою вхідний код даних a ($0 < a \le 2P-1$) подається на вхідну шину пристрою 1. Після подачі сигналу синхронізації у вигляді фронту наростання на вхідну шину 5 вхідний код даних записується в тригер 4 відповідного розряду суматора 3. Вихідні коди тригерів подаються на відповідні входи нульових чи одиничних спеціалізованих однорозрядних суматорів відповідного доповнюючого коду модуля $P_д$. У результаті підсумовування вхідного коду з кодом $P_д$ та всіх наскрізних переносів у суматорах пристрою на виході 2^k знакового розряду однорозрядного суматора (S_k) формується потенціал: 0, якщо $a \ge P$, тоді $b=(a+P_0) \bmod P$, інакше $a<P$ і $b=a$. Отриманий код b з виходів мультиплексорів 6 надходить на вихідну шину пристрою 2.

Приклади виконання модульної операції в пристрої:

1) $P=11_{(10)}$; $a=10_{(10)}$.

Представимо числа a і доповнюючий код P в нормалізованій формі:

$[a] = 0{,}01010_{(2)}$; $[P]=0{,}01011_{(2)}$; $[P_д] = \overrightarrow{0{,}010111_{(2)}} + 1_{(2)} = 1{,}10100_{(2)} + 1_{(2)} = 1{,}10101_{(2)}$.

Структура виконання операції у пристрої має наступний вигляд:

$$\begin{array}{l} [a] = 0{,}01010 \\ + \\ [P_д] = 1{,}10101 \\ \hline [a] + [P_д] = 1{,}11111 \end{array}$$

Одиниця у знаковому розряді S_k вказує, що $a<P$, при цьому на виходах пристрою 2 формується код залишку $b=a$.

2) $P=11_{(10)}$; $a=17_{(10)}$.

Представимо числа a і доповнюючий код P в нормалізованій формі:

$[a]=0{,}10001_{(2)}$.

Структура виконання операції у пристрої має наступний вигляд:

$$\begin{array}{l} [a] = 0{,}10001 \\ + \\ [P_д] = 1{,}10101 \\ \hline [a] + [P_д] = 0{,}00110 \end{array}$$

Нуль у знаковому розряді S_k вказує, що $a>P$, при цьому на виходах пристрою 2 формується код результату підсумовування $b=(a+P_д) \bmod P$.

У результаті запропонованого рішення підвищення швидкодії пристрою досягається за рахунок додаткового введених у суматори інверсних входів та виходів переносу. Це дозволило виконати наскрізні переноси між розрядами пристрою за 1 мікротакт переключення логічного елемента, що в порівнянні з прототипом [1], дозволяє підвищити швидкодію роботи пристрою у 2 рази, що особливо важливо при опрацюванні багаторозрядних чисел більше 1024 розрядів, які використовуються у асиметричній криптографії.

Розширення функціональних можливостей у пристрої досягається за рахунок підвищення рівня захисту, який досягається відсутністю вхідної шини задання коду багаторозрядного модуля P у діапазоні чисел 2^{1024} та апаратною реалізацією кристалів для виконання криптографічних операцій між двома аутентифікованими абонентами.

Зменшення апаратної складності запропонованого рішення полягає в тому, що кожний спеціалізований суматор для нульового і одиничного біт доповнюючого коду модуля $P_д$ у порівнянні з схемою прототипу містить 5 логічних елементи, а прототип - 6 логічних елементи [1], але схема прототипу має 2 елементи XOR, кожний з яких містить 4-5 логічних елементи [2], тобто зменшення апаратної складності, яке визначається, згідно з відношенням

$$K = \frac{A_1}{A_2},$$

де A_1 - апаратна складність прототипу, $A_1 = 12$ або $A_1 = 14$;

A_2 - апаратна складність запропонованого пристрою, $A_2=5$.

Тобто зменшення апаратної складності складає $K = \frac{12-14}{5} = 2{,}4 - 2{,}8$ рази.

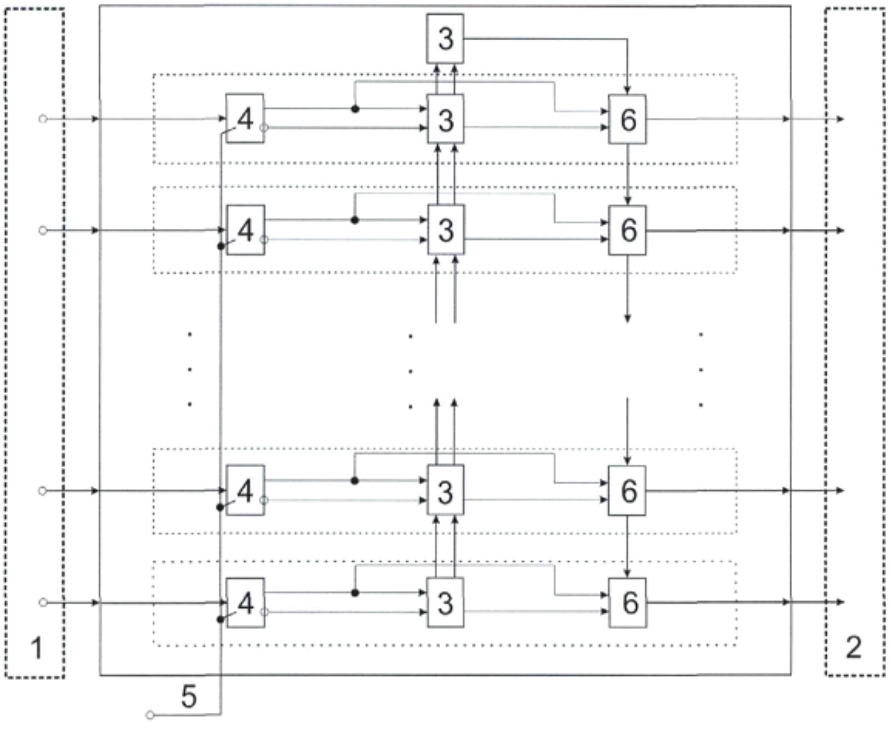
Джерела інформації:

1. Угрюмов Е.П. Цифровая схемотехника: Учеб. пособие для вузов. - 2-е изд., перераб. И доп. / Е.П. Угрюмов - СПб.: БХВ-Петербург, 2004. - С. 117, рис. 2,26 - Схема одноразрядного сумматора из библиотеки схемных решений для СБИС фирмы Altera.

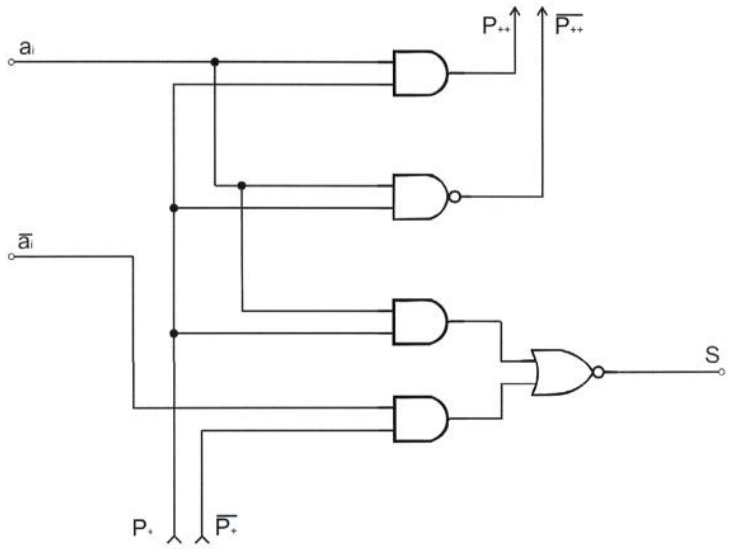
2. Deriving the XOR Function [Електронний ресурс] // Режим доступу: http://www.play-hookey.com/digital/combinational/xor_function.html.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

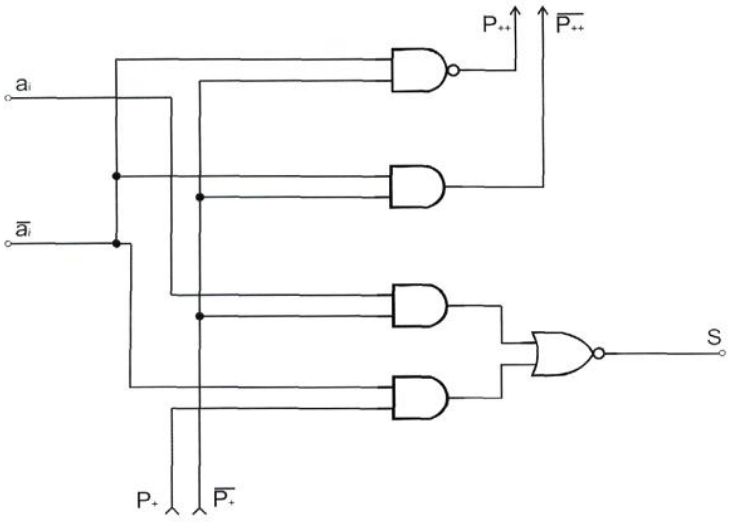
Пристрій визначення залишку по модулю багаторозрядного числа, який містить вхідну і вихідну шини, які є відповідно n-розрядними входами і n-розрядними виходами пристрою, в кожному розряді пристрою міститься однорозрядний суматор, прямий вхід переносу якого підключений до прямого виходу переносу суматора молодшого розряду пристрою, а прямий вихід переносу підключений до прямого входу переносу суматора старшого розряду пристрою, який **відрізняється** тим, що з метою розширення функціональних можливостей, підвищення швидкодії та зменшення апаратної складності, кожний і-тий розряд пристрою додатково містить відповідний спеціалізований однорозрядний суматор відповідно до і-того біта доповнюючого коду модуля $P_д$, в кожному розряді пристрою міститься D-тригер, D-вхід якого з'єднаний з відповідним розрядом вхідної шини, входи синхронізації об'єднані між собою і є другим входом пристрою, прямий вихід тригера з'єднаний з першим входом спеціалізованого однорозрядного суматора та першим входом мультиплексора, інверсний вихід тригера підключений до другого входу спеціалізованого однорозрядного суматора, вихід суми спеціалізованого однорозрядного суматора підключений до другого входу мультиплексора, а додатково введений інверсний вихід переносу спеціалізованого однорозрядного суматора підключений до додатково введеного інверсного входу переносу суматора старшого розряду пристрою, вихід суми найстаршого знакового розряду пристрою S_k з'єднаний з третіми входами мультиплексорів всіх розрядів, виходи яких підключені до відповідних виходів пристрою.



Фіг. 1



Фіг. 2



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