



УКРАЇНА

(19) UA (11) 60391 (13) U  
(51) МПК  
G06F 7/38 (2006.01)МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІОПИС  
ДО ПАТЕНТУ  
НА КОРИСНУ МОДЕЛЬвидається під  
відповідальність  
власника  
патенту

## (54) АРИФМЕТИЧНИЙ ПРИСТРІЙ

1

2

(21) u201006810

(22) 02.06.2010

(24) 25.06.2011

(46) 25.06.2011, Бюл.№ 12, 2011 р.

(72) ЖУКОВ ІГОР АНАТОЛІЙОВИЧ, КРАСОВСЬКА  
ЄВГЕНІЯ ВІКТОРІВНА, СИНЕЛЬНИКОВ ОЛЕКСІЙ  
ОЛЕКСІЙОВИЧ

(73) НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

(57) Арифметичний пристрій, який містить елемент АБО на два входи, два блоки дешифрування переносів, два блоки формування початкових чисел, три блоки комутації, блок порозрядної арифметики, блок зсуву, блок формування переносів, блок елементів АБО, блок шифрування переносів, блок формування результату, який відрізняється тим, що в нього введено два блоки розпізнавання початкових чисел.

Корисна модель належить до галузі обчислювальної техніки і може бути використана в обчислювальних пристроях, які працюють в системах числення з великою основою та арифметичних пристроях швидкодіючих спеціалізованих машинах, зокрема, у пристроях вводу інформації з функціями криптографічного перетворення інформації.

Відомий пристрій, що містить послідовно підключені модулі аналога цифрового перетворення, генератора ключів поліномів ті синтезатору сигналів на основі генератора синусоїдальних імпульсів, причому аналогово-цифровий перетворювач виконує вибір системи числення на основі числа бітових помилок в калібровочному сигналі [1].

Такі пристрої мають затримки статистичного аналізатора тренувального сигналу, оскільки при переключенні режимів роботи з'являється пакет даних з великою кількістю помилок, тобто в режимі реального часу потрібні великі апаратні витрати в цілому та на реалізацію схем контролю і схем видачі результату.

Найбільш близьким до пропонованого по технічній суті є [2] пристрій, що містить суматор по модулю, який містить матриці елементів І та групи елементів АБО, причому виходи елементів І, що формують одну і ту саму функцію, об'єднані в одну вихідну шину матриці.

Недоліком даного пристрою є обмеженість функціональних можливостей, оскільки вона виконує тільки одну логічну операцію додавання двох чисел по модулю в режимі реального часу.

Задачею корисної моделі є удосконалення арифметичного пристрою шляхом введення двох блоків розпізнавання початкових чисел та вдоско-

налення функції криптографічного перетворення інформації що передається.

Це дозволяє забезпечити підвищення достовірності зберігання та обробки інформації та скорочення ступіней у ланцюгу обробки інформації.

Поставлена задача вирішується тим, що в арифметичному пристрої, який містить елемент АБО на два входи, два блоки дешифрування переносів, два блока формування початкових чисел, три блока комутації, блок порозрядної арифметики, блок зсуву, блок формування переносів, блок елементів АБО, блок шифрування переносів, блок формування результату, а також, згідно з винаходом, введено два блоки розпізнавання початкових чисел.

Видалення комутатора, введення двох блоків розпізнавання початкових чисел та вдосконалення криптографічного перетворення інформації що передається вигідно відрізняє запропонований арифметичний пристрій від прототипу, оскільки виключає виникнення помилкових комбінацій при обробці інформації та її передаванні. В результаті зменшується кількість ступіней у ланцюгу обробки інформації, і як наслідок, підвищується достовірність тривалого зберігання та обробки інформації.

На кресленні 1 зображена блок-схема арифметичного пристрою.

Арифметичний пристрій який містить два блоки розпізнавання початкових чисел - 1, 2, елемент АБО на два входи - 3, два блоки дешифрування переносів - 4, 5, два блока формування початкових чисел - 6, 7, три блока комутації - 8, 9, 10, блок порозрядної арифметики - 11, блок зсуву - 12, блок формування переносів - 13, блок елементів

(19) UA (11) 60391 (13) U

АБО - 14, блок шифрування переносів - 15, блок формування результату - 16.

Перші групи входів блоків розпізнавання початкових чисел 1 та 2 з'єднані з першою групою входів блоку формування результату 16, а другі групи входів блоків розпізнавання початкових чисел 1 та 2 містять початкові дані обчислень. Перша група виходів блоків розпізнавання початкових чисел 1 та 2 з'єднані відповідно з першими групами входів блоків дешифрування переносів 4 та 5 виходи яких з'єднані з другими групами входів блоків формування початкових чисел - 6 та 7. Другі групи виходів блоків розпізнавання початкових чисел 1 та 2 з'єднані відповідно з третіми групами входів блоків формування початкових чисел - 6 та 7. Перша і друга групи входів елементу АБО 3 з'єднані з першими групами входів блоків комутації - 8, 9 та 10, а виходи елементу АБО 3 з'єднані з першими входами блоків формування початкових чисел - 6 та 7 виходи яких з'єднані з другими групами входів блоків комутації - 8, 9 та 10. Виходи блоків комутації 8 та 9 з'єднані з першою та другою групою входів блоку порозрядної арифметики 11, а виходи блоку комутації 10 з'єднані з входами блоку зсуву 12. Перша група виходів блоку 11 з'єднана з першою групою входів блоку формування переносу 13, а друга група виходів блоку 11 з'єднана з першою групою входів блоку елементів АБО 14, причому перша група виходів блоку зсуву 12 з'єднана з другою групою входів блоку 13, а друга група виходів блоку 12 з'єднана з другою групою входів блоку 14. Виходи блоку формування переносів 13 з'єднані з входами блоку формування переносів 15, виходи якого з'єднані з другою групою блоку формування результату 16, а виходи блоку елементів АБО 14 з'єднані з третьою групою входів блоку формування результату 16.

Блоки 1 та 2 представляють собою комбінаційні схеми, кожна з яких включає в себе  $n_p+1$  блоків та п'ять  $n_p$  блоків, де  $n_p$  - розрядність числа, представленого в системі числення з основою  $p$ . При цьому блоки 1 та 2 містять відповідно по  $p/2$  та  $p$  двовходових елементів  $I$  кожний. Блок 3 представляє собою двовходовий елемент АБО,  $I$ . Блоки 4 і 5 - комбінаційні схеми. Блоки 6 та 7 містять по групі матриць, кожна з яких має три входи та містить групу двовходових елементів  $I$ . Блоки 8-10 представляють собою комутатори, кожний з яких призначений для передачі чотирьох розрядного шістнадцятиричного числа і містить 64 двовходових елементів  $I$ . Блоки 11-14 ідентичні блокам 1-4, але застосовуються в системі числення з основою  $p=4$ . Блок 15 містить двадцять чотири двовходових елементів та представляють собою дворівневу комбінаційну схему. Блок 16 містить п'ять блоків  $n_p+1$  та п'ять блоків  $n_p$ .

Арифметичний пристрій працює в такий спосіб.

При виконанні операції додавання початкові числа в закодованому вигляді надходять на другу групу входів блоків 1 та 2. Одночасно з ними на перші групи входів блоків 1 та 2 надходить ключ - сигнал  $VI$ . При цьому для представлення кожної з цифр початкових чисел та ключа використовується позиційне представлення інформації. Напри-

клад, наявність цифри 2 або цифри 1 на входах блоків 4 або 5 передбачає наявність цифрового сигналу на вході, номер якого співпадає з номером цифри яка представляється (тобто на вхідних групах входів). Наявність цифрового сигналу  $VI$  на одній з вхідних груп з номерами 1,...,5 першої групи входів блоку 1 та блоку 2 визначає вибір строки блоків 4 та 5, які відповідають дійсному значенню початкового числа. Інформація, яка відповідає сумі по модулю в кожному розряді початкового числа, надходить на другу групу виходів блоку 1 та 2, а цифра яка відповідає інформації про переноси, що підлягають розповсюдженню в відповідних розрядах початкового числа на третю групу входів блоку 6 та 7. З першої групи виходів блоків 1 та 2 цифра, яка відповідає інформації про переноси в значеннях першого та другого початкових чисел, надходять на перші входи першого та другого дешифраторів переносів блок 4 та 5 відповідно. Одночасно на першу групу входів блоку 3 надходить керуючий сигнал  $u_2$ , який визначає проходження інформації через блоки 6 та 7, на входах яких формуються дійсні значення відповідно першого та другого початкових чисел. При цьому на першу групу входів блоків 6 та 7 надходить керуючий сигнал  $u_2$  з виходів блоку 3, на другу групу входів - значення переносів у відповідні розряди початкового числа, що передається, а також на третю групу входів значення порозрядних сум кожного із розрядів початкового числа. На першу групу входів блоків 8 та 9 керуючий сигнал  $u_2$  надходить від входу пристрою. На другу групу входів блоків 8 та 9 значення першого і другого початкових чисел надходять з виходів відповідно блоків 6 та 7. З виходів блоків 8 та 9 значення першого та другого початкових чисел надходять на першу та другу групу входів блоку 11. З першої та другої групи виходів блоку 11 значення порозрядних переносів у сусідній старший розряд та сум по модулю  $p$  (наприклад,  $p=16$ ) надходять на другу та першу групу входів відповідно блоків 13 та 14. З виходів блоку 13 значення переносів у сусідні старші розряди надходять на вхід блоку 15, в якому досягається їх заміна відповідним кодом (наприклад,  $p=16$ ). З виходів блоку 14 значення порозрядних сум результату додавання надходять на третю групу входів блоку 16, на другу групу входів якого надходять значення переносів в найближчі до розглядуваних старші розряди. При цьому інформація про перенос закодована  $p$ -ічною (16-річною) цифрою. На першу групу входів блоку 16 значення "ключа" (сигнал  $VI$ ) надходить від входу пристрою. На виході блоку 16 з'являється число, одна з цифр якого відповідає значенню переносів в найближчі до розглядуваних старші розряди, отримані в результаті додавання аргументів. При цьому місце розташування закодованого значення переносів визначається "ключем"  $VI$ . При виконанні операції зсуву  $p$ -ічного числа на один еквівалентний двійковий розряд вправо початкове число поступає на вхід пристрою, і відповідно на другу групу входів блоку 2. Одночасно з ним від входу пристрою на першу групу входів блоку 2 надходить "ключ" -  $VI$ . З першої групи виходів блоку 2 на вхід блоку 5 в цьому випадку надходить інформація про переноси, які потребують

обліку в початковому числі. Одночасно на другу групу входів блоку 3 надходить керуючий сигнал  $u_3$ , який визначає проходження вхідної інформації через блок 7, на виході якого формується дійсне значення початкового числа. При цьому на першу групу входів блоку 7 надходить керуючий сигнал з виходу блоку 3, а на другу групу входів - значення переносів у відповідні розряди початкового числа, що передається, а на третю групу входів - значення порозрядних добутків кожного із розрядів початкового числа. На першу групу входів блоку 10 керуючий сигнал  $u_3$  надходить від входу пристрою. На другу групу входів блоку 10 значення початкового числа надходить з виходу блоку 7. З виходу блоку 10 значення початкового числа надходить на вхід блоку 12, з першого блоку виходу якого на третю групу входів блоку 13 надходять сигнали переносу нулів з відповідними порядковими номерами 1, 2, 3, 4. Одночасно з другої групи виходів блоку 12 значення результату зсуву в кожному розряді надходять на другу групу входів блоку 14. З виходів блоку 13 значення переносів нулів у сусідні старші розряди надходять на вхід блоку 15, в якому досягається їх заміна відповідним кодом (наприклад,  $r=16$ ). З виходів блоку 14 результат зсуву на один еквівалентний двійковий розряд

вправо надходить на третю групу входів блоку 16, на другу групу входів якого надходить з виходів блоку 15 інформація про перенос нулів в найближчі старші розряди, що розглядаються, яка закодована  $r$ -ічною цифрою.

На першу групу входів блоку 16 значення "ключа" (сигнал VI) надходить з входу пристрою, а на виході блоку 16 формується число, одна з цифр якого з'являється число, одна з цифр якого відповідає значенням переносів в найближчі старші розряди, що розглядаються. Місце розташування закодованого значення переносів визначається кодом "ключа" VI.

Таким чином, введення двох блоків розпізнавання початкових чисел дозволяє розширити функціональні можливості запропонованого арифметичного пристрою за рахунок вдосконалення функції криптографічного перетворення інформації та дозволяє вирішити проблему автоматичного контролю в швидкодіючих спеціалізованих машинах.

Джерела інформації:

1. Патент Російської Федерації №2385539, кл. H04L 12/00, 2008.
2. Патент Російської Федерації №2047896, кл. G06F 7/49, 1995.

