УДК 681.32

МЕТОД ПОБУДОВИ БАГАТОРОЗРЯДНОГО ОПЕРАЦІЙНОГО ПРИСТРОЮ ПІДНЕСЕННЯ ЧИСЕЛ ДО КВАДРАТУ

Давлетова А.Я.
Тернопільський національний економічний університет, студент

I. Постановка проблеми

Принципове значення для подальшого розвитку цифрової обчислювальної техніки має задача вдосконалення, підвищення швидкодії, регулярності структури та розширення функціональних можливостей засобів обчислювальної техніки та розробки високопродуктивних компонентів проблемно-орієнтованих спецпроцесорів у різних теоретико-числових базисах. Актуальною науковою проблемою є створення високопродуктивних багаторозрядних спецпроцесорів, які виконують функції шифрування, дешифрування даних в комп'ютерних мережах. Важливим компонентом при цьому є багаторозрядний операційний пристрій піднесення чисел до квадрату.

II. Метод побудови пристроїв піднесення до квадрату у різних теоретико-числових базисах

Аналіз класики реалізації компонентів проблемно орієнтованих спецпроцесорів показує, що вони характеризуються рядом функціональних обмежень, оскільки були орієнтовані на побудову процесорів невеликої розрядності (до 32 біт). Відомі методи реалізації прискорювачів операцій сумування та множення характеризуються значним зростанням апаратної складності та нерегулярності структури при зростанні розрядності процесорів (1024, 2048….біт) [1].

На рис.1 наведена структура квадратора, який містить регістр-лічильник (1), елемент затримки (2), ключі (3), накоплювач (4) та вхідну шину (5) [2].

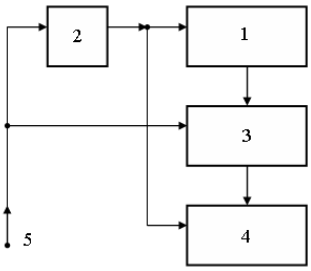

Рисунок 1 – Структурна схема квадратора

Вхідна шина квадратора з'єднана з входом ключів та входом елемента затримки, вихід якого підключений до входу накоплювача та входу лічильника-регістра, інформаційні виходи яких через ключі з'єднані з відповідними входами накоплювача із зсувом на один розряд.

Недоліком такого квадратора є низька швидкодія, яка обумовлена наявністю елемента затримки, що потребує двохразового виконання операції додавання n-розрядних двійкових кодів теоретико-числового базису Радемахера у 2n-розрядному накоплювачі з наскрізними переносами та двохразового запису кодів суми у регістрі пам'яті накоплювача.

Для множення чисел, представлених унітарним кодом у пристроях статистичної обробки інформації, цифрових взаємокореляторах та засобах паралельного розпізнавання образів використовують число-імпульсний множильний пристрій (ЧМП) [3], який містить вхідну шину, лічильник виходи якого порозрядно, через логічні ключі, підключені до накоплювача.

Недоліком такого пристрою, який при однаковому числі імпульсів на вхідних шинах, виконує обчислення їх квадрату, є низька швидкодія та висока структурна складність. Згідно структури ЧМП його часова складність та швидкодія, яка визначається сумарною затримкою сигналів після кожного вхідного імпульсу у послідовно з'єднаних компонентах пристрою визначається згідно виразу:

$$\tau_н = (\tau_л + \tau_к + \tau_р + \tau_с),$$

де $\tau_л = 2\upsilon$ - швидкодія переключення JK-тригера синхронного двійкового лічильника; $\tau_к = 2\upsilon$ - швидкодія переключення логічних елементів логічних ключів, які складаються з двох послідовно включених логічних елементів «І», «АБО»; $\tau_р = 2n \cdot \tau_с$, - швидкодія переключення D-тригера регістра накоплюючого суматора, де n – число розрядів лічильника, в якому формується двійковий

код вхідного унітарного коду з числом 2^n імпульсів; $\tau_к = (2 \div 4)\upsilon$ - часова затримка сигналів накоплюючого багаторозрядного суматора у залежності від схеми його мікроелектронної реалізації на вентилях ПЛІС (υ - швидкодія переключення вентиля).

Вдосконалення операційного пристрою піднесення чисел до квадрату можливе шляхом представлення вхідного числа імпульсів у модульному коді Хаара – Крестенсона та вилучення з його структури компоненту з найнижчою швидкодією – накоплювача та найвищою структурною складністю – двійкового суматора, з наскрізними переносами. Реалізація лічильника та накоплюючого суматора виконується на D-тригерах, а логічний ключ містить тільки логічний елемент «АБО».

На рис.2 наведена структурна схема пристрою піднесення чисел до квадрату, де 1 – вхідна шина; 2 – модульний лічильник системи числення залишкових класів теоретико-числового базису Хаара - Крестенсона; 3 – логічний модуль рандомізації; 4 – перша вихідна шина; 5 – регістр пам'яті; 6 – дешифратор; 7 – друга вихідна шина.

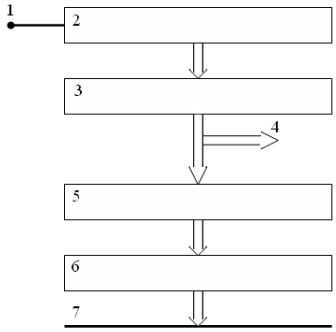

Рисунок 2 - Структурна схема пристрою піднесення чисел до квадрату

При проектуванні пристрою піднесення чисел до квадрату на ПЛІС використовується логічний модуль з повним числом логічних елементів «АБО», які синтезуються в якості відповідних утилітів по кожному модулю P_i.

Згідно системи числення залишкових класів для однозначного представлення вхідного числа імпульсів унітарного коду 2^n повинна виконуватися умова: добуток взємнопростих модулів P_i повинен бути рівний або більший 2^n, що відповідає умові: сума двійкових розрядностей модулів P_i повинна бути на 1-2 розряди більша по відношенню до розрядності двійкового числа, яке підноситься до квадрату і представляє число імпульсів унітарного коду N у двійковій системі числення, де $n = E[\log_2 N]$, є знак цілочисельної функції з округленням до більшого цілого.

При числі модулів системи залишкових класів k можуть застосовуватися набори взаємопростих модулів k, які відповідають вказаним умовам. При піднесенні до квадрату 512 розрядних двійкових чисел потрібно 101 десятибітний модуль P_i. При цьому швидкодія піднесення чисел до квадрату у базисі Хаара - Крестенсона не залежить від розрядності і в запропонованому пристрої виконується $\tau = 3\upsilon$.

Висновок

Проведені дослідження показали, що від реалізації операційного пристрою піднесення до квадрату, його апаратної, часової та структурної складності залежать системні характеристики та швидкодія спецпроцесора шифрування даних і відповідно можливість передавання великих масивів інформаційних потоків в комп'ютерних мережах на швидкості 10, 100 і більше Мб/с. Запропонований пристрій характеризується підвищеною на 1-2 порядки швидкодією по відношенню до відомих, а також більш високою регулярністю структури за рахунок реалізації модульних синхронних лічильників на D-тригерах та логічного модуля рандомізації на елементах «АБО».

Список використаних джерел

1. Албанський І.Б. Дослідження системних характеристик цифрових пристроїв множення реалізованих в різних теоретико-числових базисах / І.Б. Албанський, О.І. Волинський / Вісник Хмельницького національного університету. -№2.- 2012.- с. 179-186.
2. Грибок Н.И., Обуханич Р.-А.В. Квадратор // А.С. СССР № 475619.-Бюллетень № 24.-1975
3. Николайчук Я.М. Числоимпульсное множительное устройство // А.С. СССР № 754414.- Бюллетень № 29.- 1980.