НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
“ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА”

РОГОВЕНКО АНДРІЙ ІВАНОВИЧ

УДК 004.415.3:004.7(043)

Методи та інформаційна технологія прискореного обчислення великих даних для систем розподіленої обробки інформації

05.13.06 – інформаційні технології

Автореферат
дисертації на здобуття наукового ступеня кандидата технічних наук

Чернігів – 2021

Дисертацією є рукопис

Робота виконана в Національному університеті “Чернігівська політехніка”

Науковий керівник доктор технічних наук, доцент
Зайцев Сергій Васильович,
Національний університет «Чернігівська політехніка» Міністерства освіти і науки України, професор кафедри інформаційних та комп’ютерних систем

Офіційні опоненти: доктор технічних наук, професор
Литвинов Валерій Андроникович
Інститут проблем математичних машин і систем Національної академії наук України, провідний науковий співробітник відділу інтелектуальних інформаційно-аналітичних систем

доктор технічних наук, доцент
Семко Віктор Володимирович,
Національний авіаційний університет, професор кафедри комп’ютеризованих систем управління;

Захист відбудеться "16" грудня 2021 р. о 13 год. 00 хв. на засіданні спеціалізованої вченої ради К 79.051.03 в Національному університеті “Чернігівська політехніка” (14035, м. Чернігів, вул. Шевченка, 95, ауд. 319).

З дисертацією можна ознайомитися у бібліотеці Національного університету “Чернігівська політехніка” (14035, вул. Шевченка, 95, м. Чернігів, Україна).

Автореферат розісланий "11" листопада 2021 р.

Вчений секретар
спеціалізованої вченої ради,
кандидат технічних наук  В.П. Войтенко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Швидке зростання обсягу цифрових даних, що виробляються й оброблюються у сучасних розподілених системах обробки інформації, вимагає створення відповідної інфраструктури для їх передачі та зберігання. При цьому постійно посилюються вимоги щодо швидкості обміну даними, безпеки, енергетичної та спектральної ефективності, вартості обладнання та т.п. Прикладами задач, для яких постають питання прискорення обчислень, є використання графічних та лінгвістичних процесорів, перетворення Фур'э в спектральному аналізі сигналів, методи біоінформатики та генетичні алгоритми. Особлива потреба в прискорювачах виникає в криптографічних системах та системах завадостійкого кодування, де суттєву частину усіх обчислювальних перетворень над великими даними становлять операції в полях Галуа. Але не зважаючи на довгу історію розвитку обчислювальної техніки, обчислювальні ядра для виконання зазначених операцій і методи прискорення їх роботи, які б задовольняли вимогам до перспективних технічних систем, потребують додаткового опрацювання.

Існуючі розробки у галузі методів прискорення обчислення великих даних в основному запропоновані у математичних аспектах, а роботи присвячені впровадженню цих методів в розподілені обчислювальні системи мають ряд недоліків, наприклад, таких як: недостатня швидкодія в рамках задачі що вирішується, обмеженість у виборі значень операндів, велика надлишковість обчислювальних ресурсів, різке зростання обчислювальної складності при збільшенні розрядності операндів. Все це призводить до того, що швидкість обробки інформації у системах виявляється незадовільною, а високе енергоспоживання апаратури, залежне в значній мірі від складності використовуваних алгоритмів, істотно обмежує час автономної роботи елементів системи. Усунути ці недоліки можна декількома шляхами: використовувати нові ефективніші методи та алгоритми обробки даних, або розробити та впровадити методи прискорення виконання базових операцій над великими даними в уже існуючих методах.

Теоретичним підґрунтям для досліджень, що виконані в дисертаційній роботі, є роботи зарубіжних та вітчизняних вчених, таких як Л. М. Фінк, Л. Є. Варакін, В. Л. Банкет, Ф. Дж. Мак-Вільямс, К. Берроу, Л. Хензо, А. Голдсмит, М. Валенті, Б. Шнайєр, Н. Кобліц, Р. Крендалл, К. Померанс, А. Менезес, В.П. Тарасенко, О.В. Палагін, В.М. Опанасенко, А.О. Мельник, В.С. Харченко, Н.С. Щербаков, Г.Ф. Кривуля, В.Г. Рябцев, В.І. Хаханов, М.В. Синьков.

Аналіз наукових досліджень, що базуються на використанні арифметики полів Галуа показав, що ефективність цих методів суттєво знижується при збільшенні розрядності оброблюваних даних, а основною проблемою їх використання, особливо коли модуль є простим числом, а операції виконуються над багаторозрядними числами, є відсутність добре опрацьованої елементної бази. Це стосується, перш за все, ефективних структурних рішень та методів прискорення основних обчислювальних операцій, таких, які б враховували сучасний розвиток технологій й методології проєктування шляхом використання існуючих

спеціалізованих обчислювальних ядер. В то й же час, недостатня продуктивність виконання базових операцій, що застосовуються в існуючих методах та системах розподіленої обробки великих даних, змушує розробників застосовувати субоптимальні, з точки зору надлишковості, рішення.

У зв'язку з цим науково-прикладна задача, яка полягає у прискоренні обчислень великих даних в системах розподіленої обробки інформації за рахунок розробки методів прискорення виконання базових операцій з урахуванням особливостей і властивостей сучасних обчислювальних платформ, є актуальною.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційна робота виконувалась відповідно до планів науково-дослідних робіт Міністерства освіти і науки України і Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» у рамках держбюджетної теми № 2944-П «Розробка методів та засобів забезпечення інформаційної стійкості в дистанційних освітніх технологіях» (державний реєстраційний номер 0106U002270). А також, відповідно до планів науково-дослідних робіт Національного університету «Чернігівська політехніка» у рамках науково-дослідної роботи «Інформаційна технологія забезпечення сталої достовірності інформації в мережах Інтернету речей». (державний реєстраційний номер 0118U006996)

У наведених роботах автором розроблено метод одновимірного каскаду зменшення апаратних витрат реалізації процедури кодування/декодування кодів та метод прискорення обчисленнь операцій за модулем для чисел великої розрядності. Основні результати дисертації було викладено в окремих розділах заключних звітів указаних науково-дослідних робіт.

Мета і задачі дослідження. Метою роботи є підвищення ефективності обчислювальних платформ з адаптованою архітектурою за рахунок розробки удосконалених методів реалізації операцій за змінним простим модулем над числами великої розрядності в умовах високошвидкісного потоку великих даних.

Для досягнення вказаної мети необхідно вирішити такі задачі:

1. Проаналізувати основні методи виконання найбільш вживаних обчислювально витратних операцій у обчисльовальному процесі в системах розподіленої обробки інформації. Провести дослідження та сформувати напрямки розвитку та вдосконалення зазначених методів.
2. Удосконалити метод одновимірного каскаду реалізації процедури обчислення базових операцій, який би забезпечив зменшення обчислювальної складності виконання операцій.
3. Розробити моделі обчислювальних структур для виконання операцій за змінним простим модулем над числами великої розрядності на прикладі процесів кодування/декодування завадостійких кодів.
4. Адаптувати алгоритм обчислення операції множення та піднесення до степеню за модулем з урахуванням особливостей їх побудови методом одновимірного каскаду з метою зменшення часу обчислення.
5. Розробити інформаційну технологію прискореного обчислення великих даних для систем розподіленої обробки інформації, яка буде базуватися на запропонованому методі зменшення обчислювальної складності.

Об'єкт дослідження –процеси обчислень в реконфігуровній системі на базі програмованих логічних інтегральних середовищ, зокрема, процеси та структури обчислення операцій за модулем.

Предмет дослідження – моделі та методи підвищення ефективності цифрових обчислювальних засобів, способи зменшення апаратних витрат на рівні структурно-схемотехнічної реалізації.

Методи дослідження. Для вирішення поставленої науково-прикладної задачі були використані методи дискретної математики, теорії кодування, теорії графів, теорії інформації під час удосконалення методу зменшення апаратних витрат реалізації процедури кодування/декодування кодів; теорії обчислювальної складності алгоритмів, теорії скінченних алгебраїчних структур та схемотехнічного проєктування при розвитку методу обчислення операцій за модулем для чисел великої розрядності; методи комп'ютерного імітаційного моделювання, об'єктно-орієнтованого програмування, теорії ймовірності, математичної статистики при створенні моделі обчислювальних структур завадостійких кодів для виконання операцій за змінним простим модулем над числами великої розрядності.

Наукова новизна отриманих результатів.

1. Удосконалено метод одновимірного каскаду реалізації процедури обчислення базових операцій, який, на відміну від існуючих, використовує конструктивні модулі з наскрізним переносом та регулярною або нерегулярною структурою та забезпечує зменшення ємкостних витрат при обробці великих даних.

2. Набув подальшого розвитку метод обчисленнь операцій за модулем для чисел великої розрядності, який, на відміну від існуючих, використовує ланцюги групового та частково-групового переносу та забезпечує прискорення базових операцій.

3. Вперше розроблено модель обчислювальних структур завадостійких кодів, яка, на відміну від існуючих, дозволяє комбінувати обчислювальні ядра для виконання однотипних арифметичних інструкцій за змінним простим модулем над числами великої розрядності.

4. Вперше розроблена інформаційна технологія обчислення великих даних, яка, на відміну від існуючих, базується на запропонованому методі обчислень за модулем та забезпечує прискорення виконання обчислювальних процедур.

Практичне значення отриманих результатів роботи полягає у розробці способів організації обчислювальних структур з адаптованою логікою та організації обчислень операцій за змінним модулем шляхом використання таблиць перетворення, бібліотеки моделей на мові VHDL та програмної реалізації співпроцесора складних обчислень. Запропоновані способи забезпечують практичну реалізацію розробленої інформаційної технології прискореного обчислення великих даних, яка дозволяє зменшити час обчислень по відношенню до існуючих аналогів.

Результат роботи, зокрема, метод, що забезпечує прискорення базових операцій, був апробований та впроваджений для підвищення продуктивності спеціалізованих апаратних обчислювачів у дослідно-конструкторських роботах державного підприємства науково-дослідного інституту радіолокаційних систем «Квант-радіолокація». Удосконалений метод одновимірного каскаду та метод прискорення базових операцій був апробований та впроваджений при проєктуванні

та модернізації телеметричної апаратури супутникових систем на ПРАТ «ЧЕЗАРА». Основні положення, що стосуються методів прискореного обчислення великих даних для систем на основі сучасних серій ПЛІС, використовуються на кафедрі інформаційних та комп'ютерних систем Національного університету «Чернігівська політехніка» при викладанні дисципліни "Технології проєктування комп'ютерних систем". Усі впровадження підтверджуються відповідними актами та довідками.

Особистий внесок здобувача. Основні ідеї дисертації та отримані результати, як теоретичні, так і практичні (у тому числі конкретні реалізації цих результатів у вигляді програмних продуктів), належать особисто здобувачеві. Зі спільних публікацій особисто здобувачеві належить наступне: в [1] – моделювання та практичне порівняння моделей побудованих з використанням типового та запропонованого методу прискорення обчислень великих даних; в [2] – порівняння запропонованого удосконаленого методу прискорення обчислень операцій за змінним модулем з базовим; в [3] – варіант організації частково - групового переносу; в [5] – реалізація та аналіз роботи суматорів за змінним модулем; в [6] – структура регулярного одномірного каскаду конструктивних модулів; в [8] – реалізація та експериментальне дослідження методу групового перенесення; в [9] – схема вимірювання продуктивності суматора за змінним модулем, та її реалізація; в [11] – імітаційна модель системи передачі інформації на основі коду Ріда-Соломона; в [15-19] – відображення моделей обчислювальних пристроїв в базис ПЛІС.

Апробація результатів роботи. Основні положення дисертації та її наукові результати доповідалися, обговорювалися і отримали позитивну оцінку на:

- 4-й Міжнародній науково-технічній конференції "Сучасні комп'ютерні системи та мережі: розробка та використання" (м. Львів, 2009 р.);
- 3-й та 4-й Міжнародних науково-технічних конференціях "Гарантоздатні (надійні та безпечні) системи, сервіси та технології" (м.Кіровоград, 2008-2009 рр.)
- Ювілейна міжнародна науково-практичній конференції "Розподілені комп'ютерні системи РКС-2010" (м. Київ, НУТУ «КПІ», 2010р.);
- 7-й Міжнародній науково-практичній конференції "Математичне та імітаційне моделювання систем МОДС2012" (м. Чернігів, м. Жукин, 2012 р.)
- 15-й Міжнародній науково-технічній конференції "Системний аналіз та інформаційні технології. SAIT 2013"(м. Київ 2013 р.);
- 5-й Міжнародній науково-практичній конференції "Вільне програмне забезпечення в освіті, науці та бізнесі" (м. Чернігів 2014);

Публікації. За результатами виконаних досліджень опубліковано 18 наукових робіт, з яких 1 стаття у періодичному науковому виданні Європейського Союзу, 7 статей у наукових фахових виданнях України, 5 публікацій в збірниках тез доповідей науково-практичних конференцій та 5 патентів України на корисну модель.

Структура і обсяг дисертаційної роботи. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та 4 додатків. Загальний обсяг роботи складає 178 сторінок друкованого тексту, у тому числі містить 43 рисунки, 17 таблиць, список використаних джерел, що містить 118 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність напряму дослідження, сформульовано мету, основні завдання дослідження, положення, що визначають наукову новизну та практичну значимість виконаних досліджень, їхній зв’язок із науково-дослідними роботами. Наведено відомості про апробацію і впровадження результатів, публікації автора тощо.

Перший розділ присвячено аналізу задачі прискорення обчислень у сучасних системах розподіленої обробки інформації. Особлива потреба в прискорювачах виникає в криптографічних системах та системах завадостійкого кодування, де суттєву частину усіх обчислювальних перетворень над великими даними становлять операції в полях Галуа.

Проведений аналіз задачі прискорення обчислень у системах розподіленої обробки інформації виявив необхідність зменшення обчислювальної складності реалізації базових операцій, які використовуються у технологіях вирішення задачі виявлення та виправлення помилок у системах розподіленої обробки інформації, зокрема у сучасних системах радіозв’язку.

Проаналізовано коди, що використовуються для коригування помилок у сучасних системах радіозв’язку, та визначені основні напрямки прискорення процесу кодування/декодування при використанні алгебраїчних кодів. На основі аналізу було визначено, що процес кодування/декодування базується на апараті арифметики скінчених полів. Таким чином, спрощення та прискорення виконання операції в полях Галуа має призвести до зменшення обчислювальної складності реалізації процедур кодування/декодування завадостійких кодів.

Проведений аналіз основних методів обчисленнь операцій у полях Галуа, виявив, що більш пріоритетною є задача спрощення та прискорення виконання операцій додавання, як складових операцій множення, підведення до степеню та інших.

На основі аналізу існуючих методів обчислень операцій у полях Галуа було зроблено висновок, що сучасні широко представлені реалізації блоків обчислення операцій в скінчених полях мають обмеження та недоліки, які призводять до зменшення використовуваності алгебраїчних кодів у вирішеннях задачі виявлення та виправлення помилок, зокрема: вони орієнтовані на виконання операцій над малорозрядними числами, а при збільшенні розрядності йде різке збільшення апаратних витрат. Також представлено дуже мало рішень обчислювачів операцій за простим модулем. Отже необхідно розробити методи підвищення продуктивності спеціалізованих обчислювальних засобів із урахуванням особливостей і властивостей апаратної платформи сучасної мікропроцесорної техніки, складності реалізації та швидкодія яких задовольняла б існуючі вимоги та була прогнозованою в залежності від розрядності (розміру) оброблюваних послідовностей.

У другому розділі роботи проводиться дослідження, розробка та удосконалення методів прискорення та зменшення апаратних витрат на реалізацію блоків виконання операцій за модулем, розробка структурних рішень та модифікації алгоритмів виконання операцій за модулем.

Розроблено та запропоновано метод зменшення апаратних витрат суматора за модулем на основі одновимірного каскаду конструктивних модулів з однорідною структурою. Цей метод базується на введенні в схему ланцюгів наскрізного переносу.

Метод реалізується у наступній послідовності:

1. Аналізуються класи еквівалентності, наведені в [4], то вочевидь, що на лівих бокових виходах останнього конструктивного модуля каскаду реалізується функція (1).

$$V_{n-1}(X,Y,P) = \begin{cases} a \ \ if\ X+Y < P \\ b\ if\ 2^n \le X+Y < 2^n + P \\ d\ if\ 2^n + P \le X+Y \end{cases} \quad (1)$$

На правих бокових виходах першого конструктивного модуля каскаду реалізується функція (2).

$$U_0(X,Y,P) = \begin{cases} h \ \ if\ X+Y < P-1 \\ e\ if\ X+Y = P \\ g\ if\ X+Y > P \\ k\ if\ X+Y = P-1 \end{cases} \quad (2)$$

В загальному випадку при будь-яких значеннях *X,Y* та *P,* на первинних виходах модулів одновимірного каскаду конструктивних модулів буде реалізовуватись основна функція.

Обчислення основної функції може виконуватись або з виконанням операції віднімання, або без виконання операції віднімання. Для того, щоб позначити ці два випадки, вводиться додаткова функція SUB, яка дозволить звести обчислення основної функції до виконання декількох логічних операцій. Нехай $SUB_i = 0$, коли віднімання відсутнє, та $SUB_i = 1$, коли віднімання є.

2. Позначаються стани моделі конструктивного модуля відповідно до умов при яких віднімання буде обов'язкове, та умов, коли віднімання буде проводитись в залежності від сигналів позики та переносу сусідніх конструктивних модулів.

Стан 1: $U_i+1 = h$. У цьому випадку віднімання не буде не залежно від значень молодших розрядів.

Стан 2: $U_i+1 = g$. Віднімання буде не залежно від значень молодших розрядів.

Стан 3: $U_i+1 = k$. У даному випадку вірна рівність $X_i+1,n-1+Y_i+1,n-1 = P_i+1,n-1 - 1$. Тобто віднімання можливе, якщо в і-тому модулі буде реалізовано перенесення при додаванні з відніманням, що відповідає класу d (дивись таблицю 1).

Стан 4: $U_i+1 = e$. Відповідно вірною є рівність $X_i+1,n-1+Y_i+1,n-1 = P_i+1,n-1$. В цьому випадку віднімання не можливе, якщо в і-тому модулі буде реалізована позика при додаванні з відніманням, тобто клас a (див. таблицю 1).

Таблиця 1

Визначення функції V_i.

V_{i-1}				v_i				
a	*a*	*b*	*b*	*c*	*a*	*a*	*a*	*c*
b	*b*	*b*	*b*	*d*	*a*	*b*	*b*	*c*
c	*b*	*c*	*c*	*d*	*a*	*c*	*c*	*c*
d	*b*	*d*	*d*	*d*	*b*	*c*	*c*	*d*
x_i	0	1	0	1	0	1	0	1
y_i	0	0	1	1	0	0	1	1
p_i	0	0	0	0	1	1	1	1

3. Визначається основна функція. Відповідно до наведених вище станів відносно необхідності проведення операції віднімання можна визначити функцію SUBi, виходячи з цього обчислення основної функції змінюється і зводиться до обчислення простого логічного виразу (3)

$$W_i = \overline{sub} \cap \left[x_i \oplus y_i \oplus \left((V_{i-1} = c) \cup (V_{i-1} = d)\right)\right] \cup sub \cap \left[x_i \oplus y_i \oplus p_i \oplus \left((V_{i-1} = a) \cup (V_{i-1} = d)\right)\right] \quad (3)$$

Таким чином, раніш запропонована [4] структура моделі конструктивного модуля значно спрощується за рахунок зменшення операцій для обчислення основної функції та спрощення підмодуля, який генерує сигнали переносу.

Для реалізації цього методу зменшення апаратних витрат розроблено та запропоновано для використання структуру моделі комірки суматора за модулем. Ця модель комірки адаптується шляхом внесення змін до її структури з метою зменшення кількості первинних входів та виходів, та забезпеченням можливості будь якого допустимого кодування сигналів перенесення, що має спрощувати реалізацію комірки при орієнтації на сучасні засоби технології програмованих логічних схем та прискорювати процес обчислення цільової функції.

Шляхом зміни внутрішньої структури була досягнута можливість формування сигналу віднімання для обчислення цільової функції на основі обчислень наступної комірки, таким чином, обчислення кінцевої функції проводиться паралельно у двох логічних схемах формування результату, кожна з яких відповідає за формування результату при відніманні або без нього. Тобто, при наявності всіх бокових сигналів, затримка сигналу результату буде визначатися тільки швидкістю перемикання входів у селекторній схемі вибору результату. Виходячи з цього, швидкість роботи суматора буде визначатися часом розповсюдження сигналу перенесення із молодших розрядів, необхідних для обчислення цільової функції. Також, завдяки введенню в структуру комірки, селекторного блоку активування блоків формування кодованих сигналів перенесення, вдалося забезпечити формування активуючого сигналу для блоку формування кодованих сигналів перенесення у старші розряди V, та молодші розряди U паралельно у всіх комірках суматора. Тобто, затримка сигналів перенесення на відміну від прототипу, визначається тільки блоками їх формування.

Таким чином, з блоку обчислення кінцевої функції W були виключені блоки логічного множення, логічний елемент формування сигналу «На один менше», логічний елемент формування сигналу «Дорівнює», логічний елемент формування сигналу «Більше», інверторний елемент, перший та другий суматори за модулем 2. А також зменшено кількість первинних входів та виходів, за рахунок кодування сигналів перенесення. Таким чином, виникла можливість у запропонованій моделі змінювати значення кодів перенесення, що дозволяє заощадити обчислювальні ресурси у реалізації суматора на конкретній серії програмованих логічних схем.

Розроблено та запропоновано удосконалений метод зменшення апаратних витрат реалізвції моделі суматора за модулем на основі одновимірного каскаду конструктивних модулів з нерегулярною структурою.

Сутність вдосконалення полягає в тому, що запропонована на рис 1. структура моделі одновимірного каскаду конструктивних модулів надлишкова, тому що сигнал SUB та сигнали U частково дублюють функції один одного. Виконувати обчислення та генерацію сигналу SUB можна лише в самому крайньому лівому конструктивному модулі, на основі отриманих з інформаційних входів X, Y та P значень, й сигналу ознаки переносу V, відповідно до виразу 3. На основі вищевикладеного було запропоновано включити в метод кроки побудови моделей 2-х типів: з генерацію, та без генерації сигналу SUB.

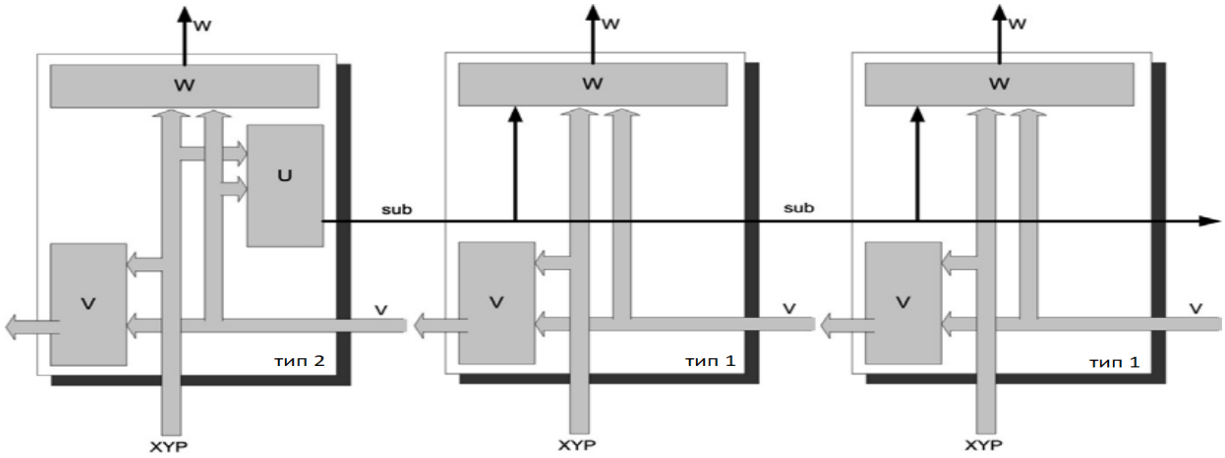

Рис. 1. Функціональна модель суматора за модулем побудована за удосконаленим методом одновимірного каскаду конструктивних модулів

Для реалізації цього методу зменшення апаратних витрат, розроблено та запропоновано для використання функціональну модель комірок суматора за модулем. До першого типу комірок відносяться модулі, які виконують обчислення основної функції, формування сигналів переносу в наступний конструктивний модуль та трансляцію сигналу SUB в попередній конструктивний модуль. Структура модуля цього типу представлена на рис. 1. Модулі цього типу становлять основу ОККМ і через істотне спрощення, за рахунок виключення блоку генерації сигналу ознаки вирахування істотно зменшують апаратні витрати на реалізацію.

До другого типу відносяться конструктивні модулі, що забезпечують генерацію сигналу ознаки вирахування. Модуль, працює за аналогічним алгоритмом що й конструктивний модуль першого типу, робить обчислення основної функції,

але на відміу від нього, не робить трансляцію в КМ старших розрядів сигнал переноса V_i, тому що є замикаючим.

Витрати при реалізації блоку типу 1 – 2 таблиці перетворення за функцією від 6 змінних (LUT – LookUpTable), а для блоку 2 – 3 таблиці перетворення за функцією від 6 змінних, що при великій розрядності суматора за модулем приводить до суттєвого зменшення обчислювальних ресурсів.

Розроблено та запропоновано метод збільшення швидкодії суматора за модулем на основі одновимірного каскаду конструктивних модулів. Сутність удосконалення методу полягає у використанні методів забезпечення швидкого переносу традиційних суматорів, зокрема методу групового переносу [4]. Розглянемо особливості застосування та адаптації цього методу для суматорів за змінним модулем на основі моделі одновимірних конструктивних модулів.

Нехай розряди *n* - розрядного суматора нумеруються числами від 0 до *n-1*. Виберемо довільну групу розрядів із *r*-того по *s*-тий включно. Кількість розрядів, які входять в групу – *k=s-r+1*. З'єднання елементів з частково-груповим переносом ілюструється рис. 2.

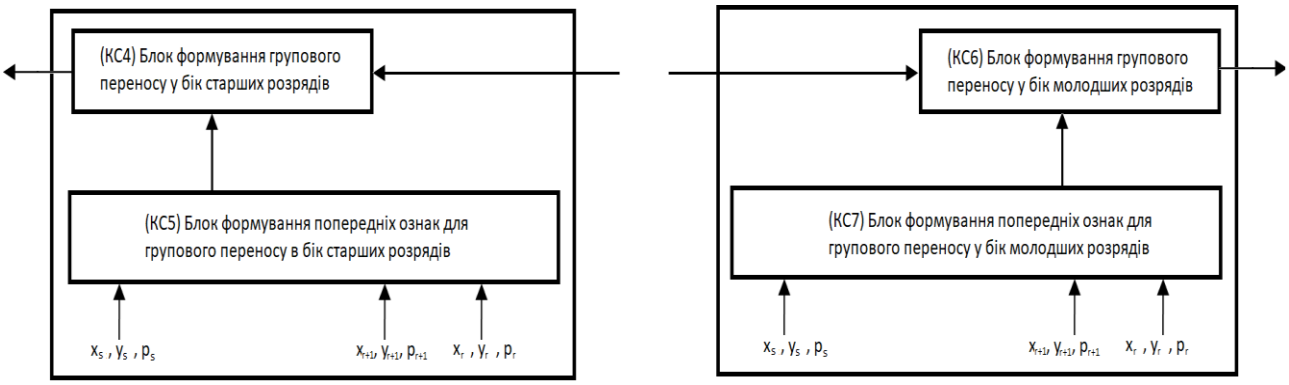

Рис. 2. Структурні елементи функціональної моделі суматора за модулем побудованої за методом одновимірного каскаду конструктивних модулів з груповим переносом

Блоки КС5 та КС7 не залежно від значень інших розрядів, які не входять в групу, формують попередні значення для переносу. КС4 на основі узагальненого переносу із *r-1*- го розряду та попередньо сформованого значення КС5 формує узагальнений перенос в *s+1*-й розряд. КС6 на основі узагальненого переносу із *s+1* – го розряду та попередньо сформованого значення КС7 формує узагальнений перенос в *r-1*-й розряд. Таким чином затримка в формуванні узагальненого переносу в групі визначається не як добуток розрядності на затримку на одній таблиці перетворення, а затримкою в КС4 або КС6. В свою чергу затримка в КС4 та КС6 визначається кількістю рівнів розкладу Шеннона для реалізації цих схем і, відповідно, мінімально можливою кількістю виходів КС5 та КС7.

Затримка сигналів узагальненого переносу через групу дорівнює часу роботи однієї таблиці перетворення t_{LUT} при умові, що затримка відповідного сигналу узагальненого переносу при вході в групу не менша за час для формування сигналу на виході КС 5, який дорівнює $(k-1)t_{LUT}$. Максимальна затримка сигналу узагальненого переносу в середині групи через конструктивний модуль дорівнює *(k-*

1)t_{LUT}. Максимальні витрати, без врахування можливої мінімізації, дорівнюють *(12k-8) LUT.*

Досліджено варіанти реалізації моделей суматорів за змінним модулем із частково-груповим переносом та визначчено нижні оцінки затримок та верхні оцінки витрат.

Варіант 1. Нехай всі блоки групового переносу мають одну і ту ж розрядність *k*. Загальна кількість блоків - *w=n/k*. Вочевидь, що використання двох крайніх блоків групового переносу (для наймолодших та для найстарших розрядів) для формування переносу через группу не має сенсу, оскільки, затримка сигналу в КС 5 та КС 4 співпадає із затримкою сигналу переносу через КМ. Крім того, необхідно враховувати затримку переносу із старших розрядів через КМ в *0*-вий (або із молодших розрядів в *n-1*-й) розряди. Оскільки затримки сигналів узагальненого переносу, як в бік старших розрядів, так і в бік молодших розрядів співпадають, то визначимо затримку переносу у суматорі в цілому на прикладі переносу в бік старших розрядів. Нижня оцінка такої затримки визначається як сума $t_{v1} = T_{low} + T_{gr} + T_{high}$, де $T_{low} = kt_{LUT}$ – затримка переносу в *k* молодших розрядах, $T_{gr}=(w-2)t_{LUT}$ – затримка наскрізного переносу через w-2 груп, $T_{high} = (k-1)t_{LUT}$ затримка переносу в *(n-1)*-й розряд. Або

$$t_{V1} = \left(2k + \frac{n}{k} - 3\right) t_{LUT} \qquad (4)$$

Із (4) вираховано, що мінімальне значення буде дорівнювати $t_{V1} \approx 2\sqrt{2n * t_{LUT}}$. Верхня оцінка в кількості 6-розрядних LUT, дорівнює $C_{V1} = 12n - 16\left(\sqrt{n/2} - 1\right) - 8\sqrt{2n}$

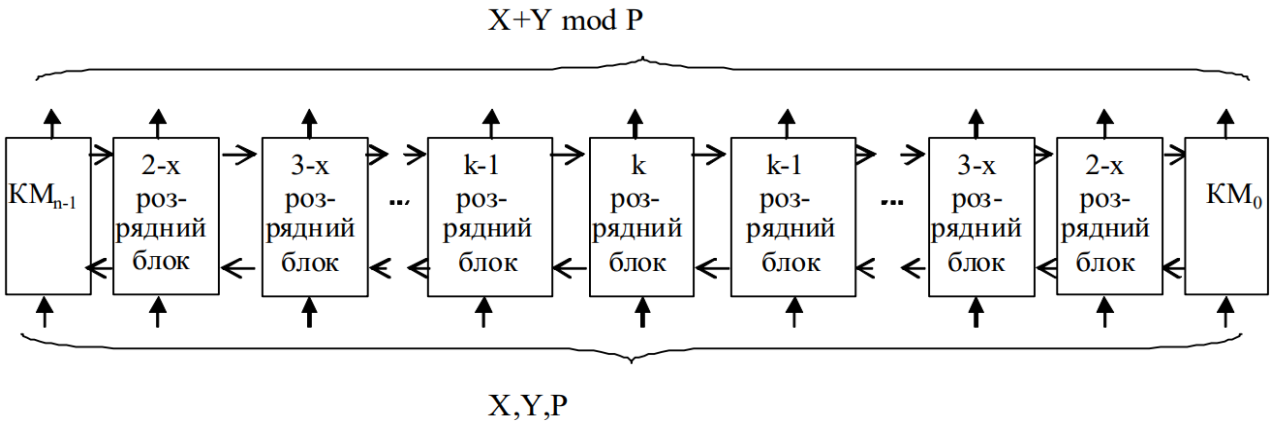

Рис. 3. Структура моделі суматора яка побудована за другим варіантом методу одновимірного каскаду конструктивних модулів з груповим переносом

Варіант 2. Для *0*-го та *(n-1)*-го розрядів суматора використовуються лише конструктивні модулі. Для наступних двох розрядів з обох боків використовується 2-х розрядний блок, далі – 3-х розрядні і т.д з максимальною розрядністю групового блоку для середніх розрядів (рис.3).

В даному випадку $n = (k+1) * {}^{k}/_{2} + k * (k-1)/2$. Звідки маємо $k = \sqrt{n}$.

Особливістю цієї моделі суматора за модулем є те, що в кожному із блоків групового переносу затримка узагальненого сигналу переносу визначається затримкою на КС 4 (або КС 6). Нижня оцінка tv2 затримки узагальненого сигналу переносу в будь який із боків визначається кількістю $w = 2k - 3$ груп плюс затримка на конструктивному модулі 0 (або n-1), тобто $t_{V2} \approx 2\sqrt{n * t_{LUT}}$. Верхня оцінка в кількості 6-розрядних LUT $C_{V1} = 12n - 16\sqrt{n}+8$.

Оцінено теоретичний приріст прискорення обчислення результату у моделі суматора з груповим переносом у відношенні до базової структури суматора на одновимірному каскаді конструктивних модулів. Затримка обчислення результату суматором з базовою структурою буде дорівнювати W=nt, де n-розрядність суматора, а t-затримка на одній комірці суматора. Відповідно для суматора з груповим переносом $W \approx t(2m + r)$, де r – кількість груп, m – розрядність однієї групи. Таким чином, якщо прийняти, що у випадку з базовою структурою W=rmt, для прикладу приведено, що якщо n=512, m=16, а r=32 маємо прискорення у 8 разів.

Запропоновано модифікацію алгоритма множення та піднесення до степеню за змінним модулем, з урахуванням особливостей застосування моделей суматорів на основі одновимірних каскадів конструктивних модулів, в якому в залежності від вхідних значень буде змінюватись час обчислення результату

У третьому розділі запропонована модель обчислювальних структур завадостійких кодів для виконання операцій за змінним простим модулем над числами великої розрядності, виконана реалізація та дослідження. Модель була створена з орієнтацією на адаптацію до елементів операційного обчислювального середовища для забезпечення можливості конструювання необхідних комбінацій виконавчих пристроїв для виконання однотипних арифметичних інструкцій за модулем над числами великої розрядності.

Також в розділі виконана адаптація алгоритму обчислення операції множення та піднесення до степеню за модулем з урахуванням особливостей її побудови раніш запропонованим методом одновимірного каскаду.

Запропонована структура моделі та алгоритм роботи спрощеного завантаження багаторозрядних операндів до блоків виконання операції за модулем. При реалізації моделі використовуався структурний опис з використанням бібліотеки стандартних ресурсів Xilinx на мові опису апаратури VHDL.

Вибір структурного способу опису пов’язаний з тим, що поведінковий опис комбінаційних схем операторами VHDL case/if не завжди призводить до оптимальних результатів, тому що такий підхід виключає можливість точного пояснення отриманих результатів у зв’язку з закритістю алгоритмів трансляції поведінкового опису у структурний у процесі синтезу.

Для оцінення можливості проведення експериментів над моделлю обчислювальних структур у реальних пристроях було прийнято, що модель має три n-розрядных вхідних сигнали, а також один n-розрядный вихідний сигнал (результат операції). Таким чином, n-розрядний експериментальний блок потребує 4n одноразрядных сигналів вводу - виводу. Для виконання експериментів з великою

розрядністю обчислювальні блоки слід доповнювати послідовним інтерфейсом FSL та блоком спрощеного завантаження операндів

Блок спрощеного завантаження операндів представляє собою блок керування без логіки вибору операції, так як для дослідження одного конкретного обчислювача вона не потрібна, але може вносити додатковий вплив на характеристики. Маємо враховувати, що внесок інтерфейсу FSL та спрощеної схеми завантаження у значення ресурсів та затримки, може не мати характеристик з високим коефіцієнтом детермінації, так як при їх реалізації використовується поведінковий опис.

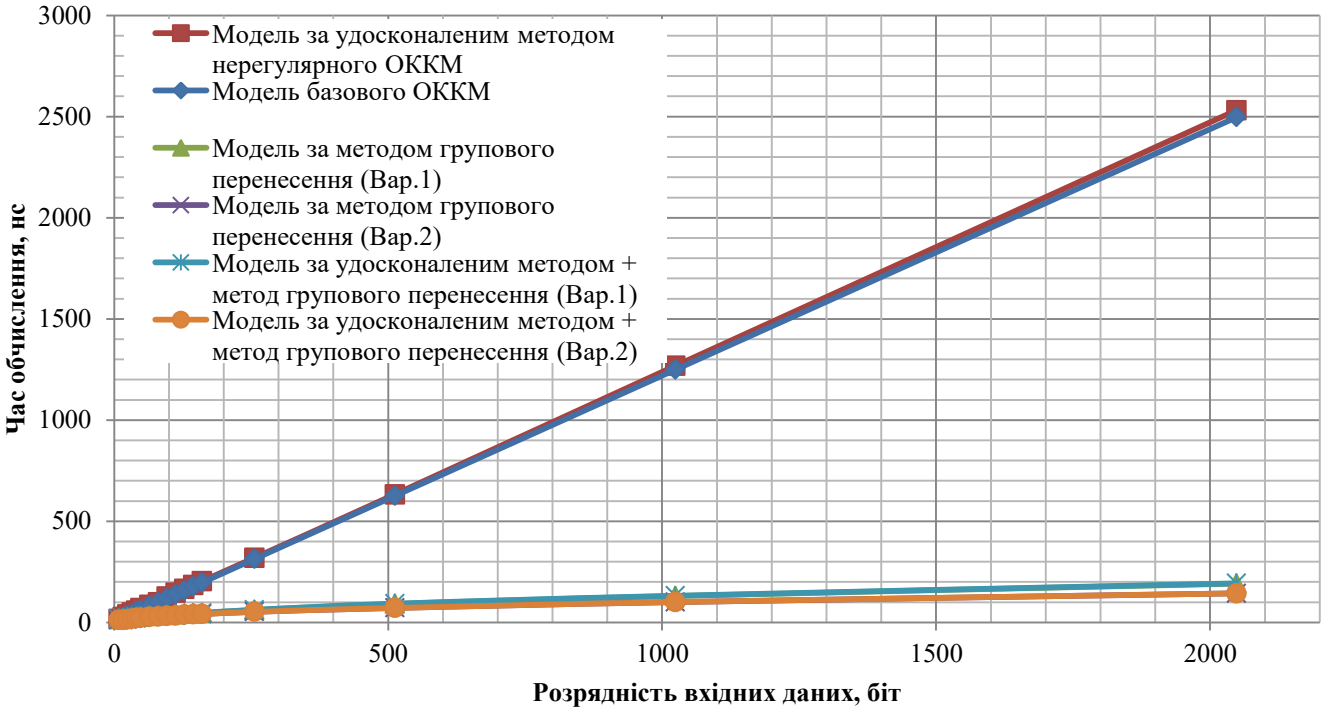

Рис. 4. Залежність часу обчислення від розрядності вхідних даних за результатами моделювання

Набори вхідних даних для проведення експериментів з блоками виконання операцій за модулем були визначені наступним чином: один набір даних складається з значень двох операндів, над якими виконується операція, та значення модуля. Для кожного набору вхідних даних було заздалегідь розраховано значення результату операцій в залежності від типу обчислювача за допомогою стандартних функцій мови програмування Python. На основі згенерованих наборів й результатів для кожного типу обчислювачів були згенеровані сутності тестування на мові VHDL (Testbench). Для експериментів з великими даними вхідні слова завантажуються послідовно, частинами по 16 біт, шляхом імітації інтерфейса ведучого FSL шини. Після чого виконувалося очікування на час максимальної затримки для обчислювача. Це значення затримки обчислюється як результат аналітичної функції від поточної розрядності. Сама функція отримана в ході виконання експеримента для цієї реалізації обчислювача. Далі проводилося порівняння значень на виході обчислювача з заздалегідь розрахованими значеннями результату для даного набору вхідних даних. Результат порівнянь відображається шляхом виконання оператора

assert мови VHDL. Потім виконується перехід до кроку 1 з наступними значеннями вхідних даних з набору. Крім перевірки правильності роботи обчислювача даний експеримент дозволив підтвердити здатність обчислювача отримати результат за розрахований час експерименту – якщо результат розраховується за більший час, ніж розрахований на кроці 2, то результат буде невірним. Результати експериментів наведені на рис.4 та рис.5.

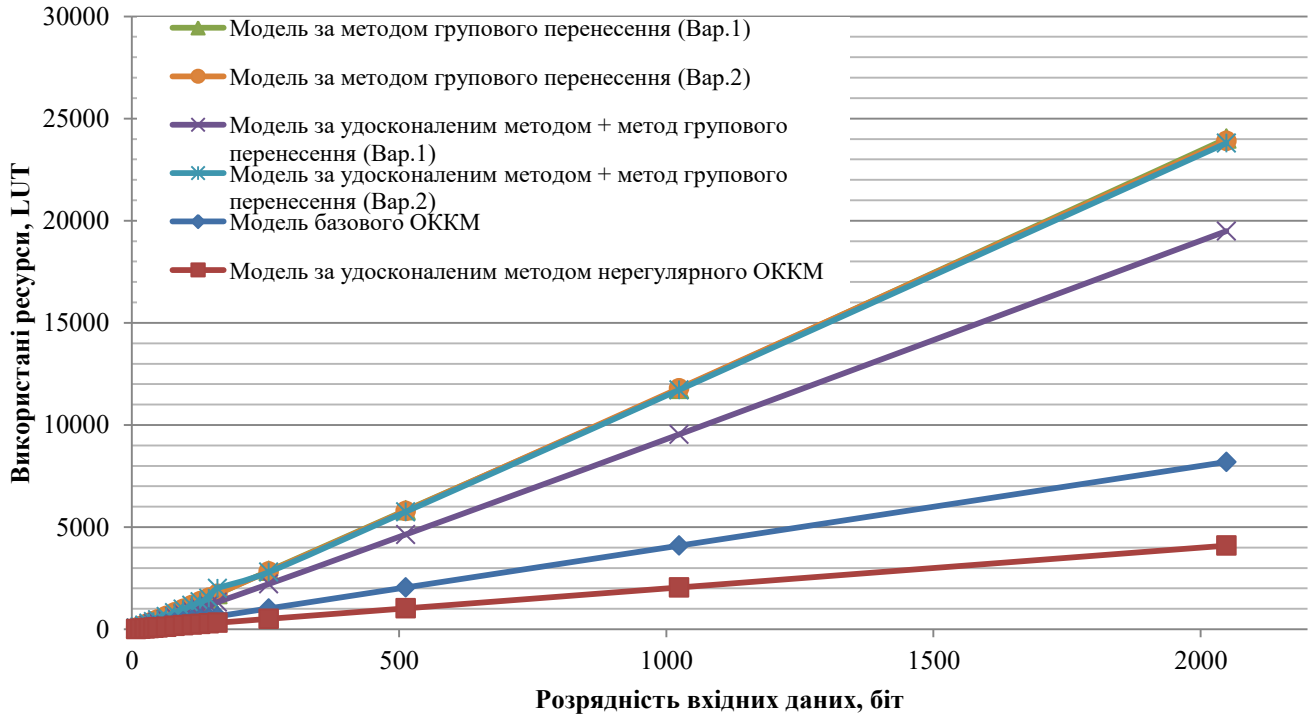

Рис. 5. Залежність кількості використаних обчислювальних ресурсів від розрядності вхідних даних за результатами моделювання

Модель обчислювальних структур завадостійких кодів для виконання операцій за змінним простим модулем як і більшість подібних до неї рідко використовуються як окрема одиниця, та зазвичай представляють собою частину більш складної синхронної системи. Тактм чином, проведені експерименти вирішили задачу визначення максимальної тактової частоти, на якій може працювати розроблена модель без помилок у обчисленнях вихідної функції.

У четвертому розділі розроблено інформаційну технологію прискореного обчислення великих даних для систем розподіленої обробки інформації. Структура інформаційної технології представлена на рис. 6. Інформаційна технологія базується на розроблених раніше удосконалених методах зменшення апаратних витрат та прискорення обчислення великих даних. Додатково, для доповнення технології було розроблено архітектуру та систему команд функціональної моделі співпроцесору, орієнтованого на виконання операцій у скінченних полях.

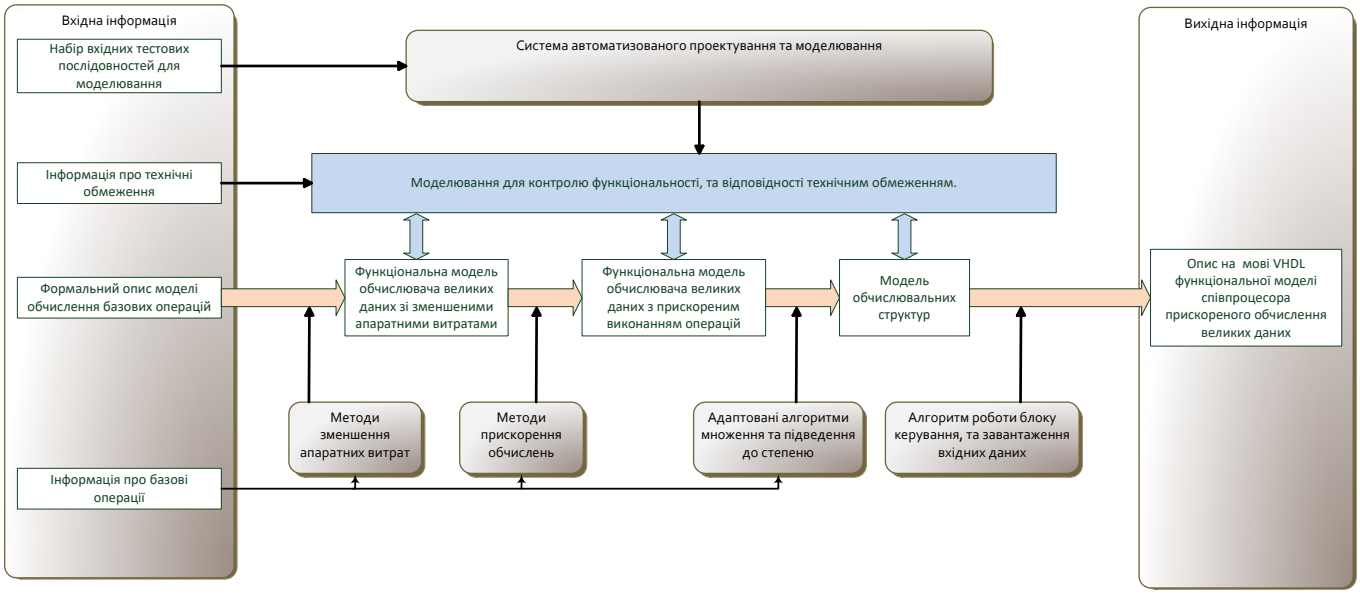

Рис. 6. Схема інформаційної технології прискореного обчислення великих даних для систем розподіленої обробки інформації.

Інформаційна технологія була доповнена розробленим алгоритмом роботи блоку керування моделі співпроцесору. Архітектура співпроцесору орієнтована на використання інтерфейсу FSL, який призначений для обміну даними між елементами обчислювальної системи. Він дозволяє приймати 32-х розрядні порції даних. Так як розрядність операндів n перевищує 32 біта у визначену кількість разів k, завантаження операндів та вивантаження результату виконується послідовно порціями даних по 32 біта. За керуючим сигналом завантаження пристрій керування інтерпретує дані як наступне неповне слово операнду, що завантажується, або як код керування. Також задіяний керуючий сигнал вивантаженя для виводу неповних слів результату в основне процесорне ядро.

У висновках викладені наукові і практичні результати роботи, сформульована вирішена наукова задача, обґрунтовано достовірність отриманих результатів і наведені рекомендації щодо їх практичного використання.

В додатках наведено документи про впровадження результатів досліджень, результати розрахунків та приклади.

ВИСНОВКИ

Запропоновані в дисертаційній роботі наукові результати у своїй сукупності утворюють нову інформаційну технологію прискореного обчислення великих даних для систем розподіленої обробки інформації

В дисертаційній роботі вирішено важливу науково-прикладну задачу - прискорення обчислення великих даних для систем розподіленої обробки інформації, за рахунок створення ефективних моделей і методів для виконання обчислень у скінченних полях, шляхом структурно-логічної оптимізації архітектур обчислювальних засобів, що реалізують процеси виконання операцій кодування/декодування кодів.

При цьому отримано такі теоретичні та практичні результати:

1. На основі проведеного аналізу були визначені основні методи виконання найбільш вживаних обчислювально витратних операцій у процесі обробки даних в розподілених системах, а саме: операція додавання та множення у скінченних полях. Показано що удосконалення цих методів є одним з напрямків пришвидшення обчислення операцій кодування/декодування кодів, що стало підставою провести ґрунтовне дослідження та сформувати напрямки розвитку та вдосконалення зазначених методів.

2. Запропоновано удосконалений метод одновимірного каскаду реалізації процедури обчислення базових операцій обробки даних, який, на відміну від наявних, використовує конструктивні модулі з наскрізним переносом, що дозволяє зменшити апаратні витрати та, як наслідок, збільшити розрядність обчислювальних данних за рахунок вивільнених апаратних ресурсів, що призводить до зменшення обчислювальної складності. Удосконалення методу забезпечує зменшення апаратних витрат в середньому на 10% порівняно з існуючим базовим методом.

3. Запропоновано модифікацію удосконаленого методу одновимірного каскаду реалізації процедури обчислення базових операцій обробки даних, який, на відміну від раніше запропонованого, використовує конструктивні модулі нерегулярного типу, що дозволяє ще зменшити апаратні витрати без втрати швидкодії. Таким чином, модифікація методу забезпечує зменшення апаратних витрат в середньому на 50% порівняно з існуючим базовим методом. Модифікацію методу можна застосовувати для зменшення обчислювальної складності у разі не критичності вимог до регулярності структури обчислювача.

4. Отримав подальший розвиток метод прискорення обчисленнь операцій за модулем для чисел великої розрядності, який, на відміну від відомих, використовує ланцюги групового переносу, що дозволяє зменшити час обчислення операцій у середньому у 8 разів, порівняно з реалізацією базовим методом.

5. Розроблено модель обчислювальних структур обчислення базових операцій за змінним простим модулем над числами великої розрядності, яка на відміну від відомих, дозволяє за рахунок адаптації елементів операційного обчислювального середовища забезпечити можливість конструювання необхідних комбінацій виконавчих пристроїв для виконання однотипних арифметичних інструкцій за модулем над числами великої розрядності.

6. Запропоновано адаптований алгоритм обчислення операції множення та піднесення до степеню за модулем з урахуванням особливостей її побудови раніш запропонованим методом одновимірного каскаду. Запропонована адаптація дозволяє зменшити час обчислення за рахунок використання меншої кількості обчислювально витратних операцій при певних наборах вхідних даних.

7. Розроблена інформаційна технологія обчислення великих даних, яка, на відміну від існуючих, базується на запропонованому методі обчислень за модулем та забезпечує прискорення виконання обчислювальних процедур.

Отримані в роботі результати дозволяють на практиці підвищити продуктивність систем захисту інформації, систем цифрової обробки сигналів та завадостійкого кодування даних.

Результати впровадження підтверджені відповідними актами.

СПИСОК ОПУБЛІКОВАНИХ РОБІТ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, в яких опубліковані основні наукові результати дисертації:

1. Андрій Роговенко. Дослідження обчислювачів прискореного обчислення даних збільшеної розрядності на основі одновимірного каскаду конструктивних модулів. Науковий журнал “Технічні науки та технології”. Чернігів, ЧНТУ, 2020. № 4. С. 109–117.

2. Andrew Rogovenko, Iryna Yakymenko. Comparison of data calculation means in distributedinformation processing systems. Multidisciplinárn í mezinárodní vědecký magazín «Věda a perspektivy». Praha, České republika, 2021. №1. С. 282–295.

3. Тарасенко В.П., Тесленко О.К., Роговенко А.І. Частково-груповий перенос суматорів в скінченому полі GF(P). Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". Львів, Львів. політехн., 2013. №773. С. 118–125.

4. Цулун О.В., Роговенко А.І. Архітектура криптографічного акселератора з можливістю зміни криптографічного алгоритму. Вісник Чернігівського державного технологічного університету. Чернігів, ЧДТУ, 2011. № (1)47. С. 214–220.

5. Тарасенко В.П., Тесленко О.К., Роговенко А.І. Створення параметричних ядер (softcores) для виконання операцій в кінцевих полях. Науково-технічний журнал “Радіоелектронні і комп’ютерні системи”. Харків, ХАІ, 2008. № 6. С. 261–263.

6. Тарасенко В.П., Тесленко О.К., Роговенко А.І. Оптимізація апаратних витрат на реалізацію параметричних ядер (soft-cores) для виконання операцій в скінчених полях. Науково-технічний журнал “Радіоелектронні і комп’ютерні системи”. Харків, ХАІ, 2009. № 5. С. 184–189.

7. Грицай Д.Д. , Роговенко А.І. Особливості побудови комп’ютерної системи тестування цифрових пристроїв на базі SOFT-процесорів. Вісник Чернігівського державного технологічного університету. Чернігів, ЧДТУ, 2011. № (2)49. С. 234–240.

8. Тарасенко В.П., Тесленко О.К., Роговенко А.І. Метод групового перенесення суматора за змінним модулем. Науково-технічний журнал “Радіоелектронні і комп’ютерні системи”. Харків, ХАІ, 2010. № 5. С. 242–245.

Праці, що засвідчують апробацію матеріалів дисертації:

9. Volodymyr Tarasenko, Olexandr Teslenko, Andriy Rogovenko. The performance defining for adders with variable module based on one-dimensional cascade of constructional modules. *Advanced Computer System and Networks: Design and Application:* proceedings Of the 4st International Conference ACSN-2009.(17-19 december 2009) Lviv, 2009. P. 11–13.

10. Грищенко О.М, Павловський В.І., Роговенко А.І. Підвищення швидкодії пристроїв цифрової обробки сигналів на основі ПЛІС. *Розподілені комп’ютерні системи. Том 1*: зб. праць міжнар. наук.-практ. конф. Київ. НТУУ КПІ, 2010. С. 184–186.

11. Баргамін О.А., Роговенко А.І. Змішане поведінкове моделювання систем передачі інформації на основі коду Ріда-Соломона. *Математичне та імітаційне моделювання систем МОДС2012.* Тези доповідей. Сьома міжнар. наук.-практ. конф. (Чернігів-Жукин, 25 червня 2012 р.). Чернігів, 2012. С. 341-344.

12. Тарасенко В.П., Тесленко О.К., Роговенко А.І. Використання схем групового перенесення у суматорах в залишках на основі одновимірних каскадів конструктивних модулів. *Системний аналіз та інформаційні технології.* SAIT 2013: матеріали 15-ї міжнар. наук.-техн. конф. (Київ, 27 травня 2013 р.). Київ: ННК "ІПСА" НТУУ "КПІ", 2013. С. 484–486.

13. Роговенко А.І. Структура операційного пристрою виконання операцій за модулем на основі одномірного каскаду конструктивних модулів . *Актуальні наукові дослідження в сучасному світі:* зб. наук. праць. XXIV міжнар. наук. конф. (Переяслав-Хмельницький, 26-27 квітня 2017 р.). Переяслав-Хмельницький, 2017. Вип. 4(24), ч. 4. С. 60–63

14. Пат. на корисну модель № 100006, МПК G06F 7/50, G06F 7/00 Багаторозрядний суматор за змінним модулем з груповим переносом / Клятченко Я.М., Роговенко А.І., Тарасенко В.П. Тесленко О.І. Шепотіннік О.Ю.; заявл. 21.03.2014; опубл. 10.07.2015, бюл. №13.

15. Пат. на корисну модель № 61647 G06F 7/00 Комірка суматора за змінним модулем / Роговенко А.І.; Тарасенко В.П.; Тесленко О.К.; заявл. 29.12.2010; опубл. 25.07.2011, бюл. №14;

16. Пат. на корисну модель № 61654 G06F 7/50 Конструктивний модуль суматора в залишках / Тарасенко В.П.; Тесленко О.К.; Роговенко А.І.; заявл. 29.12.2010; опубл. 25.07.2011, бюл. №14.

17. Пат. на корисну модель № 68397 G06F 7/50 Багаторозрядний суматор по змінному модулю / Тарасенко В.П.; Тесленко О.К.; Роговенко А.І.; Волік А.С.; заявл. 23.08.2011; опубл. 26.03.2012, бюл. №6.

18. Пат. на корисну модель № 62946 G06F 7/50 Конструктивний модуль додавача в залишках з груповим переносом / Тарасенко В.П.; Тесленко О.К. Роговенко А.І.; заявл. 02.02.2011; опубл. 26.09.2011, бюл. №18.

АНОТАЦІЯ

Роговенко А.І. Методи та інформаційна технологія прискореного обчислення великих даних для систем розподіленої обробки інформації − Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології. − Національний університет "Чернігівська політехніка", м. Чернігів, 2021.

Дисертація присвячена дослідженню актуальних проблем прискорення обчислень великих даних в системах розподіленої обробки інформації за рахунок розробки методів прискорення виконання базових операцій з урахуванням особливостей і властивостей сучасних обчислювальних платформ та зменшення

складності реалізації при умові високої швидкості й великого об’єму вхідного потоку даних.

Вперше запропоновано удосконалений метод одновимірного каскаду реалізації обчислення базових операцій обробки даних, який, на відміну від наявних, використовує конструктивні модулі з наскрізним переносом.

Визначено, що удосконалення методу забезпечує зменшення апаратних витрат в середньому на 10% порівняно з існуючим базовим методом.

Запропоновано модифікацію удосконаленого методу одновимірного каскаду реалізації процедури обчислення базових операцій обробки даних, який, на відміну від раніше запропонованого, використовує конструктивні модулі нерегулярного типу.

Встановлено, що модифікацію методу можна застосовувати для зменшення обчислювальної складності у разі не критичності вимог до регулярності структури обчислювача. Використання модифікованого методу дозволяє зменшити витрати обчислювальних ресурсів більше ніж на 50%, в залежності від розрядності, порівняно з існуючим базовим методом.

Отримав подальший розвиток метод прискорення обчисленнь операцій за модулем для чисел великої розрядності, який, на відміну від відомих, використовує ланцюги групового переносу, що дозволяє підвищити швидкість виконання операцій у 8 разів порівняно з реалізацією базовим методом.

Розроблено модель обчислювальних структур для виконання операцій за змінним простим модулем над числами великої розрядності, яка на відміну від відомих, дозволяє конструювання необхідних комбінацій виконавчих пристроїв для виконання однотипних арифметичних інструкцій за модулем над числами великої розрядності.

Запропоновано адаптований алгоритм обчислення операції множення та піднесення до степеню за модулем з урахуванням особливостей її побудови раніш запропонованим методом одновимірного каскаду. Запропонована адаптація дозволяє зменшити час обчислення за рахунок використання меної кількості обчислювально витратних операцій при певних наборах вхідних даних.

Розроблена інформаційна технологія обчислення великих даних, яка, на відміну від існуючих, базується на запропонованому методі обчислень за модулем та забезпечує прискорення виконання обчислювальних процедур.

Ключові слова: складність реалізації, обчислювалні засоби, алгоритми кодування/декодування, наскрізний перенос, числа великої розрядності, модель обчислювальних структур, адаптація, скінченні поля, продуктивність.

ANNOTATION

Rohovenko A.I. Methods and information technology of accelerated calculation of big data for distributed information processing systems - Manuscript.

Dissertation research for degree of PhDs. by specialty 05.13.06 «Information Technologies». – Chernihiv polytechnic national university, Chernihiv, 2021.

The dissertation is devoted to research of actual problems of acceleration of calculations of big data in systems of distributed information processing by development of methods of acceleration of performance of basic operations taking into account features and properties of modern computing platforms and reduction of complexity of realization at high speed and big volume of an input data stream.

For the first time, an improved method of one-dimensional cascade of calculation of basic data processing operations is proposed, which, in contrast to the existing ones, uses constructive modules with end-to-end transfer.

It is determined that the improvement of the method provides a reduction in hardware costs by an average of 10% compared to the existing basic method.

A modification of the improved method of one-dimensional cascade implementation of the procedure for calculating basic data processing operations, which, in contrast to the previously proposed, uses structural modules of irregular type, is proposed.

It is established that the modification of the method can be used to reduce the computational complexity in the case of non-critical requirements for the regularity of the computer structure. The use of a modified method reduces the cost of computing resources by more than 50%, depending on the bit rate, compared to the existing basic method.

The method of accelerating the calculations of operations modulo for large numbers, which, in contrast to the known ones, uses group transfer chains, which allows to increase the speed of operations by 8 times compared to the implementation of the basic method.

A model of computational structures for performing operations on a variable simple module over large-digit numbers has been developed, which, unlike the known ones, allows constructing the necessary combinations of actuators to perform the same type of arithmetic instructions modulo over large-digit numbers.

An adapted algorithm for calculating the operation of multiplication and exponentiation modulo taking into account the peculiarities of its construction by the previously proposed method of one-dimensional cascade is proposed. The proposed adaptation allows to reduce the computation time by using a variable number of computationally costly operations for certain sets of input data.

The information technology of calculation of big data which, unlike existing, is based on the offered method of calculations on the module and provides acceleration of performance of computational procedures is developed.

Keywords: implementation complexity, computing means, encoding / decoding algorithms, through transfer, high-bit numbers, model of computing structures, adaptation, finite fields, productivity.