ВІДГУК

офіційного опонента доктора технічних наук Гамаюна Володимира Петровича
на дисертаційну роботу Оная Миколи Володимировича
"Методи та засоби підвищення ефективності
реалізації обчислювальних операцій у скінченних полях",
поданої на здобуття наукового ступеня кандидата технічних наук
у спеціалізовану вчену раду Д 26.002.02 КПІ ім. Ігоря Сікорського
за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

Актуальність дисертаційної роботи Оная Миколи Володимировича визначається потребою розвитку конкурентоздатної комп'ютерної індустрії, яка є пріоритетною у науково-технічному процесі. Розвиток нових теоретичних та науково-практичних засад комп'ютерних наук є необхідним чинником у таких важливих напрямках діяльності як дослідження та проектування, виробництво нових зразків комп'ютерної техніки та розв'язання прикладних проблем. Розвиток теорії та методів побудови моделей, обчислювальних структур, апаратно-програмних засобів, виконання моделювання є ознакою сучасного розв'язання проблеми дослідження та проектування. Перспективність та актуальність теоретичних та практичних досліджень комп'ютерних арифметик та засобів їх реалізації, що розглядаються у дисертації Оная Миколи Володимировича підтверджується також науковими та практичними досягненнями у комп'ютерній галузі та комп'ютерних науках.

Зв'язок роботи з науковими програмами, планами підтверджується участю Оная Миколи Володимировича у виконанні науково-дослідних робіт КПІ ім. Ігоря Сікорського та Держпрограм. Тематика цих робіт відповідає розв'язанню актуальних задач комп'ютернх наук та актуальним задачам прикладних наук, що вирішуються за допомогою засобів комп'ютерної техніки та програмних засобів.

Структура та обсяг дисертації: дисертація складається зі вступу, п'яти розділів, висновків, списку літератури, додатків.

У **вступі** дисертації обґрунтована актуальність теми дисертаційної роботи; показано зв'язок роботи з науковими програмами, планами, темами; сформульовано мету і задачі наукових досліджень; визначено наукову новизну та практичне значення одержаних результатів; наведено відомості про публікації, апробацію і впровадження результатів роботи.

В огляді літератури (**перший розділ**) розкрито стан проблеми, пов'язаної з необхідністю удосконалення методів апаратної реалізації операцій у скінченних полях.

Виконано класифікацію методів обчислення мультиплікативно оберненого елемента в скінченних полях. Встановлено, що менш обчислювально витратними є методи, що ґрунтуються на знаходженні НСД двох чисел.

Досліджено та класифіковано методи модулярного піднесення до степеня, а саме: методи, що ґрунтуються на поданні показника степеня у двійковій системі числення; методи, що ґрунтуються на поданні показника степеня у симетричній трійковій системі числення та методи, що ґрунтуються на поданні показника степеня в системі числення з мультиосновою.

Показано, що для вирішення проблеми в цілому – виконання довільних обчислень у скінченних полях – необхідно розробити архітектуру комп'ютерної системи, організація та система команд якої були б орієнтовані на специфіку реалізації операцій в полях Галуа, яка б забезпечувала потрібну швидкодію.

У другому розділі досліджена апаратна реалізація операцій у скінченних полях виду $GF(p)$.

Проведено аналіз віконних методів піднесення до степеня показує, що чим більше одиниць містить бітовий блок таблиці передобчислень, тим менша кількість часовитратних операцій множення буде виконуватись при реалізації операції. На основі цього запропоновано модифікацію методу піднесення до степеня елементів поля $GF(p)$ з ковзним вікном, яка полягає в тому, що при формуванні таблиці передобчислень використовуються показники степеня, що є простими числами. Обчислювальні експерименти показали, що такий підхід до формування таблиці передобчислень дозволяє скоротити кількість операцій множення в середньому на 10%, коли показник степеня має довжину понад 256 біт, та забезпечує приріст швидкодії на 7-9 %.

У третьому розділі розроблено метод виконання операцій над елементами поля $GF(2^m)$ та запропоновано архітектуру апаратних засобів для реалізації методу.

Встановлено, що скінченним полям $GF(2^m)$ властивий ізоморфізм – елементи поля допускають степеневе та многочленне подання. Ці подання елементів поля є еквівалентними, і кожне з них є зручним для реалізації відповідних операцій над елементами.

Операцію додавання елементів поля та знаходження протилежного елемента зручно виконувати над многочленним поданням, що у випадку $p = 2$ співпадає з двійковими кодами елементів поля. А операцію множення, знаходження мультиплікативно оберненого елемента, ділення та піднесення до степеня зручно виконувати над степеневим поданням елементів поля, оскільки в цьому випадку необхідно виконувати операції лише над показниками степеня. Показано, що під час виконання операцій в $GF(2^m)$ необхідно динамічно,

залежно від характеру операції, переходити від однієї форми подання елементів до іншої, і навпаки, тобто оперативно, на апаратному рівні забезпечувати ізоморфізм поля.

Доведено, що для забезпечення виконання операцій над степеневим поданням елементів поля $GF(2^m)$ додатково необхідно чотири мікрооперації за модулем $2^m - 1$: додавання, віднімання, множення m-розрядних двійкових величин за модулем $2^m - 1$ та інвертування m-розрядної двійкової величини. Цю множину мікрооперацій апаратно реалізовано як систему мікрокоманд мікроасемблера та побудовано блок виконання мікрооперацій за модулем $2^m - 1$.

Запропоновано метод виконання операцій над елементами поля $GF(2^m)$ з використанням розрідженої таблиці елементів поля у степеневому та многочленному поданні та алгоритми перетворення зі степеневого подання у многочленне і навпаки. Розріджене формування таблиці елементів поля дозволяє у кілька разів скоротити витрати пам'яті для її зберігання. Виконувати розрідження можна за допомогою функції, для якої існує обернена. Функція визначає черговий номер елемента повної таблиці, який включається у розріджену таблицю. Показано, що оптимальним є запис кожного k-го елемента поля в *ROM*; в такому випадку ступінь розрідження таблиці дорівнює k.

Розроблено блок виконання операцій над елементами поля $GF(2^m)$, який підтримує виконання наступного набору команд: *ADD_SUB*, *MULT*, *DIV*, *POW*, *INVM* (обчислення мультиплікативно оберненого елемента), *CDP* (перетворення з числового подання у степеневе), *CPD* (перетворення зі степеневого подання у числове).

У **четвертому розділі** розроблено архітектуру спеціалізованого процесора, що орієнтований на виконання обчислень у полях Галуа (*G*-процесора).

Запропонована система команд включає: арифметичні команди (*ADD*, *MULT*, *DIV*, *POW*, *INVM*, *CDP*, *CPD*, *INVA*, *SUB*, *INC*, *DEC*), команди пересилання даних (*MOV*, *LOAD*, *OUT*) та команди передачі керування (*JMP*, *LOOP*).

Комп'ютерне моделювання обчислювальних процесів, що мають місце при реалізації операцій у скінченних полях, показало, що продуктивність системи на основі співпроцесора Галуа порівняно з універсальною обчислювальною системою зростає на 27%, залежно від команд, що використовуються в програмному коді мовою Асемблера процесора Галуа.

Особливістю архітектури *G*-процесора є те, що не змінюючи інтерфейсу процесора, шляхом зміни арифметико-логічного пристрою (АЛП) можна здійснити перехід до поля Галуа $GF(p)$ або до $GF(2^m)$.

У **п'ятому розділі** виконано оцінювання обчислювальної складності розроблених методів, наведено результати експериментальних досліджень та проведено аналіз апаратних ресурсів, необхідних для реалізації запропонованих методів на ПЛІС.

Встановлено, що метод з використанням розрідженої таблиці елементів поля характеризується слабкою залежністю кількості операцій зсуву і порозрядного додавання для виконання операції обчислення мультиплікативно оберненого елемента та ділення від параметра m поля. Для операції множення запропонований метод дає приріст швидкодії лише починаючи зі значення $m = 20$. Окрім цього, зі збільшенням значення m при фіксованому ступені розрідження перевага запропонованого методу стає більш значною.

Висновки і практичні рекомендації випливають із матеріалів дисертації, достовірні, науково обґрунтовані та чітко сформульовані. Вони містять нові важливі науково-практичні положення і пропозиції.

Бібліографія містить 143 першоджерела вітчизняних та іноземних авторів, які в цілому висвітлюють тему дисертації.

В додатках наведені програмні продукти засобів реалізації та акти впровадження.

Загальні висновки відображають результати теоретичних досліджень та моделювання, впровадження. Узагальнення результатів виконано коректно, у відповідності з отриманими результатами. В основному підкреслюється висновок про те, що результати дисертаційної роботи розвивають теорію, методи та засоби реалізації однорангових комп'ютерних мереж спеціального призначення.

Наукова новизна одержаних у дисертаційній роботі результатів полягає у наступному:

1. Вперше запропоновано метод високошвидкісного виконання адитивних та мультиплікативних операцій над елементами поля $GF(2^m)$, характерною особливістю якого, на відміну від існуючих, є застосування розрідженого табличного зберігання елементів поля у многочленному та степеневому їх поданні, що також зменшує витрати пам'яті . Метод забезпечує зростання швидкодії на 15% порівняно з існуючим рішенням.
2. Вперше запропоновано модифікацію методу піднесення до степеня елементів поля $GF(p)$ з ковзним вікном, яка полягає в тому, що при формуванні таблиці передобчислень використовуються показники степеня, що є простими числами. Такі показники степеня дозволяють отримувати кожен наступний елемент таблиці передобчислень за одну-дві операції модулярного множення та забезпечують зменшення кількості операцій множення – наслідком чого є приріст швидкодії на 7-9 %.

3. Розроблено модель обчислювального процесу, що має місце при реалізації операцій у скінченних полях.

Практичне значення дисертації полягає у наступному:

1.Спроектовано на ПЛІС фірми *Xilinx* процесор Галуа, що орієнтований на виконання операцій у скінченних полях виду $GF(p)$ та $GF(2^m)$. Розроблено структурні та схемотехнічні рішення блоків виконання обчислювальних операцій у скінченних полях виду $GF(p)$ та $GF(2^m)$, які характеризуються високою швидкістю обробки даних.

2. Побудовано програмістську модель процесора Галуа, яка дозволяє створювати програмне забезпечення довільної складності мовою Асемблера процесора Галуа. Розроблено програмний модуль для імітаційного та функціонального моделювання обчислювального процесу в процесорі Галуа, що дозволяє проводити дослідження розроблених методів виконання операцій у скінченних полях.

3. Виконано моделювання задач цифрової обробки сигналів, криптографії, завадостійких систем, що підтверджує практичне значення результатів.

Достовірність та обґрунтованість сформульованих у дисертаційній роботі наукових положень підтверджується математичними доведеннями, результатами практичного моделювання, впровадженнями, які наведені у відповідних документах, численних виступах та обговореннях у наукових колах, у публікаціях. Матеріали дисертації наведені у фахових виданнях та матеріалах конференцій. Зміст публікацій відповідає виконаним дослідженням та впровадженням.

Автореферат відповідає змісту дисертації та відображає наукові та практичні результати.

Зауваження по роботі наступні.

1. Загальний вибір проблем, що потрібно розв'язувати, виконано з перевантаженням.

Методи апаратної реалізації операцій у полях Галуа, процесор Галуа – архітектура та система команд, реалізації на ПЛІС, створення засобів моделювання та дослідження ефективності виконання операцій у полях Галуа могли б створити окрему дисертацію.

2. Здобувач посилається на результат підвищення продуктивності систем цифрової обробки сигналів, криптографічних перетворень, але в проблемах дисертації немає плану таких досліджень, та представлені матеріали по цих питаннях не є повними в сенсі комплексного розв'язання згаданих проблем.

3 Головні результати по методах обчислень поданні стисло, бажано б було мати більше інформації про процедури аналізу – діапазон даних, програмне забезпечення , техніку, що була застосована та інше.

4. Результати експериментального та натурного моделювання бажано було б підкріпити більшою кількістю практичних варіантів, що б дало окреслити конкретне впровадження та поширення теоретичних результатів

5. Здобувачем виконано переважно подання матеріалу у додатках, а не у основному тексті. Доказовий матеріал по деяким питанням треба розшукувати у додатках, а не по змісту.

6. У роботі спостерігається невідповідність посилань на джерела та інші публікації, що є у автора, або відсутність посилань, які оголошенні як обов'язкові публікації.

7. У рукопису є стилістичні помилки, але їх небагато

Вказані недоліки не впливають на загальну оцінку дисертації.

Висновки по роботі. Робота Онай Миколи Володимировича «Методи та засоби підвищення ефективності реалізації обчислювальних операцій у скінчених полях» є завершеним науковим дослідженням та присвячена розв'язанню комплексу питань з проблематики побудови теорії та нових методів високопродуктивних обчислень .

Робота виконана самостійно у вигляді підготовленого рукопису, характеризується єдністю змісту і свідчить про особистий внесок здобувача в науку. Результати дисертації повно викладені в авторефераті та публікаціях та в сукупності вирішують важливу науково-технічну задачу методів вдосконалення обчислень на базі теорії Галуа , побудови комп'ютерних засобів для такої обробки даних.

Вважаю, що за актуальністю вибраної теми, достовірністю і обґрунтованістю результатів, новизною досліджень, значенням отриманих результатів для науки та практики дисертаційна робота задовольняє вимогам п.9, 11 «Порядку присудження наукових ступенів», затверджених постановою Кабінету Міністрів України від 24 липня 2013 р. №567, а її автор Онай Микола Володимирович заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент
доктор технічних наук, професор, ст. наук. спів.,
завідувач кафедри прикладної інформатики
Навчально-наукового Інституту
комп'ютерних інформаційних технологій
Національного авіаційного університету
Міністерства освіти і науки України В.П.Гамаюн

підпис гр. Гамаюна В.
з а с в і д ч у ю
Вчений секретар
Національного авіаційного університету
Г. Енчева