ВІДГУК

офіційного опонента по дисертаційній роботі на дисертаційну роботу Оная Миколи Володимировича "Методи та засоби підвищення ефективності реалізації обчислювальних операцій у скінченних полях",представленої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Актуальність проведених досліджень.

Сьогодні для реалізації задач цифрової обробки сигналів, криптографії та завадостійкого кодування в системах реального часу широко застосовуються скінченні поля, зокрема поля Галуа. Скінченні поля використовуються для побудови більшості відомих завадостійких кодів, цифрових фільтрів, генераторів псевдовипадкових чисел та криптографічних алгоритмів. Зокрема операції над елементами полів Галуа використаються у *CRC*-кодах, кодах *BCH* (Боуза-Чоудхурі-Хоквінгема) та кодах Ріда-Соломона, вейвлетних фільтрах третього порядку над простим полем Галуа та вейвлет-перетвореннях в базисі Хаара над полем Галуа; у лінійному конгруентному генераторі псевдовипадкових чисел та його модифікаціях; у найбільш поширених симетричних криптографічних алгоритмах, таких як *AES*, *IDEA*, *RC5*, у асиметричних криптографічних шифрах, таких як *RSA*, *DSA*, протоколі Діффі-Хелмана, схемі Ель-Гамаля, потокових шифрах та алгоритмах еліптичної криптографії. Поява елементної бази ПЛІС і систем автоматизованого проектування спеціалізованих пристроїв та систем на їх основі дозволила виконати ефективну апаратну реалізацію для підтримки функціонування в реальному часу.

Таким чином, задача розробки нових і удосконалювання відомих методів побудови спеціалізованих засобів на базі ПЛІС для апаратної реалізації високопродуктивних обчислень на основі арифметики скінченних полів **є актуальною**.

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

Дисертаційна робота виконувалась відповідно до планів НДР кафедри програмного забезпечення комп'ютерних систем КПІ ім. Ігоря Сікорського. Результати дисертаційних досліджень були використані під час виконання науково-дослідної робіт "Розроблення та дослідження високоефективних архітектур спеціалізованих комп'ютерних систем для реалізації обчислень у скінченних полях" (номер державної реєстрації 0115U000319, 2015-2016 рр.) та "Методи та засоби інформаційного забезпечення систем автоматизованого імпорту об'єктів на основі графічного кодування даних" (номер державної реєстрації 0112U003175, 2012-2014 рр.).

Результати дисертаційних досліджень також впроваджено в навчальний процес (є відповідний акт) на кафедрі програмного забезпечення комп'ютерних систем КПІ ім. Ігоря Сікорського при викладанні дисциплін: «Архітектура комп'ютера»; «Цифрова обробка сигналів і зображень»; «Теорія інформації та кодування».

Наукова новизна та теоретична цінність результатів. У дисертаційній роботі виконано теоретичне обґрунтування та отримано рішення актуальної науково-прикладної задачі підвищення швидкості обчислень в скінченних полях за рахунок структурно-логічної оптимізації архітектур апаратних засобів, що реалізують процеси виконання операцій у скінченних полях.

Наукова новизна відображена у наступних отриманих результатах, які мають теоретичну цінність:

- Вперше запропоновано метод високошвидкісного виконання адитивних та мультиплікативних операцій над елементами поля $GF(2^m)$, характерною особливістю якого, на відміну від існуючих, є застосування табличного зберігання елементів поля у многочленному та степеневому їх поданні. Даний метод передбачає можливість розрідженого формування таблиці елементів поля, що зменшує витрати пам'яті для її зберігання. Метод забезпечує зростання швидкодії на 15% порівняно з існуючим рішенням.
- 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 %.
- Розроблено модель обчислювального процесу для реалізації операцій у скінченних полях, яка дозволяє виконувати порівняння методів за заданими показниками та здійснювати вибір параметрів і форм подання операндів, що забезпечують максимальну швидкодію при реалізації обчислювальних операцій.

Визначені основні наукові результати є **новими**.

Теоретичне значення роботи полягає у розвитку теорій цифрової обробки сигналів і проектування комп'ютерних систем та компонентів, а саме – удосконаленні методів та архітектур апаратних засобів для виконання операцій у скінченних полях: додавання, віднімання, множення, піднесення до степеня, обчислення мультиплікативно оберненого елемента та ділення, що дозволяє значно підвищити продуктивність цих засобів.

Практичне значення отриманих результатів. Розроблено нові засоби методи і засоби підвищення швидкості виконання обчислювальних операцій арифметики скінченних полів.

Особливу практичну цінність мають наступні результати:

- Розроблений процесор Галуа на базі ПЛІС фірми *Xilinx*, що орієнтований на виконання операцій у скінченних полях виду $GF(p)$ та $GF(2^m)$ дозволяє ефективно реалізувати розв'язання задач завадостійкого кодування даних, цифрової обробки сигналів та захисту інформації.
- Структурні та схемотехнічні рішення блоків виконання обчислювальних операцій у скінченних полях виду $GF(p)$ та $GF(2^m)$ характеризуються низькою апаратною складністю та високою швидкістю обробки даних.
- Програмістська модель процесора Галуа дозволяє створювати програмне забезпечення довільної складності мовою Асемблера процесора Галуа.
- Програмний модуль для імітаційного та функціонального моделювання обчислювального процесу в процесорі Галуа дозволяє проводити дослідження розроблених методів виконання операцій у скінченних полях.
- Генератор *Verilog*-коду для синтезу на ПЛІС елемента *ROM*, що містить розріджену таблицю елементів поля $GF(2^m)$ у многочленному та степеневому їх поданні, дозволяє автоматично генерує *Verilog*-код за заданим незвідним многочленом та ступенем розрідження таблиці.
- Програмний інструментарій для моделювання та дослідження обчислювальних процесів у полях Галуа дозволяє обирати оптимальні параметри для кожного методу залежно від класу вхідних даних.

Методологічні й наукові результати дисертаційної роботи отримали використання в системи обробки та аналізу зображень для розпізнавання реєстраційних номерів транспортних засобів (ТОВ "Відео Інтернет Технології"). Акт про впровадження наведено у додатку до дисертації.

Обґрунтованість та достовірність отриманих результатів. Отримані результати є обґрунтованими та достовірними, що підтверджується значним обсягом здійснених досліджень, поданим фактичним матеріалом та його науковою інтерпретацією, практичним використанням запропонованих розробок та апробацією на наукових конференціях й семінарах.

У роботі коректно застосовано основні положення теорії чисел, вищої алгебри, дискретної математики, теорії обчислювальної складності алгоритмів, теорії скінченних алгебраїчних структур, комп'ютерного моделювання та схемотехнічного проектування.

Достовірність висновків та рекомендацій підкріплена результатами імітаційного моделювання, а також відповідними публікаціями.

Оцінюючи зміст дисертаційної роботи в цілому, слід відмітити її обґрунтованість та практичну спрямованість, внутрішню єдність матеріалу. У цілому поставлені у розглянутій дисертації завдання вирішені повністю. Здобувачем у дисертації отримані науково обґрунтовані результати, які в сукупності вирішують актуальну науково-прикладну проблему розроблення методів та архітектур апаратних засобів для реалізації високопродуктивних

обчислень на основі арифметики скінченних полів. Дисертаційна робота оформлена згідно вимог до кандидатських дисертацій.

Рекомендації щодо використання результатів. Отримані автором результати можуть бути використані при розробці нових і модифікації методів побудови спеціалізованих засобів на базі ПЛІС. Результати роботи доцільно використовувати в організаціях та на підприємствах, які займаються розробкою та експлуатацією спеціалізованих засобів на базі ПЛІС для апаратної реалізації високопродуктивних обчислень на основі арифметики скінченних полів. Їх доцільно також використовувати в навчальному процесі, зокрема при викладанні курсів, пов'язаних з розробкою спеціалізованих засобів та методами високорівневого проектування компонентів для цифрової обробки сигналів і зображень, завадостійкого кодування.

Повнота викладу результатів роботи в опублікованих працях. Основні результати дисертації з достатньою повнотою відображено у 6 наукових фахових виданнях (у тому числі 5 статях, що реферують міжнародними наукометричними базами даних) та 4 патентах на корисну модель. Результати апробовано на науково-технічних конференціях, що зафіксовано у 9 опублікованих тезах доповідей на наукових конференціях.

Аналіз внеску автора в публікації по питаннях, висвітлених в дисертації, показав, що внесок Оная М.В. ***є вирішальним***.

Автореферат повною мірою відображає зміст та основні положення дисертаційної роботи.

Недоліки дисертаційної роботи. Разом з тим дисертаційна робота має і ряд недоліків, серед яких необхідно відзначити наступні:

1. Матеріали дисертації перевантажені довідковою та добре відомою інформацією. Бажано було б перенести її до додатків, приділяючи більш уваги оригінальним питанням.
2. У матеріалах дисертації зазначено, що "… для скорочення таблиці може бути використана будь-яка математична функція, що має обернену…" (стор. 105), але в якості прикладу обрано функцію ділення на 3, що є недоцільним, оскільки в комп'ютерних системах використовуються двійкова система числення і було б доцільно обирати коефіцієнт розрідження такий, що дорівнює степені двійки.
3. Автором не доведена коректність отриманої оцінки кількості ітерацій при перетворенні з числового подання у степеневе (стор. 152).
4. На стор. 158 наведено коефіцієнт приросту швидкодії для операції піднесення до степеня залежно від обраного поля, але не вказано які саме відношення обчислюються для отримання цього коефіцієнта.
5. У ВИСНОВКАХ роботи не наведено порівняльні оцінки із відомими рішеннями.

Зроблені зауваження суттєво не знижують якість виконаних автором наукових досліджень.

Загальний висновок по дисертації. Дисертація є завершеною науково-дослідною роботою, у якій отримано розв'язання актуальної науково-прикладної задачі підвищення швидкості обчислень в скінченних полях за рахунок структурно-логічної оптимізації архітектур апаратних засобів, що реалізують процеси виконання операцій у полях Галуа.

Таким чином, за актуальністю, обсягом проведених та використаних досліджень, науковою новизною, практичною цінністю отриманих результатів та обґрунтованістю дисертаційна робота й автореферат відповідають вимогам до кандидатських дисертацій та п.п. 9, 11 «Порядку присудження наукових ступенів …..", затвердженого постановою Кабінету Міністрів України № 567 (зі змінами) від 24 липня 2013 р.", а її автор – **Онай Микола Володимирович** заслуговує на присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – Комп'ютерні системи та компоненти.

ОФІЦІЙНИЙ ОПОНЕНТ

Провідний науковий співробітник
відділу мікропроцесорної техніки
Інституту кібернетики
ім. В.М. Глушкова НАН України,
д.т.н., професор _____ **Опанасенко В.М.**