МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО"

**Онай Микола Володимирович**

УДК 004.31:004.27

# Методи та засоби підвищення ефективності реалізації обчислювальних операцій у скінченних полях

Спеціальність 05.13.05 – Комп'ютерні системи та компоненти

**Автореферат**
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2017

Дисертацією є рукопис.

Робота виконана на кафедрі програмного забезпечення комп'ютерних систем Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор
**Дичка Іван Андрійович,**
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", декан факультету прикладної математики

Офіційні опоненти: доктор технічних наук, професор
**Опанасенко Володимир Миколайович,**
Інститут кібернетики ім. В.М. Глушкова,
НАН України, провідний науковий співробітник відділу мікропроцесорної техніки;

доктор технічних наук, професор
**Гамаюн Володимир Петрович,**
Національний авіаційний університет Міністерства освіти і науки України, завідувач кафедри прикладної інформатики.

Захист дисертації відбудеться " " листопада 2017 р. о 14:30 на засіданні спеціалізованої вченої ради Д 26.002.02 в КПІ ім. Ігоря Сікорського за адресою: 03056, м. Київ, пр. Перемоги, 37, корп. 18, ауд. 516.

Відгуки на автореферат у двох примірниках, завірені печаткою установи, просимо надсилати за адресою: 03056, м. Київ, пр. Перемоги, 37, ученому секретарю КПІ ім. Ігоря Сікорського.

З дисертацією можна ознайомитись в бібліотеці КПІ ім. Ігоря Сікорського.

Автореферат розісланий " " жовтня 2017 р.

Учений секретар
спеціалізованої вченої ради Д 26.002.02,
кандидат технічних наук, доцент М.М. Орлова

# ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Сутність наукової задачі, яка вирішується у рамках дисертаційної роботи, полягає в забезпеченні підвищення швидкості виконання обчислень у полях Галуа виду $GF(p)$ і $GF(2^m)$ та оптимізації апаратних витрат порівняно з існуючими рішеннями. Запропоноване вирішення цієї задачі базується на удосконаленні існуючих та розробленні нових методів виконання операцій додавання, віднімання, піднесення до степеня, обчислення мультиплікативно оберненого елемента та ділення у скінченних полях виду $GF(p)$ та $GF(2^m)$; отриманні архітектурних рішень для реалізації запропонованих методів та моделюванні процесів виконання операцій в скінченних полях.

**Актуальність роботи.** Основи теорії скінченних полів були сформовані в дослідженнях таких видатних математиків: П’єра Ферма, Леонарда Ейлера, Адрієна-Марі Лежандра, Карла Фрідріха Гаусса. Особливо значний внесок у розвиток теорії належить Еварісту Галуа. Тому скінченні поля також називають полями Галуа.

До останньої чверті XX-го століття теорія скінченних полів розвивалась як галузь класичної математики. Але у зв’язку з потребами цифрової обробки сигналів, завадостійкого кодування та бурхливим розвитком криптографії в наш час активно розвиваються прикладні аспекти теорії скінченних полів.

Значний внесок у розвиток прикладних аспектів теорії скінченних полів та її застосування в спеціалізованих обчислювальних засобах зробили зарубіжні та вітчизняні вчені: Ніл Кобліц, Брюс Шнайєр, Жан-П’єр Дешам, Річард Крендалл, Карл Померанс, Венбо Мао, Четін Кая Коч, Гордон Бредлі, Дарел Хенкерсон, Альфред Менезес, Р. Лідл, Г. Нідеррайтер, О.Н. Василенко, А.О. Болотов, С.Б. Гашков, О.Б. Фролов, А.О. Часовських, О.Б. Маховенко, О.В. Черемушкін, В.П. Боюн, В.М. Опанасенко, В.П. Тарасенко, Я.М. Николайчук, І.А. Жуков, В.В. Яцків та інші.

Скінченні поля використовуються у завадостійкому кодуванні, цифровій обробці сигналів та криптографічних перетвореннях. У зазначених сферах застосування обробка даних відбувається в реальному часі, що зумовлює потребу у високій швидкодії.

Сфера застосування скінченних полів в галузі інформаційних технологій постійно розширюється. Наприклад, проводяться активні дослідження щодо ущільнення даних на основі логіко-статистичних інформаційних моделей та кодів Галуа, розроблено реляційні бази даних на основі двовимірних кодів поля Галуа, сигнальні коректувальні коди в базисі Галуа. Внаслідок стрімкого розвитку хмарних обчислень зростає загроза зламу шифрів, тому з кожним роком відповідно зростає рекомендована довжина ключа. Зростання довжини ключа експоненційно збільшує кількість операцій, необхідних для виконання криптографічних перетворень, тому актуальною задачею є прискорення обчислень в скінченних полях.

Таким чином, існує важлива науково-технічна задача розроблення методів та архітектур апаратних засобів для реалізації високопродуктивних обчислень

на основі арифметики скінченних полів.

**Зв'язок роботи з науковими програмами, планами, темами.** Дисертаційне дослідження виконувалось відповідно до планів НДР, програм і договорів, що виконувались в КПІ ім. Ігоря Сікорського:

- НДР “Розроблення та дослідження високоефективних архітектур спеціалізованих комп’ютерних систем для реалізації обчислень у скінченних полях” (номер державної реєстрації 0115U000319);
- НДР “Методи та засоби інформаційного забезпечення систем автоматизованого імпорту об’єктів на основі графічного кодування даних” (номер державної реєстрації 0112U003175).

**Мета і задачі дослідження.** Метою дисертаційної роботи є підвищення швидкості обчислень в скінченних полях за рахунок структурно-логічної оптимізації архітектур апаратних засобів, що реалізують процеси виконання операцій у скінченних полях.

Досягнення зазначеної мети передбачає вирішення таких задач:

- розробити методи високошвидкісного виконання операцій в полях Галуа виду $GF(p)$: додавання, віднімання, множення, ділення, піднесення до степеня, обчислення мультиплікативно оберненого елемента;
- синтезувати структури апаратних засобів для реалізації операцій арифметики скінченних полів, які б забезпечували більш високу швидкість обчислень порівняно з існуючими рішеннями;
- розробити методи апаратної реалізації операцій в полях Галуа виду $GF(2^m)$;
- розробити архітектуру та систему команд проблемно-орієнтованого процесора Галуа для виконання операцій у скінченних полях;
- розробити модель обчислювального процесу, що має місце при реалізації операцій у скінченних полях;
- створити засоби для моделювання та дослідження ефективності методів виконання операцій в полях Галуа.

*Об’єктом дослідження* є процеси обробки даних у скінченних полях.

*Предметом дослідження* є методи обчислень та засоби апаратної реалізації операцій у скінченних полях.

**Методи дослідження** базуються на використанні теорії чисел, вищої алгебри, дискретної математики, теорії обчислювальної складності алгоритмів, теорії скінченних алгебраїчних структур, комп’ютерного моделювання та схемотехнічного проектування.

**Наукова новизна одержаних результатів** полягає в розвитку методів та удосконаленні архітектур апаратних засобів для виконання операцій у скінченних полях: додавання, віднімання, множення, піднесення до степеня, обчислення мультиплікативно оберненого елемента та ділення.

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

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.

2. 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, яка дозволяє виконувати порівняння методів за заданими показниками та здійснювати вибір параметрів і форм подання операндів, що забезпечують максимальну швидкодію при реалізації обчислювальних операцій.

**Практичне значення одержаних результатів** полягає в розробці засобів підвищення швидкості виконання обчислювальних операцій арифметики скінченних полів. Зокрема, практичну цінність мають наступні результати.

1. Спроектовано на ПЛІС фірми *Xilinx* процесор Галуа, що орієнтований на виконання операцій у скінченних полях виду $GF(p)$ та $GF(2^m)$. Процесор Галуа можна застосувати для вирішення задач завадостійкого кодування даних, цифрової обробки сигналів та захисту інформації.
2. Побудовано програмістську модель процесора Галуа, яка дозволяє створювати програмне забезпечення довільної складності мовою Асемблера процесора Галуа.
3. Розроблено структурні та схемотехнічні рішення блоків виконання обчислювальних операцій у скінченних полях виду $GF(p)$ та $GF(2^m)$, які характеризуються низькою апаратною складністю та високою швидкістю обробки даних.
4. Розроблено програмний модуль для імітаційного та функціонального моделювання обчислювального процесу в процесорі Галуа, що дозволяє проводити дослідження розроблених методів виконання операцій у скінченних полях.
5. Створено генератор *Verilog*-коду для синтезу на ПЛІС елемента *ROM*, що містить розріджену таблицю елементів поля $GF(2^m)$ у многочленному та степеневому їх поданні, який автоматично генерує *Verilog*-код за заданим незвідним многочленом та ступенем розрідження таблиці.
6. Сформовано методичні рекомендації щодо використання новорозроблених методів виконання операцій у скінченних полях для їх застосування в галузі обробки сигналів, криптографічних перетворень та завадостійкого кодування.

7. Розроблено програмний інструментарій для моделювання та дослідження обчислювальних процесів у полях Галуа, що дозволяє обирати оптимальні параметри для кожного методу залежно від класу вхідних даних.

*Теоретичні та практичні результати дисертаційної роботи використано і впроваджено:*

- на Українському державному підприємстві поштового зв'язку "Укрпошта" при розробці технології цифрових поштових марок;
- на підприємстві ТОВ "Відео Інтернет Технології" при розробці системи обробки та аналізу зображень для розпізнавання реєстраційних номерів транспортних засобів;
- у навчальному процесі кафедри програмного забезпечення комп'ютерних систем КПІ ім. Ігоря Сікорського при проведенні лекційних та лабораторних занять з дисциплін "Теорія інформації та кодування", "Архітектура комп'ютера" та "Цифрова обробка сигналів і зображень", а також при підготовці магістерських робіт зі спеціальності "Інженерія програмного забезпечення".

**Особистий внесок здобувача** полягає в теоретичному обґрунтуванні одержаних результатів, їх експериментальній перевірці та дослідженні. Основні результати дисертаційного дослідження автором отримано самостійно. У публікаціях, написаних у співавторстві, здобувачеві належить: [1, 13-15, 21] – класифікація методів обчислення мультиплікативно оберненого елемента, удосконалення модифікації Бредлі розширеного алгоритму Евкліда та методика проведення експериментального дослідження; [2] – модифікований метод піднесення до степеня в адитивній групі; [3, 17, 19] – метод високошвидкісного виконання адитивних та мультиплікативних операцій над елементами поля $GF(2^m)$ та спосіб перетворення числового подання елементів поля $GF(2^m)$ у степеневе і навпаки, що орієнтований на апаратну реалізацію на ПЛІС; [4] – спосіб ділення многочленів з остачею у скінченному полі; [5, 8] – визначення місця теорії скінченних полів при графічному кодуванні даних та архітектура апаратних засобів для реалізації обчислень в полях Галуа; [6] – система команд спеціалізованого процесора, що орієнтований на арифметику скінченних полів; [7] – схеми функціональних блоків спеціалізованої комп'ютерної системи для високошвидкісного виконання операцій у скінченних полях; [9] – архітектура апаратних засобів для реалізації операції обчислення мультиплікативно оберненого елемента в основному скінченному полі; [10, 18, 20] – архітектура пристрою для виконання обчислень у полях виду $GF(2^m)$, орієнтована на ПЛІС; [11] – спосіб виконання підсумовування елементів поля $GF(p^m)$; [12] – функціональна схема суматора за модулем простого числа; [16] – модифікація розширеного алгоритму Лемера обчислення мультиплікативно оберненого елемента в полі $GF(p)$.

**Апробація результатів дисертації.** Основні результати дисертації доповідались, обговорювались та отримали позитивну оцінку на наступних конференціях: Міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", м. Кіровоград, 2016; Міжнародна науково-практична

конференція “Методи та засоби кодування, захисту й ущільнення інформації”, м. Вінниця, 2013, 2016; Наукова конференція магістрантів та аспірантів “Прикладна математика та комп’ютинг – ПМК”, м. Київ, 2009, 2010, 2014, 2016; Міжнародна науково-практична конференція “Проблеми інформатики та комп’ютерної техніки”, м. Чернівці, 2013, 2014, 2015; Міжнародна наукова конференція імені академіка Михайла Кравчука, м. Київ, 2012, 2014, 2015; Міжнародна науково-практична конференція “Інформаційні технології та комп’ютерна інженерія”, м. Івано-Франківськ, 2014, 2015; Всеукраїнська науково-практична конференція молодих учених та студентів, м. Хмельницький, 2015; Міжнародна студентська наукова конференція з прикладної математики та інформатики СНКПМІ, м. Львів, 2012, 2013; Всеукраїнська WEB-конференція аспірантів, студентів та молодих вчених, м. Кривий Ріг, 2013; Міжнародна науково-технічна конференція “Радіотехнічні поля, сигнали, апарати та системи”, м. Київ, 2013; Всеукраїнська науково-практична конференція “Інформатика та системні науки (ІСН-2013)”, м. Полтава, 2013.

**Публікації.** За матеріалами дисертації опубліковано 21 друковану працю, серед яких 8 статей (з них одна стаття у закордонному науковому виданні, що входить до наукометричної бази даних Scopus, одна стаття у фаховому науковому виданні України, що входить до наукометричної бази даних Web of Science, одна стаття у фаховому науковому виданні України, що входить до наукометричної бази даних Index Copernicus, дві статті у фаховому науковому виданні України, що входить до наукометричної бази даних EBSCO), 4 державні патенти України на корисну модель, а також 9 тез доповідей на наукових конференціях.

**Структура та обсяг дисертації.** Дисертація складається зі вступу, п’яти розділів, висновків та додатків (339 с.). Основний зміст дисертаційної роботи викладений на 168 сторінках. Дисертація містить 101 рисунок, 29 таблиць та 143 посилання на літературні джерела.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

**У вступі** 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.

**У першому розділі** на основі аналізу літературних джерел розкрито стан проблеми, пов’язаної з необхідністю удосконалення методів апаратної реалізації операцій у скінченних полях.

Досліджено сучасний стан проблеми високоефективних обчислень у скінченних полях у світі та Україні. Розглянуто існуючі підходи до розв’язання проблеми, виявлено їх переваги та недоліки.

Проаналізовано методи редукції за довільним модулем та методи цілочисельного ділення з остачею, починаючи з методу, що був запропонований Евк-

лідом, і закінчуючи сучасними методами, що використовуються в процесорах загального призначення.

Розглянуто методи додавання, віднімання та множення елементів поля $GF(p)$, де $p$ – характеристика поля (просте число).

Виконано класифікацію методів обчислення мультиплікативно оберненого елемента в скінченних полях (рис. 1). Докладно проаналізовано методи, що ґрунтуються на модулярному піднесенні до степеня, та методи, що ґрунтуються на знаходженні найбільшого спільного дільника (НСД) двох чисел (рис. 2). Встановлено, що менш обчислювально витратними є методи, що ґрунтуються на знаходженні НСД двох чисел.


Рис. 1. Класифікація методів обчислення мультиплікативно оберненого елемента

Досліджено та класифіковано методи модулярного піднесення до степеня, а саме: методи, що ґрунтуються на поданні показника степеня у двійковій системі числення та аналізі бітів показника степеня як по одному, так і по кілька бітів за одну ітерацію роботи алгоритму; методи, що ґрунтуються на поданні показника степеня у симетричній трійковій системі числення (*Non Adjacent Form*); методи, що грунтуються на поданні показника степеня в системі числення з мультиосновою.

З’ясовано, що існуючі на даний час рішення щодо апаратної реалізації операцій над елементами скінченних полів акцентуються на вирішенні окремо взятих операцій та не є адаптованими до їх реалізації на ПЛІС.

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.

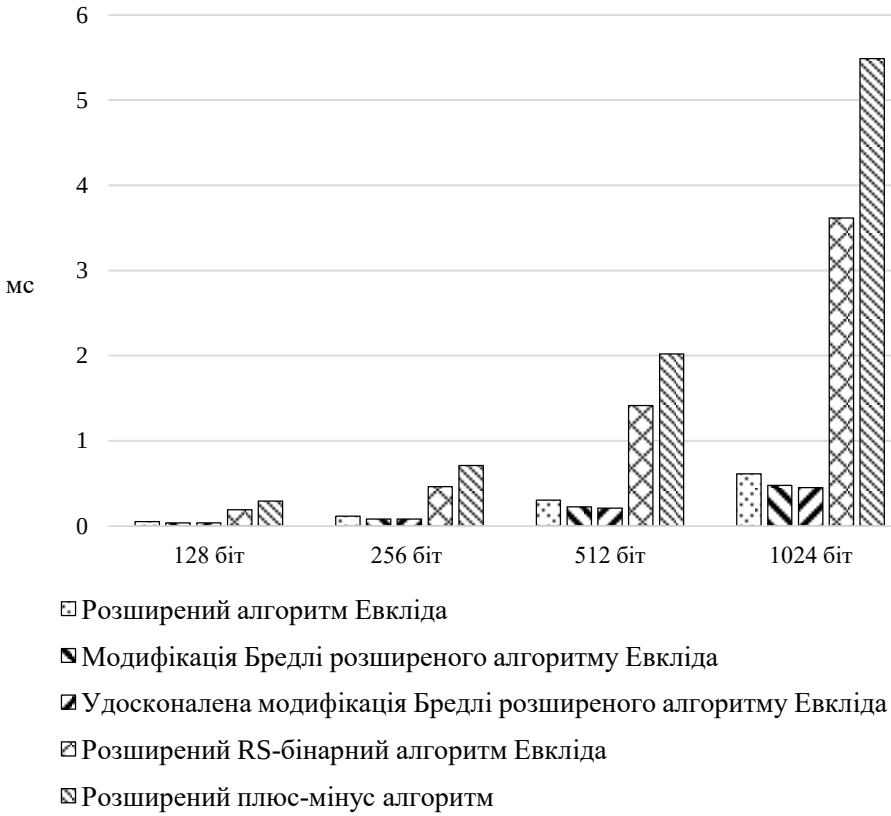


Рис. 2. Час роботи алгоритмів обчислення мультиплікативно оберненого елемента залежно від довжини операндів, мс

Проаналізовано класи задач, що мають місце в галузі криптографії, завадостійкого кодування та цифрової обробки сигналів. Зокрема, показано необхідність побудови нового високошвидкісного методу виконання операцій над елементами поля $GF(2^m)$ в задачах завадостійкого кодування. Наприклад, навіть при кодуванні (операція, яка є менш обчислювально витратною, ніж декодування) за допомогою універсальних обчислювальних засобів, для $m = 10$ при кількості контрольних розрядів $r = 512$ для коду Ріда-Соломона час кодування (табл. 1) складає понад 45 хвилин (2648425 мс), де $2^m$ – потужність поля.

Таблиця 1

Час кодування (мс) для коду Ріда-Соломона

| $m$ | $r = 0.1 \cdot 2^m$ | $r = 0.25 \cdot 2^m$ | $r = 0.5 \cdot 2^m$ |
|---|---|---|---|
| 9 | 474 | 13062 | 176721 |
| 10 | 5470 | 175290 | 2648425 |
| 11 | 75228 | 2537681 | |
| 12 | 1191844 | | |

На основі аналізу класів задач, що мають місце в галузі криптографії, завадостійкого кодування та цифрової обробки сигналів, встановлено, що можливі два підходи до створення обчислювальних засобів для реалізації обчислень в полях Галуа: побудова спеціалізованих комп'ютерних систем та побудова проблемно-орієнтованих процесорів.

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

Запропоновано модифікований спосіб схемотехнічної реалізації цілочисельного ділення.

Запропонований спосіб має меншу обчислювальну складність, ніж класичний, коли виконується нерівність

$$n + 2s + 3\tilde{k} - 3\tilde{n} - 3 > 0,$$

де $\tilde{n}$ – кількість двійкових розрядів діленого, $\tilde{k}$ – кількість двійкових розрядів модуля, $n$ – розрядність регістра діленого, $k$ – розрядність регістра модуля, $s$ – мінімально можлива різниця бітової довжини операндів.

Запропоновано модифікацію *SRT*-алгоритму та встановлено, що кількість тактів процесора при застосуванні модифікованого *SRT*-алгоритму оцінюється таким чином:

- якщо $k - \tilde{k} \geq n - \tilde{n}$, то кількість тактів дорівнює $\tilde{n} + 2k - 3\tilde{k} + 1$;
- якщо $k - \tilde{k} < n - \tilde{n}$, то кількість тактів дорівнює $n + k - 2\tilde{k} + 1$.

Узагальнено метод піднесення до степеня в полі $GF(p)$ з поданням показника степеня в системі числення з мультиосновою, що дозволяє, залежно від вхідних даних, знаходити оптимальні значення параметрів наступного подання показника степеня

$$k = \sum_{i=1}^{l} s_i \prod_{j=1}^{n} d_j^{c_{ij}},$$

де $d_j \in D$, $c_{ij}$ – цілі додатні числа, $s_i \in S$. Допустимими елементами множини $D$ є цілі додатні числа, а множини $S$ – цілі числа.

Проведений 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.

Внаслідок вивчення стану проблеми високоефективних обчислень у скінченних полях виду $GF(2^m)$ встановлено, що скінченним полям властивий ізоморфізм – елементи поля допускають 4 подання: цілочислове, степеневе, векторне, многочленне. Всі 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 векторним (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. Однак, степеневе подання елементів поля $GF(2^m)$ має істотний недолік – воно не дозволяє отримувати нульовий елемент поля. Тому 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.

Аналіз можливих операцій над елементами поля $GF(2^m)$ показав, 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 $2^m-1$ (рис. 3).

Мікрооперація додавання за модулем $2^m-1$ виконується наступним чином:

$$(a+b)\bmod\left(2^m-1\right)=\begin{cases} z, & \textit{якщо } z<2^m-1\,(c=0);\\ z+1, & \textit{якщо } z=2^m-1\,(c=0);\\ z+1, & \textit{якщо } z>2^m-1\,(c=1), \end{cases}$$

де $z$ – значущі розряди результату підсумовування операндів $a$ та $b$ на комбінаційному суматорі, $c$ – значення переносу за межі старшого розряду результату.

Нехай $w=a+\bar{b}$. Тоді мікрооперація віднімання за модулем $2^m-1$ виконується таким чином:

$$(a-b)\bmod\left(2^m-1\right)=\begin{cases} w+1, & \textit{якщо } a=b\,(c=0);\\ w+1, & \textit{якщо } a>b\,(c=1);\\ w, & \textit{якщо } a<b\,(c=0). \end{cases}$$

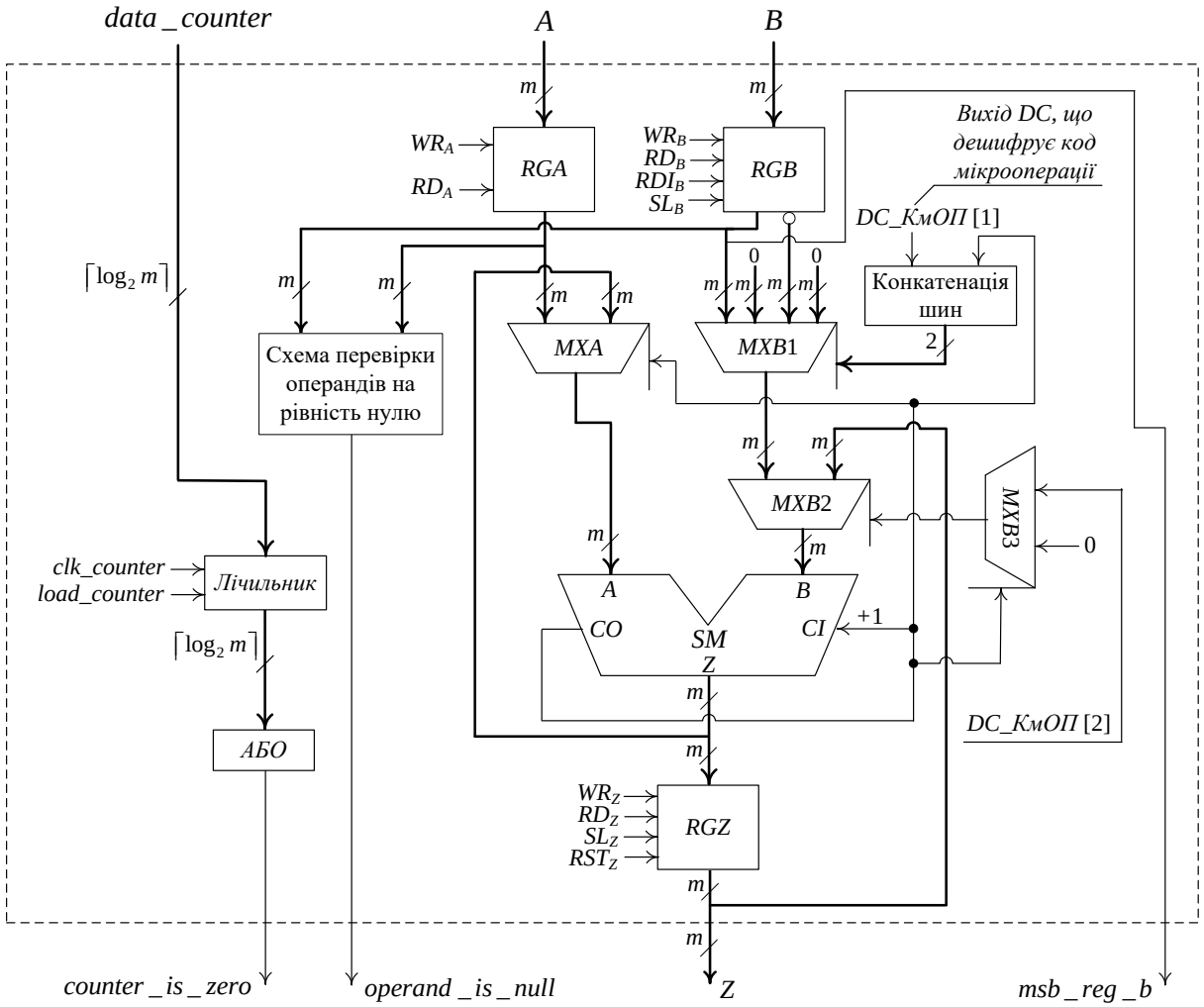


Рис. 3. Функціональна схема операційного автомата блока виконання мікрооперацій за модулем $2^m - 1$

Алгоритм виконання мікрооперації множення операндів $a$, $b$ за модулем $2^m - 1$:

1. Встановити $Z := 0$.
2. Якщо $b_{m-1} = 1$, то $Z := \left((Z + a) \cdot 2\right) \bmod \left(2^m - 1\right)$ і $b := b \cdot 2$; інакше $Z := \left(Z \cdot 2\right) \bmod \left(2^m - 1\right)$ і $b := b \cdot 2$, де $b_{m-1}$ – старший розряд множника $b$.
3. П. 2 повторити $m - 2$ рази.
4. Якщо $b_{m-1} = 1$, то $Z := \left(Z + a\right) \bmod \left(2^m - 1\right)$.

У багатьох практичних застосуваннях, пов’язаних з цифровою обробкою сигналів та завадостійким кодуванням даних, потужність поля (кількість елементів) не перевищує $2^{12} - 2^{20}$. За таких обставин найдоцільніше застосовувати табличний спосіб перетворення елементів поля з однієї форми подання в іншу. Тоді при степеневому поданні елементів у пам’яті комп’ютера достатньо збері-

гати лише показник степеня – невід'ємний або від'ємний (один з них), а при числовому – двійкові коди елементів.

Для забезпечення ізоморфізму поля необхідно використовувати таблицю елементів поля у многочленному та степеневому їх поданні (рис. 4).

| адреса | невід'ємний показник степеня примітивного елемента | числове значення |
|---|---|---|

Рис. 4. Структура таблиці елементів поля $GF(2^m)$

Така структура таблиці забезпечує перетворення як числового подання елементів поля у степеневе, так і степеневого – у числове. Розмірність таблиці $2^m \times 2m$.

Розроблено програмне забезпечення для побудови файлу, за допомогою якого ініціалізується *ROM* блока виконання операцій над елементами поля $GF(2^m)$. Експериментальні результати показали, що за допомогою розробленого програмного забезпечення за прийнятний час можливо побудувати таблиці для ініціалізації *ROM* до значення $m = 20$ включно. Для значення $m = 20$ необхідна пам'ять до 5.5 Мб.

Для значень $m \geq 11$ запропоновано метод виконання операцій з використанням розрідженої таблиці елементів поля. 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. Дослідження показали, що оптимальним є запис кожного $k$-го елемента поля в *ROM*; в такому випадку ступінь розрідження таблиці дорівнює $k$. Наприклад, для значення $m = 15$ оптимальним ступенем розрідження таблиці є значення $k = 8$.

Розроблено 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 (алгоритми 1-3).

Швидкість виконання операцій можна характеризувати кількістю звертань до пам'яті (таблиці). Так, наприклад, операції додавання і віднімання виконуються з високою швидкістю, оскільки не потребують звертання до пам'яті (таблиці), при цьому виконується лише порозрядне підсумовування за модулем два; операції множення і ділення елементів поля потребують 3 звертання до пам'яті; операція обчислення мультиплікативно оберненого елемента – 2 звертання.

Розроблений блок (рис. 5) виконання операцій над елементами поля $GF(2^m)$ 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).

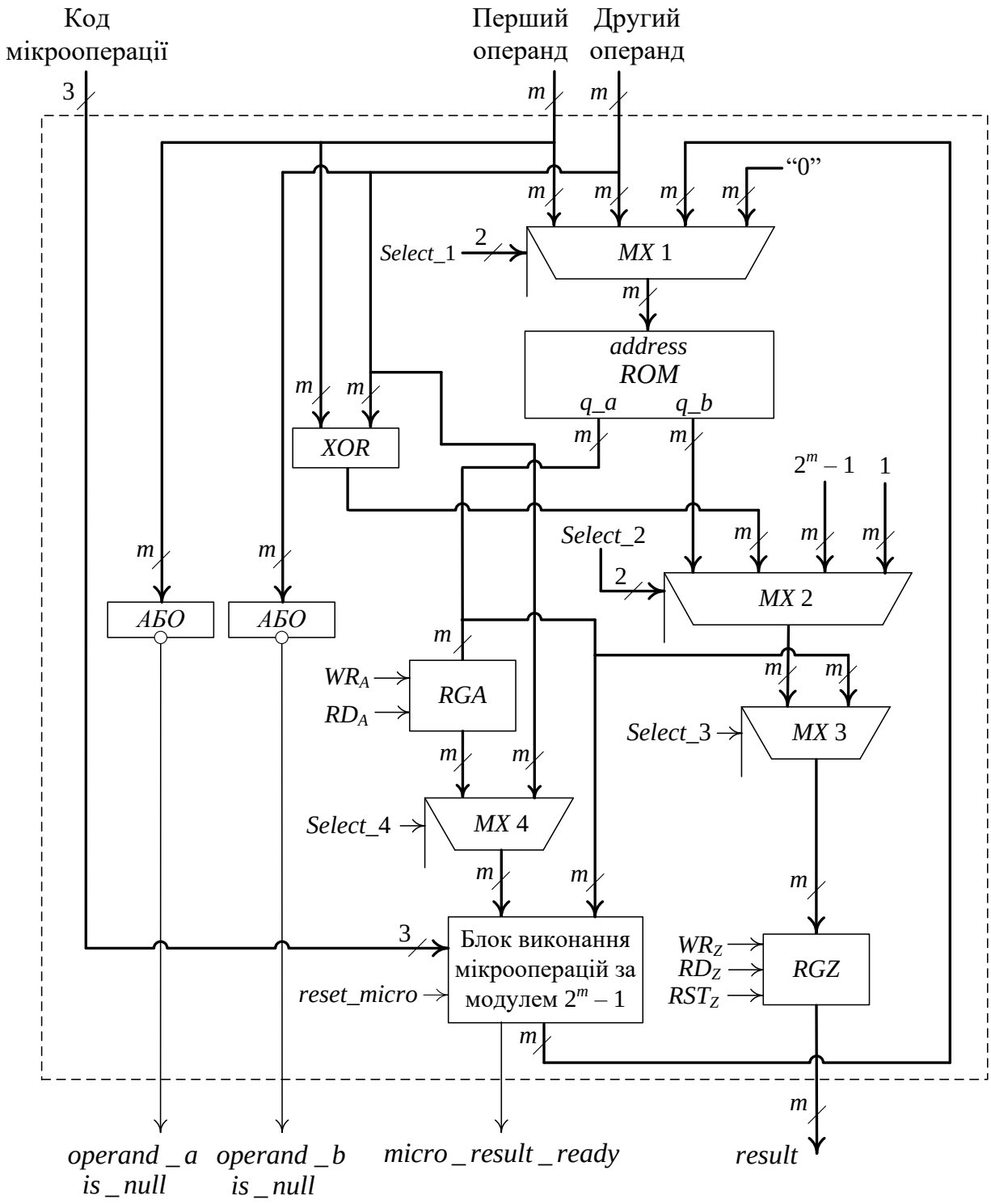


Рис. 5. Функціональна схема операційного автомата блока виконання операцій у полі $GF(2^m)$

Блок виконання операцій над елементами поля $GF(2^m)$ реалізовано таким чином, що на вхід завжди надходить многочленне подання елементів поля та отриманий результат на виході блока виконання операцій над елементами поля $GF(2^m)$ також поданий у многочленному поданні.

Алгоритм 1. Перетворення степеневого подання у многочленне з використанням розрідженої таблиці

Вхід: $table\left[\left\lfloor \frac{2^m}{k} \right\rfloor \text{ x } 2\right], ir\,[1 \text{ x } m],\ pow \in \mathbb{N}, k \in \mathbb{N}$

Вихід: $res\,[1 \text{ x } m]$

1. $adr \leftarrow \left\lfloor \frac{pow}{k} \right\rfloor; c \leftarrow \left\{ \frac{pow}{k} \right\}$
2. *if* $\left( c < k - c \ \ OR \ \ adr = \frac{2^m}{k} \right)$
   2.1. $res \leftarrow table\,[adr, 2]$ { $res$ – *многочлен* }
   2.2. $j \leftarrow 0$
   2.3. *while* $\left( j < c \right)$
      2.3.1. *while* $\left( \deg(res) < m \ \text{ and } \ j < c \right)$
         *a*) $res \leftarrow res \cdot x$ { $x$ – *одночлен* }
         *b*) $j \leftarrow j + 1$
      2.3.2. *end while*
      2.3.3. *if* $\left( \deg(res) \geq m \right)$
         *a*) $res \leftarrow res + ir$
      2.3.4. *end if*
   2.4. *end while*
3. *else*
   3.1. $adr \leftarrow adr + 1$
   3.2. $c \leftarrow k - c$
   3.3. $res \leftarrow table\,[adr, 2]$ { $res$ – *многочлен* }
   3.4. $j \leftarrow 0$
   3.5. *while* $\left( j < c \right)$
      3.5.1. *if* $\left( res\,[0] == 1 \right)$
         *a*) $res \leftarrow res + ir$
      3.5.2. *end if*
      3.5.3. *while* $\left( res\,[0] == 0 \ \text{ and } \ j < c \right)$
         *a*) $res \leftarrow res \,/\, x$ { $x$ – *одночлен* }
         *b*) $j \leftarrow j + 1$
      3.5.4. *end while*
   3.6. *end while*
4. *end if*
5. *return* $res$

Алгоритм 2. Перетворення многочленного подання у степеневе з пошуком базового елемента у верхній частині розрідженої таблиці

Вхід: $table\,[2^m \text{ x } 2], pol, ir\,[1 \text{ x } m], k \in \mathbb{N}$

Вихід: $res \in \mathbb{N}$

1. $dec \leftarrow Bin2Dec(pol)$
2. $count \leftarrow 0$
3. *while* $\left( \left\{ \frac{dec}{k} \right\} \neq 0 \right)$
   3.1. *if* $\left( \left\{ \frac{dec}{2} \right\} \neq 0 \right)$
      3.1.1. $pol \leftarrow pol + ir$
      3.1.2. $pol \leftarrow pol \,/\, x$
      3.1.3. $dec \leftarrow Bin2Dec(pol)$
      3.1.4. $count \leftarrow count + 1$
   3.2. *end if*
   3.3. *while* $\left( \left\{ \frac{dec}{k} \right\} \neq 0 \ \text{ and } \ \left\{ \frac{dec}{2} \right\} == 0 \right)$
      3.3.1. $pol \leftarrow pol \,/\, x$
      3.3.2. $dec \leftarrow Bin2Dec(pol)$
      3.3.3. $count \leftarrow count + 1$
   3.4. *end while*
4. *end while*
5. $dec \leftarrow dec \,/\, k$
6. *return* $table\,[dec, 1] + count$

Алгоритм 3. Перетворення многочленного подання у степеневе з пошуком базового елемента в нижній частині розрідженої таблиці

Вхід: $table[\,2^m \text{ x } 2],\ pol, ir\,[1 \text{ x } m],\ k \in \mathbb{N}$

Вихід: $res \in \mathbb{N}$

1. $dec \leftarrow Bin2Dec(pol)$
2. $count \leftarrow 0$
3. *while* $\left(\left\{\frac{dec}{k}\right\} \neq 0\right)$
   - 3.1. *while* $\left(\left\{\frac{dec}{k}\right\} \neq 0 \text{ and } \deg(pol) < m\right)$
     - 3.1.1. $pol \leftarrow pol \cdot x$
     - 3.1.2. $dec \leftarrow Bin2Dec(pol)$
     - 3.1.3. $count \leftarrow count + 1$
   - 3.2. *end while*
   - 3.3. *if* $(\deg(pol) = m)$
     - 3.3.1. $pol \leftarrow pol + ir$
     - 3.3.2. $dec \leftarrow Bin2Dec(pol)$
   - 3.4. *end if*
4. *end while*
5. $dec \leftarrow dec / k$
6. *return* $table[dec, 1] - count$

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

Етапами розроблення *G*-процесора є: проектування системи команд (Асемблера); розроблення компілятора для перетворення асемблерного коду в машинний код; синтез апаратної частини процесора.

Запропонована система команд дозволяє створювати програми довільної складності мовою Асемблера процесора Галуа з подальшим виконанням цих програм функціональними блоками процесора.

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*).

Два найбільш доцільних способи реалізації процесора Галуа полягають у наступному: реалізувати на ПЛІС та реалізувати як спеціалізований співпроцесор. В першому випадку процесор Галуа можна реалізувати на ПЛІС та використовувати як зовнішній пристрій по відношенню до центрального процесора.

При реалізації процесора Галуа як співпроцесора по відношенню до *CPU* необхідно в систему команд центрального процесора ввести спеціальні команди для виконання операцій у полі Галуа. При отриманні такої команди центральний процесор передає її на виконання співпроцесору Галуа. Наслідком цього є зростання продуктивності та ефективності обробки інформації.

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.

На рис. 6-8 показано порівняння методів виконання різних операцій над елементами поля $GF(2^m)$ за кількістю елементарних операцій $Q$ (операцій зсуву та порозрядного додавання). Для запропонованого методу обрано ступінь розрідження таблиці $k = 8$.

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.

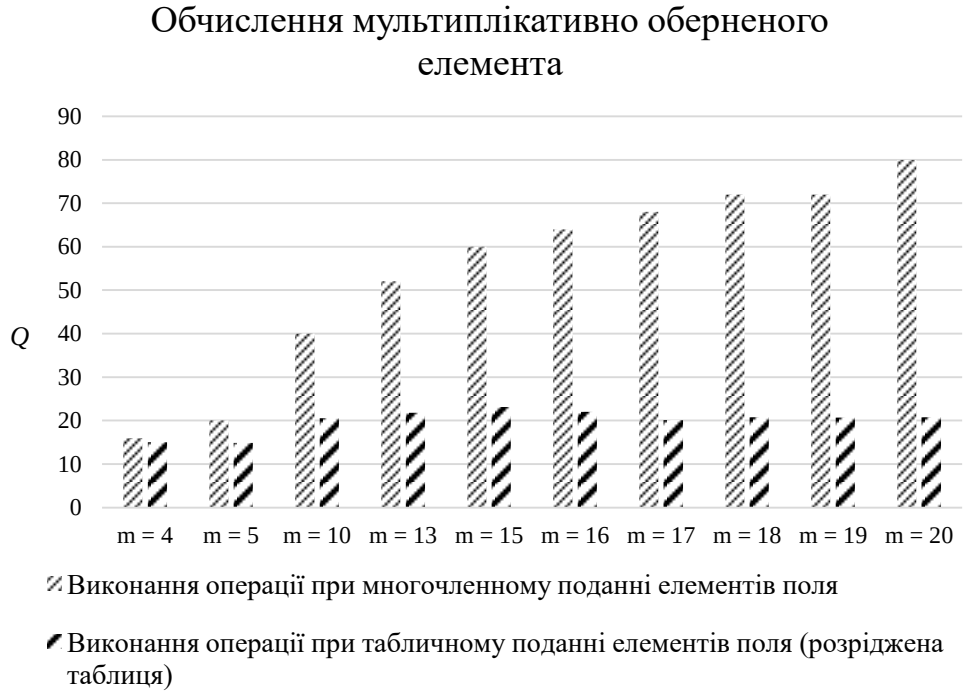


Рис. 6. Кількість елементарних операцій при обчисленні мультиплікативно оберненого елемента поля $GF(2^m)$

Порівнюючи обчислювальну складність виконання операції піднесення до степеня методом, що ґрунтується на використанні многочленного подання елементів поля $GF(2^m)$, та запропонованим методом коефіцієнт приросту швидкодії (відношення кількості елементарних операцій) залежно від потужності поля

зростає як показано на рис. 9 (для розробленого методу обрано ступінь розрідження 16).


Рис. 7. Кількість елементарних операцій при множенні елементів поля $GF(2^m)$

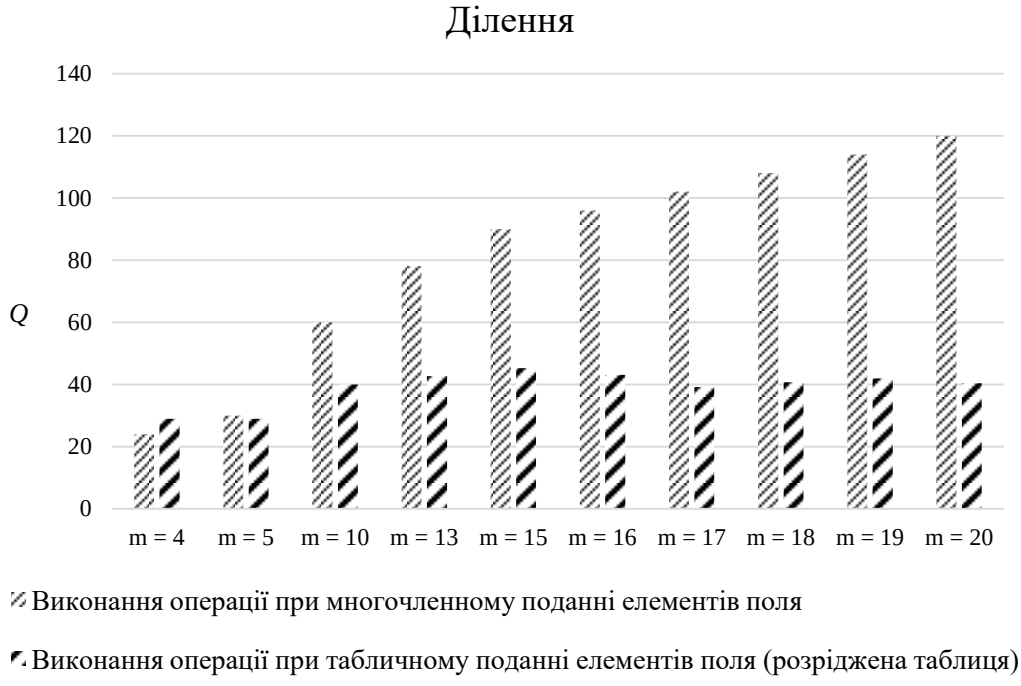


Рис. 8. Кількість елементарних операцій при діленні елементів поля $GF(2^m)$

Таким чином, оптимальним ступенем розрідження таблиці є значення $k = 8$, що забезпечує в середньому приріст швидкодії на 15% порівняно із використанням поліноміального базису.

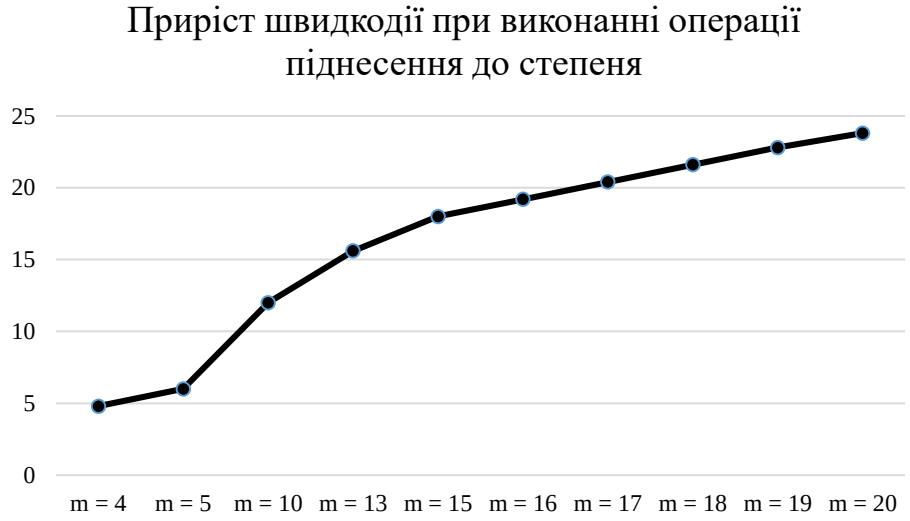


Рис. 9. Коефіцієнт приросту швидкодії виконання операції піднесення до степеня елементів поля $GF(2^m)$

**У додатках** наведено приклади програм мовою Асемблера процесора Галуа, інструкція з експлуатації інтегрованого середовища розробки "Асемблер Галуа", список повідомлень компілятора при трансляції тексту програми у машинний код, текст програми реалізації процесора Галуа мовою *Verilog* при застосуванні ПЛІС *Xilinx*, алгоритми реалізації методів виконання операцій у скінченних полях, приклади роботи алгоритмів реалізації методів виконання операцій у скінченних полях, схеми алгоритмів роботи керуючих автоматів складових частин процесора Галуа, формати команд процесора Галуа.

## ВИСНОВКИ

У дисертаційній роботі вирішено актуальну науково-прикладну задачу – підвищення продуктивності систем цифрової обробки даних, забезпечення завадостійкості зберігання і передачі даних та криптографічних перетворень за рахунок створення ефективних технічних засобів для виконання обчислень у скінченних полях шляхом структурно-логічної оптимізації архітектур апаратних засобів, що реалізують процеси виконання операцій у полях Галуа. При цьому отримано такі теоретичні та практичні результати.

1. На основі проведеного аналізу, з урахуванням виділених пріоритетних ознак, виконано класифікацію методів виконання найбільш обчислювально витратних операцій у скінченних полях, а саме: обчислення мультиплікативно оберненого елемента та піднесення до степеня, що дало

можливість провести ґрунтовне дослідження та сформувати напрямки розвитку зазначених методів.

2. Запропоновано метод високошвидкісного виконання адитивних та мультиплікативних операцій над елементами поля $GF(2^m)$ та відповідні структури апаратних засобів для його реалізації, що характеризуються універсальністю. Дослідження показали, що за рахунок табличного зберігання елементів поля у многочленному та степеневому їх поданні забезпечується максимальна швидкодія та універсальність арифметико-логічного пристрою. При використанні операндів великої розрядності запропоновано розріджене формування таблиці елементів поля, що дозволяє у кілька разів скоротити витрати пам'яті для її зберігання. Розроблений метод забезпечує зростання швидкодії в середньому на 15% порівняно з існуючим методом.
3. Розроблено модифікацію методу піднесення до степеня елементів поля $GF(p)$ з ковзним вікном та відповідні структури апаратних засобів для його реалізації. Відмінність від існуючих методів полягає в тому, що при формуванні таблиці передобчислень використовуються показники степеня, що є простими числами. Для досягнення високої швидкодії при побудові таблиці передобчислень рекомендовано використовувати заздалегідь обчислені адитивні ланцюжки з метою мінімізації кількості операцій множення, що дозволяє отримувати кожен наступний елемент таблиці за одну-дві операції модулярного множення. За допомогою розробленої моделі обчислювального процесу встановлено, що запропонована модифікація методу піднесення до степеня елементів поля $GF(p)$ з ковзним вікном забезпечує приріст швидкодії на 7-9%. Модифікацію методу піднесення до степеня елементів поля $GF(p)$ з ковзним вікном можна застосовувати в еліптичній криптографії для поліпшення часових характеристик операції скалярного множення точки еліптичної кривої на число.
4. Розроблено модель обчислювального процесу при виконанні операцій у скінченних полях, яка дозволяє на основі заданих наборів вхідних даних виконувати порівняння методів та здійснювати оптимальний вибір параметрів і форм подання операндів, що забезпечує зростання швидкодії при реалізації обчислювальних операцій на ПЛІС. На основі запропонованої моделі розроблено методики дослідження нових способів апаратної реалізації обчислень у полях Галуа. Моделювання у середовищі розробки *Xilinx ISE* та за допомогою програми *Mentor Graphics Precision* показало, що розроблені структури апаратних засобів характеризуються мінімальною апаратною складністю та високою швидкодією.
5. Дістала подальший розвиток теорія обчислень у скінченних полях, яка характеризується спрямованістю на апаратну реалізацію операцій, високою функціональністю архітектурних рішень на основі ПЛІС та дозволяє сформувати інструментально забезпечене обчислювальне сере-

довище, пристосоване до організації високоефективних обчислень у скінченних полях, зокрема з використанням ПЛІС фірми Xilinx.

6. Розроблено архітектуру та систему команд спеціалізованого процесора Галуа, орієнтованого на виконання операцій у скінченних полях, який забезпечує зростання продуктивності обчислень на 27% порівняно з універсальними обчислювальними засобами. Процесор Галуа можна використовувати в універсальній обчислювальній системі як співпроцесор, доповнюючи систему команд центрального процесора, або як спецобчислювач на основі ПЛІС, який порівняно з універсальними обчислювальними засобами підвищує продуктивність обробки інформації в реальному часі. Особливістю архітектури розробленого процесора є те, що не змінюючи інтерфейсу процесора, шляхом зміни арифметико-логічного пристрою можна здійснити перехід до поля Галуа $GF(p)$ або до $GF(2^m)$.
7. Отримані в роботі результати дозволяють на практиці підвищити продуктивність систем захисту інформації, систем цифрової обробки сигналів та завадостійкого кодування даних.

## СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ


1. Zhengbing Hu The Analysis and Investigation of Multiplicative Inverse Searching Methods in the Ring of Integers Modulo M [Text] / Zhengbing Hu, I. A. Dychka, Onai Mykola, Bartkoviak Andrii // International Journal of Intelligent Systems and Applications (IJISA), 2016. – Vol. 8, No. 11. – P. 9-18. – *Здобувачем запропонована класифікація методів обчислення мультиплікативно оберненого елемента, удосконалення модифікації Бредлі розширеного алгоритму Евкліда.* (Входить до міжнародної наукометричної бази даних SCOPUS).
2. Дичка, І.А. Модифікований віконний метод однократного множення точки еліптичної кривої на скаляр у полі $GF(p)$ [Текст] / І.А. Дичка, М.В. Онай, Т.П. Дрозда // Радіоелектроніка, інформатика, управління. – Запоріжжя. – 2016. – №2. – С. 95-102. – *Здобувачем запропонована модифікований метод піднесення до степеня в адитивній групі.* (Входить до міжнародної наукометричної бази даних Web of Science).
3. Дичка, І.А. Апаратна реалізація обчислень у скінченних полях характеристики два [Текст] / І.А. Дичка, М.В. Онай, Ю.В. Бухтіяров // Наукові вісті НТУУ “КПІ”. – 2013. – №6. – С. 20-27. – *Здобувачем запропоновано спосіб перетворення числового подання елементів поля $GF(2^m)$ у степеневе і навпаки, що орієнтований на апаратну реалізацію на ПЛІС.* (Входить до міжнародної наукометричної бази даних EBSCO).
4. Дичка, І.А. Апаратна реалізація процедур множення і ділення многочленів у скінченних полях [Текст] / І.А. Дичка, В.І. Голуб, М.В. Онай // Наукові вісті НТУУ “КПІ”. – 2012. – №5. – С. 61-66. – *Здобувачем запропоновано спосіб ділення многочленів з остачею у скінченному полі.* (Входить до між-

народної наукометричної бази даних EBSCO).

5. Дичка, І.А. Апаратна реалізація операторів та функцій в полях Галуа [Текст] / І.А. Дичка, М.В. Онай, О.В. Ващілін // Вісник Хмельницького національного університету. – 2012. – Вип. 5. – С. 234-240. – *Здобувачем запропоновано архітектуру апаратних засобів для реалізації обчислень в полях Галуа.* (Входить до міжнародної наукометричної бази даних Index Copernicus).
6. Дичка, І.А. Архітектура проблемно-орієнтованого процесора для реалізації арифметики скінченних полів [Текст] / І.А. Дичка, М.В. Онай, О.В. Ващілін // Вісник Східноукраїнського національного університету ім. В. Даля. – 2012. – №12 (183), ч.2. – С. 99-106. – *Здобувачем запропонована система команд спеціалізованого процесора, що орієнтований на арифметику скінченних полів.*
7. Дичка, І.А. Організація спеціалізованих комп'ютерних систем для реалізації обчислень у скінченних полях [Текст] / І.А. Дичка, В.І. Голуб, М.В. Онай // Вісник Східноукраїнського національного університету ім. В. Даля. – 2012. – №6 (177). – С. 268-278. – *Здобувачем запропоновано схеми функціональних блоків спеціалізованої комп'ютерної системи для високошвидкісного виконання операцій у скінченних полях.*
8. Дичка, І.А. Подання інформації у графічно-кодованому вигляді: технологія кодування та декодування [Текст] / І.А. Дичка, М.В. Онай, М.В. Новосад // Реєстрація, зберігання і обробка даних (Data Recording, Storage & Processing). – 2010. – Т. 12, №2. – С. 69-80. – *Здобувачем визначено місце теорії скінченних полів при графічному кодуванні даних.*
9. Державний патент України №111351, МПК G06F 7/00, G06F 7/50. Схема для пошуку мультиплікативно оберненого елемента за довільним модулем [Текст] / Дичка І.А., Онай М.В., Приходько Е.В.; заявник та патентовласник Дичка І.А., Онай М.В., Приходько Е.В. – № u201604179; дата подання заявки 15.04.2016; дата публ. 10.11.2016, бюл. №21, 2016 р. – 7 с. – *Здобувачем запропоновано архітектуру апаратної реалізації операції обчислення мультиплікативно оберненого елемента у основному скінченному полі.*
10. Державний патент України №73309, МПК G06F 7/50. Пристрій для виконання обчислень в полі $GF(2^n)$ [Текст] / Дичка І.А., Онай М.В. ; заявник та патентовласник Національний технічний університет України "Київський політехнічний інститут". – № u201115679; дата подання заявки 30.12.2011; дата публ. 25.09.2012, бюл. №18, 2012 р. – 10 с. – *Здобувачем запропоновано архітектуру пристрою для виконання обчислень у полях виду $GF(2^m)$, що орієнтована на ПЛІС.*
11. Державний патент України №57281, МПК G06F 7/48. Суматор елементів поля $GF(p^m)$ [Текст] / Дичка І.А., Онай М.В.; заявник та патентовласник Національний технічний університет України "Київський політехнічний інститут". – № u201004903; дата подання заявки 23.04.2010; дата публ. 25.02.2011, бюл. №4, 2011 р. – 17 с. – *Здобувачем запропоновано спосіб виконання підсумовування елементів поля $GF(p^m)$.*

12. Державний патент України №54637, МПК G06F 7/50. Суматор за модулем простого числа [Текст] / Дичка І.А., Онай М.В.; заявник та патентовласник Національний технічний університет України “Київський політехнічний інститут”. – № u201001074; дата подання заявки 02.02.2010; дата публ. 25.11.2010, бюл. №22, 2010 р. – 14 с. – *Здобувачем запропоновано архітектуру суматора за модулем простого числа.*
13. Онай, М.В. Знаходження мультиплікативно оберненого елемента у кільці лишків за довільним модулем методом Джої-Пейє [Текст] / М.В. Онай, А.Ю. Бартков’як // Міжнародна науково-практична конференція “Проблеми інформатики та комп’ютерної техніки”. Праці конференції. – Чернівці : Видавничий дім “Родовід”, 2015. – С. 91-93. – *Здобувачем запропоновано методику проведення експериментального дослідження.*
14. Онай, М.В. Пошук мультиплікативно оберненого елементу у кільці лишків за довільним модулем методами, що грунтуються на модулярному піднесенні до степеня [Текст] / М.В. Онай, А.Ю. Бартков’як // Шістнадцята міжнародна наукова конференція імені академіка Михайла Кравчука, 14-15 травня, 2015 р., Київ : Матеріали конф. Т. 2. Алгебра. Геометрія. Математичний аналіз. – К. : НТУУ “КПІ”, 2015. – С. 139-141. – *Здобувачем запропоновано методику проведення експериментального дослідження.*
15. Дичка, І.А. Застосування *k*-арного методу Евкліда для пошуку мультплікативно оберненого елемента у кільці лишків за модулем *m* [Текст] / І.А. Дичка, М.В. Онай, А.Ю. Бартков’як // Матеріали статей П’ятої Міжнародної науково-практичної конференції «Інформаційні технології та комп’ютерна інженерія». м. Івано-Франківськ : п. Голіней О.М., 2015. – С. 151-153. – *Здобувачем запропоновано способи дослідження k-арного методу Евкліда для обчислення мультплікативно оберненого елемента.*
16. Онай, М.В. Спосіб прискорення алгоритмів множення точки еліптичної кривої на число в полі $GF(p)$ [Текст] / М.В. Онай, О.С. Князькіна // Прикладна математика та комп’ютинг. ПМК, 2014 : шоста наук. конф. магістрантів та аспірантів, Київ, 16-18 квітня 2014 р. : зб. тез доп. / [ред кол.: Дичка І.А. та ін.]. – К. : Просвіта, 2014. – С. 148-154. – *Здобувачем запропоновано адаптивний розширений алгоритм Лемера обчислення мультиплікативно оберненого елемента у полі GF(p).*
17. Онай, М.В. Спосіб перетворення многочленного подання елементів поля $GF(p^m)$ у степеневе [Текст] / М.В. Онай, Ю.В. Вальчук // Шістнадцята всеукраїнська (одинадцята міжнародна) студентська наукова конференція з прикладної математики та інформатики СНКПМІ-2013: Тези доповідей, 11-12 квітня, 2013 р. – Львів : ЛНУ 2013. – С. 46-47. – *Здобувачем запропоновано спосіб перетворення многочленного подання елементів поля розширення скінченного поля у степеневе подання.*

18. Дичка, І.А. Організація проблемно-орієнтованого процесора для реалізації операцій в полях Галуа виду $GF(2^m)$ [Текст] / І.А. Дичка, М.В. Онай // Тези доповідей Четвертої Міжнародної науково-практичної конференції "Методи та засоби кодування, захисту й ущільнення інформації" м. Вінниця, 23-25 квітня 2013 року. – Вінниця: ПП "ТД "Едельвейс і К", 2013. – С. 270-273. – *Здобувачем запропоновано архітектуру пристрою для виконання обчислень у полях виду $GF(2^m)$ орієнтовану на ПЛІС.*
19. Дичка, І.А. Спосіб зберігання в пам'яті ЕОМ різних форм подання елементів скінченного поля характеристики 2 [Текст] / І.А. Дичка, М.В. Онай // Комп'ютерні інтелектуальні системи та мережі. Матеріали VI Всеукраїнської WEB-конференції аспірантів, студентів та молодих вчених (19-21 березня 2013 р.). – Кривий Ріг : Криворізький національний університет, 2013. – С. 56-59. – *Здобувачем запропоновано табличний спосіб зберігання елементів поля $GF(2^m)$.*
20. Дичка, І.А. Організація системи команд співпроцесора Галуа [Текст] / І.А. Дичка, М.В. Онай // Міжнародна науково-технічна конференція "Радіотехнічні поля, сигнали, апарати та системи". Київ, 11-15 березня 2013 р.: матеріали конференції – Київ : 2013. – С. 212-213. – *Здобувачем запропоновано дворівневу структуру системи команд співпроцесора Галуа.*
21. Дичка, І.А. Способи знаходження мультиплікативного оберненого елемента в скінченних полях [Текст] / І.А. Дичка, М.В. Онай // Друга наукова конференція магістрантів та аспірантів присвячена 20-річчю факультету прикладної математики «Прикладна математика та комп'ютинг ПМК-2010» : Київ, 14-16 квіт. 2010 р. : зб. тез доп. / ред кол. : Дичка І.А. [та ін.] – К. : Просвіта, 2010. – С. 313-317. – *Здобувачем запропоновано спосіб обчислення мультиплікативно оберненого елемента у полі $GF(p)$.*

## АНОТАЦІЯ

Онай М.В. "Методи та засоби підвищення ефективності реалізації обчислювальних операцій у скінченних полях". – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – Комп'ютерні системи та компоненти (Інформаційні технології). – Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, 2017.

У дисертаційній роботі вирішено актуальну науково-прикладну задачу – підвищення продуктивності систем цифрової обробки даних та криптографічних перетворень, забезпечення завадостійкості зберігання і передачі даних за рахунок створення ефективних технічних засобів для виконання обчислень у скінченних полях шляхом структурно-логічної оптимізації архітектур апаратних засобів, що реалізують процеси виконання операцій у полях Галуа.

Запропоновано метод виконання операцій над елементами поля $GF(2^m)$. Особливістю даного методу, на відміну від існуючих, є застосування таблично-

го зберігання елементів поля у многочленному та степеневому їх поданні з можливістю розрідженого формування таблиці елементів поля, що зменшує витрати пам'яті для її зберігання. Розроблений метод забезпечує зростання швидкодії на 15% порівняно з існуючим методом.

Запропоновано модифікацію методу піднесення до степеня елементів поля $GF(p)$ з ковзним вікном, яка забезпечує приріст швидкодії на 7-9 %.

Спроектовано на ПЛІС фірми *Xilinx* процесор Галуа, що орієнтований на виконання операцій у скінченних полях виду $GF(p)$ та $GF(2^m)$.

Запропоновано програмістську модель процесора Галуа, яка дозволяє розробляти програмне забезпечення довільної складності мовою Асемблера процесора Галуа.

**Ключові слова:** поле Галуа, скінченне поле, мультиплікативно обернений елемент, піднесення до степеня, незвідний многочлен, Асемблер Галуа, процесор Галуа, ПЛІС.

## ABSTRACT

Onai M.V. "Methods and Means of Implementation Efficiency Increasing for Computational Operations in Finite Fields". – Qualifying scientific work on the rights of the manuscript.

Thesis for a PhD degree by specialty 05.13.05 – Computer Systems and Components (Information Technologies). – National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, 2017.

The thesis is devoted to the problem of increasing the efficiency of computations in finite fields. The proposed solution to this problem is to develop methods and means for performing operations on elements of finite fields $GF(p)$ or $GF(2^m)$.

The analysis of the current state of the development of methods of operations in finite fields is carried out and priority points are highlighted. It is best to classify them on the basis of the distinguished features. The classification of the methods of performing the most computational expensive operations (the calculation of the multiplicative inverse element and the exponentiation) in the finite fields was performed. It enables to conduct thorough research and form the directions of development for these methods.

The method of high-speed implementation of additive and multiplicative operations on elements of $GF(2^m)$ and corresponding hardware structures for its implementation are proposed. Additive operations include addition and subtraction. Multiplicative operations include multiplication, exponentiation, multiplicative inverse element calculation, and division.

The research has shown that table storage of elements of the $GF(2^m)$ in their polynomial and power representation ensures the maximum speed and versatility of the arithmetic logic unit. With the use of long integer operands, the sparse formation of the table of field elements is proposed. It enables reducing the memory consumption for its storage in several times. The algorithms for converting power representation into polynomial one and polynomial representation in power one with the use of

a sparse table are constructed. The developed method provides a 15% increase in performance comparing with the existing method.

Experimental researches were performed to determine the best sparse ratio of the elements table of the $GF(2^m)$. It has been discovered that for a value of $m < 21$, the best sparse ratio is equal to 8. For the exponentiation, it is desirable to increase the sparse ratio to 16.

The algorithms for converting the power representation into polynomial one and polynomial representation into power one with the use of a sparse table are developed.

The modification of the method of exponentiation elements $GF(p)$ with sliding window and the corresponding hardware structures for its implementation are proposed. The difference from the existing methods is that when forming a precomputation table, the exponents are prime numbers, and when analyzing the binary representation of the exponent, blocks of bits forming a prime number are allocated. To achieve high performance, when constructing a precomputation table, it is recommended to use pre-calculated additive chains to minimize the number of multiplication operations, which allows each of the following table items to be obtained in one or two modular multiplication operations.

With the help of the developed computational model, it has been found out that the proposed modification of the exponentiation method of elements $GF(p)$ with a sliding window provides an increase in speed by 7-9%. The modification of the exponentiation method of elements $GF(p)$ with a sliding window can be used in elliptic-curve cryptography to improve the time characteristics of the scalar multiplication on elliptic curve.

The model of the computational process of execution of operations in finite fields is developed, which enables comparison of methods on the basis of given sets of input data and the execution of the optimal choice of parameters and forms of presentation of operands, which ensure an increase in speed for the implementation of computing operations on the *FPGA*. The research methodologies of new methods hardware implementation of calculations in Galois fields are developed on the basis of the proposed model. Simulation in the development environment of *Xilinx ISE* and using the *Mentor Graphics Precision* software showed that the developed hardware structures are characterized by minimal hardware complexity and high performance.

A *Verilog* code generator for *FPGA* synthesis of a *ROM* element containing a sparse table of $GF(2^m)$ field elements in a polynomial and power representation is created which automatically generates a *Verilog* code for a given irreducible polynomial and a sparse ratio of the table.

The architecture and the command system of the specialized Galois processor, focused on operations in finite fields, has been developed. The Galois processor can be used in a universal computing system as a coprocessor, complementing the command system of the central processor unit, or as a special device based on the *FPGA*, which increases the efficiency of processing information in real time in comparison with the universal computing means. The architecture feature of the developed pro-

cessor is that a user can change the arithmetic logic unit (*ALU*) to make the transition to the $GF(p)$ or $GF(2^m)$ without changing the processor interface.

The research of the developed Galois processor has been carried out, which showed that this processor provides an increase in the productivity of computing by 27% compared with the universal computing means.

A program model of the Galois processor is constructed, which allows the user to create software of arbitrary complexity in Assembler of the Galois processor.

**Keywords:** Galois field, finite field, multiplicative inverse element, exponentiation, irreducible polynomial, Galois Assembler, Galois processor, *FPGA*.

## АННОТАЦИЯ

Онай Н.В. “Методы и средства повышения эффективности реализации вычислительных операций в конечных полях”. – Квалификационная научная работа на правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – Компьютерные системы и компоненты (Информационные технологии). – Национальный технический университет Украины “Киевский политехнический институт имени Игоря Сикорского”, Киев, 2017.

В диссертационной работе решена актуальная научно-прикладная задача – повышение производительности систем цифровой обработки данных и криптографических преобразований, обеспечение помехоустойчивости хранения и передачи данных за счет создания эффективных технических средств для выполнения вычислений в конечных полях путем структурно-логической оптимизации архитектур аппаратных средств, реализующих процессы выполнения операций в полях Галуа.

Предложен метод выполнения операций над элементами поля $GF(2^m)$. Особенностью данного метода, в отличие от существующих, является применение табличного хранения элементов поля в многочленном и степенном их представлении с возможностью разреженного формирования таблицы элементов поля, что уменьшает затраты памяти для ее хранения. Разработанный метод обеспечивает прирост производительности на 15% по сравнению с существующим методом.

Предложена модификация метода возведения в степень элементов поля $GF(p)$ со скользящим окном, обеспечивающая прирост быстродействия на 7-9%.

Спроектирован на ПЛИС фирмы Xilinx процессор Галуа, ориентированный на выполнение операций в конечных полях вида $GF(p)$ и $GF(2^m)$.

Предложена программистская модель процессора Галуа, позволяющая разрабатывать программное обеспечение любой сложности на языке ассемблера процессора Галуа.

**Ключевые слова:** поле Галуа, конечное поле, мультипликативно обратный элемент, возведение в степень, неприводимый многочлен, Ассемблер Галуа, процессор Галуа, ПЛИС.