ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, СИСТЕМНИЙ АНАЛІЗ ТА КЕРУВАННЯ

УДК 681.3.04

І.А. Дичка, М.В. Онай, Ю.В. Бухтіяров

АПАРАТНА РЕАЛІЗАЦІЯ ОБЧИСЛЕНЬ У СКІНЧЕННИХ ПОЛЯХ ХАРАКТЕРИСТИКИ ДВА

The article substantiates the need for hardware implementation of computational procedures in finite fields of the form GF(2^m) with a high rate of speed. Analysis of different forms of the field elements GF(2^m) representation was performed and showed that there is a need (in the process of computation) to move from one form of presentation elements to another, namely provide isomorphism field in hardware implementation. It was specified that for Galois fields with never-exceed 220 capacities it is expedient to use tabular method of elements field storage. Group of operations which should be performed on a numerical representation, and group operations, which should be performed on exponential representation elements field were selected. Architecture of computational tools for the implementation of operations in the field GF(2^m), which during the computation combines exponential and numeric representation of the field elements, was proposed and it allows carrying out basic operations set of operands in a finite field. Simulation results of performance computations in finite fields of two properties in two ways of realization operations – software and hardware were shown.

Вступ

Теорія скінченних полів має дедалі ширше застосування в галузі криптографії, цифрової обробки сигналів і завадостійкого кодування [1–4]. Відповідно, з'являється потреба в удосконаленні організації обчислень у скінченних полях, які часто також називають полями Галуа [1–4].

Обчислювальні операції в скінченних полях можна реалізовувати як програмно, так і апаратно. Через специфіку обчислень у полях Галуа їх програмна реалізація не завжди забезпечує потрібну швидкість отримання результату [5, 6]. Тому останнім часом дедалі більша увага приділяється питанням апаратної реалізації арифметики скінченних полів, оскільки при цьому істотно зростає продуктивність обчислень, що має важливе значення для задач криптографії з відкритим ключем і завадостійкого кодування даних [6, 7].

У наукових статтях, присвячених питанням практичного застосування теорії скінченних полів, здебільшого висвітлюються математичні аспекти виконання операцій у скінченних алгебричних структурах [3, 7–9] та не приділяється достатньої уваги організації апаратних засобів для реалізації обчислювальних операцій. Зрозуміло, що для досягнення потрібної ефективності обчислень у скінченних полях, особливо в задачах прикладного характеру, необхідно істотно знизити часові витрати на реалізацію операцій і функцій.

Тому актуальною є проблема апаратної реалізації обчислювальних процедур у скінченних полях.

Постановка задачі

Розрізняють два види полів Галуа: 1) поля виду GF(p), кількість елементів p у яких є простим числом (величину p називають характеристикою поля); 2) поля виду GF(p^m), кількість елементів у яких є степенем простого числа. Поле виду GF(p) називають основним полем; в основному полі операції виконують за модулем простого числа p. Поле виду GF(p^m) називають розширенням основного поля, операції в такому полі виконують за модулем незвідного многочлена $P_m(x)$ степеня m, де m – ціле додатне число.

У прикладних задачах найчастіше використовують скінченні поля характеристики два ($p = 2$), тобто поля виду GF(2^m), над елементами яких виконують операції додавання, знаходження адитивно оберненого елемента, віднімання елементів поля, множення, знаходження мультиплікативно оберненого елемента, ділення, піднесення до степеня, обчислення значення многочлена в заданій точці.

Існують 4 форми подання елементів поля GF(2^m): степеневе подання – у вигляді степеня примітивного елемента α поля з невід'ємним або від'ємним показником, поліноміальне, векторне та числове. Примітивним елементом поля називають елемент, усі можливі степені якого породжують ненульові елементи поля. Зазначені форми подання елементів поля є ізоморфними (тотожними), однак операцію додавання елементів поля та знаходження протилежного елемента зручно виконувати над вектор-

ним поданням, що у випадку $p = 2$ збігається 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 дає змоги отримувати нульовий елемент поля. Це означає, що при степеневому поданні неможливо виконати такі операції, як додавання та віднімання однакових елементів поля, а також $0 \cdot b$, $0 : b$, 0^b $(b \in GF(2^m))$, тобто коли один з операндів дорівнює нулю, оскільки результатом цих операцій є нуль (нульовий елемент поля), а подати його у вигляді степеня неможливо.

У загальному випадку степеневе подання не можна застосовувати при виконанні довільних операцій, оскільки воно дає (відтворює) лише ненульові елементи поля. Тому під час виконання операцій у $GF(2^m)$ необхідно динамічно, залежно від характеру операції, переходити від однієї форми подання елементів до іншої, і навпаки, тобто оперативно, на апаратному рівні забезпечувати ізоморфізм поля.

Таким чином, необхідно розробити архітектуру апаратних засобів, які б у ході обчислювального процесу в полях Галуа виду $GF(2^m)$ за рахунок апаратної реалізації ізоморфізму (перехід від однієї форми подання до іншої і навпаки) забезпечували б зменшення часу обчислень.

Побудова поля $GF(2^m)$

Зазначені перетворення розглянемо на прикладі поля $GF(2^4)$ (табл. 1), тобто при $m = 4$. Для побудови такого поля застосовують незвідний многочлен $P_4(x)$ четвертого степеня. Нехай $P_4(x) = x^4 + x + 1$. Загалом існує 3 многочлени степеня 4 [3], і будь-який з них можна використати для побудови поля. Отримувані при цьому поля будуть різнитися лише порядком слідування елементів.

При $m = 4$ поле складається з 16-ти елементів, із яких один елемент є нульовим (це елемент 0), а решта 15 – ненульовими.

При степеневому поданні ненульові елементи поля $GF(2^4)$ подають у вигляді: α^0, α, α^2, α^3, ..., α^{14}, де α – примітивний елемент поля. Це степеневе подання з невід'ємним показником степеня.

Степеневе подання передбачає й інший спосіб позначення ненульових елементів поля з від'ємним показником степеня: α^{-15}, α^{-14}, α^{-13}, ..., α^{-1}. Очевидно, що $\alpha^0 = \alpha^{15} = \alpha^{-15} = 1$.

Для отримання поліноміального подання елемента поля необхідно взяти його степеневе подання з невід'ємним показником і поділити на незвідний многочлен $P_4(x)$. Отримана остача й буде поліноміальним поданням цього елемента. При цьому дії над коефіцієнтами виконують за модулем 2 (у загальному випадку (поле $GF(p^m)$) – за модулем p).

***Таблиця* 1.** Форми подання елементів поля $GF(2^4)$ (за модулем незвідного многочлена $P_4(x) = x^4 + x + 1$)

Степеневе подання у вигляді степеня примітивного елемента α поля		Поліноміальне подання (у вигляді многочлена від α)	Векторне подання	Числове подання
з невід'ємним показником	з від'ємним показником			
–	–	0	0000	0
α^0	α^{-15}	1	0001	1
α^1	α^{-14}	α	0010	2
α^2	α^{-13}	α^2	0100	4
α^3	α^{-12}	α^3	1000	8
α^4	α^{-11}	$\alpha + 1$	0011	3
α^5	α^{-10}	$\alpha^2 + \alpha$	0110	6
α^6	α^{-9}	$\alpha^3 + \alpha^2$	1100	12
α^7	α^{-8}	$\alpha^3 + \alpha + 1$	1011	11
α^8	α^{-7}	$\alpha^2 + 1$	0101	5
α^9	α^{-6}	$\alpha^3 + \alpha$	1010	10
α^{10}	α^{-5}	$\alpha^2 + \alpha + 1$	0111	7
α^{11}	α^{-4}	$\alpha^3 + \alpha^2 + \alpha$	1110	14
α^{12}	α^{-3}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111	15
α^{13}	α^{-2}	$\alpha^3 + \alpha^2 + 1$	1101	13
α^{14}	α^{-1}	$\alpha^3 + 1$	1001	9

Коефіцієнти при відповідних степенях α в поліноміальному поданні утворюють векторне подання елемента поля. У загальному випадку (поле $GF(p^m)$) компоненти векторів (коефіцієнти поліноміального подання) належать множині $\{0, 1, 2, ..., p-1\}$. При $p = 2$ компоненти векторів будуть двійковими. Числове подання елемента поля отримують перетворенням вектора як числа в системі числення з основою p на десяткове число. При $p = 2$ це буде перетворення з двійкового вигляду на десятковий.

Операцію додавання елементів поля $GF(p^m)$ та знаходження протилежного елемента зручно виконувати над числовим поданням у двійковому вигляді. При цьому виконується порозрядне (без переносу) підсумовування двійкових кодів елементів за модулем 2, тобто операція хог.

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.

Наприклад, якщо необхідно елемент α^7 помножити на елемент α^{13}, то за правилами множення степенів маємо $\alpha^7 \cdot \alpha^{13} = \alpha^{7+13} = \alpha^{20}$. Оскільки максимально можливий показник степеня примітивного елемента в полі $GF(2^4)$ дорівнює 14, то отриманий показник степеня необхідно взяти за модулем 15: $\alpha^{20 \bmod 15} = \alpha^5$.

У загальному випадку множення виконують так: $\alpha^t \cdot \alpha^d = \alpha^{(t+d) \bmod 2^m - 1}$.

Для пошуку оберненого елемента необхідно показник степеня помножити на -1.

Нехай необхідно знайти мультиплікативно обернений до α^7 елемент поля. Таким елементом буде $(\alpha^7)^{-1} = \alpha^{-7}$ або у вигляді невід'ємного показника степеня: $\alpha^{-7} = \alpha^{15-7} = \alpha^8$. У загальному випадку маємо: $(\alpha^s)^{-1} = \alpha^{-s} = \alpha^{2^m - 1 - s} = \alpha^{s_{\text{інв}}}$, де $s_{\text{інв}}$ — інверсне значення величини s. При виконанні операції піднесення до степеня необхідно виконати множення показників степеня за модулем $2^m - 1$, тобто $(\alpha^t)^r = \alpha^{(t \cdot r) \bmod 2^m - 1}$.

Оскільки в полях Галуа характеристики два векторне подання елемента збігається з двійковим (комп'ютерним) кодом числового подання елемента, то для виконання будь-яких операцій над елементами поля достатньо розглядати лише перетворення степеневого подання елементів поля на числове і навпаки.

Перетворення числового подання елементів поля на степеневе

Числове подання елементів є найзручнішою формою задання скінченного поля $GF(2^m)$ у комп'ютері. При такому поданні елементу поля відповідає m-розрядне двійкове число. Числове подання елементів поля також зручно використовувати під час програмування обчислень у скінченних полях.

У багатьох практичних застосуваннях, пов'язаних із цифровою обробкою сигналів і завадостійким кодуванням даних, потужність поля (кількість елементів) не перевищує 2^{12}–2^{20}. Відповідно, для зберігання поля в пам'яті комп'ютера необхідно виділити від 2^{12} до 2^{20} (12–20)-розрядних слів. Це невеликий обсяг пам'яті порівняно із загальним обсягом оперативної пам'яті сучасних комп'ютерів. За таких обставин найдоцільніше застосовувати табличний спосіб перетворення елементів поля з однієї форми подання на іншу.

***Таблиця* 2.** Подання елементів поля $GF(2^4)$ у пам'яті комп'ютера

Степеневе подання		Числове подання
У вигляді невід'ємного показника степеня α	У вигляді від'ємного показника степеня α	
–	–	0000
0	–15	0001
1	–14	0010
2	–13	0100
3	–12	1000
4	–11	0011
5	–10	0110
6	–9	1100
7	–8	1011
8	–7	0101
9	–6	1010
10	–5	0111
11	–4	1110
12	–3	1111
13	–2	1101
14	–1	1001

Таким чином, якщо використовувати табличний спосіб зберігання елементів поля $GF(2^m)$, то при степеневому поданні елементів у пам'яті комп'ютера достатньо зберігати лише показник степеня – невід'ємний або від'ємний (один із них), а при числовому – двійкові коди елементів (табл. 2).

Нехай у пам'яті у вигляді таблиці зберігаються невід'ємні показники степеня (рис. 1). Тоді адреса комірки пам'яті, в якій зберігається показник степеня, є числовим поданням цього елемента. Таким чином, для перетворення елемента з числового подання на степеневе необхідно з пам'яті прочитати значення, що записане за адресою, яка є кодом числового подання елемента поля. Зчитане число буде невід'ємним показником степеня примітивного елемента поля.

Але для виконання операції знаходження мультиплікативно оберненого елемента необхідно отримувати від'ємний показник степеня примітивного елемента поля. Для того щоб перейти від невід'ємного показника степеня до від'ємного ($-s$), немає потреби зберігати в пам'яті від'ємні показники степеня: достатньо лише знайти доповнення s до $2^m - 1$, тобто обчислити значення $2^m - 1 - s$. Значення $2^m - 1 - s$ можна отримати інверсією всіх двійкових розрядів числа s.

Тобто для того щоб отримувати як невід'ємний, так і від'ємний показник степеня, необхідно до складу регістра (RG) ввести додатковий розряд (знаковий розряд), в якому після зчитування даних записувати 1, якщо в поточному такті буде використовуватись від'ємний показник, і 0 – якщо невід'ємний.

Перетворення степеневого подання елементів поля на числове

Перетворення елементів поля зі степеневого подання на числове також доцільно реалізувати таблично. В цьому випадку значення невід'ємного показника степеня примітивного елемента буде використовуватись як адреса, а за цією адресою в пам'яті слід розмістити значення елемента в числовій формі (рис. 2).

Якщо в поточному такті використовується невід'ємний показник степеня, то знаковий розряд регістра RG1 містить 0, і адресою є пряме значення s – показника степеня. При цьому для видачі слова s з RG1 використовується мікрооперація ВК – видача коду. Якщо в поточному такті слід використати від'ємний показник степеня, то знаковий розряд регістра RG1 містить 1 і адресою є інверсне значення s. При цьому для видачі слова $s_{\text{інв}}$ (тобто $\bar{s}$) з RG1 використовується мікрооперація ВІК – видача інверсного коду.

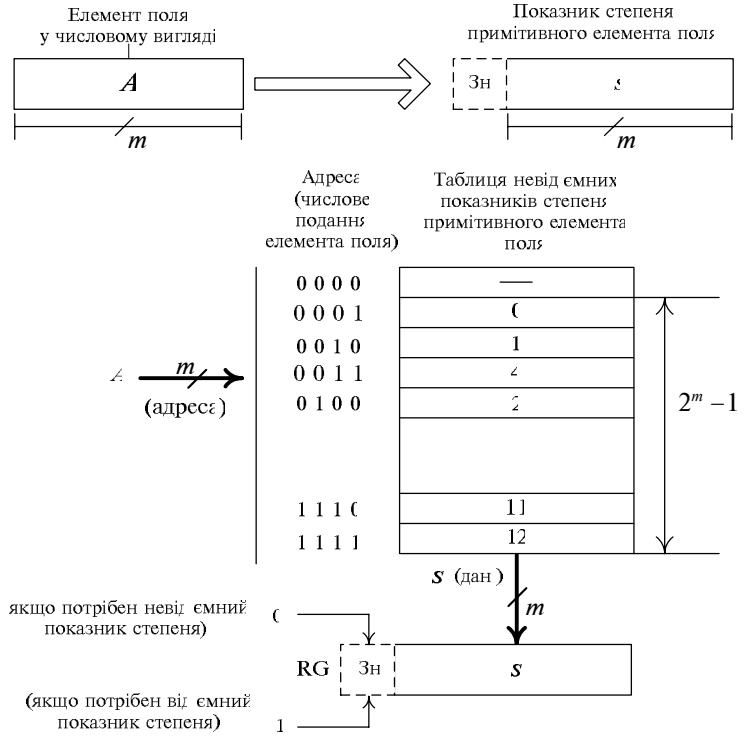

Рис. 1. Перетворення числового подання елемента поля на степеневе ($A \to s\,(-s)$)

Формування тієї чи іншої адреси (s або $\bar{s}$) забезпечує мультиплексор (MUX).

Числове подання елемента поля отримують в RG2.

Для забезпечення ізоморфізму поля – перетворення числової форми подання елементів поля на степеневу і навпаки, необхідно таблиці на рис. 1 і 2 звести в одну таблицю з такою структурою: адреса | невід'ємний показник степеня примітивного елемента | числове значення.

Така структура таблиці забезпечує перетворення як числового подання елементів поля на степеневе, так і степеневого на числове (рис. 3). Розмірність таблиці $2^m \times 2m$.

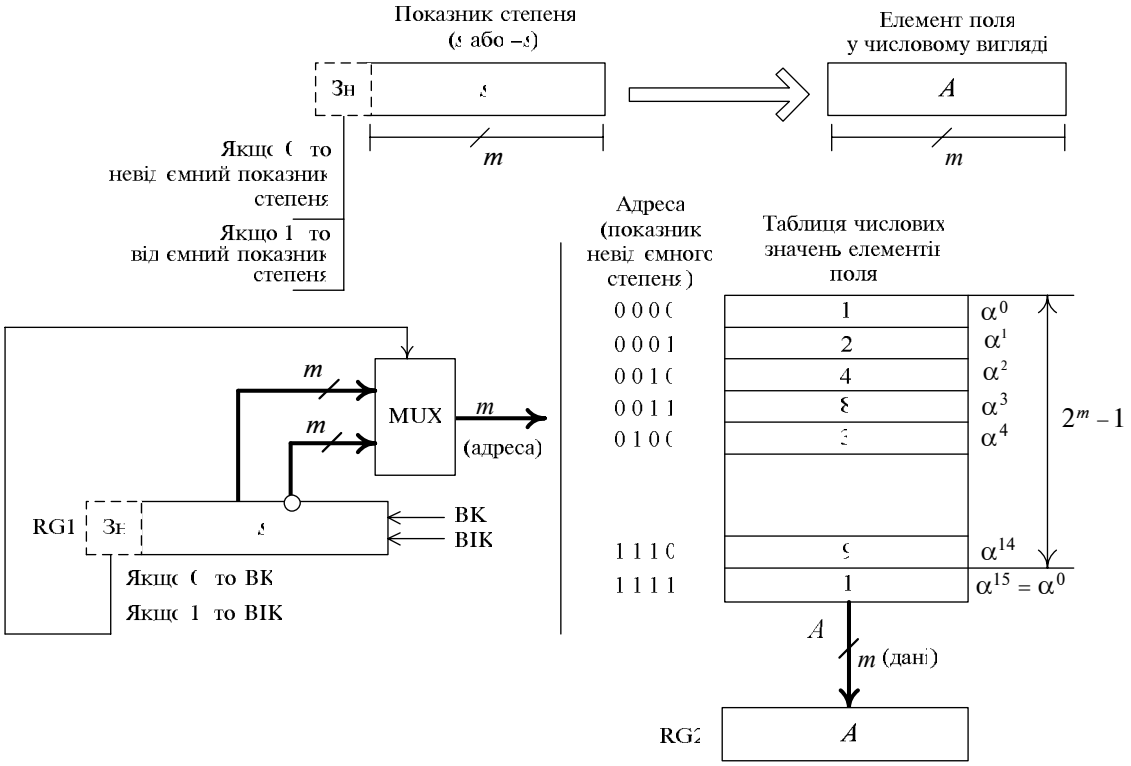

Рис. 2. Перетворення елемента поля зі степеневого подання на числове ($s\,(-s) \to A$)

Адреса	Невід'ємний показник степеня примітивного елемента α поля	Числове значення елемента поля
0 0 0 0	–	1 (α^0)
0 0 0 1	0	2 (α^1)
0 0 1 0	1	4 (α^2)
0 0 1 1	4	8 (α^3)
0 1 0 0	2	3 (α^4)
0 1 0 1	8	6 (α^5)
0 1 1 0	5	12 (α^6)
0 1 1 1	10	11 (α^7)
1 0 0 0	3	5 (α^8)
1 0 0 1	14	10 (α^9)
1 0 1 0	9	7 (α^{10})
1 0 1 1	7	14 (α^{11})
1 1 0 0	6	15 (α^{12})
1 1 0 1	13	13 (α^{13})
1 1 1 0	11	9 (α^{14})
1 1 1 1	12	1 (α^{15})

$2^m = 16$

m m

Рис. 3. Зведена таблиця зберігання елементів поля в пам'яті комп'ютера

Якщо адресою є числове значення елемента поля, то звертання відбувається до відповідного рядка лівої частини таблиці (права частина таблиці при цьому не використовується). Результатом читання з таблиці є невід'ємний показник степеня примітивного елемента α поля. Якщо адресою є невід'ємний показник степеня примітивного елемента поля, то звертання відбувається до відповідного рядка правої частини таблиці (ліва частина таблиці при цьому не використовується), і результатом читання з таблиці є числове значення елемента поля.

Організація обчислень у полі GF(2^m)

Розглянемо функціональну схему пристрою для виконання операцій в полі GF(2^m) (рис. 4). Він забезпечує виконання операцій додавання, віднімання, множення, ділення та знаходження мультиплікативно оберненого елемента поля. На основі перелічених операцій можна реалізувати будь-які інші операції в полі GF(2^m).

Операнди, що беруть участь в операціях, надходять на входи A, B пристрою. Операнди та результат операції (вихід Y) є елементами поля у числовому поданні. Код операції подається на вхід OP.

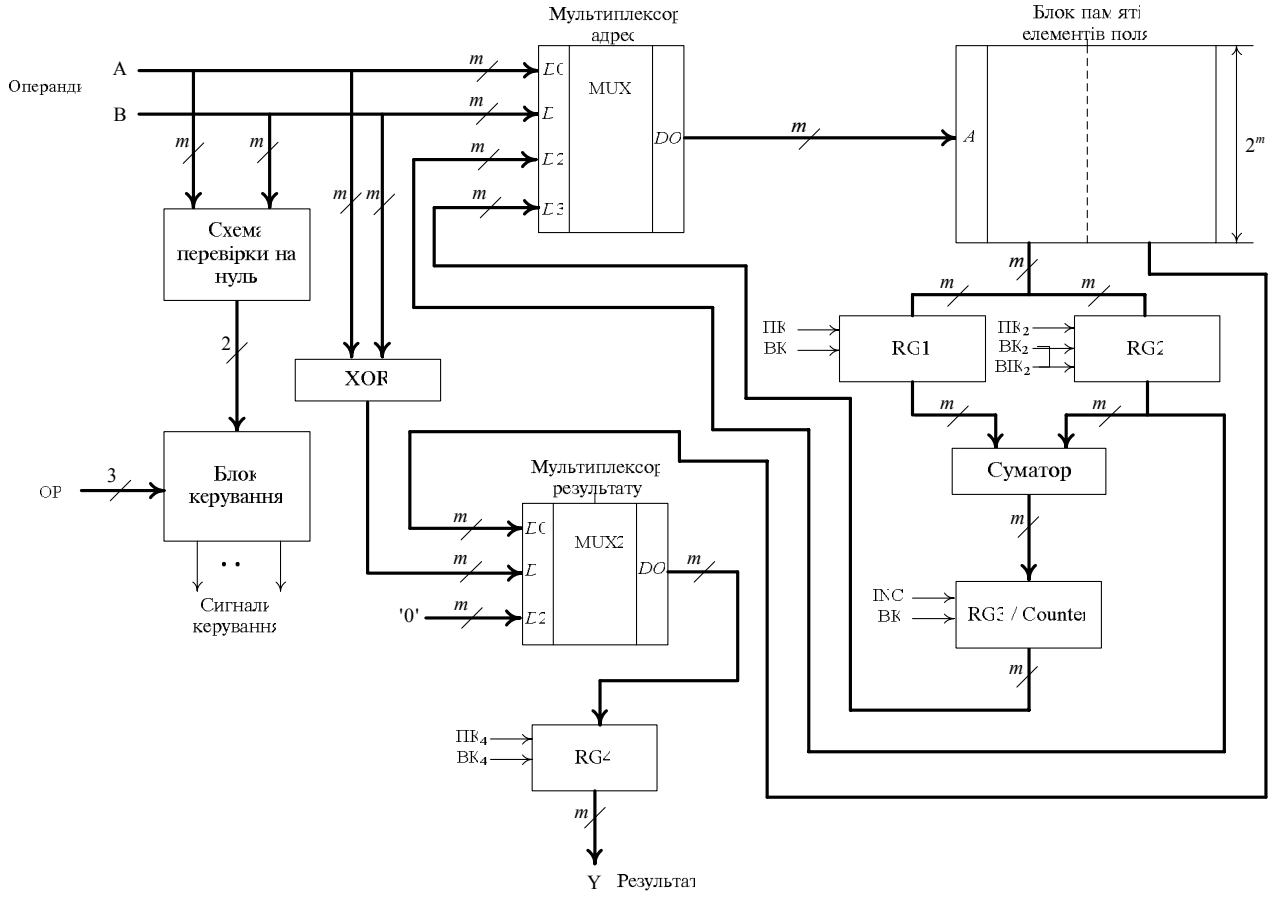

Рис. 4. Функціональна схема пристрою виконання операцій у полі GF(2^m)

Якщо адресою блока пам'яті елементів поля є числове значення елемента поля, то в RG1 або RG2 приймаємо ліву частину зчитаного слова – невід'ємний показник степеня, а правою частиною нехтуємо. Якщо адресою є невід'ємний показник степеня примітивного елемента α поля, то в RG4 приймаємо праву частину зчитаного слова, а лівою нехтуємо.

Додавання елементів поля. Операнди надходять на входи елементів XOR, де відбувається їх порозрядне додавання за модулем 2. Сума через MUX2 надходить у регістр RG4 результату.

Віднімання елементів поля. В полі GF(2^m) операція віднімання еквівалентна додаванню елементів поля.

Множення елементів поля. Операцію множення доцільно виконувати над степеневим поданням операндів. Якщо бодай один із операндів дорівнює нулю, то в регістр результату RG4 (через MUX2) записується нуль. Якщо обидва операнди ненульові, то необхідно отримати їх степеневе подання та виконати додавання невід'ємних показників степеня примітивного елемента. Значення першого операнда в числовому поданні є адресою, що надходить на адресний вхід блока пам'яті елементів поля GF(2^m). За цією адресою зчитується невід'ємний показник степеня примітивного елемента поля та фіксується в регістрі RG1. Значення другого операнда в числовому поданні надходить на адресний вхід блока пам'яті елементів поля. За цією адресою зчитується невід'ємний показник степеня примітивного елемента та фіксується в регістрі RG2. На комбінаційному суматорі виконується підсумовування двійкових кодів, що надходять з RG1 і RG2. Далі в RG3/лічильнику здійснюється корекція отриманого результату (якщо має місце перенос зі старшого розряду результату). Корекція полягає у додаванні 1 до отриманого результату. Якщо перенос зі старшого розряду відсутній, то корекція отриманого результату не виконується.

Результат отримано в степеневому поданні, а саме у вигляді невід'ємного показника

степеня примітивного елемента. Його необхідно перетворити на числове подання. Для цього результат (як адресу) слід подати на адресний вхід блока пам'яті елементів поля. На другому виході блока пам'яті елементів поля з'являється числове подання результату, яке приймається в регістр RG4 результату.

Знаходження мультиплікативно оберненого елемента поля. Цю операцію доцільно виконувати над степеневим поданням операнда. Якщо операнд є нульовим, то в регістр RG4 результату записується нуль (через MUX2). Якщо операнд є ненульовим, то необхідно отримати степеневе подання операнда у вигляді невід'ємного показника степеня примітивного елемента та знайти доповнення отриманого невід'ємного показника степеня до "$2^m - 1$", а це еквівалентне інвертуванню невід'ємного показника степеня. Значення операнда в числовому поданні як адреси надходить на адресний вхід блока пам'яті елементів поля. За цією адресою зчитується невід'ємний показник степеня примітивного елемента та видається на перший вихід блока пам'яті елементів поля і фіксується в регістрі RG2. Далі інверсне значення невід'ємного показника степеня операнда надходить на адресний вхід блока пам'яті елементів поля, і на другому виході блока пам'яті елементів поля GF(2^m) з'являється числове подання результату, яке фіксується в регістрі RG4 результату.

Ділення елементів поля. Цю операцію доцільно виконувати над степеневим поданням операндів. Якщо перший операнд є нульовим, то в регістр RG4 результату записується нуль.

Якщо обидва операнди ненульові, то необхідно отримати степеневе подання першого операнда, знайти невід'ємний показник степеня мультиплікативно оберненого елемента до другого операнда та додати його до невід'ємного показника степеня примітивного елемента першого операнда. Значення першого операнда в числовому поданні надходить на адресний вхід блока пам'яті елементів поля. За цією адресою зчитується невід'ємний показник степеня примітивного елемента і приймається в регістр RG1. Значення другого операнда в числовому поданні надходить на адресний вхід блока пам'яті елементів поля. За цією адресою зчитується невід'ємний показник степеня примітивного елемента і приймається в регістр RG2. На комбінаційному суматорі виконується підсумовування двійкових кодів, що надходять із RG1 та інверсного виходу RG2, і результат підсумовування записується в RG3/лічильник. Якщо має місце перенос зі старшого розряду, то потрібно виконати корекцію отриманого результату. Якщо перенос зі старшого розряду відсутній, то корекція отриманого результату не виконується.

Оскільки результат отримано у степеневому поданні, а саме у вигляді невід'ємного показника степеня примітивного елемента, то його необхідно перетворити на числове подання. З цією метою результат у вигляді невід'ємного показника степеня примітивного елемента подають на адресний вхід блока пам'яті елементів поля, внаслідок чого з другого виходу блока пам'яті елементів поля отримують числове подання результату, що фіксується в регістрі RG4 результату.

Висновки

Аналізуючи форми подання елементів поля GF(2^m) (див. табл. 1), доходимо висновку, що поліноміальне (та похідне від нього – векторне) подання є універсальним, оскільки воно забезпечує виконання довільних операцій над усіма без винятку елементами поля. Але при поліноміальній формі подання елементів скінченного поля виконання таких операцій, як множення, ділення елементів і знаходження мультиплікативно оберненого елемента, пов'язане з надто високою обчислювальною складністю і, як наслідок, з низькою швидкодією, оскільки реалізовувати операції доводиться лише програмним способом.

Але оскільки в скінченних полях характеристики два векторна форма (яка є віддзеркаленням поліноміальної форми) подання елементів поля збігається з числовою формою подання, то прийнятним для подання поля GF(2^m) в цілому є поєднання двох форм – степеневої та числової. В рамках цих двох форм переходи від однієї форми до іншої і навпаки в ході обчислень дають змогу виконувати будь-які операції над елементами і, таким чином, забезпечують ізоморфізм поля. Найдоцільніше такі переходи реалізовувати таблично. Це дає можливість виконувати обчислення з високою швидкістю.

При цьому швидкість виконання операцій можна характеризувати кількістю звертань до пам'яті (таблиці). Так, наприклад, операції додавання і віднімання не потребують звертання до пам'яті, при цьому виконується лише порозрядне підсумовування за модулем 2; операції множення і ділення елементів поля потребують 3 звертання до пам'яті; операція обчис-

лення мультиплікативно оберненого елемента – 2 звертання до пам'яті.

Моделювання процесу обчислень у скінченних полях характеристики два при двох способах реалізації операцій – програмному і апаратному, показує, що швидкість виконання операцій у випадку їх апаратної реалізації вища не менше ніж у 10 разів.

Подальші дослідження слід зосередити на вивченні особливостей апаратної реалізації обчислень у скінченних полях великої потужності, тобто коли параметр m перевищує 20.

1. *Элементарное* введение в эллиптическую криптографию. Алгебраические и алгоритмические основы / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М.: КомКнига, 2006. – 328 с.
2. *Коблиц Н.* Курс теории чисел и криптографии. – М.: Научное изд-во ТВП, 2001. – 254 с.
3. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки / Пер. с англ. – М.: Мир, 1976. – 600 с.
4. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки / Пер. с англ. – М.: Мир, 1986. – 576 с.
5. *P. Kisos et al.,* "An efficient reconfigurable multiplier architecture for Galois field GF(2^m)", Microelectronics J., vol. 34, pp. 975–980, 2003.
6. *C.-Y. Lee and P.K. Meher,* "Efficient bit-parallel multipliers over finite fields GF(2^m)", Computers and Electrical Eng., vol. 36, pp. 955–968, 2010.
7. *M. Morales-Sandoval et al.,* "An area/performance tradeoff analysis of a *GF*(2^m) multiplier architecture for elliptic curve cryptography", Ibid, vol. 35, pp. 54–58, 2009.
8. *S.S. Erdem et al.,* "Polynomial Basis Multiplication over *GF*(2^m)", Acta Appl. Math., vol. 93, is. 1-3, pp. 33–55, 2006.
9. *Hyun-Sung Kim and Il-Soo Jeon,* "Semi-systolic Architecture for Modular Multiplication over *GF*(2^m)", in Computational Sci – ICCS 2005, Atlanta, vol. 3516, pp. 912–915, 2005.

Рекомендована Радою
факультету прикладної математики
НТУУ "КПІ"

Надійшла до редакції
21 жовтня 2013 року