ОРГАНІЗАЦІЯ СИСТЕМИ КОМАНД СПІВПРОЦЕСОРА ГАЛУА

Дичка І. А., д.т.н., проф.; Онай М. В., аспірант
Національний технічний університет України
«Київський політехнічний інститут», м. Київ, Україна

В сучасних криптографічних системах та системах завадостійкого кодування даних майже всі обчислення виконуються в полях Галуа, тому виникає необхідність в удосконаленні структур обчислювальних засобів, які реалізують операції в скінченних полях [1, 2]. Розрізняють основні поля Галуа $GF(p)$ та розширення полів Галуа $GF(p^m)$, де p — просте число [3]. Розглянемо поле $GF(2^m)$. Програмна реалізація обчислень в полі $GF(2^m)$ з використанням універсальних комп'ютерних засобів є не завжди ефективною з точки зору швидкодії. Тому актуальною є проблема апаратної або апаратно-програмної реалізації обчислень у скінченних полях такого виду, а саме реалізації у вигляді співпроцесора (*G*–процесора). Центральний процесор при цьому залишається універсальним, однак його продуктивність при виконанні операцій в полі $GF(2^m)$ значно підвищується.

При додаванні в ЕОМ співпроцесора в систему команд центрального процесора необхідно ввести спеціальні команди, а співпроцесор має реалізовувати їх виконання апаратно. Наслідком цього має стати зростання продуктивності та ефективності обробки інформації.

Найбільш вживаними операціями в полях виду $GF(2^m)$ є додавання елементів поля, знаходження адитивно оберненого (протилежного) елемента поля, віднімання елементів поля, множення елементів поля, знаходження мультиплікативно оберненого елемента поля, ділення елементів поля, піднесення до степеня елемента поля, обчислення значення многочлена у заданій точці. На основі перелічених операцій можна реалізовувати інші — складніші операції в полі $GF(2^m)$.

Систему команд співпроцесора пропонується організувати у вигляді трирівневої ієрархічної структури. Першому та другому рівню будуть відповідати команди мікроасемблера, тобто внутрішні команди *G*–процесора, а третій рівень — рівень команд асемблера, тобто команд *G*–процесора, які будуть використовуватись центральним процесором для організації формульних обчислень, необхідність в яких виникає в завадостійкому кодуванні та в криптографічних алгоритмах.

Разом мікрооперації першого та другого роду утворюють набір мікрокоманд мікроасемблера. Поставимо у відповідність кожній мікрооперації певне мнемонічне позначення та значення коду мікрооперації (табл. 1).

Таблиця 1. Система мікрокоманд мікроасемблера

КмОП	Мнемо-ніка	Опис мнемоніки	Призначення мікрооперації
0 0 0	XOR	eXclusive OR	підсумовування за модулем два m-розрядних двійкових величин
0 0 1	CPL	ComPLiment	інвертування m-розрядної двійкової величини
0 1 0	INC	INCrement	інкремент m-розрядної двійкової величини
0 1 1	ADM	ADdition by Modulo	додавання m-розрядних двійкових величин за модулем $2^m - 1$
1 0 0	SBM	SuBtraction by Modulo	віднімання m-розрядних двійкових величин за модулем $2^m - 1$
1 0 1	MLM	MuLtiplication by Modulo	множення m-розрядних двійкових величин за модулем $2^m - 1$
1 1 0	CDP	Conversion Digit to Power	перетворення числового подання елемента поля у його степеневе подання
1 1 1	CPD	Conversion Power to Digit	перетворення степеневого подання елемента поля у його числове подання

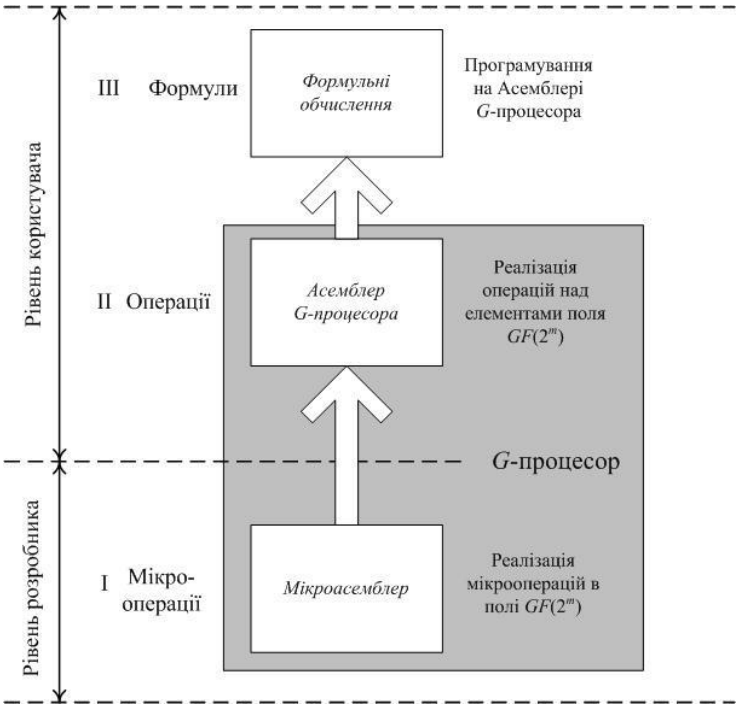

Рис.1. Ієрархічні рівні організації системи команд співпроцесору Галуа

Таким чином, організацію обчислень в полях Галуа $GF(2^m)$ можна подати у такому вигляді як наведено на рис. 1.

Подальші дослідження необхідно зосередити на побудові обчислювальних структур для ефективної реалізації зазначених операцій.

Література

1. Wu H. Bit-parallel finite field multiplier and squarer using polynomial basis / IEEE Trans. Comput. 51(7), July 2002 — P. 750 — 758.

2. Lidl R. Finite fields / Lidl R, Niederreiter H. Addison Wesley. — 1983.