УДК 004.9

АНАЛІТИЧНА ОЦІНКА СТРУКТУРНОЇ СКЛАДНОСТІ ПОМНОЖУВАЧІВ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА

Глухова О.В.[1)], Лозинський А.Я.[2)], Яремкевич Р.І.[2)], Ігнатович А.О.[3)]
Національний університет «Львівська політехніка»
[1)] бакалавр; [2)] магістр; [3)]аспірант.

Вступ

В даний час математичною основою опрацювання цифрового підпису є еліптичні криві. Обробка точок еліптичної кривої базується на виконанні операцій у полях Галуа GF(2^m). Апаратна реалізація помножувача для таких полів вимагає великих витрат обладнання. Секційний помножувач формує m біт добутку порціями по n біт. Апаратна складність ядер помножувачів дозволяє їх реалізацію на сучасних ПЛІС. Але при великих значеннях m і n неможливо реалізувати ядра через їх високу структурну складність. Відомий метод точної кількісної оцінки структурної складності таких помножувачів. У даній роботі пропонується аналітичний метод. Метод заснований на аналізі топології помножувальних матриць, які використовуються для множення представлених в гаусівськомк нормальному базисі типу 2 елементів поля Галуа.

I. Огляд літератури і визначення проблеми

Математичними основами цифрового підпису є еліптичні криві і поля Галуа. Одним з представлень елементів поля Галуа GF (2^m) є його подання у гаусівському нормального базисі типу 2. Для даного базису відомі послідовний помножувач Мессі-Омури [1], паралельний помножувач і паралельно-послідовний помножувач (секційний) [2]. Помножувальні матриці для них досліджувалися в роботі [3]. В [4] наведено особливості генераторів VHDL-описів (ядер) секційних помножувачів і оцінена їх апаратна складність. Також було показано, що при великих значеннях m неможливо реалізувати ядра через їх високу структурну складність.

Кількісну оцінку структурної складності було зроблено в роботах [5, 6].

II. Мета роботи

Метою роботи є знаходження аналітичної оцінки структурного складності помножувачів представлених в гаусівському нормальному базисі типу 2 елементів двійкових полів Галуа.

III. Реалізація секційного помножувача

Розряд r0 добутку R обчислюється як $r0=AMB^T$ (наприклад, на рисунок 1 $r_0 = a_2b_0 \oplus (a_2 \oplus a_3)b_1 \oplus (a_0 \oplus a_1)b_2 \oplus (a_1 \oplus a_3)b_3$ відповідно до схеми обчислення рисунок 2).

$$r_0 = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Рисунок 1 – Обчислення добутку

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_3 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Рисунок 2 – Схема обчислення добутку

Ми можемо оцінити кількісну структурну складність топології помножувача загальною довжиною L з'єднань усередині квадратної області на рисунок 3 [5, 6]. Для цього була розроблена спеціальна програма для обчислення L для двійкових полів Галуа з великими m.

Для аналізу структурної складності потрібно мати аналітичну залежність, яка з'єднює структурну складність та порядок полів Галуа.

Особливістю квадратної області помножувальної матриці є те, що у кожному її рядку і стовпчику використовується не більше двох операційних елементів (маленькі прямокутники на рисунок 3).

Загальна кількість операційних елементів для двійкових полів Галуа, представлених у гаусівському нормальному базисі типу 2 дорівнює 2m-1.

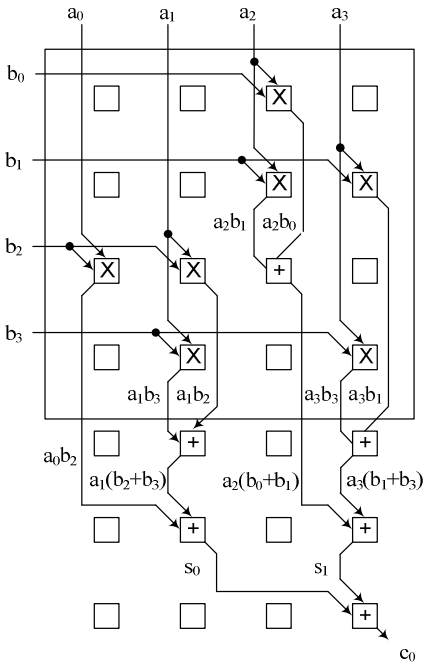

Рисунок 3 – Топологія кристалу помножувача.

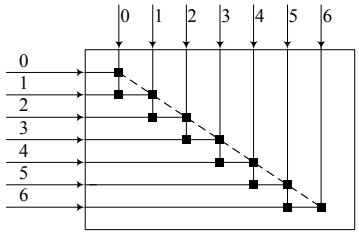

Рисунок 4 – Схема обчислення добутку з мінімальною структурною складністю.

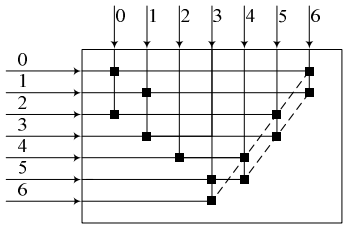

Рисунок 5 – Схема обчислення добутку з максимальною структурною складністю.

Розглянемо два варіанти розміщення цих елементів у квадратній області помножувальної матриці: рисунок 4 - min горизонтальна довжина; рисунок 5 - max горизонтальна довжина.

Перший варіант (рисунок 4): мінімальна довжина визначається як сума арифметичної прогресії

$$S_{\min} = \frac{(m+1)m}{2} = \frac{m^2}{2} + \frac{m}{2} \approx \frac{m^2}{2} \tag{1}$$

Другий варіант (рисунок 5): максимальна довжина визначається як сума двох арифметичних прогресій

$$S_1 = \frac{1}{2}\left(\frac{m+1}{2} + m\right)\frac{m+1}{2} = \frac{3m^2 + 4m + 1}{8}, \tag{2}$$

$$S_2 = \frac{1}{4}\left(\frac{m+3}{2} + m\right)\frac{m-1}{2} = \frac{3}{8}(m^2 - 1), \tag{3}$$

$$S = S_1 + S_2 = \frac{1}{4}(3m^2 + 2m - 1), \tag{4}$$

$$S_{\max} = \frac{3}{4}m^2 + \frac{m}{2} - \frac{1}{4} \approx \frac{3}{4}m^2. \tag{5}$$

Як видно структурна складність пропорційна квадрату порядку m поля Галуа та лежить приблизно в межах від S_{min} до S_{max}.

Висновок

У роботі зроблено аналітичну оцінку структурної складності помножувачів представлених в гаусівському нормальному базисі типу 2 елементів двійкових полів Галуа. Структурна складність пропорційна квадрату порядку m поля Галуа та лежить приблизно в межах від (1/2 … 3/4) m^2.

Список використаних джерел

1. В.С.Глухов., Р.М.Еліас, А.О.Мельник. Особливості реалізації на ПЛІС секційних помножувачів елементів полів Галуа $GF(2^m)$ з надвеликим степенем// "Комп'ютерно-інтегровані технології:освіта, наука, виробництво" - науковий журнал, Луцький національний технічний університет. № 12, 2013. С. 103 – 106.
2. Глухов В.С., Глухова О.В. Результати оцінки структурної складності помножувачів елементів полів Галуа//Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі" №773, 2013. С.27-32.
3. Глухов В.С. Особливості виконання операцій над матрицями в полях Галуа. Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи проектування. Теорія і практика". Вип. 564. Львів, 2006. С.35-39.
4. Hlukhov V., Hlukhova A. Galois field elements multipliers structural complexity evaluation. Proceedings of the 6-th International Conference ACSN-2013. September 16–18. – Lviv, 2013. – P. 18–19.

УДК 004.75

ЗАСІБ РОЗПОДІЛУ ДОСТУПУ В КОМП'ЮТЕРНІЙ МЕРЕЖІ

Дубчак Л.О.[1)], Мамончук М.Ю.[2)]

Тернопільський національний економічний університет

[1)] к.т.н., ст. викладач; [2)] магістрант

Вступ

Для здійснення захисту даних в мережі існують багато методів. Основні з них протистоять несанкціонованому доступу до інформації [1]. Система захисту повинна враховувати рівень доступу клієнта, можливість проведення атаки під час передачі даних, а також працездатність самої комп'ютерної системи.

Захист конфіденційної інформації може здійснюватись шляхом вибору найоптимальнішого методу піднесення до степеня за модулем, що реалізується під час шифрування інформації. Крім того, варто застосувати апарат нечіткої логіки для побудови такої системи, оскільки вона дозволяє працювати в режимі реального часу [2, 3].

Метод розподілу доступу в комп'ютерній мережі

Суть пропонованого методу полягає в тому, що процес оброблення вхідної нечіткої інформації розділено на етапи навчання та експлуатації.

Під час навчання засобу оброблення нечіткої інформації визначено області функцій належності виходу для кожного з правил.

Під час експлуатації спочатку відбувається порівняння вхідних даних зі значеннями функцій належності виходу у визначених базою правил областях пам'яті, де зберігаються значення згаданих функцій належності виходу, відповідних до кожного правила нечіткого висновку. Далі відсікаються значення функцій належності виходу, які перевищують вхідні дані. Потім вибираються мінімальні значення функцій належності виходу, отриманих після відсікання, і будується з цих мінімальних значень відповідна фігура. Останньою операцією методу оброблення нечітких даних є пошук центра ваги фігури, отриманої в результаті додавання відсічених функцій належності виходу [4, 5].

Всі операції пропонованого методу близькі до операцій класичного механізму Мамдані і за складністю не перевищують їх. Однак кількість операцій у пропонованому методі менша, що сприяє зростанню його швидкодії [6].

Засіб розподілу доступу, реалізований в середовищі Simulink

Схема розробленого нечіткого контролера, що реалізує пропонований метод оброблення нечіткої інформації, подана на рисунку 1.