

ОБЧИСЛЕННЯ СТРУКТУРНОЇ СКЛАДНОСТІ ПОМНОЖУВАЧІВ У ПОЛІНОМІАЛЬНОМУ БАЗИСІ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА $GF(2^m)$

© Шологон О. З., 2014

Проаналізовано структурну складність помножувачів, представлених у поліноміальному базисі елементів полів Галуа $GF(2^m)$. Для визначення структурної складності множення в полях Галуа було обрано помножувач, на якому реалізовано алгоритм Мастровіто. Запропоновано визначення структурної складності за допомогою об'єднання SH- та VHDL-моделей в одну VHDL-SH-модель.

Ключові слова: поля Галуа $GF(2^m)$, поліноміальний базис, SH-модель, VHDL-модель, структурна складність, алгоритм множення Мастровіто.

STRUCTURAL COMPLEXITY CALCULATION OF MULTIPLIERS BASED ON POLYNOMIAL BASIS OF GALOIS FIELDS ELEMENTS $GF(2^m)$

© Sholohon O., 2014

The structural complexity of multipliers in polynomial basis for Galois field $GF(2^m)$ is analyzed in paper. Mastrovito multiplication algorithm was chosen to determine the structural complexity of multiplication in Galois fields. The definition of structural complexity is calculated by combining the SH- and VHDL-models into a VHDL-SH model.

Key words: Galois field $GF(2^m)$, polynomial basis, SH-model, VHDL-model, structural complexity, mastrovito multiplication algorithm.

Вступ

Одна з найгостріших проблем в інформаційних технологіях – це захист даних від зламу. На сучасному етапі математичною основою для побудови пристроїв захисту інформації є поля Галуа та еліптичні криві.

Основними недоліками програмної реалізації є недостатня стійкість до зламу, часто недостатня продуктивність, особливо при обробці інтенсивних потоків даних. Тому для збільшення надійності реалізації захисту інформації, для збільшення продуктивності створюють апаратні засоби для виконання операцій над елементами скінченних полів.

У помножувачах, в яких використовуються поля Галуа $GF(2^m)$ з великим порядком, апаратна складність дає змогу проводити реалізації на кристалі ПЛІС, однак велика структурна складність перешкоджає це зробити. Тому важливим є її визначення. Розглянуто метод обчислення структурної складності об'єднанням VHDL- та SH-моделей в одну VHDL-SH-модель.

Аналіз останніх досліджень та публікацій

В Україні сьогодні чинні два стандарти на цифровий підпис: національний стандарт України ДСТУ 4145-2002 [1] та міждержавний стандарт ГОСТ 34.310-95 [2]. В останньому описано використання полів Галуа та еліптичних кривих під час роботи з цифровим підписом. Стандарт визначає максимальну характеристику поля Галуа $m=509$, тоді як міжнародний стандарт [3] дає змогу працювати з більшими полями ($m \leq 998$). Під час роботи з такими полями найбільш

трудомісткою є операція множення, оскільки потребує багатьох апаратних та часових витрат. Є відомим генератор ядер секціонованих помножувачів елементів полів Галуа $GF(2^m)$ [4]. Однак для полів Галуа, де $m > 500$, не вдалося провести імплементацію багатосекційних помножувачів на кристалі ПЛІС внаслідок їхньої високої структурної складності [4]. У роботі [5] пропонується обчислювати структурну складність за методом на основі аналізу структури помножувальних матриць, які використовуються для множення представлених в гауссівському нормальному базисі типу 2 елементів поля Галуа. Загальний підхід до визначення структурної складності за допомогою об'єднання VHDL- і SH-моделі в одну VHDL-SH-модель запропоновано в роботі [9].

Окреслення проблеми

Апаратна складність багатосекційних помножувачів дає змогу реалізувати їх на кристалі ПЛІС. Але для елементів полів Галуа $GF(2^m)$ з великим порядком або для великої кількості секцій реалізація таких пристроїв є неможливою через збільшення структурної складності.

Цілі статті

Метою роботи є оцінювання структурної складності помножувачів, представлених у поліноміальному базисі полів Галуа $GF(2^m)$. Буде запропоновано визначення структурної складності помножувача в полях Галуа шляхом об'єднання VHDL- та SH-моделей в одну VHDL-SH-модель.

Характеристика VHDL-SH-моделі

Точний припис в SH-моделі (Software/Hardware – апаратно/програмна модель) задається апаратними і програмними засобами [6]. Принциповою відмінністю SH-моделі від математичних моделей абстрактних алгоритмів є наявність у її визначенні деякої конфігурації апаратних засобів $G=(X,U)$, що складається з двох множин: множини елементарних перетворювачів X і множини міжз'єднань U [5]. Математичні моделі абстрактних алгоритмів таких засобів не мають. Отже, наявність апаратних засобів у складі SH-моделі алгоритму за змістом наближає її до комп'ютерної системи. Центральним елементом структури SH-моделі є елементарний перетворювач. Апаратні засоби представлені множиною:

$$G = (X, U), \quad (1)$$

де X – множина елементарних перетворювачів; U – множина міжз'єднань; [7]

На даний момент є відомими 5 характеристик складності для аналізу і оптимізації SH-моделей [8]:

Апаратна складність – кількість елементарних перетворювачів і елементів тимчасової пам'яті деякого ієрархічного рівня апаратних засобів SH-моделі:

$$A = |X|, \quad (2)$$

де X – множина елементів схеми.

Часова складність визначається кількістю елементів схеми, розташованих вздовж максимального критичного шляху розповсюдження сигналу:

$$L = |\max X_i|, \quad (3)$$

де $\max X_i$ – кортеж елементів SH-моделі, що належать до максимального критичного шляху розповсюдження сигналу, включаючи повторні проходження елементів у циклі.

Ємнісна складність SH-моделі дорівнює кількості комірок зовнішньої пам'яті, яка потрібна для розв'язання цієї задачі.

Програмна складність. Часова діаграма – це двовимірна таблиця в координатах: дискрети часу; входи керування. На процесорному рівні кожній асемблерній команді відповідає власна часова діаграма мікропрограми. Програмна складність оцінюється ступенем нерегулярності (ентропії) часової діаграми:

$$P = -F \log_2 \frac{F}{a \times b}, \quad (4)$$

де $F = \sum_L f_l$; a – кількість входів керування; b – кількість дискрет часу часової діаграми; $l f$ – кількість сигналів керування l -го фрагмента часової діаграми для обраного рівня ієрархії

побудови апаратних засобів; L – кількість фрагментів часової діаграми, конфігурації яких не повторюються.

Структурна складність відображає ступінь нерегулярності міжзв'язків схеми деякого рівня ієрархії побудови апаратних засобів. Структурна складність алгоритмічного пристрою – це ентропія матриці інцидентів:

$$S = -E \log_2 \frac{E}{q \times r}, \quad (5)$$

де E – кількість елементів матриці інцидентів системи; q і r – розмір матриці.

Структурну складність визначають в три етапи:

1. Схема SH-моделі перетворюється на орграф.
2. Орграф кодується у вигляді матриці інцидентів.
3. Розраховується значення нерівномірності матриці інцидентів [7].

Множина зв'язків в SH-моделі задає структурну складність. У VHDL-моделі зв'язки є елементами схеми, з'єднаннями, які не мають інтелектуального значення. VHDL-моделі не фіксує програмної та структурної складності, і для цього немає підстав, оскільки ієрархічний об'єкт може мати будь-яку внутрішню складність. Об'єднання SH- та VHDL-моделей в одну VHDL-SH-модель полягає у повторному виконанні таких дій: спочатку будується VHDL-модель, потім проводяться (за необхідності) певні зміни до SH-моделі (оптимізація), в такому випадку необхідно знову повертатися до корегування VHDL-моделі. Проектування проводиться ітераціями з врахуванням оптимізації (мінімізації) характеристик складності [6].

Алгоритм множення Мاستровіто

Для визначення структурної складності множення в полях Галуа було обрано помножувач, у якому реалізовано алгоритм Мاستровіто. Згідно з цим алгоритмом вхідне значення a множиться на нескорочуваний поліном, утворюючи матрицю скорочень. Потім матриця скорочень множиться на вхідне значення b (рис. 1).

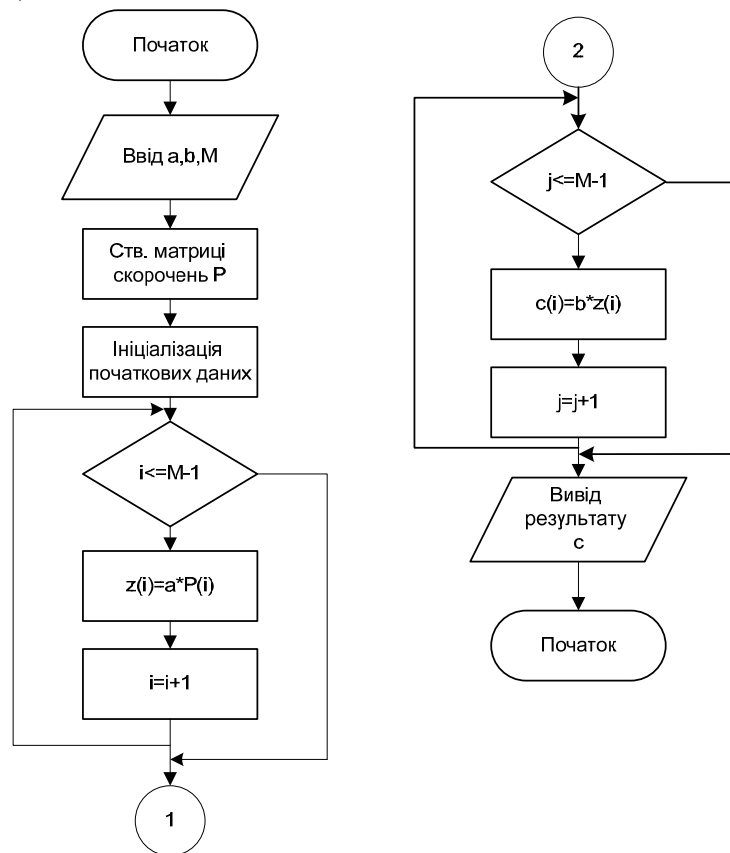


Рис. 1. Блок-схема алгоритму множення Мастровіто

Розрахунок структурної складності

Структурна складність помножувача в полях Галуа пропонується обчислювати, об'єднуючи VHDL- та SH-моделі в одну VHDL-SH-модель. У разі об'єднання моделей елементи VHDL-SH-моделі набувають всіх властивостей SH-моделі – вони є дискретними, детермінованими, мають елементарність та масовість. Характеристики складності розглядаються в ієрархічній побудові. Кожну з характеристик можна обчислювати для елементів різних рівнів ієрархій. Сумарна величина обчислених характеристик є складністю пристрою [7].

На рис. 2, а наведено детальну блок-схему алгоритму множення Мاستровіто для поля Галуа $GF(2^4)$. Структурна складність є основним показником інтелектуальних витрат під час розроблення програм. Блок-схему алгоритму перетворюємо на оргграф – кожен блок алгоритму відповідає одній вершині оргграфа (рис. 2, б):

- | | |
|-------------------------------------|------------------------------|
| K1 – Початок | K8 – Обчислення Z (3) |
| K2 – Ввід a, b, M | K9 – Обчислення C для Z (0) |
| K3 – Створення матриці скорочень | K10 – Обчислення C для Z (1) |
| K4 – Ініціалізація початкових даних | K11 – Обчислення C для Z (2) |
| K5 – Обчислення Z (0) | K12 – Обчислення C для Z (3) |
| K6 – Обчислення Z (1) | K13 – Виведення результату |
| K7 – Обчислення Z (2) | K14 – Кінець |

Блоки “Початок” і “Ввід a, b, M”, “Створення матриці скорочень” і “Ініціалізація початкових даних”, “Вивід результату” і “Кінець” мають однакову структурну складність, тому їх можна об'єднати в одну вершину, утворюючи стиснений оргграф (рис. 2, в).

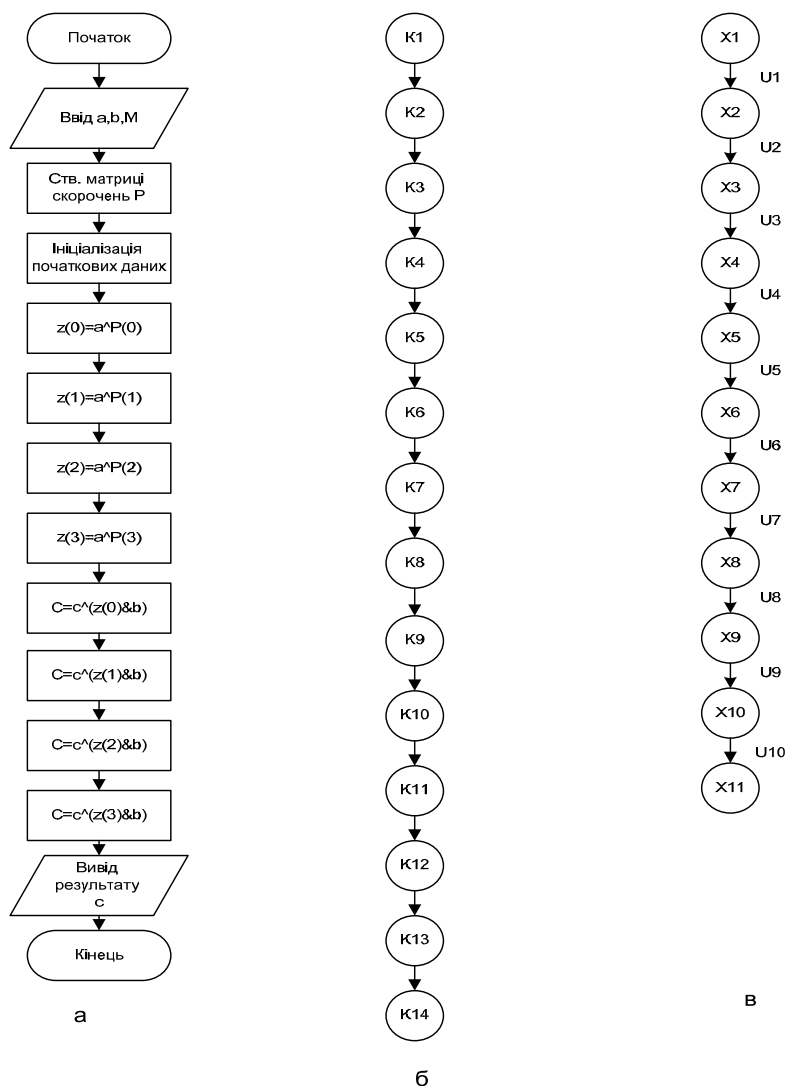


Рис. 2. Блок-схема роботи алгоритму множення Мастровіто (а); оргграф алгоритму множення (б), в – скорочений оргграф алгоритму множення (в)

На основі стисненого орграфу будується матриця інциденцій. Кількість рядків матриці дорівнює кількості вершин скороченого орграфу X , кількість стовпців дорівнює кількості переходів U . Тобто у цьому випадку кількість рядків 11, кількість стовпців 10. На рис. 3 наведено матрицю інциденцій.

	U1	U2	U3	U4	U5	U6	U7	U8	U9	U10
X1	1									
X2	-1	1								
X3		-1	1							
X4			-1	1						
X5				-1	1					
X6					-1	1				
X7						-1	1			
X8							-1	1		
X9								-1	1	
X10									-1	1
X11										-1

Рис. 3. Матриця інциденцій множення в полі $GF(2^4)$

Відповідно до формули (5) для обчислення структурної складності кількість елементів матриці $E = 20$, $q = 11$, $r = 10$. Отже, $S = -20 \times \log_2 \frac{20}{11 \times 10} = 49.18$.

Можна вивести загальну формулу обчислення структурної складності для множення Мastrovito у полі Галуа $GF(2^m)$.

$$q = 3 + m \times 2; \quad r = q - 1 = 2 + 2 \times m, \quad E = 2 \times r = 4 + 4 \times m \quad (4)$$

Отже

$$S = -E \times \log_2 \frac{E}{q \times r} = -(4 + 4m) \log_2 \frac{4 + 4m}{(3 + 2m) \times (2 + 2m)} =$$

$$= -(4 + 4m) \log_2 \frac{4 + 4m}{4m^2 + 10m + 6} = 49.18.$$

Також можна обчислити структурну складність помножувача елементів полів Галуа $GF(2^m)$. У табл. 1 та 2 наведено результати дослідження для помножувача в полях Галуа для $m=8, 16, 32, 64, 128, 163, 233, 283$. Дослідження проводили на кристалі фірми Xilinx XC5VLX50T-FF1738 [8].

Таблиця 1

Порядок двійкового поля Галуа	8	16	32	64
Кількість Slice	32	129	538	2161
Кількість Slice (%)	0.11 %	0.45 %	1.87 %	7.5 %
Структурна складність	116.93	280.79	668.72	1568.69

Таблиця 2

Порядок двійкового поля Галуа	128	163	233	283
Кількість Slice	8190	13349	25995	32096
Кількість слайсів (%)	28.44 %	46.35 %	90.26 %	98 %
Структурна складність	3620.67	4829.44	7369.54	9261

Як видно з табл. 1 та 2, із збільшенням порядку двійкового поля Галуа збільшується структурна складність елементів та кількість конфігурованих логічних блоків (слайсів).

Максимальний порядок двійкового поля, за якого вдалось провести імплементацію, є 283. Для полів, де структурна складність є більшою за 9261, провести імплементацію не вдалось.

Висновки

У роботі наведено спосіб обчислення структурної складності для помножувача Мастрівіто в полях Галуа $GF(2^m)$. Структурну складність запропоновано визначати за допомогою об'єднання SH- та VHDL-моделі в одну VHDL-SH-модель. Для поля Галуа $GF(2^m)$ було побудовано орфограф та матрицю інцидентів, на основі яких було обчислено структурну складність присторою. На основі проведених досліджень було виведено загальну формулу для обчислення структурної складності помножувача Мастрівіто в полях Галуа $GF(2^m)$. Було обчислено значення структурної складності помножувача Мастрівіто, який реалізується на обраному кристалі ПЛІС.

1. ДСТУ 4145-2002. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К.: Держ. комітет України з питань техн. регулюв. та споживч. політ., 2003. 2. Межгосударственный стандарт ГОСТ 34.310-95. Информационная технология. Криптографическая защита информации процедура выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. Межгосударственный совет по стандартизации, метрологии и сертификации. – Минск: Госстандарт Белоруссии, с дополнениями, 1997. 3. IEEE Std 1363-2000 IEEE Standard Specifications for Public-Key Cryptography Sponsor Microprocessor and Microcomputer Standards Committee of the IEEE Computer Society. Approved 30 January 2000. 4. Еліас Р. Генератор ядер секціонованих помножувачів елементів полів Галуа $GF(2^m)$ для оптимального нормального базису 2-го типу / Глухов В., Еліас Р. // Вісник Нац. ун-ту “Львівська політехніка”. – 2012. – № 732 5. Глухов В. С., Глухова О. В. Результати оцінки структурної складності помножувачів елементів полів Галуа // Вісник Нац. ун-ту “Львівська політехніка”. – 2013. – № 773. 6. Черкаський М. В. Співвідношення об'єктів SH- та VHDL-моделей / М. В. Черкаський, Ю. І. Бережанський // Вісн. Нац. ун-ту “Львів. політехніка”. – 2012. – № 717. – С. 199–203. – Бібліогр.: 3 назв. - укр. 7. Черкаський М.В., Мурад Хусейн Халіл. “Універсальна SH-модель” // Вісник Нац. ун-ту “Львівська політехніка”. – 2004. – № 523. – С. 150–154. 8. Virtex-5 FPGA Family: Data Sheet.- Xilinx, January 2009/ - DS312.10 9. Черкаський М.В., Абдалла Саїд Садек, “Псевдо SH-модель” Комп'ютерні системи та мережі // Вісник Нац. ун-ту “Львівська політехніка”. – 2004. – № 523. – С. 145–150.