УДК 004.032.2

Ю. З. Шологон
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

ОЦІНЮВАННЯ СТРУКТУРНОЇ СКЛАДНОСТІ ПОМНОЖУВАЧІВ ПОЛІВ ГАЛУА НА ОСНОВІ ЕЛЕМЕНТАРНИХ ПЕРЕТВОРЮВАЧІВ

Проаналізовано структурну складність помножувачів у поліноміальному базисі елементів полів Галуа *GF* (2^m) за допомогою об'єднання VHDL- та SH-моделей в одну VHDL-SH-модель. Для порівняння результатів аналізу структурної складності було обрано алгоритм множення Мастровіто та класичний двокроковий алгоритм. Порядок поля Галуа, який розглянуто у статті, є < 409.

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

CALCULATING STRUCTURAL COMPLEXITY OF GALOIS FIELDS MULTIPLIERS BASED ON ELEMENTARY CONVERTERS

Calculating structural complexity of Galois fields multiplier based on elementary converters is analyzed in paper. Structural complexity is determined by combing VHDL- SH-models into a VHDL-SH model. Mastrovito multiplier and classic Galois fields multiplier were chosen for calculation results analysis. The order of the Galois field, which is considered in the article is ≤ 409.

Key words: Galois field *GF* (2^m) , polynomial basis, SH-model, VHDL-model, structural complexity, classic two-step algorithm, Mastrovito multiplication algorthm.

Вступ

Еліптичні криві використовуються у криптографії як математична основа опрацювання цифрового підпису. Еліптичні криві над скінченними полями (полями Галуа) утворюють скінченні групи, що є математичною основою для опрацювання цифрового підпису. Операції в полях Галуа *GF* (2^m), а саме операція множення вимагає великих апаратних витрат обладнання. Оцінка структурної складності пристрою дасть змогу визначити характеристики, які повинен мати помножувач для імплементації на кристалі ПЛІС. У роботі запропоновано метод оцінювання структурної складності помножувача, коли елементи представлено в поліноміальному базисі. Метод базується на об’єднанні VHDL- і SH-моделей у VHDL-SH-модель, при цьому елементами найнижчого рівня (моделі) є елементи I, XOR.

Аналіз останніх досліджень та публікацій

Національний стандарт України ДСТУ 4145-2002 [*1*] та міждержавний стандарт ГОСТ 34.310-95 [2] описують використання цифрового підпису. Відповідно до національного стандарту України максимальна характеристика поля Галуа m=509, однак міжнародний стандарт [3] рекомендує роботу з більшими полями Галуа, де m≤998. Оцінка структурної складності пристрою дозволить визначити можливості використання окремих ПЛІС для реалізації помножувача [4–6]. Метод оцінювання структурної складності, що пропонується у роботі [7], не є точним, оскільки складність елементів блок-

схеми є неоднаковою. Метод, що запропонований у роботі, описує спосіб обчислення структурної складності, де всі елементарні перетворювачі структурної схеми мають приблизно однакову структурну складність [8, 9]. Однак за великої кількості ядер та великої характеристики поля Галуа [10, 11] через збільшення структурної складності реалізувати такі пристрої неможливо [12, 13].

Окреслення проблеми

Апаратна складність багатоядерних помножувачів дає змогу реалізувати їх на кристалі ПЛІС. Але за великих значень m, а також великої кількості ядер реалізація таких пристроїв є не можливою через збільшення структурної складності [8, 9].

Цілі статті

Метою роботи є оцінювання структурної складності помножувачів у поліноміальному базисі полів Галуа $GF(2^m)$, коли елементарним перетворювачем є елементи І та XOR.

Особливості SH-моделі

SH-модель алгоритму (Software/Hardware – апаратно-програмна модель) задається програмними і апаратними засобами. SH-модель не має раз і назавжди встановленої структури апаратних засобів. Точний припис в SH-моделі 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=(XU), що складається з двох множин: множини елементарних перетворювачів X і множини міжз'єднань U [9]. 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.

Кожна конкретна модель алгоритму стосовно апаратної побудови має точно окреслену структуру, яка складається з двох множин [7]: множини елементарних перетворювачів і множини міжз'єднань:

$$E = \{e_1, e_2 ... e_n\} \quad (1)$$

$$U = \{u_1, u_2 ... u_n\} \quad (2)$$

Елементарний перетворювач – це неподільний елемент схеми, який має приблизно однакову з іншими елементами структурну складність. На сучасному етапі елементної бази як елементарний перетворювач можна вибрати елементи, які реалізовані в одному LUT (I, XOR) і вважати, що вони мають однакову складність.

Методи розрахунку структурної складності

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

$$S = -E \times \log_2 \frac{E}{n \times m}, \quad (3)$$

де E – кількість елементів матриці інциденцій системи; n і m – розмір матриці.

У роботі [*8*] обчислення структурної складності складається з трьох етапів:

Схема SH-моделі перетворюється на орграф: кожен окремий елемент блок-схеми відповідає одній вершині орграфу.

1. Після аналізу вершин орграфу визначається, які вершини можна об'єднати в одну. Так будують скорочений орграф.
2. Орграф кодується у вигляді матриці інциденцій. На основі стисненого орграфу будується матриця інциденцій. Кількість рядків матриці дорівнює кількості вершин скороченого орграфу X, кількість стовпців дорівнює кількості переходів U.
3. Розраховується значення нерівномірності матриці інциденцій.

Такий метод розрахунку структурної складності [7] є неточним, оскільки структурна складність кожного окремого елемента блок-схеми не є однаковою. Наприклад, структурна складність блоку "Початок" не може дорівнювати структурній складності блоку множення. Тому для схеми SH-моделі краще використовувати не блок-схему алгоритму, а детальну структурну схему

алгоритму. Кожен елемент схеми повинен мати приблизно однакову структурну складність (реалізується в LUT), тому в цьому випадку якнайкраще підійде структурна схема, що складається з and і xor елементів. У такому випадку структурна складність визначатиметься так:

$$S = -E \times \log_2 \frac{E}{X \times U}, \quad (4)\ [9]$$

де X – кількість вершин блок-схеми, у даному випадку кількість елементів and і xor; U – множина орієнтованих міжз'єднань, у даному випадку кількість виходів

$$U = X, \quad (5)$$

де E – множина елементарних перетворювачів, тобто сума кількості з'єднань кожного фрагмента схеми.

Отже, структурна складність обчислюється [9]

$$S = -E \times \log_2 \frac{E}{X^2}.$$

Розрахунок структурної складності

Структурна складність помножувача в полях Галуа визначається за допомогою об'єднання VHDL- та SH-моделей в одну VHDL-SH-модель [6]. У разі об'єднання моделей елементи VHDL-SH-моделі набувають всіх властивостей SH-моделі – вони є дискретними, детермінованими, характеризуються елементарністю та масовістю. Характеристики складності розглянуто у їх ієрархічній побудові. Кожну з характеристик можна обчислити для елементів різних рівнів ієрархій. Сумарна величина обчислених характерстик є складністю пристрою [6].

Алгоритм множення Мастровіто. На рис. 1 наведено структурну схему помножувача Мастровіто для поля Галуа GF(2^4) [11].

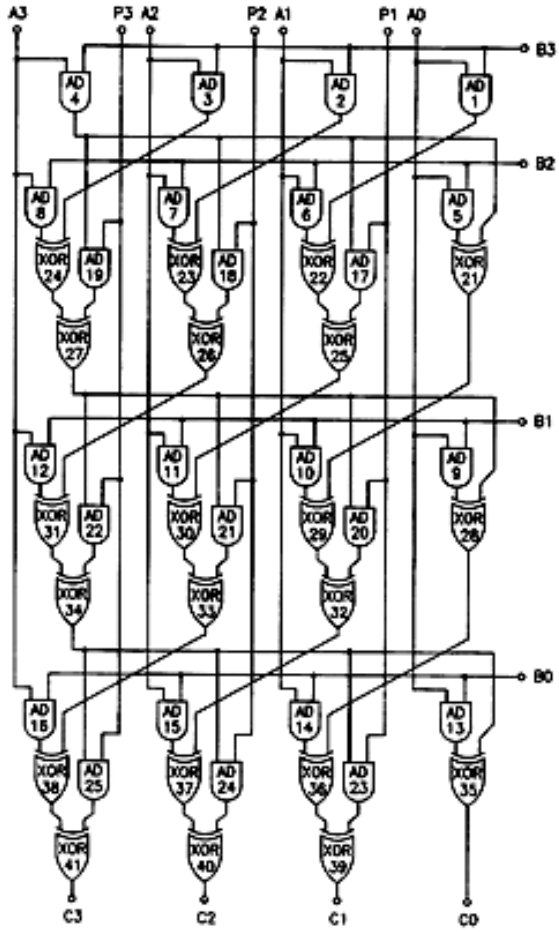

Рис. 1. Структурна схема помножувача Мастровіто для GF(2^4)

Згідно з формулою (5) для обчислення структурної складності необхідно знати кількість елементів системи X, в даному випадку кількість логічних елементів AND і XOR. Згідно з рис.1 кількість елементів схеми можна обчислити за формулою:

$$X = Mand + (M-1)and + (M-1)xor + (2and + 2xor)\times(m-1)^2, \quad (6)$$

де M – розрядність поля Галуа; and і xor – умовне позначення кількості логічних блоків.

Отже, для поля Галуа GF(2^4):

$$X = 4and + 3and + 3xor + (2and + 2xor)\times 9 = 25and + 21xor = 46$$

Тоді для GF(2^4) U=46.

Логічний елемент схеми (LUT) має два входи і один вихід. Кількість елементів матриці інциденцій обчислюється як:

$$E = 3\times X\ . \quad (7)$$

Тоді для GF(2^4) $E = 3\times 46 = 138$.

Структурна складність S дорівнює:

$$S = -E\times\log_2\frac{E}{X\times U} = -138\times\log_2\frac{138}{46\times 46} = 543\,.$$

Класичний двокроковий алгоритм. На рис. 2 наведено структурну схему класичного помножувача в полях Галуа [12].

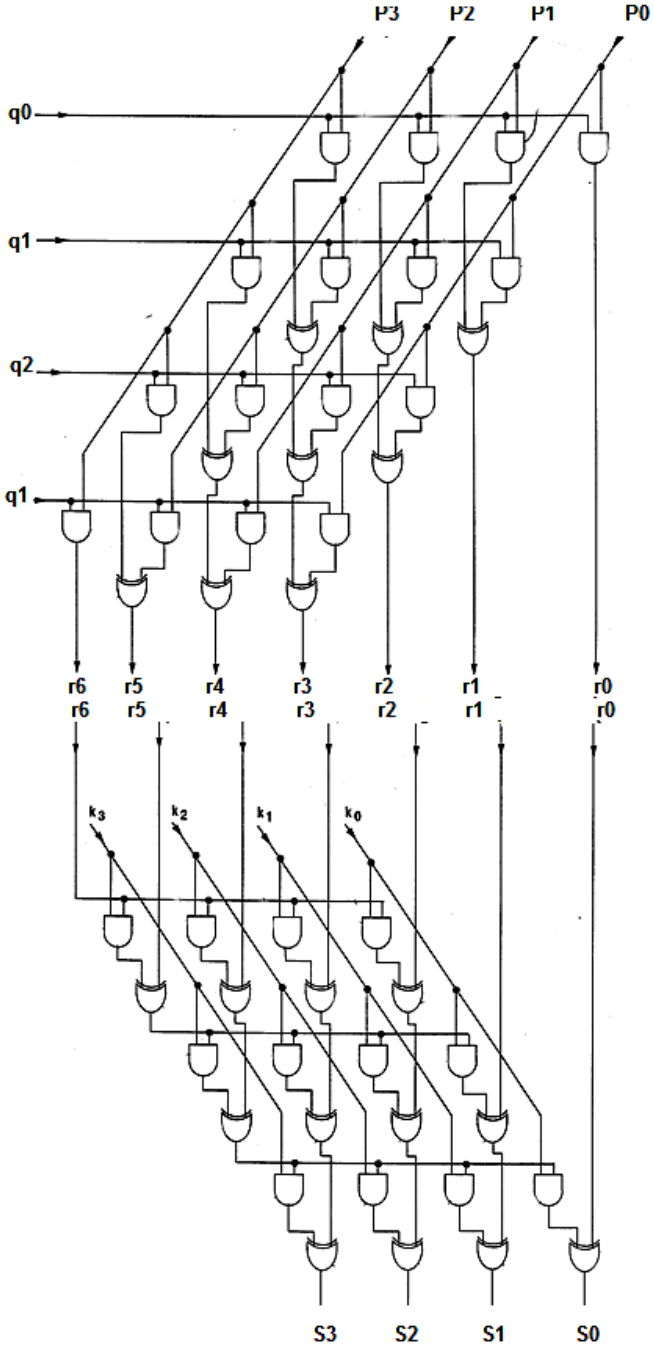

Рис. 2. Структурна схема класичного помножувача для GF(2^4)

Кількість елементів можна обчислити за формулою знаходження суми елементів арифметичної прогресії:

$$X = M^2 and + (M-1)^2 xor + M \times (M-1) and + M \times (M-1) xor \quad . \qquad (8)$$

Тоді для поля Галуа GF(2^4) $X = 16 and + 9 xor + 12 and + 12 xor = 49$ згідно з формулами (7), (8) множина міжз'єднань U та кількість елементів матриці інциденцій відповідно дорівнюватимуть

$$U=49$$

$$E = 3 \times X = 3 \times 49 = 147$$

Маючи значення X, U та E, можна визначити структурну складність пристрою

$$S = -E \times \log_2 \frac{E}{X \times U} = -147 \times \log_2 \frac{147}{49 \times 49} = 588$$

Результати імплементації в ПЛІС

З формул (6), (7), (8), (9) можна визначити структурну складність для двох помножувачів, що розглядаються у роботі. У табл. 1 та 2 наведено результати дослідження для помножувачів, які реалізують алгоритм множення Мастровіто в полях Галуа для m=8, 16, 32, 64, 128, 163, 233, 283.

Дослідження проводили на кристалі Virtex-6 фірми Xilinx XC6VCX75T-FF484 [13].

Таблиця 1

Значення M	8	16	32	64
Кількість Slice	32	129	538	2161
Кількість Slice (%)	1%	1%	1%	5%
Структурна складність	4043.827	23557.48	122372.8	597017.1

Таблиця 2

Значення M	128	163	233	283
Кількість Slice	8190	13349	25995	47002
Кількість Slice (%)	18%	29%	56%	101%
Структурна складність	2803769	4777917	10455566	15977104

У табл. 3 та 4 наведено результати дослідження для помножувача в полях Галуа для m = 8, 16, 32, 64, 128, 163, 233, 283 для класичного двокрокового алгоритму множення.

Таблиця 3

Значення M	8	16	32	64
Кількість Slice	28	113	477	1885
Кількість Slice (%)	1%	1%	1%	4%
Структурна складність	4200.115	23992.12	123466.5	599627.1

Таблиця 4

Значення M	128	163	233	283	409
Кількість Slice	9602	11295	21948	36296	76464
Кількість Slice (%)	19%	24%	47 %	78 %	164%
Структурна складність	2809806	4785958	10467801	15992451	35570662

На рис. 3 наведено графік порівняння структурної складності для алгоритму множення Мастровіто і класичного двокрокового алгоритму.

Рис. 3. Порівняння структурної складності для помножувача Мастровіто та класичного помножувача

З рис. 3 видно, що із збільшенням розрядності m поля Галуа різниця між структурною складністю двох помножувачів зростає. Структурна складність помножувача класичного помножувача є більшою за складність помножувача Мастровіто, отже, реалізація класичного помножувача є більш трудомісткою.

Висновок

Запропоновано метод обчислення структурної складності помножувача в полях Галуа GF (2^m) за допомогою об'єднання SH- і VHDL-моделі у одну VHDL-SH-модель, де за елементарний перетворювач прийнято елементи І та XOR Для обчислення структурної складності було обрано два помножувача: помножувач Мастровіто та класичний помножувач. Структурна складність для помножувача Мастровіто є меншою за структурну складність класичного помножувача, отже, при реалізації помножувача в полях Галуа GF(2^m), де m>128, краще використовувати помножувач Мастровіто.

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 асиметричного криптографического алгоритма. Межгосударственный совет по стандартизации, метрологии и сертификации. – Минск: Госстандарт Белоруссии, с дополнениями, 1997.16. 3. IEEE Std 1363-2000 IEEE Standard Specifications for Public-Key Cryptography Sponsor Microprocessorand Microcomputer Standards Committeeofthe IEEE Computer Society. Approved 30 January 2000. 4. 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. 5. Еліас Р. Генератор ядер секціонованих помножувачів елементів полів Галуа GF(2m) для оптимального нормального базису 2-го типу / В. Глухов, Р. Еліас // Вісник Нац. ун-ту "Львів. політехніка". – 2012. – № 732. – С. 78–84. 6. 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.

9. Jean-Pierre Deschamps, Jose Luis Imana, Gustavo D.Sutter Hardware Implementation of Finite-Field Arithmetic. McGraw Hill, March 2009. 7. Шологон О. З. Обчислення структурної складності помножувачів у поліноміальному базисі елементів полів Галуа GF(2^m). Шологон О. З. // Вісник Нац. ун-ту "Львів. політехніка", 2014 8. Черкаський М. В., Мурад Хусейн Халіл. Універсальна SH-модель Комп'ютерні системи та мережі // Вісник Нац. ун-ту"Львівська політехніка". – 2004. – № 523. – С. 150–154. 9. Глухов В. С., Глухова О. В. Результати оцінки структурної складності помножувачів елементів полів Галуа // Вісник Нац. ун-ту "Львів. політехніка", – 2013. – № 773. 10. Албанський І. Б. Дослідження системних характеристик цифрових пристроїв множення реалізованих в різних теоретико-числових базисах [Електронний ресурс] / І. Б. Албанський, О. І. Волинський // Вісник Хмельницького національного університету. – 2012. – № 2. – С. 179–186. 11. Пат. US 5768168A US 08/656,784 Universal Galois field multiplier/ Jin-Hyeok Im; заявл. 30.05.1996, опубл. 16.061998. 12. Пат US 4918638A US 07/107,363 Multiplier in a galois field/ Michihito Matsumoto, Kazuhiro Murase; заявл. 9.10.1987, опубл. 17.04.1990. 13. Virtex-6 FPGA Family: Data heet.- Xilinx, January 2009/ - DS312.10.

УДК 004.052

В. С. Яковина
Національний університет "Львівська політехніка",
кафедра програмного забезпечення

МОДЕЛЮВАННЯ ПАРАМЕТРА ПОТОКУ ВІДМОВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ВИЗНАЧЕННЯ ДІАПАЗОНІВ ПОКАЗНИКА ЙОГО СКЛАДНОСТІ

Проведено моделювання поведінки параметра потоку відмов програмного забезпечення у випадку моделі надійності ПЗ з індексом складності, що дало змогу встановити діапазони значень цього індексу та пояснити поведінку функції виявлення помилок залежно від складності програмного продукту.

Ключові слова: програмне забезпечення, якість, надійність, складність, параметр потоку відмов.

SOFTWARE FAILURE INTENSITY MODELLING AND IDENTIFICATION THE MARGINS OF THE COMPLEXITY INDEX

The behaviour of failure intensity function for software reliability model with complexity index depending on the model parameters has been simulated. It allows identifying the margins of the complexity index and explaining the defect revealing function behaviour depending on software complexity.

Key words: software, quality, reliability, complexity, failure intensity.

Вступ

Надійність програмного забезпечення (ПЗ) є одним з найважливіших атрибутів його якості. Сьогодні значні досягнення в науці та створення проривних технологій вимагають все більшого зростання потужностей сучасної обчислювальної техніки. Так, від суто обчислювальних