УДК 004.032.2

В.С. Глухов[1], О.В. Глухова[2]
[1]Національний університет "Львівська політехніка",
[1]кафедра електронних обчислювальних машин,
[2]кафедра систем автоматичного проектування

РЕЗУЛЬТАТИ ОЦІНЮВАННЯ СТРУКТУРНОЇ СКЛАДНОСТІ ПОМНОЖУВАЧІВ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА

Розглядаються результати оцінювання структурної складності помножувачів елементів двійкових полів Галуа. Елементи поля представлено у нормальному базисі типу 2. Порядок поля сягає 998. Апаратна складність дає змогу реалізувати помножувачі на ПЛІС. Але велика структурна складність унеможливлює це зробити. У роботі структурна складність вираховується як загальна довжина внутрішніх зв'язків помножувачів. Для конкретних помножувачів визначена їхня структурна складність. Для окремих ПЛІС визначений показник складності, за якого імплементація стає вже неможливою.

Ключові слова: поля Галуа $GF(2^m)$, нормальний базис типу 2, помножувач, структурна складність.

In the article the results of the evaluation of the structural complexity of multiplier of elements of binary Galois fields . Elements of the field are represented in normal basis of type 2 . The order of the field reaches 998. The hardware complexity allows implement them on the FPGA . But great structural complexity can not do it. In this paper, structural complexity is calculated as the total length of the internal connections inside multipliers. Created cores hardware complexity allows their implementation in FPGA. Structural complexity for some multipliers is determined. Indices of structural complexity for which implementation becomes impossible where determined for some FPGA.

Key words: Galois field $GF(2^m)$, normal basis of type 2, multiplier, structural complexity.

Вступ

Сьогодні математичною основою опрацювання цифрового підпису є еліптичні криві. Обробка точок еліптичної кривої ґрунтується на виконанні операцій у полях Галуа $GF(2^m)$. Апаратна реалізація помножувача для таких полів вимагає великих витрат обладнання. Помножувачі можуть бути паралельними, послідовними і паралельно-послідовними – секційними. У роботі аналізуються результати синтезу секційних помножувачів елементів поля Галуа $GF(2^m)$ генератором ядер помножувачів. Помножувач обробляє m-розрядні елементів поля Галуа $GF(2^m)$, елементи подано з використанням нормального базису типу 2. Секційний помножувач формує m біт добутку порціями по n біт. Апаратна складність ядер помножувачів дає змогу їх реалізувати на сучасних ПЛІС. Але за великих значень m і n неможливо реалізувати ядра через їх високу структурну складність. Тут запропоновано метод оцінки структурної складності таких помножувачів. Метод ґрунтується на аналізі структури помножувальних матриць, які використовуються для множення представлених у гауссівському нормальному базисі типу 2 елементів поля Галуа.

1. Аналіз останніх досліджень та публікацій

Математичними основами цифрового підпису є еліптичні криві і поля Галуа. Одним з представлень елементів поля Галуа $GF(2^m)$ є його подання у гауссівському нормальному базисі типу 2.

Для цього базису відомі послідовний помножувач Мессі-Омури [1], паралельний помножувач і паралельно-послідовний помножувач (секційний). Помножувальні матриці для них досліджувалися у [2]. У [3, 4] особливості генераторів *VHDL*-описів (ядер) секційних помножувачів наведені і оцінена апаратна складність для згенерованих ядер з m = 515, 519, 998. Також було показано, що апаратна складність згенерованих ядер помножувачів уможливлює їхню реалізацію на сучасних ПЛІС. Але за великих значень m і n неможливо реалізувати ядра через їх високу структурну складність.

Оцінку структурної складності у попередніх дослідженнях не проводили. Першу спробу оцінити структурну складність було зроблено у [5].

2. Окреслення проблеми

Апаратна складність згенерованих ядер помножувачів дозволяє їх реалізацію на сучасних ПЛІС. Але за великих значень порядку поля і кількості ядер помножувачів реалізація на ПЛІС стає неможливою через високу структурну складність проекту. Тому актуальним стає завдання оцінки структурної складності окремих функціональних вузлів і можливості використання окремих ПЛІС для реалізації вказаних вузлів.

3. Цілі статті

Мета роботи – оцінити структурну складність помножувачів елементів двійкових полів Галуа при використанні нормального базису типу 2 і визначити можливості використання деяких ПЛІС для реалізації таких помножувачів.

4. Реалізація секційного помножувача

Послідовний помножувач Мессі-Омура (рис. 1) складається з двох регістрів зсуву операндів RGA та RGB і помножувальної матриці *M*. Секційний помножувач містить кілька помножувальних матриць (наприклад, *M*0, ..., *M*15 на рис. 2) і конвеєрний регістр *Output RG file* для накопичення результатів.

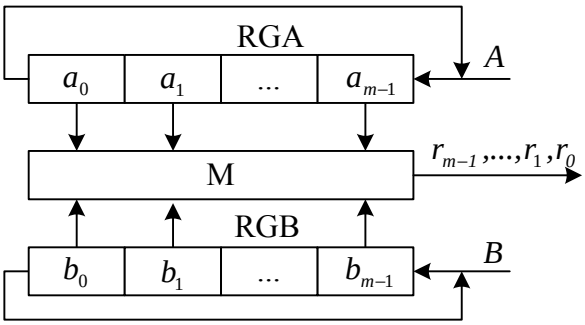

Рис. 1. Помножувач Мессі-Омури

Розряд r_0 добутку R обчислюється як $r_0=AMB^T$ (наприклад, на рис. 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 рис. 3).

Можна оцінити структурну складність умовної топології помножувача загальною довжиною L з'єднань усередині квадратної області на рис. 4: довжина горизонтального з'єднання g_i у i-му рядку дорівнює $g_i = x_i+1$, де x_i – номер стовпця найправішої “1” в i-му рядку, вертикальна довжина з'єднання в j-му стовпці дорівнює $v_j=m+d_j+1$, де d_j – різниця номерів рядків у j-му стовпці з “1”.

Кінцевий вираз:

$$L = \sum_{i=0}^{m-1} (g_i + v_i).$$

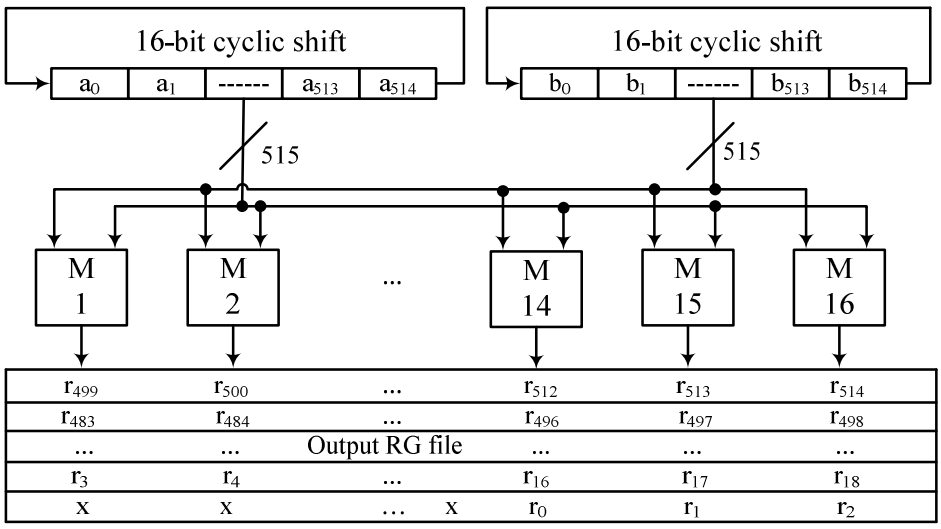

Рис. 2. Секційний помножувач

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

Рис. 3. Обчислення добутку та схема обчислення

5. Результати імплементації в ПЛІС

Для обчислення *L* для двійкових полів Галуа з великими *m* була розроблена спеціальна програма [5]. Вхідними даними для програми є порядок поля *m* та кількість секцій *n*. За їх допомогою визначається математичний опис помножувальної матриці. Результатами роботи програми є загальна довжина внутрішніх зв'язків у прямокутній області рис. 4. Умовна топологія багатосекційного помножувача показана на рис. 5. Результати підрахунків містять табл. 1–4.

Як бачимо з табл. 1–4, граничне значення структурної складності для обраних ПЛІС дорівнює приблизно 4…8 млн. умовних одиниць – для ПЛІС Virtex 6vlx130t, і приблизно 2 млн. – для ПЛІС Spartan xc6slx150t.

Схему стенда для дослідження помножувачів показано на рис. 6. Склад стенда:

– вузли пам'яті типу FIFO (FIFO1, FIFO2) для формування багаторозрядних операндів;
– вузли пам'яті типу FIFO (FIFO3) для збереження результату множення;
– власне помножувач (MCED1). Досліджувані помножувачі мають додатковий вихід CED (Concurrent Error Detection – вбудований вузол виявлення помилок), на якому формується ознака неправильного результату множення. Особливістю помножувачів, які працюють з елементами двійкових полів Галуа, представлених у нормальному базисі, є одночасність формування цієї ознаки і результату множення. При цьому структурна складність вбудованого вузла виявлення помилок є незначною порівняно із структурною складністю помножувача і у цій роботі вона не враховувалася.

Параметри стенда встановлюються глобальними константами:

MaxPosible (=1023), MinPosible (=0) – найбільший та найменший порядок двійкового поля Галуа, помножувачі якого можна досліджувати на цьому стенді;

GF_Order – порядок двійкового поля Галуа;

Slice_Number – кількість секцій у помножувачі.

6. Подальший напрямок роботи

Наведені результати є наближеними і унеможливлюють встановити чітку і очевидну границю можливостей ПЛІС для реалізації окремих проектів із відомою структурною складністю. Подальші роботи полягають в уточненні запропонованого методу оцінювання структурної складності функціональних вузлів. При цьому повинні враховуватися:

– зв’язки за межами прямокутної області однорозрядного помножувача (рис. 4);

– нерівномірність топології сучасних ПЛІС (площа, де розташовані логічні елементи, не є прямокутником);

– більші функціональні можливості сучасних ПЛІС (логічні елементи сучасних ПЛІС мають 4 … 6 входів, а не 2, як прийнято у цій роботі).

Також необхідно скласти базу даних структурної складності основних функціональних вузлів сучасних цифрових схем.

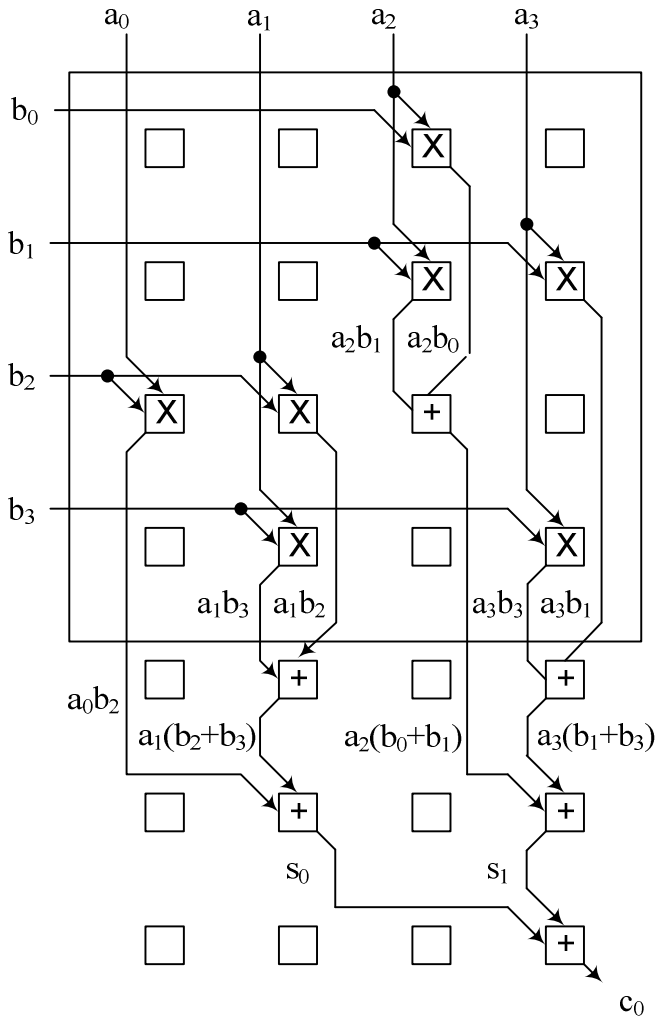

Рис. 4. Умовна топологія кристала односекційного помножувача

Таблиця 1

Virtex 6vlx130t (m=515)

m=515, n=	1	8	16	32
Кількість слайсів (%)	688 (3%)	1771 (8%)	2307 (11%)	7018 (35%)
Час імплментації, хв		5	304	**не розведено**
Структурна складність, довжини зв'язків	265139	2121112	4242224	8484448

Таблиця 2

Virtex 6vlx130t (m=519)

m=519, n=	1	8	16	32
Кількість слайсів (%)	675 (3%)	2248 (11%)	3240 (16%)	6,112 (30%)
Структурна складність, довжини зв'язків	268456	2147648	4295296	8590592

Таблиця 3

Virtex 6vlx130t (m=998)

m=998, n=	2	4	8	16
Кількість слайсів (%)		2,396 (11 %)	3,792 (18 %)	6,635 (33%)
Час імплментації, хв		3,5	145	102 (**не розведено**)
Структурна складність, довжини зв'язків	559624	1119248	2238496	4476992

Таблиця 4

Spartan xc6slx150t (m=998)

m=998, n=	2	4	8
Кількість слайсів (%)	1,323 (5%)	1,896 (8%)	3,253 (14%)
Час імплментації, хв	1	20	133, не розведено)
Структурна складність, довжини зв'язків	559624	1119248	2238496

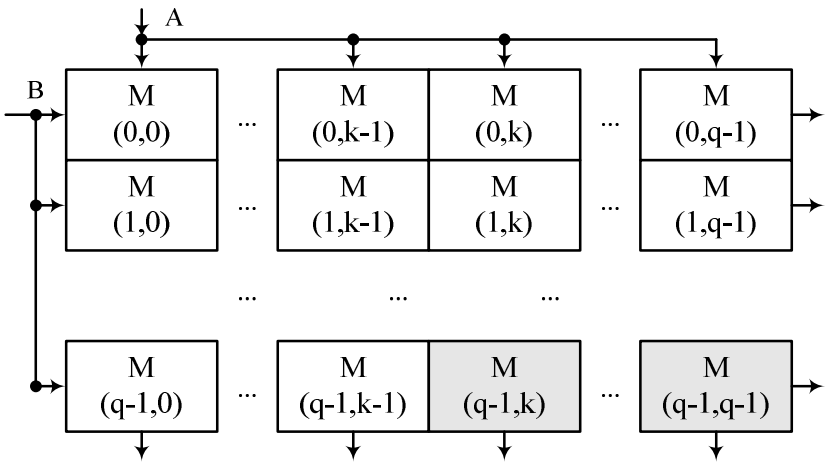

Рис. 5. Умовна топологія багатосекційного помножувача

Умовна топологія кристала ПЛІС багатосекційного помножувача зображена на рис. 5. Окремі секції розташовані у вигляді неповного квадрата розміром q x q секцій ($q = ceil(\sqrt{n})$ – заокруглення до найближчого більшого цілого кореня квадратного з кількості секцій n). Останній нижній рядок квадрата може бути заповнений частково, k визначає границю заповнення, незаповнені позиції квадрата виділено сірим кольором на рис. 6. Структурна складність S_M багатосекційного помножувача складається з сукупної складності усіх секцій $S_S=nL$ і структурної складності

S_{AB} (довжини зв'язків) шини операндів A та B. Структурна складність S_{AB} складається із структурної складності вхідної шини $S_{inA}=S_{inB}=mq$, структурної складності S_A внутрішньої шини A у рядках 0, …, q-2 та структурної складності S_B внутрішньої шини B у стовпцях 0, …, q-2 ($S_A=S_B=m(q-1)$).

$S_M= S_S+ S_{AB}= S_S+ S_{inA}+S_{inB} +S_A +S_B =nL+2\ mq+2\ m(q-1)= nL+2\ m(2q-1)$.

Табл. 1–4 містять тільки значення $S_S= nL$. Значення S_{AB} розраховується аналітично і не вимагає створення спеціального програмного забезпечення.

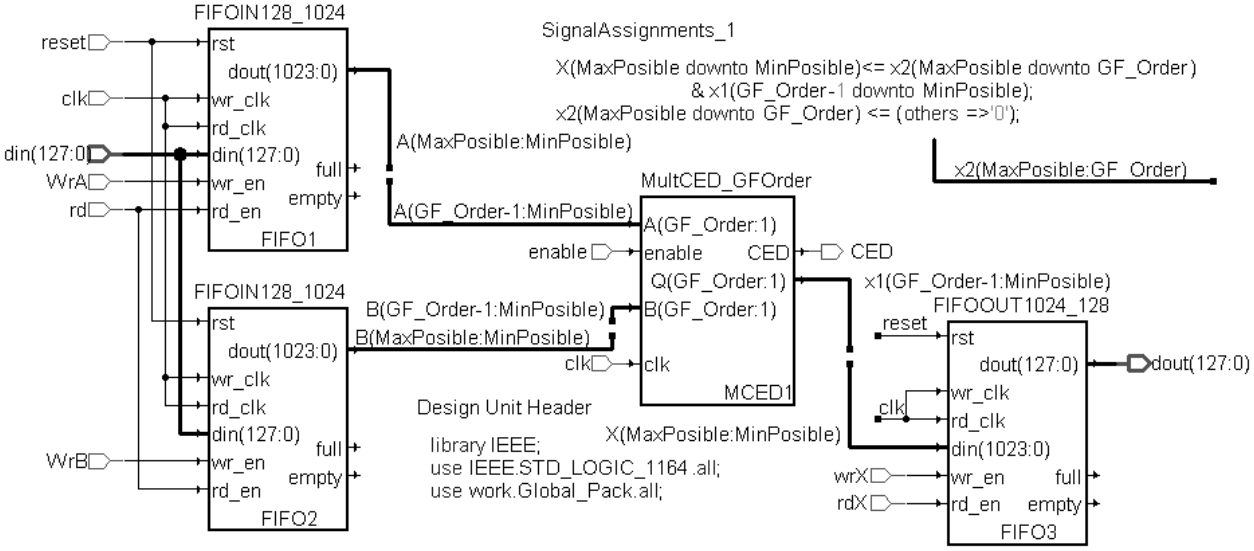

Рис. 6. Схема дослідження помножувачів

Висновки

У роботі наведено результати застосування раніше розробленого методу оцінки структурної складності на прикладі помножувачів елементів двійкових полів Галуа (елементи представлені у гауссівському нормальному базисі типу 2). Метод ґрунтується на дослідженні умовної топології кристала помножувача та обчисленні загальної умовної довжини його внутрішніх зв'язків. Була обчислена структурна складність деяких багатосекційних помножувачів, отримані значення складності були зіставлені з результатами проектування топології ПЛІС помножувачів. Були визначені наближені граничні значення структурної складності помножувачів, за яких ще можна реалізувати ці помножувачі на вибраних для аналізу ПЛІС.

1. Elias Rodrigue. Design of an Elliptic Curve Cryptography Using A Finite Field Multiplier in GF(2^{521}). Proceedings of the Lviv Polytechnic National University "Computer Systems and Networks". – Lviv, 2009. – № 658. – P. 144 – 149. 2. Глухов В.С. Особливості виконання операцій над матрицями в полях Галуа // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи проектування. Теорія і практика". – 2006. – Вип. 564. – С.35–39. 3. Еліас Р. Генератор ядер секціонованих помножувачів елементів полів Галуа GF(2m) для оптимального нормального базису 2-го типу / Р. Еліас, В. Глухов // Вісник Національного університету "Львівська політехніка" "Комп'ютерні науки та інформаційні технології". – 2012. – Вип. 732. – С.78–84. 4. Глухов В.С., Еліас Р.М., Мельник А.О. Особливості реалізації на ПЛІС секційних помножувачів елементів полів Галуа GF(2m) з надвеликим степенем // "Комп'ютерно-інтегровані технології: освіта, наука, виробництво" – науковий журнал Луцького національного технічного університету. – 2013. – № 12. – С. 103–106. 5. 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.