УДК 004.032.2

В. С. Глухов, Г. М. Тріщ
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

ОЦІНКА СТРУКТУРНОЇ СКЛАДНОСТІ БАГАТОСЕКЦІЙНИХ ПОМНОЖУВАЧІВ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА

Розглянуто результати оцінювання структурної складності багатосекційних помножувачів елементів двійкових полів Галуа. Елементи полів представлено у нормальному базисі типу 2. Порядок поля сягає 998. Апаратна складність помножувачів дає змогу реалізувати їх на ПЛІС. Але з-за великої структурної складності для деяких комбінацій порядку поля і кількості секцій зробити це практично неможливо. Для виявлення шляхів зменшення структурної складності у роботі структурну складність та її складові оцінено для основного елемента помножувачів – помножувальних матриць. Структурна складність при цьому визначається як загальна довжина внутрішніх зв’язків помножувальних матриць за їх реалізації на умовній ПЛІС.

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

GALOIS FIELD ELEMENTS MULTIPLIER STRUCTURAL COMPLEXITY EVALUATION

The article describes the results of evaluation of structural complexity of multi-section binary Galois fields elements multipliers. Elements of the fields are presented in the normal basis of type 2. The order of the field reaches 998. The hardware complexity multipliers allows to implement them on the FPGA. But because of the large structural complexity for certain combinations of the order of the field and the number of sections it is impossible. To identify ways to reduce structural complexity it and its components in main multiplier element – the multiplier matrix are estimated. Structural complexity thus defined as the total length of the internal connections inside multiplier matrices in their implementation on conventional FPGAs.

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

Вступ

Сьогодні 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 потребує великих витрат обладнання. Помножувачі можуть бути паралельними, послідовними і паралельно-послідовними – секційними. У роботі проаналізовано результати синтезу секційних помножувачів елементів поля Галуа $GF(2^m)$ генератором ядер помножувачів. Помножувач обробляє m-розрядні елементів поля Галуа $GF(2^m)$, елементи представлено з використанням нормального базису типу 2.

Секційний помножувач формує m бітів добутку порціями по n бітів. Апаратна складність помножувачів уможливлює їхню реалізацію на сучасних ПЛІС. Але за великих значень m і n неможливо реалізувати ядра через їхню високу структурну складність. Метод оцінки структурної складності таких помножувачів пропонується в цій роботі. Метод оснований на аналізі структури

помножувальних матриць, які використовують для множення представлених у гауссівському нормальному базисі типу 2 елементів поля Галуа.

Аналіз останніх досліджень та публікацій

Математичними основами цифрового підпису є еліптичні криві та поля Галуа. Одним з представлень елементів поля Галуа $GF(2^m)$ є його подання у гауссівському нормального базисі типу 2. Для цього базису відомі послідовний помножувач Мессі–Омури [1], паралельний помножувач і паралельно-послідовний помножувач (секційний). Помножувальні матриці для них досліджено в роботі [2]. В [3] описано алгоритм аналізу двійкових розрядів, що використовується для знаходження оберненого елемента матриці. Першу спробу оцінити структурну складність односекційного помножувача зроблено у [4].

Окреслення проблеми

Апаратна складність помножувачів дозволяє реалізувати їх на сучасних ПЛІС. Але за великих значень порядку поля і кількості секцій реалізація на ПЛІС унеможливлюється через високу структурну складність проекту. Тому актуалізується оцінка структурної складності окремих функціональних вузлів помножувачів для визначення шляхів її зменшення.

Цілі статті

Метою роботи є розроблення методів оцінки і оцінка структурної складності багатосекційних помножувачів елементів двійкових полів Галуа з використанням нормального базису типу 2, коли кількість секцій дорівнює 2^k (k = 1, 2,...).

Реалізація секційного помножувача

Послідовний помножувач Мессі–Омури (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.

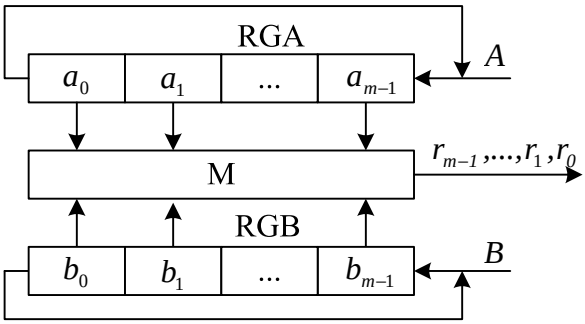

Рис. 1. Помножувач Мессі–Омури

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

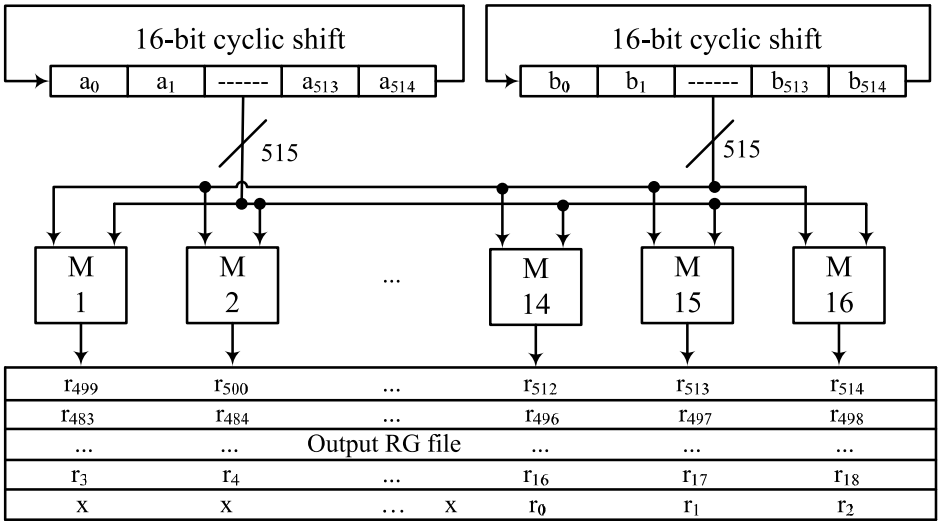

Рис. 2. Секційний помножувач

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

Рис. 3. Обчислення добутку та схема обчислення

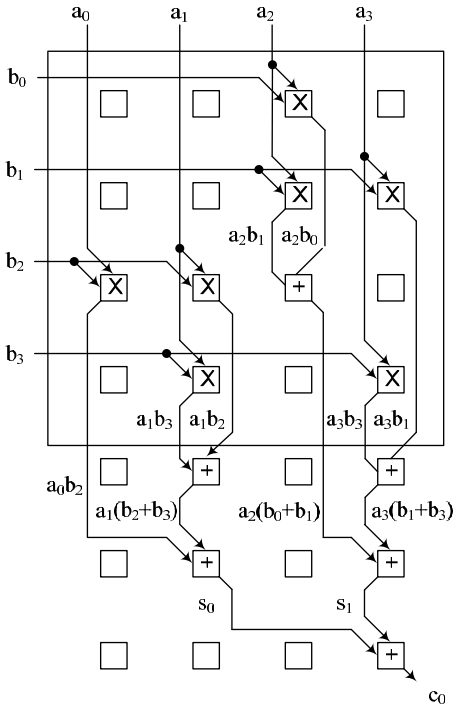

Рис. 4. Умовна топологія кристала односекційного помножувача

Для оцінки структурної складності за межами квадратної області потрібно здійснити згортання *m* сигналів, які формуються за межами квадратної області, в один. Для цього необхідно розробити алгоритм, який аналізуватиме двійкові розряди *m*. Схожий алгоритм аналізу двійкових розрядів використовується для знаходження оберненого елемента матриці [3].

Спираючись на алгоритм [3] знаходження оберненого елемента у нормальному базисі, а саме на метод аналізу двійкових розрядів, сформуємо власний алгоритм.

Вхід: Порядок поля Галуа (розмірність *m*).

Вихід: Довжина з'єднань *S* за межами квадратної області.

1. *Let* $m - 1 = m_r m_{r-1} \ldots m_1 m_0$ *be the binary representation of* $m - 1$*, where the most significant bit* m_r *of* $m - 1$ *is 1.*
2. *Set level* $\leftarrow 0$ *and* $k \leftarrow m/2$.
3. *For i from r – 1 down to 1 do*
   - 3.1. *Set* $S \leftarrow S + k*(2^{level} + 2)$.
   - 3.2. *If* $m_i = 0$*, then set* $S \leftarrow S$ *and* $k \leftarrow k/2$.
     - 3.2.1. *If* $m_{i+1} = 0$*, then set* $S \leftarrow S$ *and* $k \leftarrow k/2$.
     - 3.2.2. *If* $m_{i+1} = 1$*, then set* $S \leftarrow S + 1$ *and* $k \leftarrow k/2$.
   - 3.3. *If* $m_i = 1$ *and* $m_{i+1} = 0$*, then then set* $S \leftarrow S + 1$ *and* $k \leftarrow k/2$.
     - 3.3.1. *If* $m_i = 1$ *and* $m_{i+1} = 1$*, then then set* $S \leftarrow S + (2^{level-1} + 2)$ *and* $m_i \leftarrow 0$ *and* $k \leftarrow k/2+1$.
     - 3.3.2. *Set* $S \leftarrow S + 1$ *and* $k \leftarrow k/2$.
   - 3.4. *Set level* $\leftarrow$ *level + 1.*
4. *If* $2^{level} - m != 0$*, then set* $S \leftarrow S + (m \bmod 2^{level}) + 2$.
5. *Output S.*

Як бачимо, крайній лівий розряд m_r завжди є 1, тому підрахунок довжини з'єднань під час аналізу цього розряду буде відбуватися лише в тому випадку, коли виконається умова ($2^{level} - m != 0$).

Результати роботи запропонованого алгоритму і порівняння структурних складностей в квадратній області та за її межами для односекційного помножувача елементів полів Галуа подано в табл. 1 та на рис. 5.

Таблиця 1

Порівняння структурних складностей у квадратній області та за її межами

№	Розмірність *m*	Довжина з'єднань в квадратній області		Довжина згортки	
		L	%	S	%
1	4	37	78,72	10	21,28
2	7	111	83, 46	22	16,54
3	515	531394	99,37	3345	0,63
4	530	561772	99,39	3422	0,61
5	998	1992352	99,65	6914	0,35

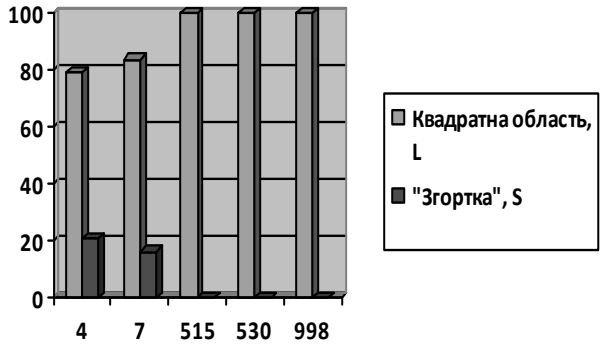

Рис. 5. Відсоткове порівняння структурних складностей односекційного помножувача елементів полів Галуа в квадратній області та за її межами

З порівняння структурних складностей у квадраті та за його межами видно, що структурна складність згортки S є набагато меншою, а за великих порядків поля Галуа у процентному співвідношенні менша за 1.

Оцінка структурної складності багатосекційних помножувачів елементів полів Галуа

Спробуємо об'єднати помножувачі в одну більшу структуру, збільшуючи кількість секцій 2^k (k=1, 2, …), усі секції однакового розміру.

Міжсекційні зв'язки розглядаємо як ще один додатковий "верхній" шар зв'язків, який лежить над квадратами. Цей шар утворюють горизонтальні й вертикальні зв'язки, які проходять від одного краю ПЛІС до другого, відповідно, зліва – направо і зверху – донизу.

Складність верхнього шару дорівнює складності вертикальних і горизонтальних зв'язків, які проходять від краю до краю ПЛІС.

$S = A + B$

де A – структурна складність по вертикалі;

$A = n \cdot m \cdot (n \cdot (m + level + 1))$

де level – рівень "глибини" згортки нижнього рівня;

B – структурна складність по горизонталі;

$B = n \cdot m \cdot (m + 1)$

Оскільки у такій моделі на нижньому шарі відсутні міжсекційні зв'язки, то його складність складається з квадратів і зв'язаних із ними згорток, а також складності виводів r_{ij} від кожного квадрата.

Структурна складність "нижнього" шару визначається підрахунком складності односекційного помножувача M(i,j) (рис. 4) для кожного M:

$L = q \cdot M$

де q – організація багатосекційної структури (у наведеному прикладі q = 4·4).

Для оцінки структурної складності згортки потрібно також обчислити додаткові виводи r_{ij} з кожного M(i,j):

$r_{ij} = (n-1) \cdot (m + level) + 1$

де level – рівень "глибини" згортки;

також зауважимо, що r_{0j} мають рівну довжину, тому:

$r_{0j} = n \cdot ((n-j-1) \cdot (m + level) + 1)$

…

Довжина всіх додаткових виводів:

$$R = \sum^{j}\sum^{j} n*(n-j-1)*(m+level+1)$$

Загальна структурна складність:

$C = L + S + R.$

На рис. 6 наведено приклад умовної структури багатосекційного помножувача елементів поля Галуа, порядок поля 4, кількість секцій 2^4.

У багатосекційних помножувачах для полів з великим порядком структурна складність у межах квадратних областей стає досить великою (табл. 2).

Відсоткове співвідношення структурної складності в квадратній області, за її межами та для "верхнього" шару, показує, що структурна складність згортки за малих порядків поля Галуа є значною, а за великих – стає меншою за 1 відсоток (рис. 7). Складність "верхнього" шару, як і складність у квадратних областях, в процентному співвідношенні – близько ½ кожна.

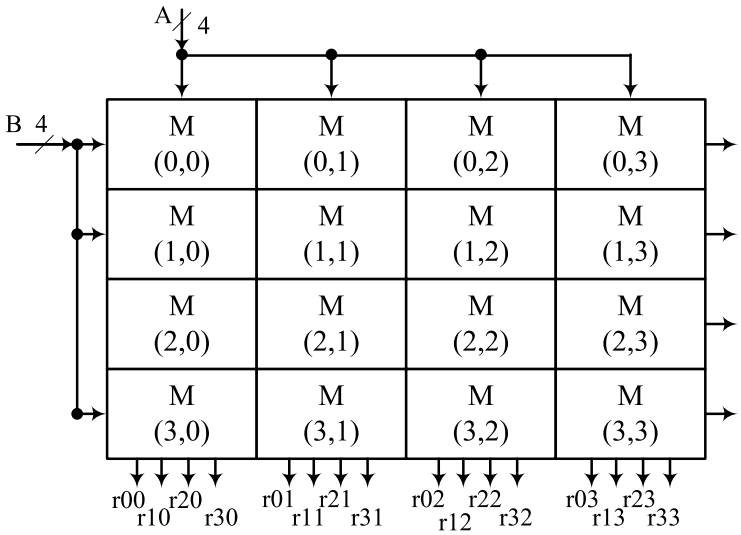

Рис. 6. Умовна топологія кристала багатосекційного помножувача

Таблиця 2

Порівняння структурних складностей

№	Роз-мір-ність	Структурна складність M(i,j)		Структурна складність виводів r_{ij}		Структурна складність "верхнього" шару		Загальна структурна складність багатосекційного помножувача
	m	L	%	R	%	S	%	C
1	4	752	51,7	168	11,5	528	36,8	1452
2	515	8555824	61,2	12624	0,2	5397200	38,6	13965648
3	998	31988256	61,5	24216	0,5	19956008	38	51968480

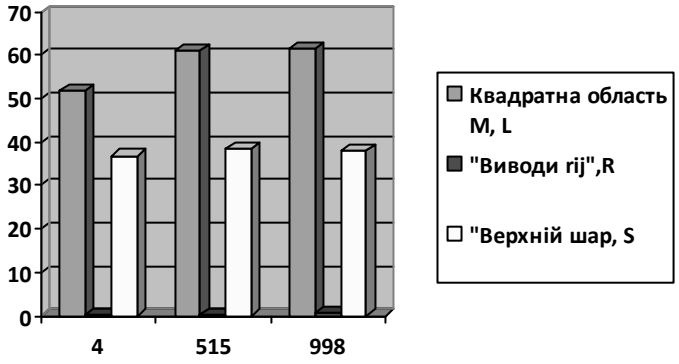

Рис. 7. Відсоткове порівняння структурних складностей, багатосекційних структур, у квадратній області, структурної складності згортки та "верхнього" шару

Подальший напрям роботи

Наведені результати є наближеними і не дозволяють встановити чітку і очевидну межу можливостей ПЛІС для реалізації окремих проектів із відомою структурною складністю. Подальші дослідження полягають у створенні методів та способів мінімізації оцінювання структурної складності як інших функціональних вузлів (а не тільки помножувачів), так і структурних можливостей ПЛІС. При цьому повинні враховуватися:

розташування окремих секцій у багатосекційних структурах;

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 у прийнято у цій роботі).

Також необхідно створити базу даних структурної складності основних функціональних вузлів сучасних цифрових схем та базу даних структурних можливостей ПЛІС.

Висновки

У роботі виконано порівняння структурних складностей одно- та багатосекційних структур на прикладі помножувачів елементів двійкових полів Галуа (елементи полів при цьому представлено у гауссівському нормальному базисі типу 2). Метод оснований на дослідженні умовної топології кристала помножувача та на обчисленні загальної умовної довжини його внутрішніх зв'язків. Обчислено структурну складність деяких багатосекційних помножувачів. Найбільший внесок у загальну структурну складність помножувача дають його помножувальна матриця і міжматричні зв'язки.

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 Нац. ун-ту "Львівська політехніка" "Комп'ютерні системи проектування. Теорія і практика". – 2006. – № 564. – С. 35–39. 3. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К.: Державний комітет України з питань технічного регулювання та споживчої політики. 2003. 4. Hlukhov V., Hlukhova A. Galois field elements multipliers structural complexity evaluation // Proceedings of the 6-th International Conference ACSN-2013. September 16–18, 2013. – Lviv, Ukraine. – P. 18–19.