УДК 004.032.2

СТРУКТУРНА СКЛАДНІСТЬ ПОМНОЖУВАЧІВ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА У НОРМАЛЬНОМУ ТА ПОЛІНОМІАЛЬНОМУ БАЗИСАХ

В. С. Глухов[1], Р. Еліас[2], М. Рахма[1]
[1]Національний університет «Львівська політехніка»
[2]Ліванський міжнародний университет, Ліван, м. Бейрут

***Анотація**. Опрацювання цифрового підпису базується на опрацюванні елементів поля Галуа $GF(2^m)$ з їхнім представленням у нормальному або поліноміальному базисах. Структурну складність помножувачів для таких полів Галуа, яка визначається як сумарна довжина зв'язків в топології досліджуваного вузла на уявній ПЛІС, для нормального та поліноміального базисів можна оцінити як $O(m^3)$ та $O(m^2)$ відповідно.*

Ключові слова: структурна складність, розширені поля Галуа, нормальний базис, поліноміальний базис, помножувач.

Вступ

У даний час математичною основою опрацювання цифрового підпису є еліптичні криві [1]. При цьому опрацювання точок еліптичної кривої базується на виконанні операцій у полях Галуа $GF(2^m)$, $m \le 998$, елементи яких може бути представлено у поліноміальному та нормальному базисах. Апаратна реалізація помножувачів для таких задач та полів вимагає великих витрат обладнання. У роботі [2] показано, що апаратне множення в поліноміальному і нормальному базисах вимагає приблизно однакових апаратних і часових витрат, програмно множення у поліноміальному базисі виконується на 1-2 порядки швидше. Але недоліком поліноміального базису є залежність часу обчислення обернених елементів полів Галуа від значення операндів [2]. Помножувачі можуть бути паралельними (в тому числі, на основі комірок Гілда [3]), послідовними і паралельно-послідовними - секційними. Для нормального базису апаратна складність послідовних помножувачів дозволяє проводити їхню реалізацію на сучасних ПЛІС. Але при великих значеннях порядків поля та кількості секцій неможливо реалізувати секційні та паралельні помножувачі через їхню високу структурну складність [4], методи та результати оцінювання структурної складності послідовного помножувача наведено в [5], багатосекційних помножувачів – у [6], оцінювання, що базується на використанні програмно-апаратної моделі – у роботах [7, 8], у [9], показано, що структурна складність помножувача для нормального базису поля Галуа $GF(2^m)$ лежить в межах від $(1/2 \dots 3/4)m^2$. Розроблення методів оцінювання структурної складності дозволили розробити методи її зменшення [10].

Одним з можливих варіантів розв'язку задачі є перехід на використання полів Галуа з основою n, більшою ніж 2, в першу чергу – з основою 3 [11]. При зміні поля можуть змінитися часові характеристики помножувача. У [12] з цієї точки зору оцінюється помножувачі для розширених полів Галуа $GF(d^n)$ з основами d, більшими за 2, і з приблизно однаковою кількістю елементів $d^n \approx 2^m$, що реалізуються на ПЛІС. Для аналізу обрано поліноміальний базис представлення елементів полів Галуа та помножувач з матричною структурою на основі модифікованих комірок Гілда [9]. Показано, що часова складність помножувача для поля $GF(3^n)$ для ПЛІС з 6-входовими комбінаційними програмованими логічними вузлами приблизно в 1,5 разів менша за часову складність помножувача для поля Галуа $GF(2^m)$. У роботі [13] показано, що і за апаратною складністю трійкові поля у поліноміальному базисі мають перевагу перед двійковими.

Порівняння структурної складності помножувачів для розширених полів Галуа з представленням їхніх елементів у поліноміальному та нормальному базисах не проводилося. Першим кроком може бути порівняння паралельних помножувачів, які одночасно формують усі розряди добутку, для двійкових полів Галуа $GF(2^m)$.

Метою роботи є дослідження структурної складності паралельних помножувачів для двійкових полів Галуа $GF(2^m)$ з представленням їхніх елементів у поліноміальному та нормальному базисах для визначення найкращого базису для побудови багатоядерних та багатосекційних помножувачів.

1. Секційний помножувач для нормального базису

Послідовний помножувач Мессі-Омури для множення у нормальному базисі елементів поля

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

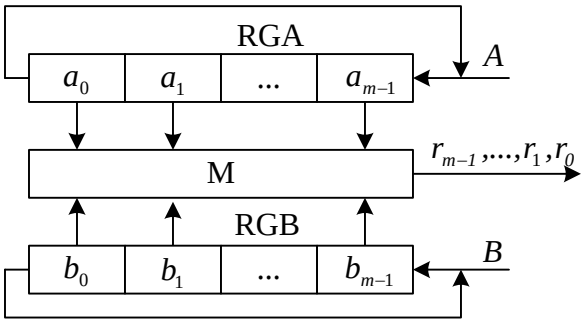

Рис. 1. Помножувач Мессі-Омури

Розряд r_0 добутку *R* обчислюється як $r_0=AMB^T$. Наприклад, відповідно до схеми обчислення рис. 3:

$$r_0 = a_2b_0 \oplus (a_2 \oplus a_3)b_1 \oplus (a_0 \oplus a_1)b_2 \oplus (a_1 \oplus a_3)b_3 .$$

Кожний наступний розряд добутку обчислюються після циклічного зсуву множників на один розряд.

Структурну складність помножувачів можна оцінити шляхом аналізу їхньої реалізації на умовній ПЛІС, кожний логічний елемент якої (квадрати на рис. 4, якому відповідає схема обчислення рис. 3) може реалізувати довільну функцію двох змінних.

Можна оцінити структурну складність топології помножувача загальною довжиною *L* з'єднань усередині квадратної області *Sqr* на рис. 4 (у [6] показано, що вузол згортки *Conv* дає незначний внесок до структурної складності помножувача): довжина горизонтального з'єднання g_i у *i*-тому рядку дорівнює $g_i = x_i+1$, де x_i - номер стовпця найправішої "1" в і-тому 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:

$$L = \sum_{i=0}^{m-1} (g_i + v_i) \approx (1/2 \ldots 3/4)m^2 .$$

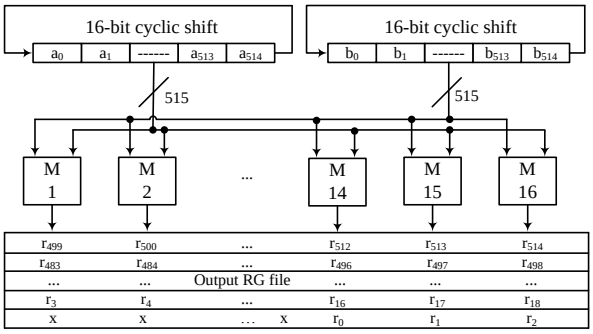

Рис. 2. Секційний помножувач

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

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

Рис. 3. Обчислення добутку та схема обчислення

2. Оцінка структурної складності багатосекційних помножувачів для нормального базису

Секційний помножувач (рис. 5) утворюється з послідовних помножувачів (секцій), кількість секцій *n* може бути від 1 (послідовний помножувач) до *m* (паралельний помножувач), усі секції однакового розміру і різняться циклічним зміщення по вертикалі і горизонталі суматорів і помножувачів у квадратній області (рис. 4) помножувальних матриць, що еквівалентно циклічному зсуву множників при обчисленні кожного наступного розряду добутку. Будемо вважати, що структурна складність помножувальних матриць не зменшується з-за циклічного зсуву їхніх елементів. Для спрощення будемо вважати, що секції розміщуються на кристалі у вигляді квадратної матриці максимальним розміром для паралельного помножувача $V=q*q$ елементів, $q = \lceil \sqrt{m} \rceil$.

Міжсекційні зв'язки розглядаємо як ще один додатковий «верхній» шар зв'язків, який лежить над квадратами *Sqr* та вузлами згортки *Conv*. Цей шар утворюють горизонтальні *B* та вертикальні *A* (рис. 5) зв'язки, які проходять від одного краю

ПЛІС до другого, відповідно, зліва - направо і зверху - донизу.

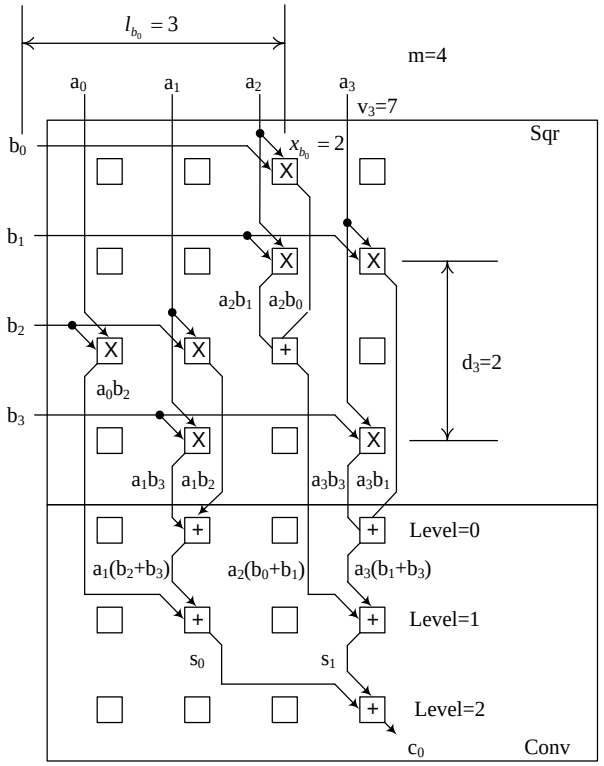

Рис. 4. Топологія умовної ПЛІС односекційного помножувача

Структурна складність *S* «верхнього» шару дорівнює сумарній довжині вертикальних і горизонтальних зв'язків, які проходять від краю до краю ПЛІС *S = V + G,*

де *V* – структурна складність по вертикалі топології сигналів A та B;

$$V=(V_{Sqr}+V_{Conv})m+V_B;$$

$$V_{Sqr}=(L_{Sqr}\cdot H_{Sqr})m;$$

$$L_{Sqr}=m; H_{Sqr}=m;$$

$$V_{Conv}=L_{Conv}\cdot H_{Conv};\ L_{Conv}=m;$$

$$HConv=level+1;$$

$$V=m^3+m^2log_2m+m\cdot q\cdot(m+log_2m)=$$

$$=(m^2+m\cdot q)(m+log_2m)=$$

$$=m(m+q)(m+log_2m)=$$

$$=m(m+\sqrt{m})(m+log_2m).$$

V_{Sqr}, V_{Conv} – структурна складність проведення по вертикалі сигналів *A* «над» квадратною частиною секції та над її вузлом згортки;

L_{Sqr}, H_{Sqr} – ширина та висота квадратної частини секції;

L_{Conv}, H_{Conv} – ширина та висота вузла згортки секції;

$Level = log_2m$ – рівень «глибини» згортки – кількість рядків логічних елементів ПЛІС за межами квадратної зони (рис. 4);

V_B – структурна складність проведення по вертикалі сигналів B,

$$V_B=m\cdot q\cdot(m+log_2m),$$

G – структурна складність по горизонталі топології сигналів *B*, $G=m*m=m^2$.

Оскільки при такій моделі на нижньому шарі відсутні міжсекційні зв'язки, то його складність дорівнює складається усіх квадратів *Sqr* і зв'язаних із ним згорток *Conv*, а також складності виведення результатів r_{ij} від кожної згортки до периферії кристалу ПЛІС.

Структурна складність «нижнього» шару *L* дорівнює складності *M* усіх помножувальних матриць $M_{i,j}$ (кожна з яких складається з квадратної частини $Sqr_{i,j}$ та вузла згортки $Conv_{i,j,}$ рис. 5):

$$L=m\cdot M=km^3, k=½\ \ldots ¾\ .$$

При оцінюванні структурної складності потрібно також обчислити додаткові витрати на виведення результатів r_{ij} з кожної матриці *M(i,j)* до периферії кристалу ПЛІС:

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

$$r_{1j}=(q-2)\cdot(m+level),$$

…

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

Довжина всіх додаткових виводів:

$$R=\sum_{i=1}^{q}\sum_{j=0}^{q-1} r_{ij}=q(m+level)\sum_{i=1}^{q}(q-i)=$$

$$=q(m+level)\sum_{i=0}^{q-1} i=$$

$$=q(m+level)q(q-1)/2=$$

$$=m(m+log_2m)(\sqrt{m}-1)/2.$$

Загальна структурна складність:

$$C=L+S+R,$$

$$C=km^3+m(m+log_2m)(m+\sqrt{m})+m^2+$$

$$+m(m+log_2m)(\sqrt{m}-1)/2.$$

Для великих m (m прямує до 1000)

$$C \approx (k+1)m^3, k = ½ \ldots ¾.$$

Структурну складність паралельного помножувача для нормального базису двійкових полів Галуа $GF(2^m)$ можна оцінити як $O(m^3)$.

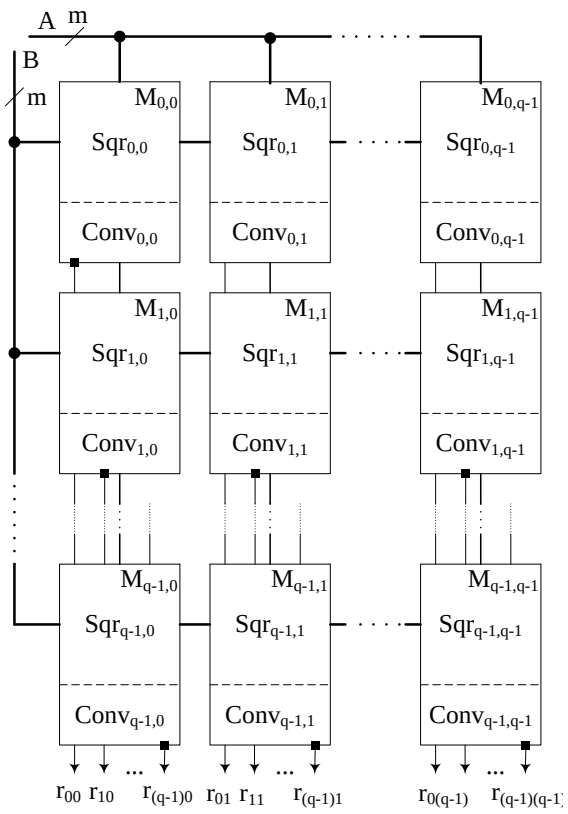

Рис. 5. Умовна топологія кристалу багатосекційного помножувача

3. Паралельний помножувач для поліноміального базису.

На рис. 6 показано функціональну схему помножувача двох елементів поля $GF(d^m)$ з використанням модифікованих комірок Гілда, детальну схему яких наведено на рис. 7. На рисунках позначено: p_i – розряди утворюючого поле полінома, $p = \lceil log_2 d \rceil$ – кількість біт у записі числа d (для двійкових полів Галуа $d = 2$, $p = 1$).

Пояснення до розрахунку структурної складності комірки Гілда для розширеного двійкового поля $GF(2^m)$ дає рис. 8.

Структурна складність C_a топології сигналу a через комірку Гілда дорівнює 2 (у комірці сигнал проходить повз 2 логічних елементи, один з них реалізує функцію множення, другий - додавання за модулем 2).

Структурна складність C_b топології сигналу b через комірку Гілда дорівнює 3 (у комірках сигнал проходить вниз повз 1 логічний елемент і проходить ліворуч повз 2 логічних елементи). Структурні складності топологій інших сигналів (ab, c_q) всередині комірки дорівнює 1, оскільки вони всі проходять повз або через 1 логічний елемент. Сумарна структурна складність комірки Гілда $C_{Gd} = C_a + C_b + C_{ab} + C_{c\_q} = 7$.

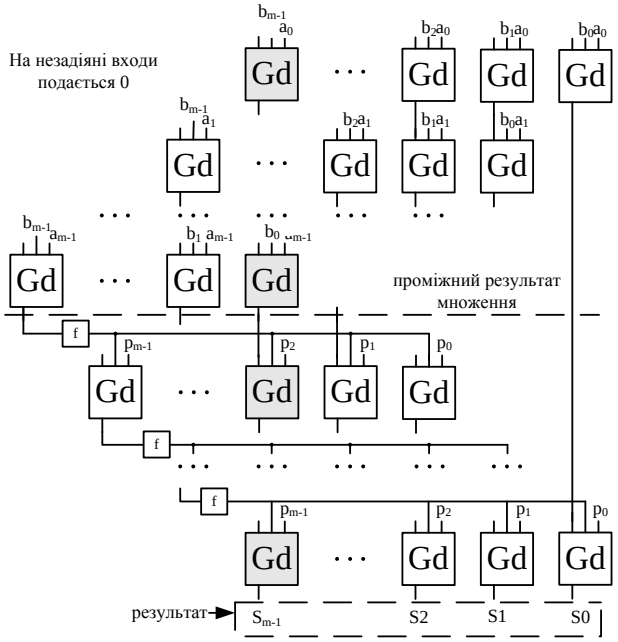

Рис. 6. Помножувач для елементів поля $GF(d^m)$ з використанням модифікованих комірок Гілда

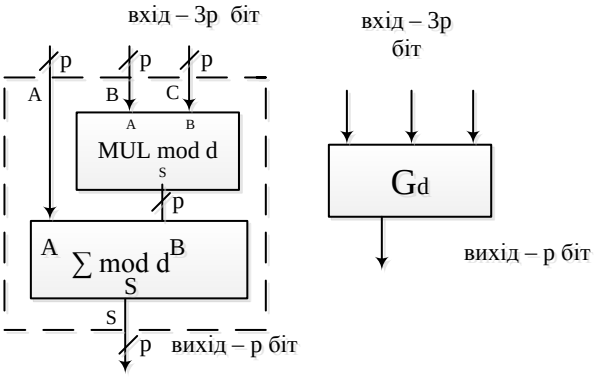

Рис. 7. Модифікована комірка Гілда для поля Галуа $GF(d^m)$

Структурна складність C_{PB} паралельного помножувача для поліноміального базису (рис. 6) складається з:

структурної складності всіх комірок Гілда $C_G = C_{Gd} \cdot m \cdot m \cdot 2 = 2C_{Gd} \cdot m^2 = 14m^2$;

структурної складності проведення вертикальних зв'язків між комірками Гілда:

$$C_V = C_S + C_f,$$

C_S – довжина зв'язків на вертикалі формування вихідних сигналів S, $C_S = 2m^2$;

C_f - довжина вертикальних зв'язків, що використовуються для формування сигналів *f*:

$$C_f = 1+3+5+\ldots+m-2 = m(m-1)/4;$$

структурної складності C_a проведення горизонтальних зв'язків *a* до перших справа комірок Гілда, які використовують відповідний сигнал, у кожному рядку верхньої частини помножувача:

$$C_a = 2(1+2+3+\ldots+(m-1)) = m(m-1)$$

(«ширина» комірки Гілда дорівнює 2 одиницям структурної складності);

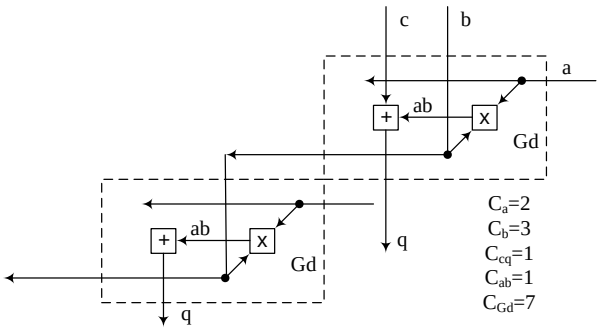

Рис. 8. Структурна складність комірки Гілда

структурної складності проведення горизонтальних зв'язків *f* між комірками Гілда:

$$C_f = m^2;$$

структурної складності C_p доведення розрядів p_i утворюючого полінома до першої заправа комірки Гілда, яка використовує відповідний сигнал:

$$C_p = C_{p0} + C_{p1} + C_{p2} + \ldots + C_{p(m-1)} =$$

$$= 1*2 + 2*2 + 3*2 + \ldots + (m-1)*2 = m(m-1).$$

Загалом

$$C_{PB} = C_G + C_S + C_f + C_a + C_g + C_p =$$

$$= 14m^2 + 2m^2 + m(m-1)/4 +$$

$$+ m(m-1) + m^2 + m(m-1) =$$

$$= 19m^2 + m(m-1)/4 - 2m .$$

Для великих *m* (*m* прямує до 1000)

$$C_{PB} \approx 20m^2 .$$

Структурну складність паралельного помножувача для поліноміального базису двійкових полів Галуа $GF(2^m)$ можна оцінити як $O(m^2)$.

4. Порівняння структурної складності помножувачів

Результати порівняння структурної складності помножувачів для поліноміального та нормального базисів показано на рис. 9, рис. 10 та рис. 11.

Для порядків $m < 12$ (рис. 9) двійкових полів Галуа $GF(2^m)$ меншу структурну складність мають помножувачі для роботи у нормальному базисі. Для більших порядків (рис. 10) меншу структурну складність мають помножувачі для роботи у поліноміальному базисі. Для $m >> 12$ (рис. 11, за [1] $m \geq 163$) використання поліноміального базису дає зменшення структурної складності в порівнянні з нормальним базисом приблизно в *m* разів.

Більша структурна складність помножувачів для нормального базису ускладнює і робить неможливим створення їхніх багатосекційних та паралельних версій [4]. Менша структурна складність помножувачів для поліноміального базису дозволить створити їхні багатосекційні версії з більшою кількістю секцій (з більшим рівнем паралелізму і, відповідно, більшою продуктивністю) ніж у аналогічних помножувачів для нормального базису.

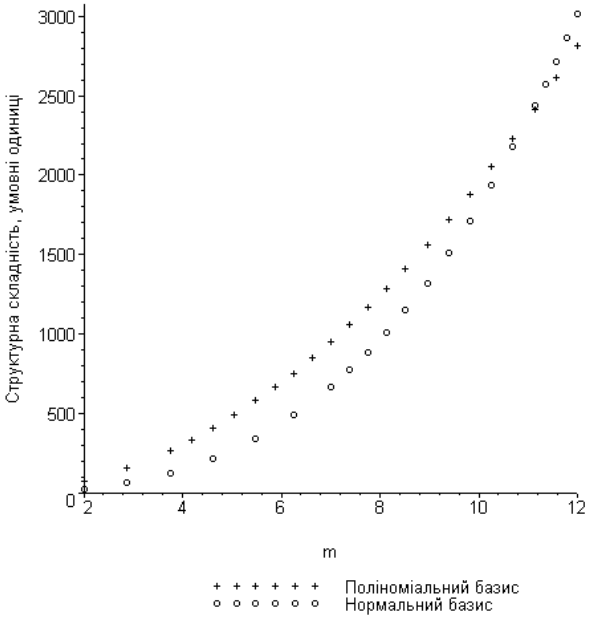

Рис. 9. Структурна складність помножувачів для поліноміального та нормального базисів ($m < 12$)

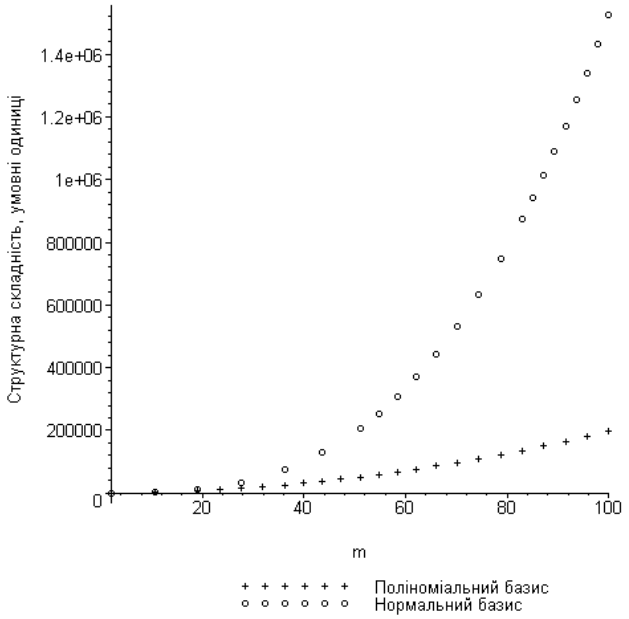

Рис. 10. Структурна складність помножувачів для поліноміального та нормального базисів ($m < 100$)

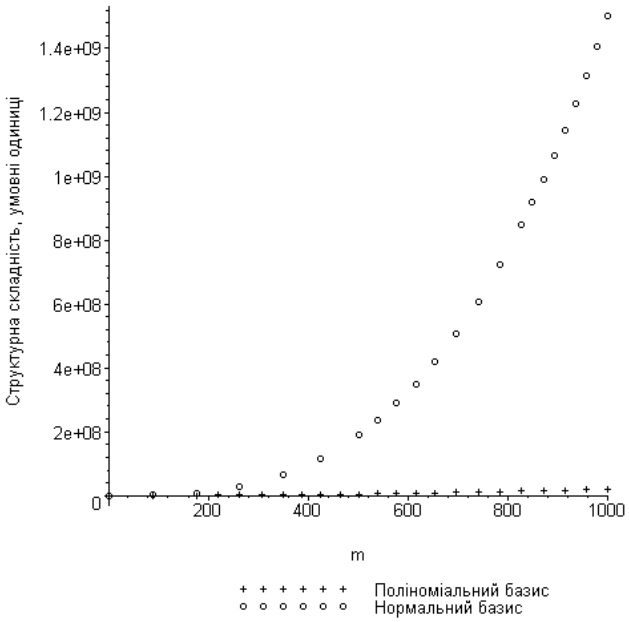

Рис. 11. Структурна складність помножувачів для поліноміального та нормального базисів ($m < 1000$)

Висновки

Проведено дослідження структурної складності паралельних помножувачів для двійкових полів Галуа з представленням їхніх елементів у поліноміальному та нормальному базисах.

Структурну складність паралельного помножувача для нормального базису двійкових полів Галуа $GF(2^m)$ можна оцінити як $O(m^3)$, для поліноміального базису - як $O(m^2)$.

Для порядків $m < 12$ двійкових полів Галуа $GF(2^m)$ меншу структурну складність мають помножувачі для роботи у нормальному базисі. Для більших порядків меншу структурну складність мають помножувачі для роботи у поліноміальному базисі. Для $m >> 12$ використання поліноміального базису дає зменшення структурної складності в порівнянні з нормальним базисом приблизно в m разів.

Менша структурна складність помножувачів для поліноміального базису дозволить створити їхні багатосекційні версії з більшою кількістю секцій (з більшим рівнем паралелізму і, відповідно, більшою продуктивністю) ніж у аналогічних помножувачів для нормального базису.

Список використаної літератури

1. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. [Текст] – К.: Державний комітет України з питань технічного регулювання та споживчої політики. 2003.

2. Глухов, В. С. Порівняння поліноміального та нормального базисів представлення елементів полів Галуа [Текст] / В. С. Глухов // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи проектування. Теорія і практика". № 591, Львів, 2007. С. 22–27.

3. H. H. Guild. Fully iterative fast array for binary multiplication and addition [Текст]. Electronics Letters, Volume 5, Issue 12, 12 June 1969, page 263.

4. Глухов, В. С., Еліас, Р. М., Мельник, А. О. Особливості реалізації на ПЛІС секційних помножувачів елементів полів Галуа $GF(2^m)$ з надвеликим степенем [Текст] / В. С. Глухов., Р. М. Еліас, А. О. Мельник // "Комп'ютерно-інтегровані технології:освіта, наука, виробництво" - науковий журнал, Луцький національний технічний університет. – Луцьк: 2013. - № 12. - С. 103–106.

5. Глухов, В. С., Глухова, О. В. Результати оцінювання структурної складності помножувачів елементів полів Галуа [Текст] / В. С. Глухов, О. В. Глухова // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – Львів: - 2013. – Вип. 773. – С. 27–32.

6. Глухов, В. С., Тріщ, Г. М. Оцінка структурної складності багатосекційних помножувачів елементів полів Галуа [Текст] / В. С. Глухов, Г. М. Тріщ // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – Львів: – 2014. – Вип. 806. – С. 27–33.

7. Шологон, О. З. Обчислення структурної складності помножувачів у поліноміальному базисі елементів полів Галуа GF(2^m) [Текст] / О. З. Шологон // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – Львів: – 2014. – Вип. 806. – С. 284–289.

8. Шологон, Ю. З. Оцінювання структурної складності помножувачів полів Галуа на основі елементарних перетворювачів [Текст] / Ю. З. Шологон // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – Львів: – 2014. – Вип. 806. – С. 290–295.

9. Глухова, О.В., Лозинський, А.Я., Яремкевич, Р.І., Ігнатович, А.О. Аналітична оцінка структурної складності помножувачів елементів полів Галуа [Текст]. / О. В. Глухова, А. Я. Лозинський, Р. І. Яремкевич, А. О. Ігнатович // Матеріали V Всеукраїнської школи-семінару молодих вчених і студентів. Сучасні комп'ютерні інформаційні технології. ACIT'2015. 22-23 травня 2015 року. Тернопіль. ТНЕУ. 2015. С. 166–167.

10. Глухов В. С., Элиас Р. Уменьшение структурной сложности многосекционных умножителей элементов полей Галуа [Текст]. / В. С. Глухов, Р. Элиас // Электротехнические и компьютерные системы. – 2015. – № 19(95) – С. 222–226.

11. І. М. Жолубак, А. Т. Костик, В. С. Глухов. Особливості опрацювання елементів трійкових полів Галуа на сучасній елементній базі [Текст] / І. М. Жолубак, А. Т. Костик, В. С. Глухов // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – Львів: – 2015. – Вип. 830. – С. 27–33.

12. Еліас, Р., Рахма, М., Глухов, В. С. Часова складність помножувачів для полів Галуа [Текст]. / Р. Элиас, М. Рахма, В. С. Глухов // Электротехнические и компьютерные системы. – 2016. – № 22 (98) – С. 323–327.

13. Жолубак, І. М., Глухов, В. С. Визначення розширеного поля Галуа GF(d^m) з найменшою апаратною складністю помножувача [Текст]. / І. М. Жолубак, В. С. Глухов // Вісник Національного університету «Львівська політехніка» "Інформаційні системи та мережі", № 854. Львів, 2016. С. 63–69.

References

1. DSTU 4145-2002 (2002), Information Technology. Cryptographic Techniques. Digital Signatures Based on Elliptic Curves. Generation and Verification [Informatsiyni tekhnolohiyi. Kryptohrafichnyy zakhyst informatsiyi. Tsyfrovyy pidpys, shcho gruntuyet'sya na eliptychnykh kryvykh. Formuvannya ta pereviryannya], *Derzhavnyy komitet Ukrayiny z pytan' tekhnichnoho rehulyuvannya ta spozhyvchoyi polityky*, Kiyv, Ukraine, 2003 (In Ukrainian).

2. Hlukhov, V. S. (2007), Comparison of polynomial and normal bases of Galois fields elements presentation [Porivnyannya polinomial"noho ta normal"noho bazysiv predstavlennya elementiv poliv Halua, *Visnyk Nacional"noho universytetu "L"vivs"ka politexnika" "Komp'yuterni systemy proektuvannya. Teoriya i praktyka"*, Lviv, Ukraine, vol. 591, pp. 22–27 (In Ukrainian).

3. Guild, H. H. (1969), Fully iterative fast array for binary multiplication and addition. Electronics Letters, Volume 5, Issue 12, 12 June , page 263 (In English).

4. Hlukhov, V. S., Elias, R. M., Mel'nyk A. O. (2013), Features of the FPGA-based Galois Field GF(2^m) Elements Sectional Multipliers with Extra Large Exponent, [Osoblyvosti realizatsiyi na PLIS sektsiynykh pomnozhuvachiv elementiv poliv Halua GF(2^m) z nadvelykym stepenem], *Komp"yuterno-intehrovani tekhnolohiyi:osvita, nauka, vyrobnytstvo - naukovyy zhurnal, Luts'kyy natsional'nyy tekhnichnyy universytet*, Luts'k, Ukraine, vol. 12, pp. 103–106 (In Ukrainian).

5. Hlukhov, V. S., Hlukhova, O. V. (2013), Structural Complexity of Galois Field Elements Multipliers Evaluation Results [Rezul'taty otsinky strukturnoyi skladnosti pomnozhuvachiv elementiv poliv Halua], *Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi"*, Lviv, Ukraine, vol. 773, pp. 27–32 (In Ukrainian).

6. Hlukhov, V. S., Trishch, H. M. (2014), Evaluation of structural complexity of multisection multiplier for Galois field elements [Otsinka strukturnoyi skladnosti bahatosektsiynykh pomnozhuvachiv elementiv poliv Halua], *Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi"*, Lviv, Ukraine, vol. 806, pp. 27–33 (In Ukrainian).

7. Sholohon, O. Z. (2014), Structural Complexity of Galois Field GF(2^m) Elements Multipliers in Polynomial Basis Calculation [Obchyslennya strukturnoyi skladnosti pomnozhuvachiv u polinomial'nomu bazysi elementiv poliv Halua GF(2^m)], *Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi"*, Lviv, Ukraine, vol. 806, pp. 284–289 (In Ukrainian).

8. Sholohon, Yu. Z. (2014), Based on Elementary Transducers Structural Complexity of Galois Field Multipliers Evaluation [Otsinyuvannya strukturnoyi skladnosti pomnozhuvachiv poliv Halua na osnovi elementarnykh peretvoryuvachiv], *Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi"*, Lviv, Ukraine, vol. 806, pp. 290–295 (In Ukrainian).

9. Hlukhova, O. V., Lozynskyi, A. Ya., Yaremkevych, R. I., Ihnatovych, A. O. (2015), Analytical evaluation of Galois field elements multipliers structural complexity [Analitychna otsinka strukturnoi skladnosti pomnozhuvachiv elementiv poliv Halua], *Materialy V Vseukrainskoi shkoly-seminaru molodykh vchenykh i studentiv. Suchasni kompiuterni informatsiini tekhnolohii. ACIT'2015*, 22-23 may 2015 year. Ternopil. Ukraine. TNEU. Pp. 166–167 (In Ukrainian).

10. Hlukhov, V.S., Elias, R. (2015), Galois Fields Elements Multisection Multipliers Structural Complexity Reduction [Umenshenie strukturnoy slozhnosti mnogosektsionnyih umnozhiteley elementov poley Galua], *Elektrotehnicheskie i kompyuternyie sistemyi*, Odessa, Ukraine, № 19 (95), pp. 222–226 (In Russian).

11. Zholubak, I. M., Kostyk, A. T., Hlukhov, V. S. (2015), Features of processing Binary Galois fields elements on modern hardware base [Osoblyvosti opratsyuvannya elementiv triykovykh poliv Halua na suchasniy elementniy bazieskye y komp'yuternыe systemy], *Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi"*, Lviv, Ukraine, vol. 830, pp. 27–33 (In Ukrainian).

12. Elias, R., Rahma, M., Hlukhov, V. (2016), Multipliers for Galois fields time complexity [Chasova skladnist' pomnozhuvachiv dlya poliv Halua], *Elektrotehnicheskie i kompyuternyie sistemy*, Odessa, Ukraine, № 22 (98), pp. 323–327 (In Ukrainian).

13. Zholubak, I. M., Hlukhov, V. S. (2016), Definition of the extended Galois field GF(d^m) with multiplier minimal hardware complexity [Vyznachennia rozshyrenoho polia Halua GF(d^m) z naimenshoiu aparatnoiu skladnistiu pomnozhuvacha], *Visnyk Natsionalnoho universytetu «Lvivska politekhnika» "Informatsiini systemy ta merezhi"*, vol. 854. Lviv, Ukraine, Pp. 63–69 (In Ukrainian).

STRUCTURAL COMPLEXITY OF MULTIPLIERS FOR GALOUAN FIELDS ELEMENTS IN NORMAL AND POLYNOMIAL BASES

V. S. Hlukhov[1], R. Elias[2], M. Rahma[1]
[1]Lviv Polytechnic National University
[2]Lebanese international university

Abstract*. Currently, the mathematical basis for digital signature processing are elliptic curves. Elliptic curve points processing is based on the performance of operations in Galois field GF(2^m) in normal or polynomial bases. Characteristics of multipliers for these bases are different. Software implementation for polynomial basis multiplier is one to two orders faster than one for normal basis implementation. Hardware implementations have similar hardware and time complexity. But normal basis multiplier provides a time constant inverse element calculation, and in the polynomial basis that time depends on the operands. The study of the structural complexity of multipliers is based on the use of an imaginary FPGA, all its logical elements can implement an arbitrary function of two variables. The structural complexity is estimated as the total length of studied unit links in the FPGA topology. It is shown that the structural complexity of parallel multipliers for normal and polynomial bases can be estimated as O(m^3) and O(m^2), respectively. The lower structural complexity for polynomial basis multipliers allow to create their multisection versions with higher number of sections (with higher concurrency and therefore better performance) than similar multipliers for normal basis.*

Key words*: Structural complexity, Galois fields, extended fields, normal basis, polynomial basis, multiplier.*

СТРУКТУРНАЯ СЛОЖНОСТЬ УМНОЖИТЕЛЕЙ ЭЛЕМЕНТОВ ПОЛЕЙ ГАЛУА В НОРМАЛЬНОМ И ПОЛИНОМИАЛЬНОМ БАЗИСАХ

В. С. Глухов[1], Р. Элиас[2], М. Рахма[1]
[1]Национальный университет «Львовская политехника»
[2]Ливанский международный университет

***Аннотация**. Обработка цифровой подписи базируется на обработке элементов поля Галуа GF (2^m) с их представлением в нормальном или полиномиальном базисах. Структурную сложность умножителей для таких полей Галуа, которая определяется как суммарная длина связей в топологии исследуемого узла на воображаемой ПЛИС, для нормального и полиномиального базисов можно оценить как $O(m^3)$ и $O(m^2)$ соответственно.*

***Ключевые слова:** структурная сложность, поля Галуа, расширенные поля, нормальный базис, полиномиальное базис, умножитель.*

Отримано 10.05.2017

Глухов Валерий Сергеевич, доктор технических наук, профессор, профессор кафедры электронных вычислительных машин Национального университета «Львовская политехника», ул. С. Бандеры, 12, Львов, Украина, E-mail: glukhov@polynet.lviv.ua , м/т.: +38-063-75-72-330.
Valeriy Hlukhov, Dr. of Science, Professor, Professor of the Department of Computer Engineering, Lviv Polytechnic National University, S. Bandera Str., 12, Lviv, Ukraine, E-mail: glukhov@polynet.lviv.ua, м/т.: +38-063-75-72-330.

ORCID ID:0000-0002-0542-7447

Элиас Родриг Митри, кандидат технических наук, инструктор кафедры электротехники и электронной инженерии Ливанского международного университета, Школа инженерии, Блок 1G, Ливанский международный университет, P.O. Box: 146404, Бейрут, Ливан, E-mail: rodrigue.elias@liu.edu.lb, м/т.: 961.3.492949
Elias Rodrigue Metri, PhD, an instructor at the School of Engineering at the Lebanese International University, School of Engineering, Block G, Lebanese International University, P.O. Box: 146404 Beirut, Lebanon
E-mail: rodrigue.elias@liu.edu.lb, Tel.: 961.3.492949

ORCID ID: 0000-0003-4506-0368

Рахма Мохаммед Кадим, аспирант кафедры электронных вычислительных машин Национального университета «Львовская политехника», ул. С. Бандеры, 12, Львов, Украина, E-mail: muhamed_kadhem@yahoo.com , +38-093-19-62-350
Rahma Mohammed Kadhim, PhD student of the Department of Computer Engineering, Lviv Polytechnic National University, S. Bandera Str., 12, Lviv, Ukraine, E-mail: muhamed_kadhem@yahoo.com, +38-093-19-62-350

ORCID ID: 0000-0002-8377-1833