УДК 004.032.2
Еліас Р., канд. техн. наук,
Рахма М.,
Глухов В. С., д-р. техн. наук

ЧАСОВА СКЛАДНІСТЬ ПОМНОЖУВАЧІВ ДЛЯ ПОЛІВ ГАЛУА

Анотація. *Апаратна складність помножувачів для двійкових полів Галуа GF(2^n) дозволяє реалізувати на ПЛІС операційний пристрій з декількома помножувачами. Але з-за великої структурної складності для деяких комбінацій великого порядку поля n і кількості помножувачів зробити це практично неможливо. Одним з можливих варіантів розв'язку такої задачі є перехід на використання полів Галуа з основою d, більшою ніж 2. У статті оцінюється помножувачі для таких розширених полів Галуа GF(d^m) з приблизно однаковою кількістю елементів $d^m \approx 2^n$ з точки зору їхньої часової складності для визначення поля, в якому помножувач буде мати найменшу часову складність.*

Ключові слова: *часова складність – поля Галуа - розширені поля – основа поля – порядок поля - помножувач.*

Элиас Р., канд. техн. наук,
Рахма М.,
Глухов В. С., д-р. техн. наук

ВРЕМЕННАЯ СЛОЖНОСТЬ УМНОЖИТЕЛЕЙ ДЛЯ ПОЛЕЙ ГАЛУА

Аннотация. *Аппаратная сложность умножителей для двоичных полей Галуа GF (2^n) позволяет реализовать на ПЛИС операционное устройство с несколькими умножителями. Но из-за большой структурной сложности для некоторых комбинаций большого порядка поля n и количества умножителей сделать это практически невозможно. Одним из возможных вариантов решения такой задачи является переход на использование полей Галуа с основанием d, больше чем 2. В статье оцениваются умножители для таких расширенных полей Галуа GF (d^m) с примерно одинаковым количеством элементов $d^m \approx 2^n$ с точки зрения их временной сложности для определения поля, в котором умножитель будет иметь наименьшую временную сложность*

Ключевые слова: *временная сложность – поля Галуа – расширенные поля – основание поля – порядок поля - умножитель.*

Elias R., PhD**,**
Rahma M.,
Hlukhov V., DrS

MULTIPLIERS FOR GALOIS FIELDS TIME COMPLEXITY

Abstract. *Multipliers for binary Galois field GF (2^n) hardware complexity allows to implement in FPGA an operational device with multiple multipliers. But because of the large structural complexity for some combinations of large order n of field and the multipliers number to make it is practically impossible. One of the possible choices of this problem solving is the move to using Galois fields with the base d, greater than 2. Multipliers for such extended Galois field GF (d^m) with approximately the same number of elements $d^m \approx 2^n$ are estimated in the article in terms of their time complexity to determine the fields in which the multiplier will have the least time complexity.*

Keywords*: time complexity - Galois field - expanded field - base of the field - order of the field – multiplier*

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^n), елементи яких можуть бути представлені у поліноміальному та нормальному базисах. Апаратна реалізація помножувача для таких полів вимагає великих витрат обладнання. Помножувачі можуть бути паралельними (в тому числі, на основі комірок Гілда [2]), послідовними і паралельно-послідовними - секційними. Для нормального базису апаратна складність помножувачів дозволяє проводити їхню реалізацію на сучасних ПЛІС. Але при великих значеннях порядків поля та кількості секцій неможливо реалізувати такі помножувачі через їх високу структурну складність [3], методи та результати оцінювання структурної складності окремого помножувача наведено в [4], багатосекційних помножувачів – у [5], оцінювання, що базується на використанні

програмно-апаратної моделі – у роботах [6, 7]. Розроблення методів оцінювання структурної складності дозволили розробити методи її зменшення [8].

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 [9]. При зміні поля можуть змінитися часові характеристики помножувача. У статті оцінюється помножувачі для розширених полів Галуа $GF(d^m)$ з основами d, більшими за 2, і з приблизно однаковою кількістю елементів $d^m \approx 2^n$, для визначення поля, в якому помножувач буде мати найменшу часову складність. Часова складність при цьому визначається відносно двійкового розширеного поля Галуа $GF(2^n)$ з приблизно такою ж кількістю елементів ($d^m \approx 2^n$) як кількість послідовно з'єднаних комбінаційних логічних програмованих вузлів LUT, що входять до складу ПЛІС [10, 11], знаходяться на найдовшому ланцюжку проходження вхідних сигналів помножувача на вихід і визначають час появи результату на виході помножувача після подачі операндів на його вхід. Для аналізу обрано поліноміальний базис представлення елементів полів Галуа та помножувач з матричною структурою на основі модифікованих комірок Гілда [8] (модифікована комірка Гілда не має входу та виходу переносу).

Метою роботи є визначення з множини полів Галуа $GF(d^m)$ (з приблизно однаковими кількостями елементів) поля, у якому часова складність помножувача буде найменшою.

Структура матричного помножувача для розширених полів Галуа.

На рис. 1 схематично показано функціональну схему помножувача двох елементів поля $GF(d^m)$ з використанням модифікованих комірок Гілда, детальна схема яких наведена на рис. 2. На рисунках позначено: q_i – розряди утворюючого поле полінома, $p = \lceil log_2 d \rceil$ – кількість біт у записі числа d.

Найбільша затримка виникає під час формування розряду S_{m-1}. Вона складається з затримок послідовно з'єднаних комірок Гілда, що утворюють вертикальний стовпчик, на виході якого формується розряд S_{m-1}. Ця найбільша затримка $t_{Mul} = 2mt_G$, де t_G – затримка сигналів однією коміркою Гілда (рис. 2).

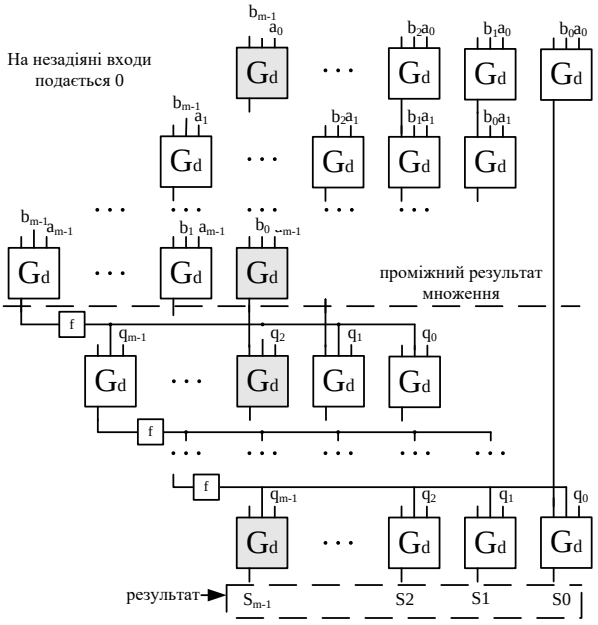

Рис. 1 Помножувач для поля $GF(d^m)$ з використанням модифікованих комірок Гілда

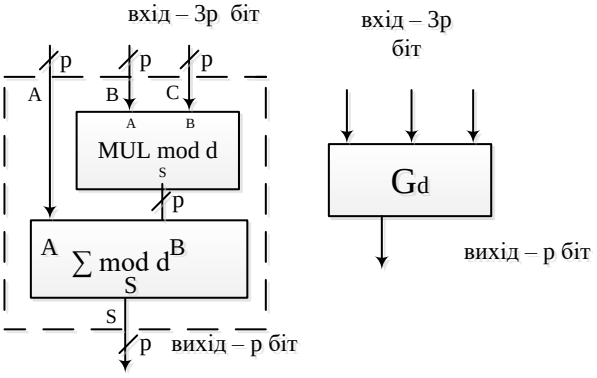

Рис. 2 Модифікована комірка Гілда для поля Галуа $GF(d^m)$

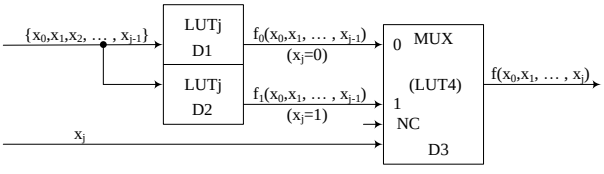

Рис. 3 Утворення LUTj з LUT(j-1)

Формальний підхід до визначення затримки модифікованої комірки Гілда

Модифіковані комірки Гілда при реалізації на ПЛІС будуються з

програмованих комбінаційних логічних вузлів (LUTv), кожний з яких має v входів та 1 вихід і може бути запрограмований на реалізацію довільної логічної функції v змінних. До складу сучасних ПЛІС входять логічні комбінаційні вузли LUTv з кількістю входів v=4 та v=6 (ПЛІС Spartan 3 та Spartan 6, відповідно, [10, 11]). При необхідності утворення з таких LUTv j-входової комбінаційну схему LUTj з і виходами необхідно задіяти $N_{j,i} = i(2^{j-v+1}-1)$ LUTv (j > v, i > 0, рис. 3). При цьому послідовно буде з'єднано $M_{j,i} = (j-v+1)$ LUTv. Якщо j≤v, то $N_{j,i} = i$, $M_{j,i} = 1$.

Модифікована комірка Гілда має 3p входів. Для випадку (3p > v, v = 4) p>1, що відповідає полям з основою d > 2, затримка модифікованої комірки Гілда дорівнює $t_G = (3p-v+1)t_v = (3p-3)t_v$, де t_v – затримка одного елемента LUTv, а $t_{Mul} = 2mt_G = 2m(3p-v+1)t_v = 2m(3p-3)t_v = C_{t,d}t_v$, де $C_{t,d} = 2m(3p-v+1) = 2m(3p-3)$ - часова складність помножувача для розширеного поля Галуа $GF(d^m)$.

Для випадку (3p ≤ v, v = 4) p = 1, що відповідає двійковим полям з основою d = 2, затримка модифікованої комірки Гілда дорівнює $t_G=t_v$, а $t_{Mul} = 2mt_G = 2mt_v = C_{t,2}t_v$, де $C_{t,2} = 2m$ - часова складність помножувача для двійкового поля Галуа $GF(2^m)$. Відповідно, $C_{t,2} = 2n$ - часова складність помножувача для двійкового поля Галуа $GF(2^n)$.

Оцінювання часової складності

За базу для оцінювання часової складності та для визначення кількості елементів поля береться розширене двійкове поле Галуа $GF(2^m)$, тоді $d^m \approx 2^n$, $m \approx log_d 2^n = \frac{n}{log_2 d}$, часова складність для розширеного поля з основою d $C_{t,d} = \frac{2n(3\lceil log_2 d \rceil - v + 1)}{log_2 d}$. Відносно часової складності розширеного двійкового поля Галуа $GF(2^m)$ часова складності розширеного поля Галуа $GF(d^n)$ (відносна часова складність) $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{(3\lceil log_2 d \rceil - v + 1)}$, $R_{2,2} = 1$.

Якщо прийняти v=4, тоді $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{(3\lceil log_2 d \rceil - 3)}$.

Якщо прийняти v=6, тоді $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{(3\lceil log_2 d \rceil - 5)}$. Якщо $R_{d,2} > 1$, то розширене поле з основою d має меншу часову складність в порівнянні із розширеним двійковим полем. Як видно (рис. 4), перевагу перед двійковим полем має тільки поле з основою d=3 (серед простих основ) при використанні LUT6 з 6 входами.

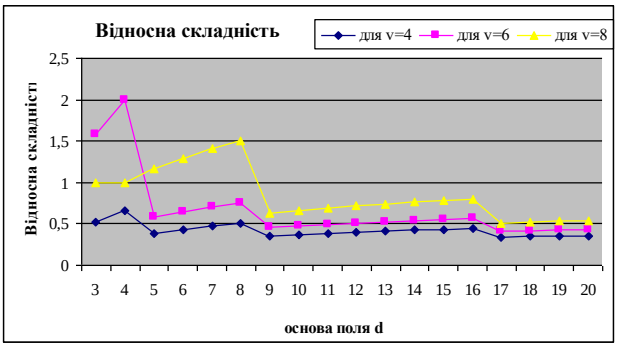

Рис. 4 Відносні часові складності для v=4 та v=6

На рис. 4 також показано оцінку часової складності при реалізації помножувача на гіпотетичній ПЛІС з логічними комірками, які мають 8 входів (LUT8). В цьому випадку перевагу перед двійковими полями будуть додатково мати розширені поля з простими основами d=5 та d=7.

Висновки

У статті для множини розширених полів Галуа $GF(d^m)$ з приблизно однаковими кількостями елементів поля визначається поле, у якому часова складність помножувача при його реалізації на сучасних ПЛІС є найменшою і меншою за часову складність помножувача для двійкового розширеного поля. Для аналізу обрано поліноміальний базис представлення елементів поля і матричний помножувач на основі модифікованих комірок Гілда.

Таким полем є поле $GF(3^m)$ для ПЛІС з 6-входовими комбінаційними програмованими логічними вузлами (LUT6), часова складність помножувача для нього приблизно в 1,5 разів менша за часову

складність помножувача для поля Галуа GF(2^m).

Запропонований метод може бути застосовано при аналізі інших помножувачів, а також при аналізі помножувачів для полів з нормальним базисом представлення елементів поля.

Список використаної літератури

1. 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.

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

3. Глухов В. С. 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.

4. Глухов В. С. 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.

5. Глухов В. С. 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.

6. 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.

7. 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.

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

9. Жолубак І. М. 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.

10. Spartan-3 FPGA Family: Introduction and Ordering Information. DS099 (v3.1) June 27, 2013. © Copyright 2003–2013 Xilinx, Inc.

11. Spartan-6 Family Overview. DS160 (v2.0) October 25, 2011. © 2009–2011 Xilinx, Inc.

Получено 30.04.2016

References

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

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

3. V.S. Hlukhov, R.M.Elias, A.O.Mel'nyk. Osoblyvosti realizatsiyi na PLIS sektsiynykh pomnozhuvachiv elementiv poliv Halua GF(2m) z nadvelykym stepenem [Features of the FPGA-

based Galois Field GF(2^m) Elements Sectional Multipliers with Extra Large Exponent]. *Komp"yuterno-intehrovani tekhnolohiyi:osvita, nauka, vyrobnytstvo - naukovyy zhurnal, Luts'kyy natsional'nyy tekhnichnyy universytet*. Luts'k, Ukraine, 2013, vol. 12, pp. 103 – 106 (In Ukrainian).

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

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

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

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

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

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

10. Spartan-3 FPGA Family: Introduction and Ordering Information. DS099 (v3.1) June 27, 2013. © Copyright 2003–2013 Xilinx, Inc. (In English).

11. Spartan-6 Family Overview. DS160 (v2.0) October 25, 2011. © 2009–2011 Xilinx, Inc. (In English).

Элиас Родриг Митри,
канд. техн. наук,
доц. Ливанского международного университета
м/т.: 961.3.492949.
E-mail: rodrigue.elias@liu.edu.lb

Рахма Мохаммед Кадим,
аспирант каф. ЕОМ Национального университета «Львовская политехника»
E-mail: muhamed_kadhem@yahoo.com

Глухов Валерий Сергеевич,
д-р. техн. наук, проф.,
проф. каф. Национального университета «Львовская политехника»
м/т.: +38(063)75-72-330.
E-mail: glukhov@polynet.lviv.ua