УДК 004.032.2

В. С. Глухов[1], Р. М. Еліас[2], М.К. Р. Рахма[1]
[1)]Національний університет «Львівська політехніка»,
кафедра електронних обчислювальних машин;
[2)]Ліванський міжнародний университет,
кафедра електротехніки та електронної техніки

ЧАСОВА СКЛАДНІСТЬ ОРІЄНТОВАНИХ НА ВИКОНАННЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ В СКЛАДІ КІБЕРФІЗИЧНИХ СИСТЕМ ПОМНОЖУВАЧІВ НА ОСНОВІ МОДИФІКОВАНИХ КОМІРОК ГІЛДА

© Глухов В.С., Еліас Р.М., Рахма М.К.Р., 2016

На елементи кіберфізичних систем, як правило, накладаються суворі обмеження на їхню апаратну, структурну та часову складності. Апаратна складність помножувачів для двійкових полів Галуа GF(2^n), що використовуються при криптографічному захисті інформації в КФС, 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 роботі оцінюється помножувачі на основі модифікованих комірок Гілда для таких розширених полів Галуа GF(d^m) з приблизно однаковою кількістю елементів d^m» 2^n з точки зору їхньої часової складності для визначення поля, в якому вона буде мати найменше значення. Оцінка проводилася для двох варіантів представлення комірок Гілда: коли комірка розглядається як «чорна скринька», тобто, для оцінювання використовуються тільки кількість входів та виходів комірки, та коли додатково враховується внутрішня структура комірки. Показано, що при реалізації на сучасних ПЛІС помножувач для розширених полів Галуа з основами d=3, 5, 7 має меншу часову складність ніж помножувач для двійкових полів. Ключові слова – розширені поля Галуа *GF*(d^n), комірка Гілда, помножувач, часова складність.

Вступ

На елементи кіберфізичних систем, як правило, накладаються суворі обмеження на їхню апаратну, структурну та часову складності. Апаратна складність помножувачів для двійкових полів Галуа GF(2^n), що використовуються при криптографічному захисті інформації в КФС, 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. При цьому необхідно оцінити апаратну, структурну та часову складність помножувачів для різних полів, для того щоб визначити поле, у якому ці складності будуть мати (окремо чи у сукупності) найменше значення.

У роботі оцінюється помножувачі на основі модифікованих комірок Гілда 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 вона буде мати найменше

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

значення. Оцінка проводилася для двох варіантів представлення комірок Гілда: коли комірка розглядається як «чорна скринька», тобто, для оцінювання використовуються тільки кількість входів та виходів комірки, та коли додатково враховується внутрішня структура комірки.

Аналіз останніх досліджень та публікацій

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. Відомий аналіз часової складності, коли комірка Гілда розглядається як «чорна скринька», що не враховує її внутрішню структуру. 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] та 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, 9]. .

Окреслення проблеми

При переході від обчислень у розширеному двійковому полі Галуа до обчислень у розширених полях з основами більшими 2 та приблизно однаковими кількостями елементів можуть змінитися часові параметри операційних вузлів, таких як помножувачі, а також їхні апаратні та структурні складності. Оцінка зміни складностей операційних вузлів при зміні поля не відома. Також не досліджувався вплив сучасної елементної бази на складність таких операційних вузлів.

Цілі статті

Метою роботи є визначення з множини полів Галуа $GF(d^m)$ (з приблизно однаковими кількостями елементів) поля, у якому часова складність помножувача при його реалізації на сучасній елементній базі (ПЛІС) з модифікованих комірок Гілда з відомою структурою буде найменшою.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Структура матричного помножувача для розширених полів Галуа.

На рис. 2 схематично показано функціональну схему помножувача двох елементів поля $GF(d^m)$з використанням модифікованих комірок Гілда (p_i – розряди утворюючого поле полінома, на незадіяні входи комірок Гілда подається 0), детальну схему яких наведено на рис. 1, де позначено $p = \lceil log_2 d \rceil$ – кількість біт у записі числа d.

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

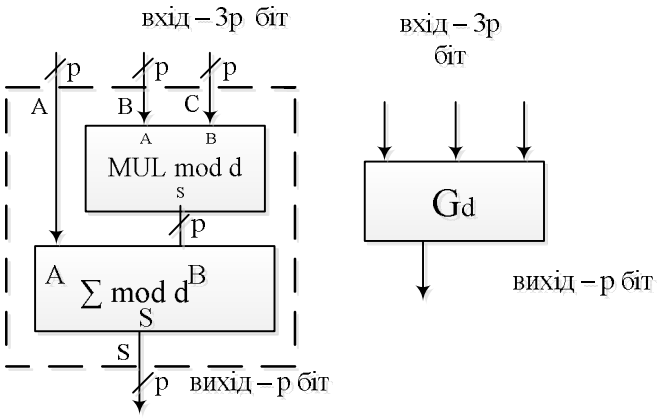

Рис. 1. Модифікована комірка Гілда для поля Галуа $GF(d^m)$

Для усунення впливу вузла f, якій змінює знак вхідних даних, на оцінку часової складності схема рис. 2 модифікується відповідно до рис. 4, де на прикладі трійкового поля Галуа $GF(d^m)$, d=3, показано, що якщо на один із входів комірки Гілда подавати від'ємне (за модулем d=3) значення операнду, то на її виході зформується ві'ємний (за модулем d=3) результат. Колами на символах комірок Гілда (рис. 4) показано входи та виходи з від'ємними значеннями даних. Від'ємні значення, що подаються на входи комірок Гілда, можуть бути розраховані наперед з використанням вузлів f, що не впливає на оцінку часової складності. Таким чином, частина комірок Гілда на схемі (рис. 2, рис. 4) буде формувати додатній результат, а частина – від'ємний, інверсний.

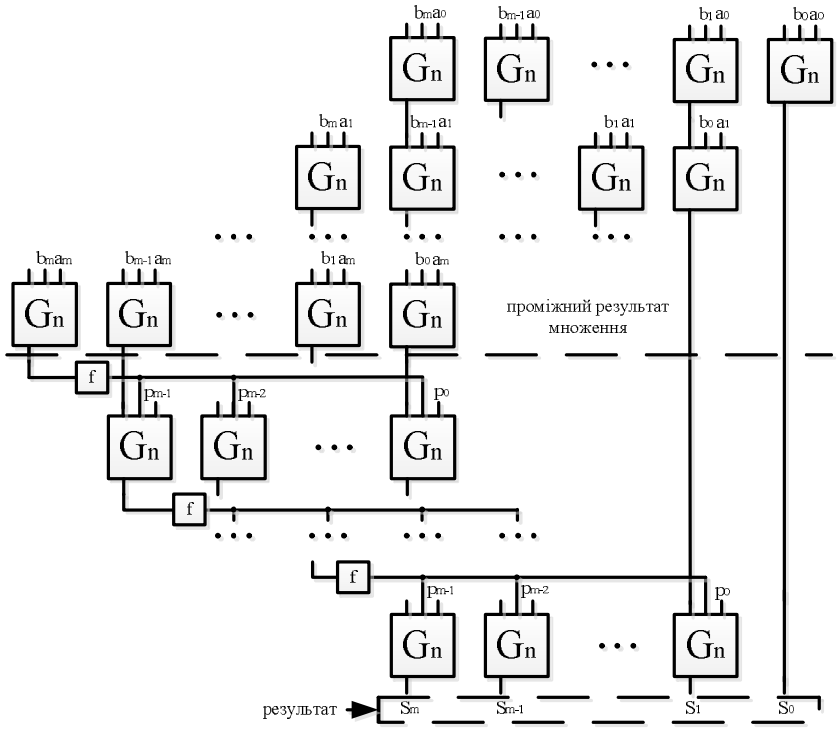

Рис. 2. Помножувач для поля $GF(d^m)$ з використанням модифікованих комірок Гілда

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

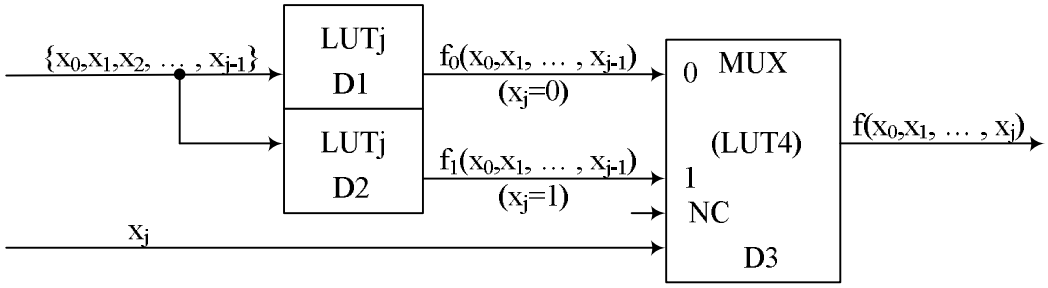

Рис. 3. Утворення LUT(j+1) з LUTj

Формальний підхід до визначення затримки модифікованої комірки Гілда

При формальному підході комірка Гілда розглядається як «чорна скринька» з відомою кількістю входів та виходів і з невідомою внутрішньою структурою. Це відповідає табличному методу обчислення (у даному випадку – множення) і реалізації помножувача у вигляді ПЗП на основі LUT

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 бінарних входів. Для випадку p>1 (3p > v, v = 4) , 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 $t_{Mul}=(2m-1)t_G=$ $=(2m-1)(3p-v+1)t_v = (2m-1)(3p-3)t_v = C_{t,d}t_v$, де $C_{t,d} = (2m-1)(3p-v+1) = (2m-1)(3p-3)$ – 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 $t_{Mul} = (2n-1)t_G = (2n-1)t_v = C_{t,2}t_v$, де $C_{t,2} = 2n-1$ – 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 $C_{t,d} = \frac{(2n-1)(3\lceil log_2 d \rceil - v+1)}{log_2 d}$. 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 $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{(3\lceil log_2 d \rceil - 3)}$.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

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.

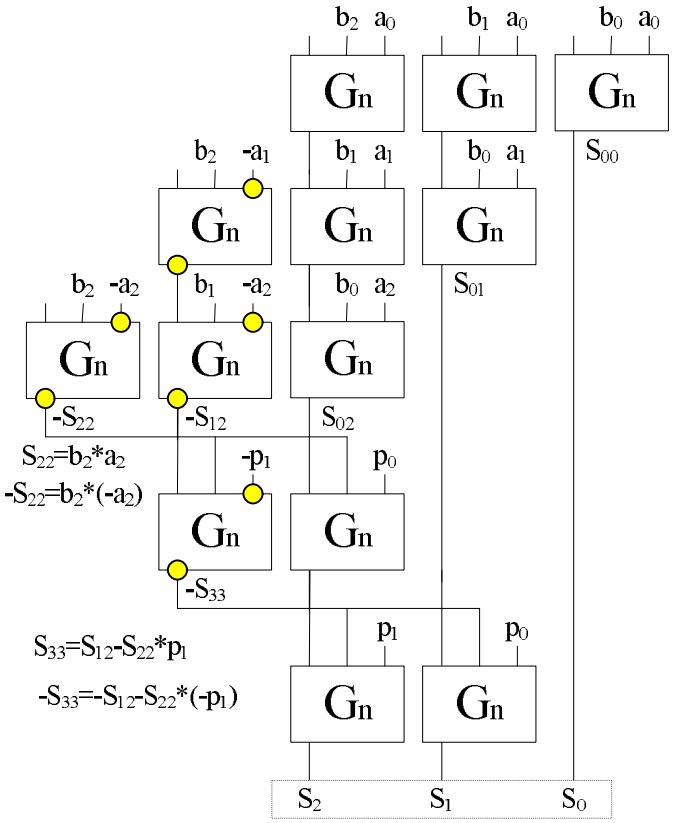

Рис. 4. Помножувач без вузла f (усі операції виконуються за модулем d=3)

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.

Визначення затримки модифікованої комірки Гілда з врахуванням її внутрішньої структури

При цьому підході комірка Гілда розглядається як така, що складається з модульного помножувача та модульного суматора (рис. 1), кожний з цих елементів має 2p входів та p виходів.

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

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

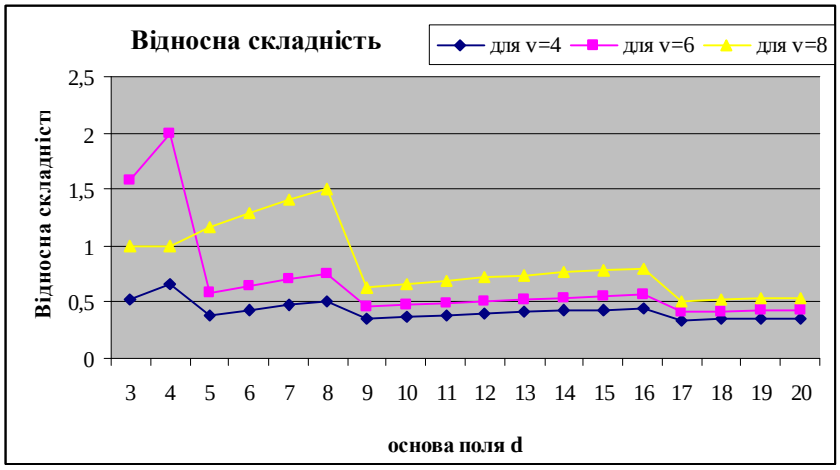

Рис. 5. Відносні часові складності для v=4 та v=6

Оцінювання часової складності помножувача з врахуванням його структури

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 $C_{t,d} = \frac{2(2n-1)(2\lceil log_2 d \rceil - v + 1)}{log_2 d}$. Відносно часової складності розширеного двійкового поля Галуа GF(2^m) часова складності розширеного поля Галуа GF(d^n) (відносна часова складність) $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{2(2\lceil log_2 d \rceil - v + 1)}$, $R_{2,2} = 1$.

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

Якщо прийняти v=6, тоді $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{2(2\lceil log_2 d \rceil - 5)}$. Якщо $R_{d,2} > 1$, то розширене поле з основою d має меншу часову складність в порівнянні із розширеним двійковим полем. Як видно (рис. 5), перевагу перед двійковим полем мають поля з простими основами d=5 GF(5^n) та d=7 GF(7^n) при використанні LUT6 з 6 входами та поля d=11 GF(11^n) та d=13 GF(13^n) при використанні LUT8 з 8 входами.

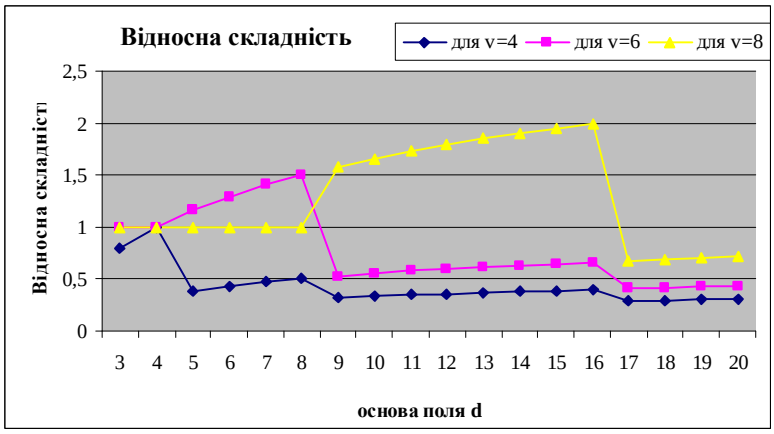

Рис. 6. Відносні часові складності з врахуванням структури помножувача

Як видно, внутрішня структура комірки Гілда суттєво впливає на оцінку її часової складності.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Висновки

У статті для множини розширених полів Галуа GF(d^m) з приблизно однаковими кількостями елементів поля визначаються поля, у яких 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. В залежності від обраної структури комірки Гілда та характеристик логічних вузлів (LUT) ПЛІС кращі часові характеристики можуть мати помножувачі для роботи у розширених полях Галуа GF(d^m) з основами d=3, 5, 7. Зменшення часової складності при цьому по відношенню до часової складності для полів Галуа не перевищує 1,6 разів.

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

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., 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 – 106.4. 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 – 32.5. 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 – 33.6. 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., Элиас Р. Уменьшение структурной сложности многосекционных умножителей элементов полей Галуа. / В.С.Глухов, Р.Элиас // Электротехнические и компьютерные системы. – 2015. – № 19(95) – С. 222-226.9. 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 – 33.10. 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.12. Р. Еліас, М. Рахма, В.С. Глухов. Часова складність помножувачів для полів Галуа. Програма II міжнародної науково – технічної конференції "Електротехнічні і комп'ютерні системи: теорія та практика" ELTECS – 2016. м. Одеса, 26 – 28 червня 2016.

Наукові результати, подані у цій статті, було отримано в рамках дослідницького проекту ДБ/КІБЕР з реєстраційним номером 0115U000446, 01.01.2015 – 31.12.2017, фінансово підтриманим Міністерством освіти та науки України.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua