УДК 004.382

І. Жолубак, В. Глухов
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

АПАРАТНІ ВИТРАТИ ПОМНОЖУВАЧІВ ПОЛІВ ГАЛУА GF (D^M) З ВЕЛИКОЮ ОСНОВОЮ

Порівняно апаратні витрати помножувачів елементів полів Галуа GF (d^m) з великою основою з метою визначення поля, у якому помножувач у разі його реалізації на сучасних ПЛІС матиме найменшу апаратну складність. Детально розглянуто внутрішню структуру основного елемента помножувача – модифікованої комірки Гілда, що складається із помножувача та суматора, які працюють за модулем m. Показано, що апаратні витрати помножувачів для розширених полів Галуа з основою, набагато більшою за 2, будуть асимптотично у 4 рази більшими за апаратні витрати помножувачів двійкових розширених полів Галуа.

Ключові слова: поля Галуа GF (d^m), помножувач, модифікована комірка Гілда, LUT.

The paper compares realised on modern FPGA Galois fields GF (d^m) elements multipliers hardware costs for great basis d to determine the field in which the multiplier has the lowest hardware complexity. Guild cell internal structure consisting of modul n multiplier and adder. It is shown that hardware costs will have a constant value 4 which tends to increase when the foundations of the field.

Key words: Galois fields GF (d^m), multiplier, modified Guild cell, LUT.

Вступ

У сучасних засобах захисту інформації використовують операції над полями Галуа GF (2^n) з великою кількістю елементів, які представлено в поліноміальному базисі. Опрацювання елементів таких полів характеризується високою апаратною, структурною та часовою складностями. Тому визначення можливості зменшення апаратної складності у разі використанняі замість двійкових розширених полів GF (2^n) полів Галуа GF (d^m) з основою $d \le 998$ та приблизно однаковою кількістю елементів ($d^m \approx 2^n$) є актуальною задачею.

Аналіз літературних джерел

За останні роки поняття еліптичних кривих знайшло своє застосування у криптографії. Причиною цього є те, що еліптичні криві над скінченними полями утворюють скінченні групи, на яких легко визначити арифметичні операції завдяки багатій структурі груп. Дотепер у криптографії працювали з мультиплікативними групами над деякими скінченними полями. За своїми властивостями еліптичні криві дещо нагадують ці групи, але їхня перевага полягає в тому, що існує більша свобода вибору еліптичної кривої, ніж вибору скінченного поля. Крім того, еліптичні криптосистеми забезпечують кращий захист інформації. Для виконання операцій над еліптичними кривими використовують арифметику полів Галуа, коди елементів таких полів [1, 2] подають у поліноміальному або нормальному базисах.

Помножувачі для таких полів характеризуються високою апаратною [3], структурною [4, 5] та часовою [6] складностями.

З літератури відомо багато пристроїв для опрацювання елементів полів Галуа GF (d^m) [7], які використовують у різних криптографічних перетвореннях. Відомий матричний помножувач для

двійкових чисел [8], який складається з комірок Гілда [9]. Також відомий помножувач на основі модифікованих комірок Гілда для виконання операцій множення елементів полів Галуа GF (d^m) [10]. У статті [11] розглянуто апаратні витрати матричних помножувачів полів Галуа GF (d^m), коли $d < 4$, у роботі [12] розглянуто апаратні витрати помножувачів, коли $d \le 998$, але не розглянуто внутрішньої структури модифікованих комірок Гілда та її впливу на оцінювання апаратної складності, що і є предметом цієї роботи.

Мета роботи

Метою роботи є дослідження апаратних витрати помножувачів полів Галуа GF (d^m) (з приблизно однаковими кількостями елементів) з великою основою та з врахуванням внутрішньої структури комірки Гілда. Коди елементів полів Галуа при цьому представляються в поліноміальному базисі.

Реалізація на ПЛІС

Помножувач для полів Галуа GF (d^m) може бути реалізований на основі модифікованих комірок Гілда (КГ). Модифіковані КГ для полів Галуа GF (d^m) мають 3 входи та 1 вихід розрядністю $p = \lceil \log_2 m \rceil$ біт кожний (рис. 1). У разі використання сучасних ПЛІС, логічні комірки яких будуються на основі програмовних 6-входових комбінаційних схеми (LUT - 6 входів, 1 вихід), реалізація на ПЛІС таких комірок Гілда у самому загальному випадку, коли не уточнюється структура КГ, а враховується тільки кількість її входів та виходів, потребує $q_1 = (2^{3p-5} - 1) \cdot p$ LUT.

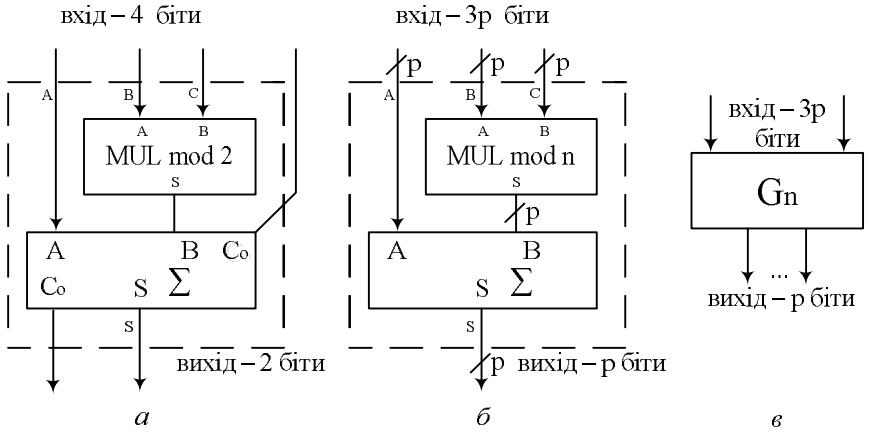

Рис. 1. Комірка Гілда, (а); модифікована комірки Гілда для обробки елементів полів Галуа GF (d^m), (б); умовне графічне позначення (символ) модифікованої комірки Гілда GF (d^m) (в)

Оцінити кількість LUT у комірці Гілда можна за кількома варіантами:

1) вважати комірку Гілда "чорною скринькою" – повністю цілісним елементом, в якому несуттєвою є внутрішня структура, а до уваги береться тільки кількість входів та виходів;

2) з уточненням внутрішньої структури (комірка Гілда складається з помножувача та суматора);

3) помножувач та суматор, що працюють за модулем m, у комірці Гілда складаються з базових функціональних елементів: мультиплексорів, однорозрядних двійкових суматорів та інших.

Два перші варіанти було розглянуто в попередніх роботах [10, 11], тому розглянемо тільки третій випадок.

Апаратні витрати зручно оцінювати, порівнюючи із витратами помножувача для двійкового поля Галуа GF (2^n).

Помножувач модифікованої комірки Гілда можна представити як матричний помножувач з прямим та зворотним ходом (рис. 3). За прямого ходу обчислень виконується операція множення, а за зворотного – знаходження остачі від ділення методом без відновлення залишків. За прямого ходуі одну комірку SMn можна реалізувати на KLUT1 = 2 елементах LUT (4 входи та 2 виходи), за зворотного – один елемент SMch на KLUT2 = 2 елементах LUT (5 входів, 2 виходи), а елементи Sn – на KLUT3 = 1 (3 входи, 1 вихід) та Rn – на KLUT4 = 1 (2 входи, 1 вихід) елементі LUT. Суматор SUM_G модифікованої комірки Гілда будується за допомогою ланцюжка повних однорозрядних двійкових суматорів. Два такі суматори (5 входів, 3 виходи) можна представити за допомогою 3 LUT – KLUT5 = 3. Дані представлення наведено на рис. 2.

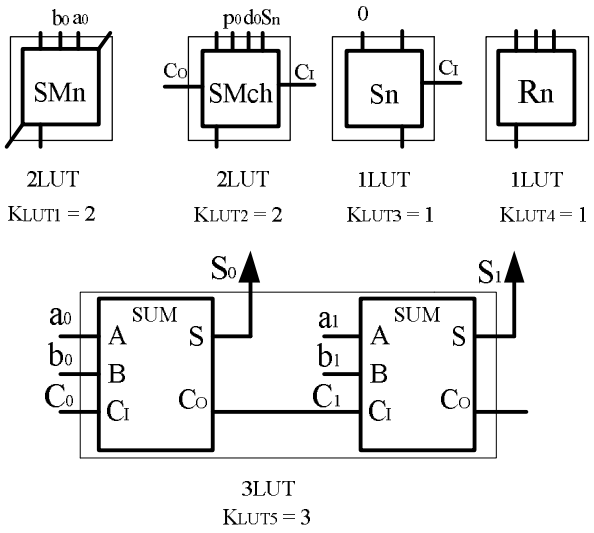

Рис. 2. Реалізація основних блоків в комірці Гілда GF (d^m) з великою основою на 6-входових LUT

SMn – елемент помножувача, який виконує операцію модульного множення та додавання і має виходи результату та перенесення, тобто це модифікована комірка Гілда. SMch – елемент, який виконує операцію додавання або віднімання числа в доповняльному коді у разі ділення без відновлення залишків. Sn – це вузол, який визначає тип операції, віднімання чи додавання у разі ділення без відновлення залишків. Rn – елемент, який визначає, чи потрібно проводити ще одну операцію додавання для знаходження результату.

Коефіцієнт апаратних витрат помножувача для елементів поля *GF (d^m)* відносно аналогічних витрат помножувача для елементів поля *GF (2^n)* $k_{mul} = k_g * k_k$, де $k_g = k_{gd} / k_{g2}$, $k_k = \frac{k_{kd}}{k_{k2}}$ – коефіцієнти складності та кількості КГ, k_{gd} та k_{g2}, k_{kd} та k_{k2} – кількість LUT у КГ та кількість КГ для полів Галуа *GF (d^m)* та *GF (2^n)*, відповідно.

Для двійкових полів Галуа GF (2^n) $k_{g2} = 1$, для інших:

k_{gd} = KSMn *KLUT1 + KSMch *KLUT2 + KSn *KLUT3 + KRn *KLUT4 + KSUMn *KLUT5,

KSMn, KSMch, KSn, KRn – кількості елементів, відповідно, SMn, SMch, Sn, Rn у помножувачі полів Галуа (рис. 3).

$$k_{gd} = (\lceil \log_2 d \rceil)^2 * 2 + (\lceil \log_2 d \rceil)^2 * 2 + \lceil \log_2 d \rceil * 1 + \lceil \log_2 d \rceil * 1 + \lceil \log_2 d \rceil * \frac{3}{2}$$

$k_{gd} = 2(\lceil log_2 d \rceil)^2 + 2(\lceil log_2 d \rceil)^2 + 2\lceil log_2 d \rceil + \frac{3}{2}\lceil log_2 d \rceil = 4(\lceil log_2 d \rceil)^2 + \frac{7}{2}\lceil log_2 d \rceil$. Отже:

$$k_g = 2(\lceil log_2 d \rceil)^2 + 2(\lceil log_2 d \rceil)^2 + \frac{1}{2}\lceil log_2 d \rceil + 2\lceil log_2 d \rceil = 4(\lceil log_2 d \rceil)^2 + \frac{7}{2}\lceil log_2 d \rceil \quad (1)$$

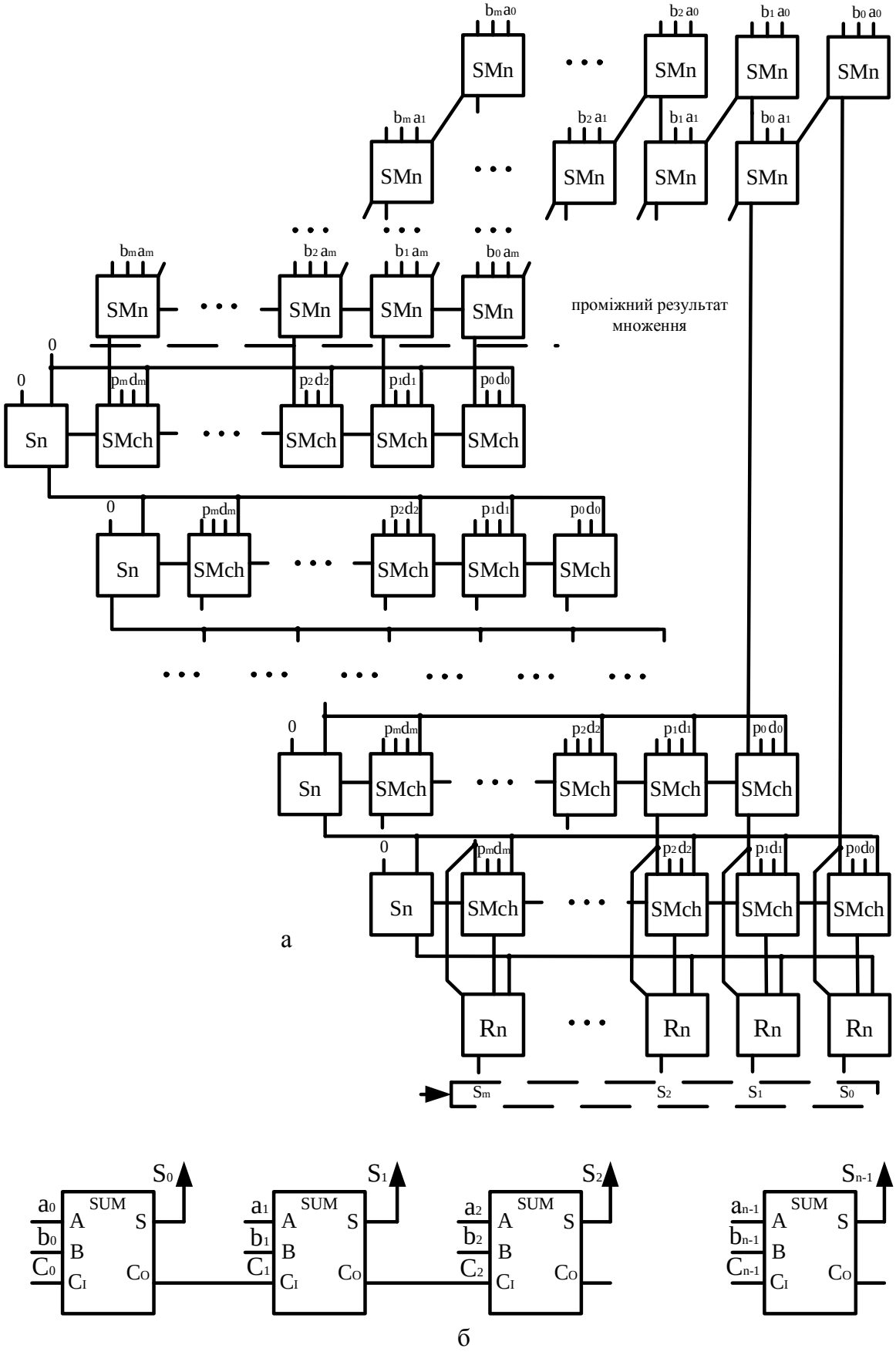

Рис. 3. Представлення внутрішньої структури помножувача MUL_G комірки Гілда GF (d^m) (а); суматора SUM_G комірки Гілда GF (d^m) (б)

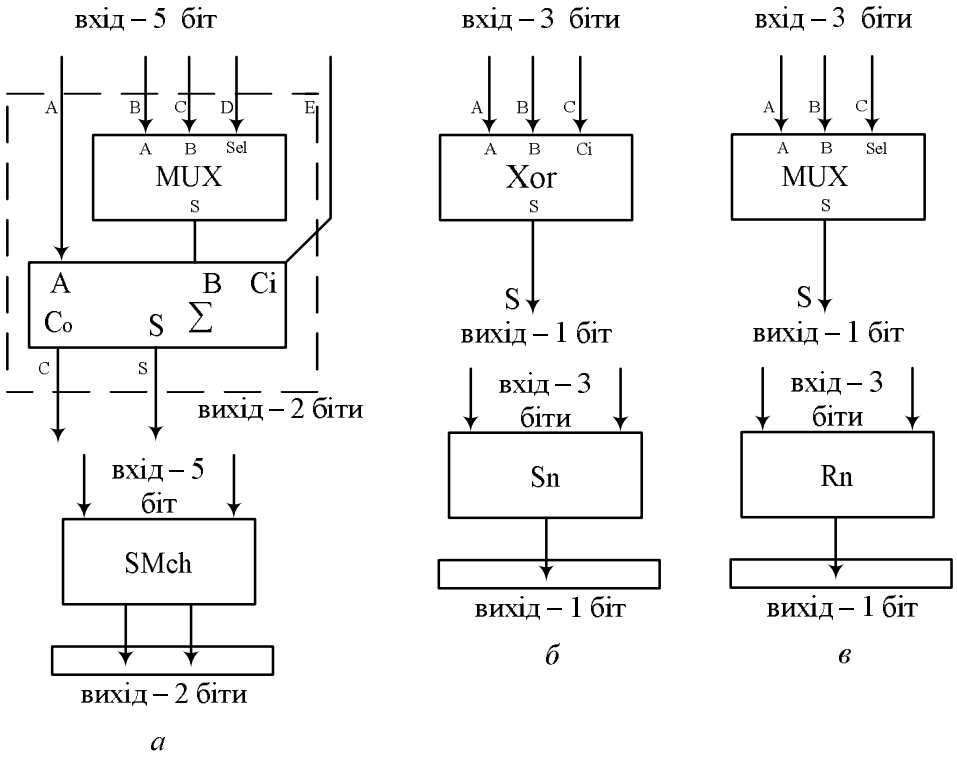

Рис. 4. схема елемента SMch, (а); схема елемента Sn, (б); схема елемента Rn (в)

У двійкових полях GF (2^n) для реалізації помножувача потрібно $k_{k2} = 2n^2 - 2n + 1$ комірок Гілда, а в полях Галуа GF (d^m) з основою d – $k_{kd} = 2m^2 - 2m + 1$. Також додатково $(m-1)*(2^{3*\lceil \log_2 d \rceil - 5} - 1)*\lceil \log_2 d \rceil$ LUT для знаходження коефіцієнта, на який потрібно перемножити незвідний поліном (цими апаратними можна в цьому випадку знехтувати, оскільки вони малі порівняно з витратами на реалізацію самих комірок Гілда). Отже:

$$k_k \approx \frac{2m^2 - 2m + 1}{2n^2 - 2n + 1} \approx \frac{m^2}{n^2} \approx \left(\frac{m}{n}\right)^2 \text{ для великих n,} \tag{2}$$

$$k_{mul} \approx \frac{(4(\lceil log_2 d \rceil)^2 + \frac{7}{2}\lceil log_2 d \rceil)m^2}{n^2} \tag{3}$$

При цьому $d^m \approx 2^n$. Тоді $m \approx log_d 2^n = \frac{n}{log_2 d}$, $k_k \approx log_2^{-2} d$,

$k_{mul} \approx \frac{4(\lceil \log_2 d \rceil)^2 + \frac{7}{2}\lceil \log_2 d \rceil}{(\log_2 d)^2}$. $lim_{d \to \infty} k_{mul} = 4$. Графік функції kmul наведено на рис. 4.

Для малих n k_{mul} треба розраховувати за точнішими формулами (1, 2, 3).

Як видно з рис. 4, відношення апаратних витрат на реалізацію помножувачів у полі GF (d^m) до апаратних витрат на реалізацію помножувачів у полі GF (2^n) у разі збільшення розміру поля прямуватимуть до асимптотичного значення 4, що свідчить про перевагу, з погляду апаратних витрат, використання двійкових розширених полів Галуа перед використанням розширених полів з великою основою.

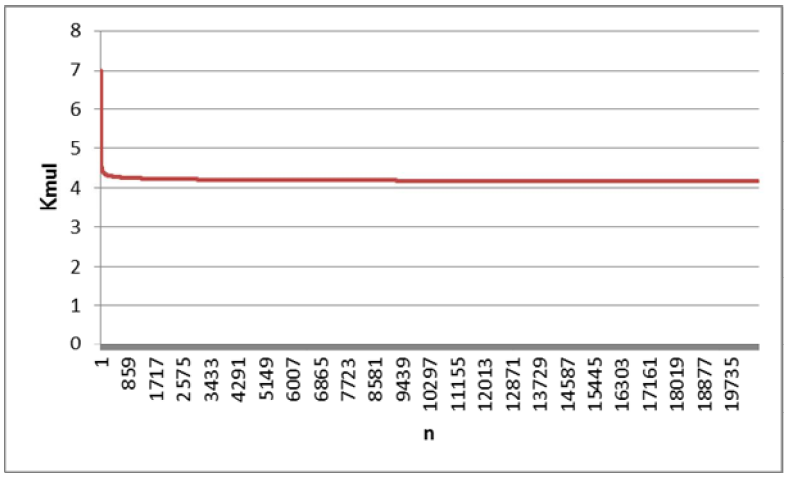

Рис. 4. Графік функції k_{mul}

Висновки

У сучасних ПЛІС при реалізації побудованих на основі модифікованих комірок Гілда помножувачів елементів полів Галуа GF (d^m), за умови, що помножувач та суматор у комірці Гілда складаються з базових функціональних елементів: мультиплексорів, однорозрядних двійкових суматорів та інших елементів, відношення апаратних витрат на реалізацію помножувачів у полі GF (d^m) до апаратних витрат на реалізацію помножувачів у полі GF (2^n) із збільшенням величини основи поля прямуватимуть до асимптотичного значення 4. Тобто для розширених полів Галуа з приблизно однаковою кількістю елементів менших апаратних витрат вимагають помножувачі для двійкових полів Галуа, якщо елементи полів представлено в поліноміальному базисі.

1. Журавлев Ю. И., Флеров Ю. А., Вялый М. Н. Дискретный анализ. Основы высшей алгебры. – М. : МЗ Пресс, 2007. – С. 151. 2. Габидулин Э. М., Кшевецкий А. С., Колыбельников А. И., Владимиров С. М. Защита информации: учеб. пособ. 22 листопада 2015 р. – С. 249. 3. Глухова О. В., Лозинський А. Я., Яремкевич Р.І., Ігнатович А. О. // Аналітична оцінка структурної складності помножувачів елементів полів Галуа // АСІТ'2015. – Тернопіль: ТНЕУ, 2015. – 1–5 с. 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 // "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 // Вісник Нац. уні-ту "Львівська політехніка" "Комп'ютерні системи та мережі". – 2013. – Вип. 773. – С. 27–32. 6. Еліас Р., Рахма М., Глухов В. С. Часова складність помножувачів для полів Галуа // Журнал "Електротехнические и компьютерные системы". – 2015. – Вип. XX. – С. 1 – 4. 7. Арнольд В. И. Динамика, статистика и проективная геометрия полей Галуа. – М.: МЦНМО, 2005. – 72 с. 8. Кузнєцов М. О., Дрозд О. В. Дослідження матричного помножувача працюючого із числами із плаваючою точкою при виникненні характерних несправностей типу "закоротка" // Радіоелектронні і комп'ютерні системи. – 2007. – № 6 (25). – 135–140 с. 9. Guild H. H. Fully iterative fast array for binary multiplication and addition. Electronics Letters, Volume 5, Issue 12, 12 June 1969, page 263 (In English). 10. Черкаський М. В., Ткачук Т. І. Характеристики складності пристроїв множення // Радіоелектронні і комп'ютерні системи. – 2012. – № 5. – С. 142–147. 11. Жолубак І. М., Костик А. Т., Глухов В. С. Особливості опрацювання елементів трійкових полів Галуа на сучасній елементній базі // Вісник Нац. ун-ту "Львівська політехніка" "Комп'ютерні системи та мережі". – 2015. – Вип. 830– С. 27–33. 12. Жолубак І. М., Глухов В. С. Визначення розширеного поля галуа GF (d^m) з найменшою апаратною складністю помножувача // Вісник Нац. ун-ту "Львівська політехніка" "Інформаційні системи та мережі". – 2016.