

ВИЗНАЧЕННЯ РОЗШИРЕНОГО ПОЛЯ ГАЛУА $GF(d^m)$ З НАЙМЕНШОЮ АПАРАТНОЮ СКЛАДНІСТЮ ПОМНОЖУВАЧА

© Жолубак І. М., Глухов В. С., 2016

Для сучасних ПЛІС порівняно апаратні витрати помножувачів елементів різних полів Галуа $GF(d^m)$ з приблизно однаковою кількістю елементів поля з метою визначення поля, у якому помножувач має найменшу апаратну складність. Показано глобальне зростання апаратних витрат за збільшення основи поля. При цьому існують локальні мінімуми, яким серед непарних d відповідають $d=2^i-1$, а глобальному мінімуму для комірок Гілда за двома розглянутими в роботі методами оцінювання апаратної складності – $d=3$ та $d=7$, відповідно, коли для оцінювання використовують тільки кількість входів та виходів комірки та коли додатково враховується внутрішня структура комірки.

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

The paper compares realised on modern FPGA Galois fields multipliers hardware costs to select Galois field $GF(d^m)$ with approximately the same number of elements and the lowest multiplier hardware complexity. The total increase in hardware costs depending on the increase of the basics of the field has been demonstrated. Local minimums for odd d correspond to $d = 2^i-1$ and the global minimum for analysis based on Guild cell with realization like single unit corresponds to the value $d = 3$ and based on Guild cell with its multiplier and adder separate realization – the value $d=7$.

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

Вступ. Загальна постановка проблеми

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 складністю. Тому визначення можливості зменшення апаратної складності при використанні полів Галуа $GF(d^m)$ з основою $d > 2$ (d – просте число) та приблизно однаковою кількістю елементів ($d^m \approx 2^n$) є актуальною задачею.

Аналіз джерел

У сучасних засобах захисту інформації використовують поля Галуа $GF(2^n)$, коди елементів таких полів [1, 2] представляються в поліноміальному або нормальному базисах.

Математичною основою опрацювання цифрового підпису є еліптичні криві [3]. При цьому опрацювання точок еліптичної кривої ґрунтується на виконанні послідовностей операцій у полях Галуа $GF(2^n)$. Помножувачі для таких полів характеризуються високою апаратною [4], структурною [5, 6] та часовою [7] складністю.

З літератури відомо багато пристроїв для опрацювання елементів полів Галуа $GF(d^m)$ [8], які використовуються у різних криптографічних перетвореннях. Відомий матричний помножувач [9], який складається з комірок Гілда, для виконання операцій множення двійкових чисел. 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 $d < 4$, але не розглядаються апаратні витрати таких помножувачів для полів Галуа $GF(d^m)$ з вищими основами $d > 4$, що і є предметом цієї роботи.

Формулювання мети

Метою роботи є визначення поля з множини полів Галуа $GF(d^m)$ (з приблизно однаковими кількостями елементів), помножувач для якого матиме найменшу апаратну складність. Коди елементів полів Галуа при цьому представляються в поліноміальному базисі.

Алгоритмічні та математичні основи

На рис. 1. наведено відомий матричний помножувач для множення цілих чисел без знаку, де SM_n – комірка Гілда.

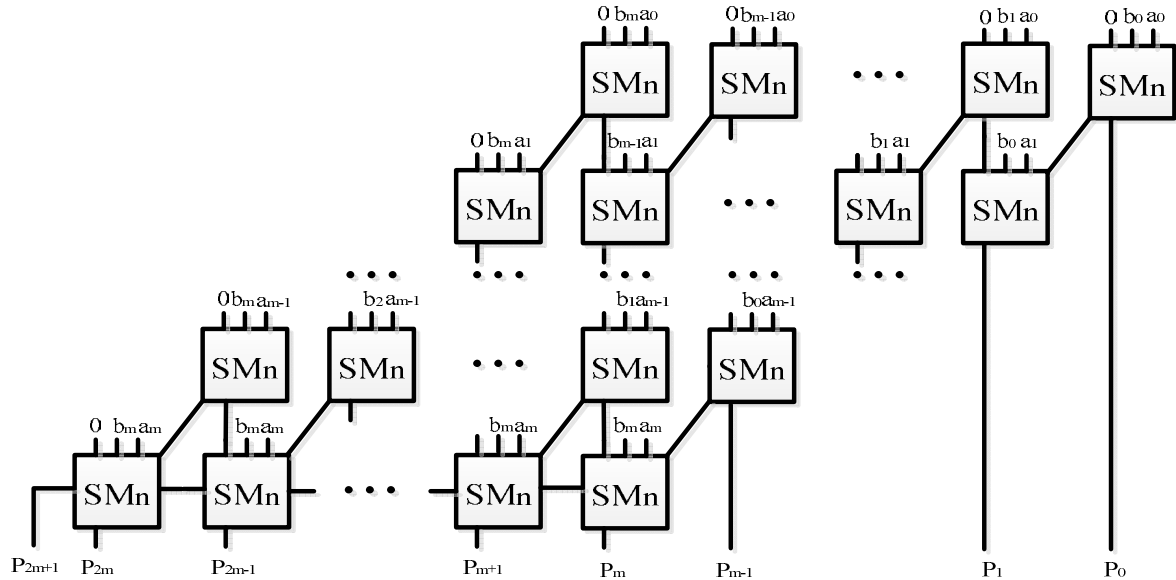


Рис. 1. Схема матричного помножувача на основі комірок Гілда

Матричний помножувач для елементів полів Галуа $GF(d^m)$ у поліноміальному базисі будується на основі схеми рис. 1. Схему такого помножувача для полів $GF(3^m)$ наведено на рис. 2 та загальний випадок для полів $GF(n^m)$ наведено на рис. 3. Вони складаються з модифікованих комірок Гілда (G_n) та вузлів f для знаходження коефіцієнта, на який перемножується утворюючий поле поліном при зведенні проміжного результату за модулем такого полінома.

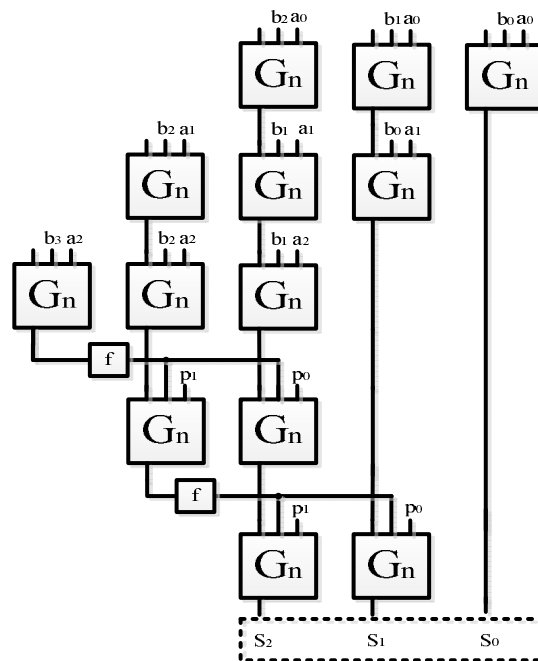


Рис. 2. Матричний помножувач поля $GF(3^m)$ з використанням модифікованих комірок Гілда

Елемент f , що використовується для знаходження коефіцієнта, на який потрібно перемножити поліном для зведення проміжного результату, обчислює функцію, яка залежить від двох параметрів: $f = (d - G_m) \bmod d = (-G_m) \bmod d$, де d – основа поля, G_m – результат на виході модифікованої комірки Гілда при прямому ході обчислень. Коефіцієнт при старшому розряді незвідного полінома завжди дорівнює 1[12].

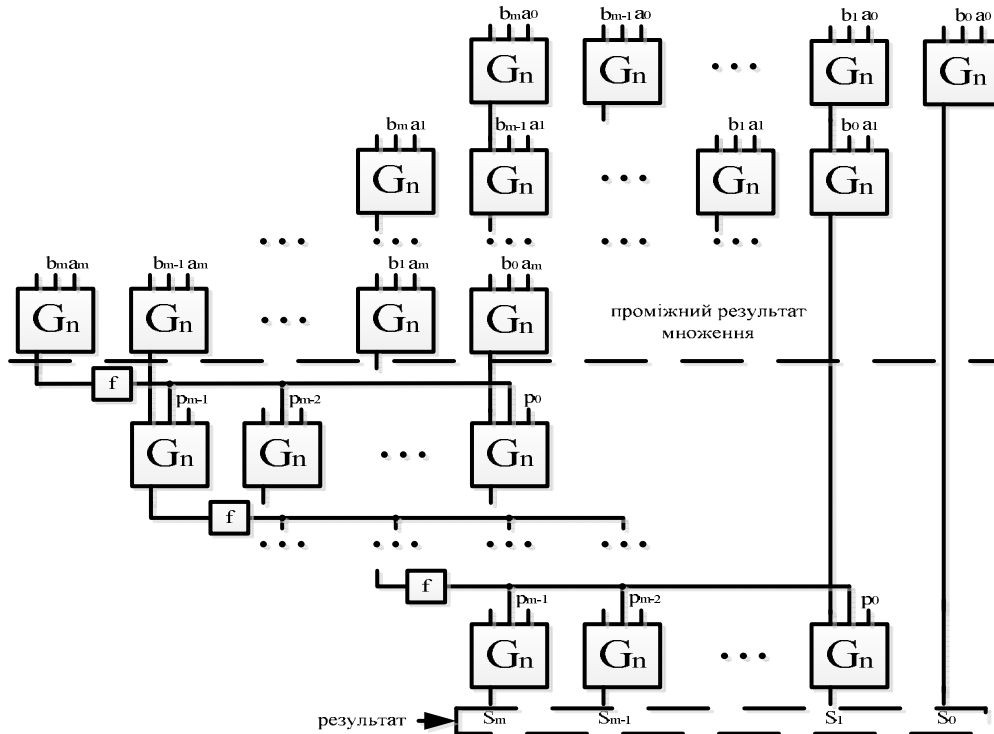


Рис. 3. Матричний помножувач поля $GF(d^m)$ з використанням модифікованих комірок Гілда

Реалізація на ПЛІС

Помножувач для полів Галуа $GF(d^m)$ може бути реалізований на основі модифікованих комірок Гілда (КГ). Модифіковані КГ для полів Галуа $GF(d^m)$ повинні мати $3p$ входи та p виходів, розрядністю $p = \lceil \log_2 m \rceil$ бітів кожний (рис.4). При використанні сучасних ПЛІС, логічні комірки яких будуються на основі програмовних 6-входових комбінаційних схеми (LUT), реалізація на ПЛІС таких комірок Гілда у 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.

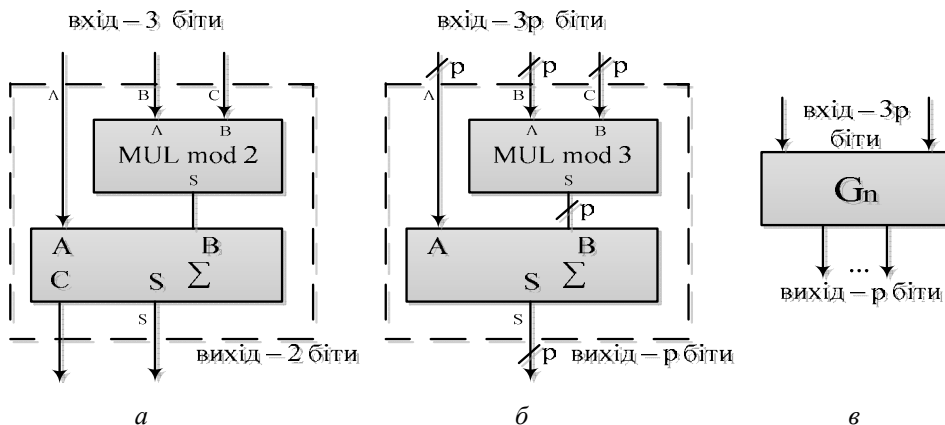


Рис. 4. Комірка Гілда (а), схема модифікованої комірки Гілда для обробки елементів полів Галуа $GF(d^m)$ (б), символ модифікованої комірки Гілда $GF(d^m)$ (в)

Оцінити кількість LUT у комірці Гілда можна за двома варіантами:

- 1) вважати комірку Гілда «чорною скринькою» – повністю цілісним елементом, в якому несуттєвою є внутрішня структура комірки, а до уваги береться тільки кількість її входів та виходів;
- 2) з уточненням внутрішньої структури (комірка Гілда складається з помножувача та суматора).

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

Для першого варіанта коефіцієнт апаратних витрат $k_{mul} = k_g * k_k$, де $k_g = \frac{k_{gd}}{k_{g2}}$, $k_k = \frac{k_{kd}}{k_{k2}}$ – 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 $k_{gd} = (2^{p-5} - 1) * k$, де $p = 3 * \lceil \log_2 d \rceil$, а $k = \lceil \log_2 d \rceil$. Отже, $k_{gd} = (2^{3 * \lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil$;

$$k_g = (2^{3 * \lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil. \quad (1)$$

У двійкових полях $GF(2^n)$ для реалізації помножувача потрібно $k_{k2} = 2n^2 - 2n + 1$ комірок Гілда, а в полях Галуа з основою d $GF(d^m)$ – $k_{kd} = 2m^2 - 2m + 1$ (рис.2) та 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 витратами на реалізацію елемента f (рис. 2), який формує цей коефіцієнт, можна в цьому випадку знехтувати, оскільки вони малі порівняно з витратами на реалізацію самих комірок Гілда. Отже:

$$k_k \approx \frac{2m^2 - 2m + 1}{2n^2 - 2n + 1} \quad (2)$$

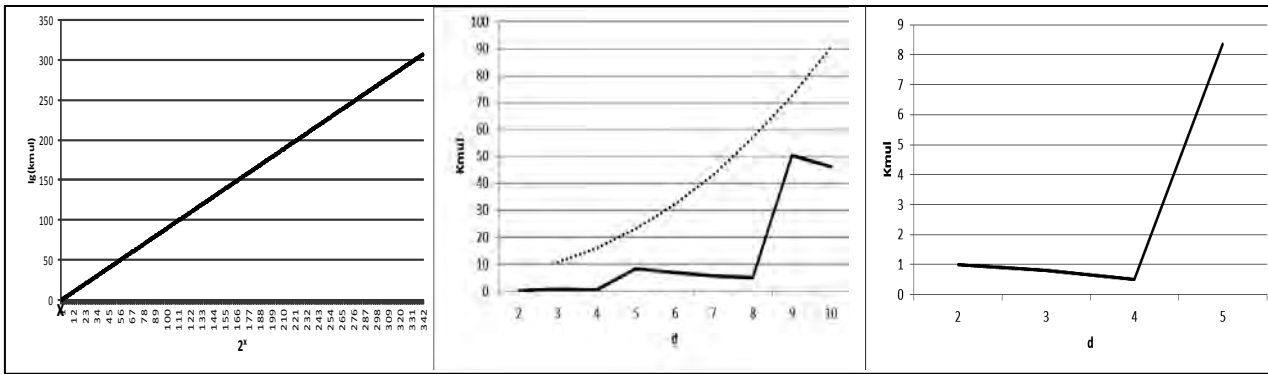
$$k_{mul} \approx \frac{(2^{3 * \lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil (2m^2 - 2m + 1)}{2n^2 - 2n + 1} \quad (3)$$

При цьому $d^m \approx 2^n$. Тоді $m \approx \log_d 2^n = \frac{n}{\log_2 d}$, $k_k \approx \frac{\frac{2n^2}{(\log_2 d)^2} - \frac{2n}{\log_2 d} + 1}{2n^2 - 2n + 1} \approx \log_2^{-1} d$,

$$k_{mul} \approx \frac{(2^{3 * \lceil \log_2 d \rceil - 5} - 1)(\log_2 d)}{\log_2 d} \approx 2^{3 * \lceil \log_2 d \rceil - 5}.$$

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

Початкову ділянку графіка функції k_{mul} наведено на рис. 5, де суцільною лінією позначено відношення апаратних витрат помножувачів елементів полів Галуа $GF(d^m)$ та $GF(2^n)$, а пунктирною – їх наближену оцінку. На рис. 5 видно, що із збільшенням основи апаратні витрати стрімко зростають. Найменші апаратні витрати при реалізації комірки Гілда як «чорної скриньки» для розширених полів з простою основою матимуть помножувачі для полів Галуа $GF(3^m)$, що видно із рис. 5.



а

б

в

Рис. 5. Відношення апаратних витрат помножувачів елементів полів Галуа $GF(d^m)$ та $GF(2^n)$ для:
 а – проміжку від 1 до 2^{342} ; б – проміжку від 1 до 10; в – проміжку від 1 до 5

Для другого варіанта, коли помножувач та суматор, які мають $2p$ входів та p виходів кожний, оцінюються окремо, для реалізації однієї комірки Гілда буде потрібно $q_2 = 2 \cdot (2^{2p-5} - 1) \cdot p$ LUT.

Тоді $\frac{q_1}{q_2} = \frac{(2^{3p-5} - 1) \cdot p}{2 \cdot (2^{2p-5} - 1) \cdot p} \approx \frac{2^{3p-5}}{2 \cdot 2^{2p-5}} = 2^{p-1}$ – відношення витрат для реалізації однієї комірки Гілда

за першим та другим варіантами. З формули випливає, що внутрішня структура модифікованої комірки Гілда суттєво впливає на оцінку апаратних витрат. Порівняно з першим варіантом оцінки апаратних витрат, коли до уваги приймається тільки кількість входів і виходів, додаткове врахування внутрішньої структури модифікованої комірки Гілда зменшує оцінкове значення апаратної складності.

Оцінимо апаратні витрати за другим варіантом. Для двійкових полів Галуа $k_{g2} = 1$, для інших

$$k_{gd} = (2^{2 \cdot \lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil * 2.$$

Отже:

$$k_g = (2^{2 \cdot \lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil * 2. \quad (4)$$

У двійкових полях $GF(2^n)$ для реалізації помножувача потрібно $2n^2 - 2n + 1$ модифікованих КГ, а в полях Галуа $GF(d^m)$ – $2m^2 - 2m + 1$ КГ. Отже:

$$k_k \approx \frac{2m^2 - 2m + 1}{2n^2 - 2n + 1}. \quad (5)$$

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

$$k_k \approx \frac{\left(\frac{2n^2}{\log_2^2 d} - \frac{2n}{\log_2 d} + 1\right)}{2n^2 - 2n + 1} \approx \log_2^{-1} d,$$

$$k_{mul} \approx \frac{(2^{2 \cdot \lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil * 2}{\log_2 d} \approx 2^{2 \cdot \lceil \log_2 d \rceil - 4}$$

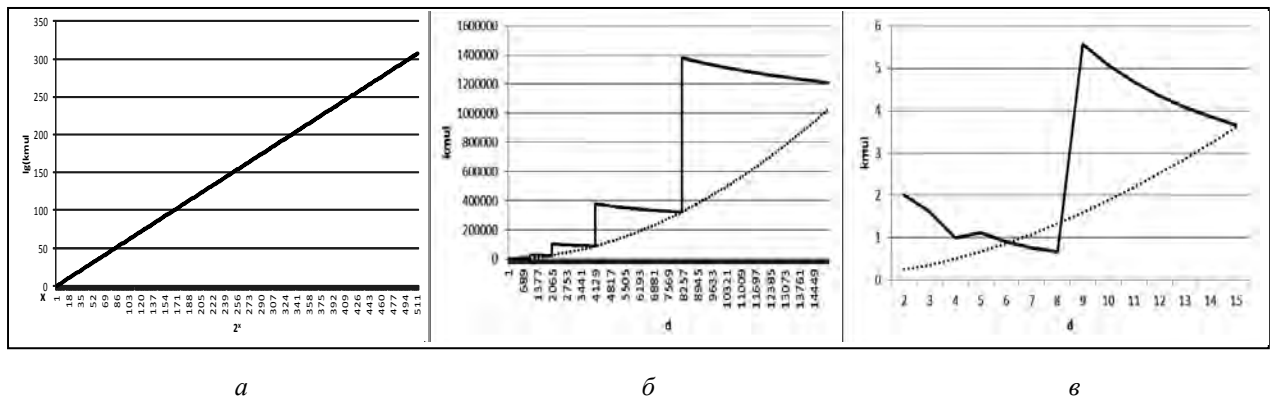


Рис. 6. Відношення апаратних витрат помножувачів елементів полів Галуа $GF(d^m)$ та $GF(2^n)$) для:
 а – проміжку від 1 до 2^{513} ; б – проміжку від 1 до 14449; в – проміжку від 1 до 15

Порівнюючи формули для знаходження k_{mul} для першого та другого випадків, бачимо, що за другим варіантом аналізу апаратної складності комірки Гілда, за великих значень p загалом дає зменшене значення апаратної складності в 2^{p-1} разу.

Для малих n (рис. 6) k_{mul} розраховували за точними формулами (4), (5).

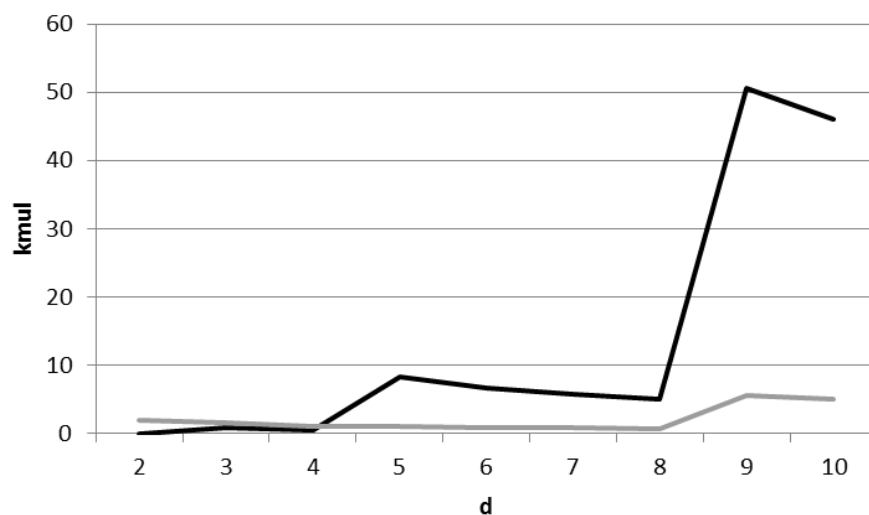


Рис. 7. Відношення апаратних витрат помножувачів елементів полів Галуа $GF(d^m)$ та $GF(2^n)$ за першим та другим варіантами

Початкову ділянку графіка функції k_{mul} наведено на рис. 6, де суцільною лінією позначено відношення апаратних витрат помножувачів елементів полів Галуа $GF(d^m)$ та $GF(2^n)$, а пунктирною – їх наближену оцінку. З рис. 6 можемо бачити, що на початку графіка апаратні витрати із збільшенням основи стрімко зростають. Як видно з рис. 6, найменші апаратні витрати за 2-м варіантом оцінювання будуть для поля Галуа з простою основою $GF(7^m)$.

Висновки та перспективи подальших наукових розвідок

У сучасних ПЛІС при реалізації побудованих на основі модифікованих комірок Гілда помножувачів елементів полів Галуа $GF(d^m)$ з приблизно однаковою кількістю елементів поля із збільшенням основи d апаратні витрати загалом збільшуються. На окремих локальних ділянках із збільшенням d апаратні витрати зменшуються. Локальним мінімумам серед непарних d

відповідають $d = 2^i - 1$. При цьому глобальному мінімуму при представленні комірки Гілда «чорною скринькою» відповідає значення $d = 3$, а при поданні як сукупності помножувача та суматора – значення $d = 7$.

1. Кушнеров А. Троицная цифровая техника. Перспектива и современность / Кушнеров А.; Университет им. Бен-Гуриона, Беэр-Шева Беэр-Шева, 2005. – С. 1–7. 2. Oded Goldrich Foundations of Cryptography/ Oded Goldrich. Volume 1: Basic Tools . –Cambridge: Cambridge University Press, 2014. – С. 7–10. 3. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння / Державний комітет України з питань технічного регулювання та споживчої політики. –К, 2002. – С. 5–7. 4. Аналітична оцінка структурної складності помножувачів елементів полів Галуа / Глухова О. В., Лозинський А. Я., Яремкевич Р. І., Ігнатович А. О.// АСІТ'2015. – Тернопіль: ТНЕУ, 2015. – С. 1–5. 5. Глухов В. С. Особливості реалізації на ПЛІС секційних помножувачів елементів полів Галуа $GF(2^m)$ з надвеликим степенем / Глухов В. С., Еліас Р. М., Мельник А. О. // Комп'ютерно-інтегровані технології: освіта, наука, виробництво/ Луцький національний технічний університет. – 2013. – № 12. – С. 103–106. 6. Глухов В. С. Результати оцінювання структурної складності помножувачів елементів полів Галуа / Глухов В. С., Глухова О. В. // Вісник Нац. ун-ту “Львівська політехніка”. – 2013. – № 773: Комп'ютерні системи та мережі. – С. 27–32. 7. Еліас Р., Рахма М., Глухов В. С. Часова складність помножувачів для полів Галуа // Електротехніческие и компьютерные системы. – 2015. – Вып. XX. – С. 1–4. 8. Арнольд В. И. А84 Динамика, статистика и проективная геометрия полей Галуа/ Арнольд В. И. – М.: МЦНМО, 2005. – 72 с. 9. Кузнєцов М. О. Дослідження матричного помножувача працюючого із числами із плаваючою точкою при виникненні характерних несправностей типу “закоротка” / Кузнєцов М. О., Дрозд О. В. // Радіоелектронні і комп'ютерні системи. – 2007. – № 6 (25). – С. 135–140. 10. Черкаський М. В. Характеристики складності пристроїв множення / Черкаський М. В., Ткачук Т. І. // Радіоелектронні і комп'ютерні системи. – 2012. – № 5. – С. 142–147. 11. Жолубак І. М. Особливості опрацювання елементів трійкових полів Галуа на сучасній елементній базі / Жолубак І. М., Костик А. Т., Глухов В. С. // Вісник Нац. ун-ту “Львівська політехніка”. – 2015. – № 830: Комп'ютерні системи та мережі. – С. 27–33. 12. Hansen Tom. Primitive polynomials over finite fields / Tom Hansen, Gary L. Mullen // “Mathematics of computation”. – New York: – 1992. – No. 200. – P. 639–643.