

# Визначення розширеного поля Галуа $GF(d^m)$ з найменшою апаратною складністю помножувача

І.М. Жолубак

Національний університет “Львівська політехніка”,  
кафедра електронних обчислювальних машин  
Україна, Львів, вул. С. Бандери 12  
IvanZholubak7@ukr.net

В. С. Глухов

Національний університет “Львівська політехніка”,  
кафедра електронних обчислювальних машин  
Україна, Львів, вул. С. Бандери 12  
valeriygl@ukr.net

## Definition of the extended Galois field $GF(d^m)$ with minimal hardware complexity multiplier

I. Zholubak

Lviv Polytechnic National University,  
Computer Engineering Department  
Ukraine, Lviv, S. Bandery street 12,  
IvanZholubak7@ukr.net

V. Hlukhov

Lviv Polytechnic National University,  
Computer Engineering Department  
Ukraine, Lviv, S. Bandery street 12,  
valeriygl@ukr.net

**Анотація**—У роботі для сучасних ПЛІС проведено порівняння апаратних витрат 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 при збільшенні основи поля. При цьому існують локальні мінімуми, яким серед непарних  $d$  відповідають  $d=2^i-1$ , а глобальному мінімуму - значення  $d=7$ .

**Abstract**—The paper compared the modern FPGA hardware cost to reduce hardware complexity implement multipliers for Galois field  $GF(d^m)$  with approximately the same number of elements. Totally the hardware cost increases while basics of the field increase. Local minimums for odd  $d$  correspond to  $d = 2^i - 1$  and the global minimum corresponds to the value  $d = 7$ .

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

**Keywords**—Galois fields  $GF(d^m)$ , multiplier, modified Guild cell, LUT.

### I. ВСТУП

У сучасних засобах захисту інформації широко використовуються поля Галуа  $GF(2^n)$ , опрацювання елементів таких полів [1, 2] 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.

Метою роботи є визначення поля, помножувач для якого буде мати найменшу апаратну складність.

### II. РЕАЛІЗАЦІЯ НА ПЛІС

Операція множення в полях Галуа  $GF(d^m)$ , може бути реалізована на основі модифікованих комірок Гілда (КГ). Модифіковані КГ для полів Галуа  $GF(d^m)$  повинні мати  $3r$  входів та  $p$  виходів ( $p = \lceil \log_2 m \rceil$ ) [3] (рис.1).

Для їхньої реалізації на сучасних ПЛІС треба використати 6-виходів елементи LUT у кількості

$$q_1 = (2^{3p-5} - 1) \cdot p.$$

Якщо ж помножувач та суматор (рис. 1), які мають  $2r$  входів та  $p$  виходів кожний) реалізовувати окремо, то для цього буде потрібно

$$q_2 = 2 \cdot (2^{2p-5} - 1) \cdot p \text{ аналогічних LUT. Тоді:}$$

$$\frac{q_1}{q_2} = \frac{(2^{3p-5} - 1) \cdot p}{2 \cdot (2^{2p-5} - 1) \cdot p} \approx \frac{2^{3p-5}}{2 \cdot 2^{2p-5}} = 2^{p-1} = \frac{m}{2}.$$

Розглянемо апаратні витрати для реалізації комірок Гілда з двох складових – помножувача та суматора. Обчислення будемо проводити за формулами: коефіцієнт апаратних витрат  $k_{mul} = k_g * k_k$ , де

$$k_g = \frac{k_{gd}}{k_{g2}}, \quad k_k = \frac{k_{kd}}{k_{k2}} \text{ - коефіцієнти складності та}$$

кількості КГ,  $k_{gd}$  та  $k_{g2}$ ,  $k_{kd}$  та  $k_{k2}$  – кількість LUT у КГ та кількість КГ у помножувачі для полів Галуа  $GF(d^m)$  та  $GF(2^n)$ , відповідно.

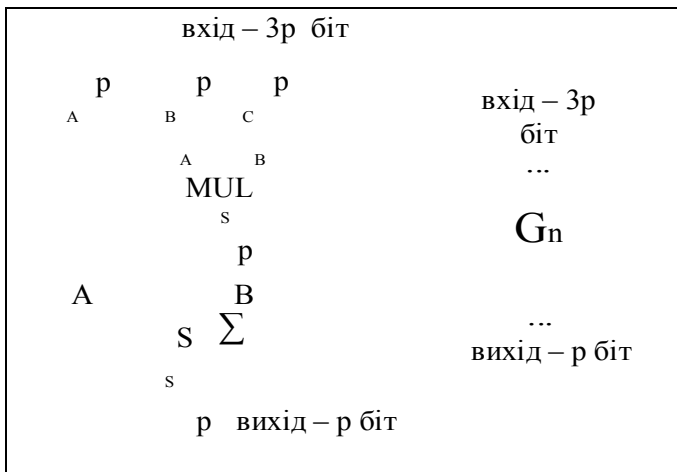


Рис. 1. Модифікована комірка Гілда для обробки елементів полів Галуа  $GF(d^m)$

При формальному підході для двійкових полів Галуа  $k_{g2} = 1$ , для інших

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

$k_g = (2^{2^{\lceil \log_2 d \rceil - 5}} - 1) * \lceil \log_2 d \rceil * 2$ . У двійкових полях  $GF(2^n)$  для реалізації помножувача потрібно  $2n^2 - n$  модифікованих КГ, а в полях Галуа  $GF(d^m)$  -  $2m^2 - m$  КГ (та  $m-1$  LUT для знаходження коефіцієнта, на який потрібно перемножити незвідний поліном для зведення результату). Отже  $k_k \approx \frac{2m^2 - m}{2n^2 - n}$ .

При цьому  $d^m \approx 2^n$ . Тоді для великих  $n$

$$m \approx \log_d 2^n = \frac{n}{\log_2 d}, \quad k_k \approx \frac{\left(\frac{2n^2}{\log_2^2 d} - \frac{n}{\log_2 d}\right)}{2n^2 - n} \approx \log_2^{-2} d$$

$$k_{mul} \approx \frac{(2^{2^{\lceil \log_2 d \rceil - 5}} - 1) * \lceil \log_2 d \rceil * 2}{\log_2^2 d} \approx \frac{d^2}{16 \log_2 d}$$

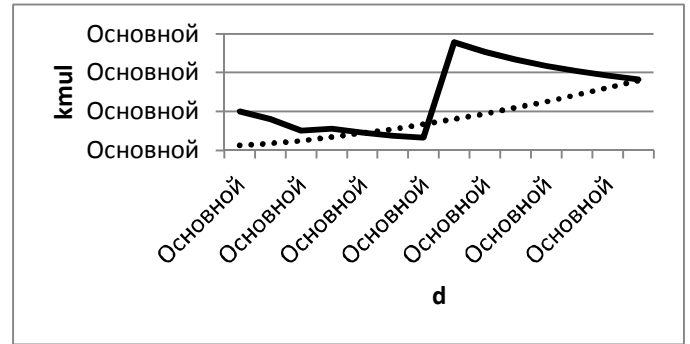
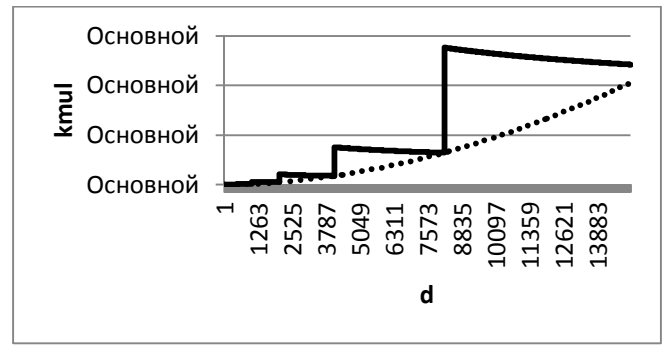


Рис. 2. Відношення апаратних витрат помножувачів елементів полів Галуа  $GF(d^m)$  та  $GF(2^n)$

Для малих  $n$   $k_{mul}$  треба розраховувати за точними формулами.

Графік функції  $k_{mul}$  для  $n=998$  наведено на рис. 2, де суцільною лінією позначено відношення апаратних витрат помножувачів елементів полів Галуа  $GF(d^m)$  та  $GF(2^n)$ , а пунктирною – їх наближена оцінка.

Як видно з рис.2 найменші апаратні витрати будуть для полів Галуа  $GF(7^m)$ .

### ВИСНОВКИ

В сучасних ПЛІС при реалізації побудованих на основі модифікованих комірок Гілда помножувачів елементів різних полів Галуа  $GF(d^m)$  з приблизно однаковою кількістю елементів поля при збільшенні основи  $d$  апаратні витрати глобально збільшуються. На окремих локальних ділянках при збільшенні  $d$  апаратні витрати зменшуються. Локальним мінімумам серед непарних  $d$  відповідають  $d=2^i-1$ . При цьому глобальному мінімуму відповідає значення  $d=7$ .

### ЛІТЕРАТУРА REFERENCES

- [1] Проективання комп'ютерних систем на основі мікросхем програмованої логіки : монографія / С. А. Іванець, Ю. О. Зубань, В. В. Казимир, В. В. Литвинов. – Суми : Сумський державний університет, 2013. – 313 с. – С. 17-20.
- [2] ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. Київ. Державний комітет України з питань технічного регулювання та споживчої політики. 2003. –С.40-50.
- [3] І. М. Жолубак, В. С. Глухов, А. Т. Костик Особливості обробки трійкових полів Галуа на сучасній елементній базі// Вісник Національного університету “Львівська політехніка” “Комп’ютерні системи та мережі”. – 2015. – Вип. 830. – С. 33-39.