УДК 004.382

ПОРІВНЯННЯ АПАРАТНИХ ВИТРАТ ПОМНОЖУВАЧІВ ЕЛЕМЕНТІВ РОЗШИРЕНИХ ПОЛІВ ГАЛУА

І. М. Жолубак, д. т. н. В. С. Глухов

Національний університет «Львівська політехніка»
Україна, м. Львів
IvanZholubak7@ukr.net, valeriygl@ukr.net

У роботі проведено порівняння апаратних витрат сучасних ПЛІС з метою зменшення апаратної складності при реалізації помножувачів елементів полів Галуа GF(d^m) з приблизно однаковою кількістю елементів поля. Показано 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 $d=3$.

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

У сучасних засобах захисту інформації широко використовуються поля Галуа $GF(2^n)$, опрацювання елементів таких полів характеризується високою апаратною, структурною та часовою складностями. 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. У даній роботі проводиться порівняння апаратних витрат помножувачів елементів розширених полів Галуа і пошук помножувача, який буде мати найменшу апаратну складність.

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 $3p$ входи та p виходів розрядністю $p = \lceil log_2 m \rceil$ біт кожний [1] (рис. 1). Для їхньої реалізації на ПЛІС треба використати 6-входові елементи LUT у кількості $q_1 = (2^{3p-5} - 1) \cdot p$.

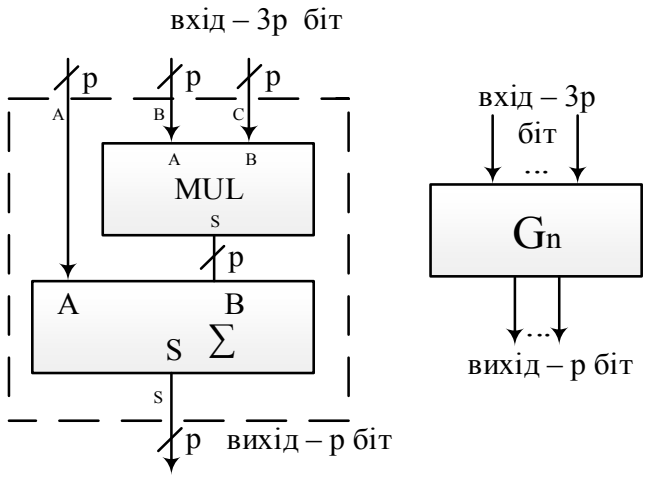

Рис. 1. Модифікована комірка Гілда для обробки елементів полів Галуа $GF(d^m)$

Якщо ж помножувач та суматор (рис. 1, $2p$ біт на вході та p біт на виході) реалізовувати окремо, то для цього буде потрібно $q_2 = 2 \cdot (2^{2p-5} - 1) \cdot p$ аналогічних LUT. Тоді

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

Для великих p (коли $2^{3p-5}>10$, $p\geq 3$ і $2^{2p-5}>10$, $p\geq 5$, разом $p \geq 5$) другий спосіб вимагає менших витрат, але є повільнішим. Для менших p виграш треба розраховувати за точними формулами. Для першого варіанту коефіцієнт апаратних витрат $k_{mul} = k_g \cdot k_k$, 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.

При формальному підході для двійкових полів Галуа приймемо $k_{g2} = 1$, для інших $k_{gd} = (2^{3 \cdot \lceil \log_2 d \rceil - 5} - 1) \cdot \lceil \log_2 d \rceil$.

Отже $k_g = (2^{3\cdot\lceil \log_2 d\rceil - 5} - 1)\cdot\lceil \log_2 d\rceil$. У двійкових полях $GF(2^n)$ для реалізації помножувача потрібно $2n^2 - n$ модифікованих КГ, а в полях Галуа з основою $d > 2$ потрібно $2m^2 - m$ КГ (та $m - 1$ LUT для знаходження коефіцієнта, на який потрібно перемножити незвідний поліном для зведення результату). Отже, $k_k \approx \dfrac{2m^2 - m}{2n^2 - n}$. При цьому $d^m \approx 2^n$. Тоді для великих n $m \approx \log_d 2^n = \dfrac{n}{\log_2 d}$,

$$k_k \approx \frac{\dfrac{2n^2}{\log_2^2 d} - \log_2 d}{2n^2 - n} \approx \log_2^{-2} d\,,\quad k_{mul} \approx \frac{2^{3\cdot\lceil \log_2 d\rceil - 5} - 1}{\log_2^2 d} \approx \frac{d^3}{\log_2^2 d}.$$

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 апроксимацію.

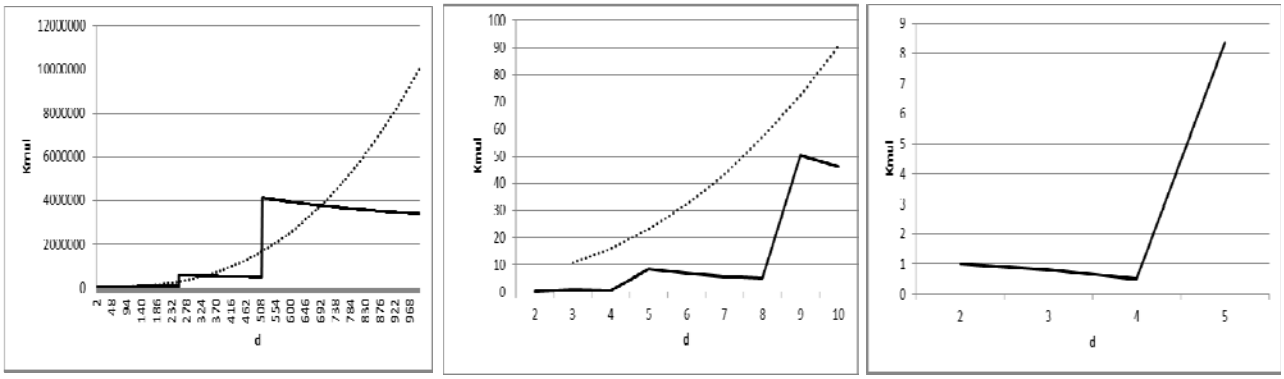

Рис. 2. Відношення апаратних витрат помножувачів елементів полів Галуа $GF(d^m)$ та $GF(2^n)$

Найменші апаратні витрати будуть мати помножувачі для полів Галуа $GF(3^m)$.

При реалізації в сучасних ПЛІС, побудованих на основі модифікованих комірок Гілда, помножувачів елементів полів Галуа $GF(d^m)$ з приблизно однаковою кількістю елементів поля при збільшенні основи d апаратні витрати 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=3.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Жолубак І. М., Глухов В. С., Костик А. Т. 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.

I. M. Zholubak , V. S. Hlukhov

Hardware resources of multipliers for extended Galois fields comparison

The paper compares the hardware cost of the modern FPGA in order to reduce hardware complexity in implementing multipliers for Galois field GF (dm) with approximately the same number of elements of the field. It is shown that the hardware costs increase when the basis of the field increases. Local minima for odd d correspond to $d = 2^i–1$ and the global minimum corresponds to the value $d = 3$.

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