УДК 004.382

І. М. Жолубак, А. Т. Костик, В. С. Глухов
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

ОСОБЛИВОСТІ ОПРАЦЮВАННЯ ЕЛЕМЕНТІВ ТРІЙКОВИХ ПОЛІВ ГАЛУА НА СУЧАСНІЙ ЕЛЕМЕНТНІЙ БАЗІ

Розглянуто особливості побудови операційних пристроїв для опрацювання елементів трійкових полів Галуа GF(3^m) у сучасній елементній базі. Показано, що виконання операцій над елементами трійкових полів Галуа має переваги над виконанням аналогічних операцій над елементами двійкових полів Галуа. Перехід до операцій над елементами трійкових полів Галуа дає змогу уникнути надлишковості у разі використання конфігуровних комбінаційних схем у сучасних програмованих логічних інтегральних схемах (ПЛІС) та знизити апаратні витрати.

Ключові слова: трійкові поля Галуа GF(3^m), помножувач, конфігурована комбінаційна схема.

FEATURES OF TERNARY GALOIS FIELDS ELEMENTS PROCESSING ON MODERN ELEMENT BASIS

Features of ternary Galois fields GF(3^m) elements processing operation units development for modern component base considered in this article. It is shown that operations execution over ternary Galois fields elements have several advantages over binary Galois fields ones. Moving to ternary elements of Galois fields operations decreases lookup table (LUT) redundancy in modern field programmable gate arrays (FPGA) and reduce hardware costs.

Key words: ternary Galois fields GF(3^m), multiplier, LUT (Lookup Table).

Вступ

У роботі розглянуто особливості виконання операцій над елементами трійкових полів Галуа GF(3^m) та їх реалізацію у ПЛІС. Поля Галуа використовуються для завадостійкого кодування та у криптографічних перетвореннях. З розвитком технології ПЛІС усе більшої практичної значущості набуває апаратна реалізація складних операцій, що потребує пошуку ефективних структур за такими критеріями, як швидкодія та апаратні витрати. У роботі порівняно апаратні витрати на реалізацію операційних вузлів для елементів полів Галуа GF(3^m) та GF(2^m). Показано, що для реалізації помножувачів для елементів трійкових полів Галуа GF(3^m) потрібні менші апаратні витрати порівняно з двійковими полями GF(2^m).

Аналіз літературних джерел

Трійкові ЕОМ мають певні переваги порівняно з двійковими ЕОМ. Натуральнологарифмічне число кодів (чисел) (густота запису інформації) описується рівнянням $y = \ln(x)/x$, де x – основа системи числення. З рівняння випливає що найбільшою є густота запису інформації у системи числення з основою, що дорівнює основі натурального логарифма, тобто числу Ейлера ($e = 2.71\ldots$). Цю задачу розв'язували ще в часи Непера для вибору основи для логарифмічних таблиць. Із цілочислових систем числення найбільшу густоту запису інформації має трійкова система числення [1]. Трійкова логіка цілком вміщує двійкову логіку як центральну підмножину [2].

Теорія полів Галуа є центральною математичною теорією, яку покладено в основу завадостійкого кодування і криптології [3]. Скінченні поля використовують у сучасних блокових шифрах, таких як IDEA і AES, в поточних шифрах, а також у відкритих криптосистемах, наприклад, у протоколі обміну ключами Діффі–Геллмана і криптосистемах на основі використання еліптичних кривих [4]. Основою електронного цифрового підпису є використання розширених полів Галуа GF(n^m) та обчислень над точками еліптичних кривих [5]. У роботі [6] описуються особливості реалізації логічних елементів на ПЛІС. В роботі [7] наведена структурна схема процесора для обробки елементів полів Галуа. Але в проаналізованих роботах не досліджуються можливі переваги використання трійкових полів Галуа над двійковими.

Мета роботи

Метою роботи є визначення особливостей виконання операцій додавання і множення над елементами полів Галуа GF(3^m), дослідження особливостей реалізації цих операцій на сучасній елементній базі, порівняння особливостей виконання цих операцій над елементами двійкових та трійкових полів Галуа, визначення переваг використання трійкових полів Галуа.

Алгоритмічні та математичні основи

Арифметичні операції у полях Галуа GF(n^m) широко використовують у теорії кодування, цифрової обробки сигналів та у криптосистемах з відкритим ключем. Додавання в полях Галуа GF(n^m) виконується як порозрядна операція додавання за модулем n. Операції знаходження оберненого елемента і піднесення до степеня потребують більше часу, ніж базові операції: додавання і множення. Операція знаходження оберненого елемента виконується за допомогою ітеративного множення. Тому ефективна реалізація множення елементів полів Галуа є основною у криптографічних пристроях, які використовують такі поля.

Припустимо, що *F* є множиною з двома бінарними операціями + і *. *F* є полем, якщо:

1) *F* є абелевою групою за додаванням +;

2) *F* = F\{0}* є абелевою групою за множенням*;

3) виконується дистрибутивність для всіх *a, b, c* з множини *F*:

a(b + c) = a*b + a*c, (a + b)*c = a*c + b*c.*

Якщо кількість елементів *F* скінченна, то *F* називається скінченним полем.

Елементи $\{t^{m-1},...,t^2,t,1\}$ основного поля Галуа утворюють поліноміальний базис, елементи $\{\theta,\theta^2,\theta^{2^2},...,\theta^{2^{m-1}}\}$ основного поля Галуа утворюють нормальний базис (t і θ – корені полінома *p*, що утворює поле). Усі інші елементи основного поля Галуа можна подати як у поліноміальному базисі (у вигляді $a_{m-1}t^{m-1}+...+a_2t^2+a_1t+a_0$), так і у нормальному базисі (у вигляді $a_0\theta+a_1\theta^2+a_2\theta^{22}+...+a_{m-1}\theta^{2m-1}$), де a_i – розряди коду елемента поля (i = 0, 1, …, m–1). Під час множення двох елементів поля Галуа у поліноміальному базисі додавання та множення виконується за модулем *n*.

Елементи множини поліноміального базису можна подати у вигляді двійкових рядків: $(a_{m-1},...,a_2,a_1,a_0)$.

Запишемо формули для операцій додавання елементів полів Галуа GF(n^m). Припустимо, що в нас є два елементи A та *B* поля GF(n^m):

$A=(a_{m-1},..,a_2,a_1,a_0)$,

$B=(b_{m-1},...,b_2,b_1,b_0)$, тоді

$A+B=(S_{m-1},...,S_2,S_1,S_0)$,

$S_i=a_i\oplus_n b_i$, де $\oplus_n$ позначає операцію додавання за модулем *n*.

Один з методів множення елементів полів Галуа GF(n^m) полягає у виконанні двох етапів: знаходження проміжного добутку та знаходження остачі від його ділення на простий поліном, що утворює це поле Галуа. Щоб знайти проміжний результат, кожен розряд одного елемента множать на кожен розряд другого елемента за модулем *n* у стовпчик.

$S_{пром._k} = \sum_{i+j=k} a_i b_j$, якщо $0 \le k \le 2m-1$ – формула для знаходження *k*-го розряду проміжного результату множення, $\sum_{i+j=k}$ позначає операцію додавання за модулем *n*.

Далі отриманий проміжний добуток ділять на простий многочлен степеня m, що утворює це поле Галуа. Остача від ділення буде результатом множення. Ділення зводиться до додавання до проміжного результату добутку многочлена та старшої частини проміжного результату, як показано на формулах нижче.

$A * B = ((a_{m-1},...,a_2,a_1,a_0) * (b_{m-1},...,b_2,b_1,b_0)) = (S_{m-1},...,S_2,S_1,S_0)$,

$S_{пром.} = (S_{2m-1},...,S_2,S_1,S_0)$,

$S_{пром.} = S_{ст.} \,\&\&\, S_{мол.}$, де $\&\&$ позначає об'єднання двох частин результату (конкатенацію),

$S_{ст.} = (S_{2m-1},...,S_m)$,

$S_{мол.} = (S_{m-1},...,S_0)$,

$S = S + p * S_{ст.} = p * (S_{2m-1},...,S_m)$.

На рис. 1 подано функціональну схему помножувача двох елементів поля GF(n^m) з використанням модифікованих комірок Гілда, детальна схема яких наведена на рис. 2.

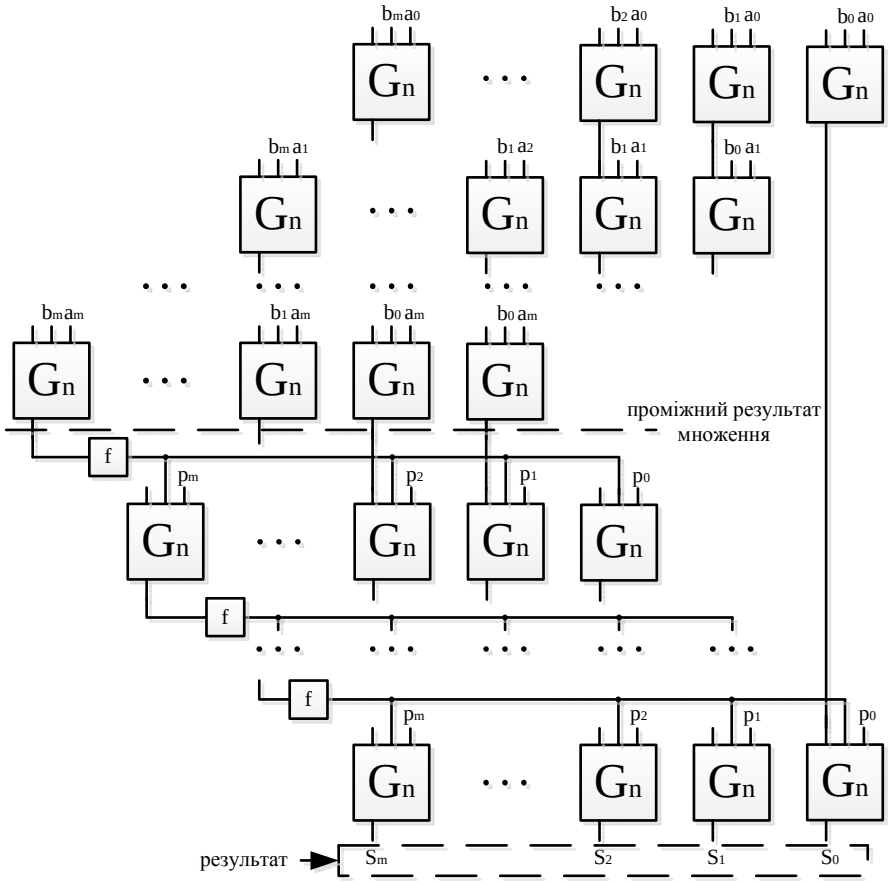

Рис. 1. Схема множення двох елементів поля GF(n^m) з використанням модифікованих комірок Гілда

На рис. 1 спочатку обчислено проміжний результат множення, потім отриманий результат поділено за модулем простого полінома. Поліном для поля GF(n^m) має вигляд: $c_m n^m + ... + c_2 n^2 + c_1 n^1 + c_0 n^0$. Ділення на схемі реалізується покроковим додаванням добутку простого полінома на коефіцієнт, який обчислюється у вузлі f. Цей вузол не потрібний тільки для помножувача двійкових полів Галуа. Вузол f має $2\lceil \log_2 n \rceil$ входів та $\lceil \log_2 n \rceil$ виходів, де $\lceil \log_2 n \rceil$ позначає операцію заокруглення до найближчого більшого цілого. Для полів Галуа GF(3^m) значення (k_1 та k_0) на виході вузла f визначаються як:

$k_1 = \overline{\alpha_1}\alpha_0\,\overline{p_1}p_0 \vee \alpha_1\overline{\alpha_0}p_1\,\overline{p_0}$

$k_0 = \overline{\alpha_1}\alpha_0 p_1\,\overline{p_0} \vee \alpha_1\overline{\alpha_0}\,\overline{p_1}p_0$

$\alpha_1\alpha_0$ – двійкові розряди старшого розряду коду, який коректується;

$p_1 p_0$ – двійкові розряди старшого розряду простого полінома.

Модифікована комірка Гілда складається з помножувача і суматора. Розрядність входів модифікованої комірки Гілда для поля GF(n^m) визначають за формулою $p = \lceil log_2 n \rceil$, загальна розрядність входів комірок дорівнює 3p.

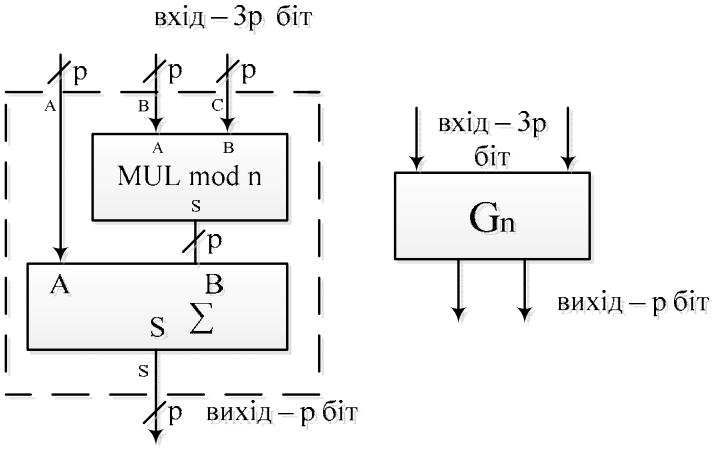

Рис. 2. Модифікована комірка Гілда
для обробки елементів полів Галуа GF(n^m)

Виконання операцій у сучасних ПЛІС

Інтегральні мікросхеми з логікою, що програмується (ПЛІС), або FPGA (field programmable gate arrays) є цифровими інтегральними мікросхемами, що складаються з програмованих логічних блоків і програмованих з'єднань між цими блоками.

ПЛІС – мікросхеми, основою логічного блока більшості з яких є конфігуровна комбінаційна схема (Look-Up Table – LUT). Конфігуровна комбінаційна схема може реалізувати будь-яку логічну функцію. Крім конфігуровних комбінаційних схем, логічний блок містить також конфігуровний тригер та схему перенесення.

Логічний блок може працювати у двох режимах роботи:

1) нормальному режимі;

2) арифметичному режимі [6].

Подальший аналіз особливостей реалізації помножувачів і суматорів у полях Галуа виконано для ПЛІС сім'ї Virtex-7 [7], які містять шестивходові елементи LUT.

Для виконання операції додавання одного розряду в трійковому полі Галуа потрібно два елементи LUT, а у двійковому – один, як показано на рис. 3. Для двійкових і трійкових полів Галуа з однаковою кількістю елементів буде справедливою наближена рівність $3^m \approx 2^n$, де $n > 0$ і n – нату-

ральне число. З неї випливає, що $m \approx \log_3 2^n$ та $n \approx \log_2 3^m$. $\frac{2m}{n} = k_{add}$ – величина, що характеризує співвідношення у використанні елементів LUT.

$$k_{add} \approx \frac{2\log_3 2^n}{n} \approx \frac{2n\log_3 2}{n} \approx 2\log_3 2 \approx 1,26 .$$

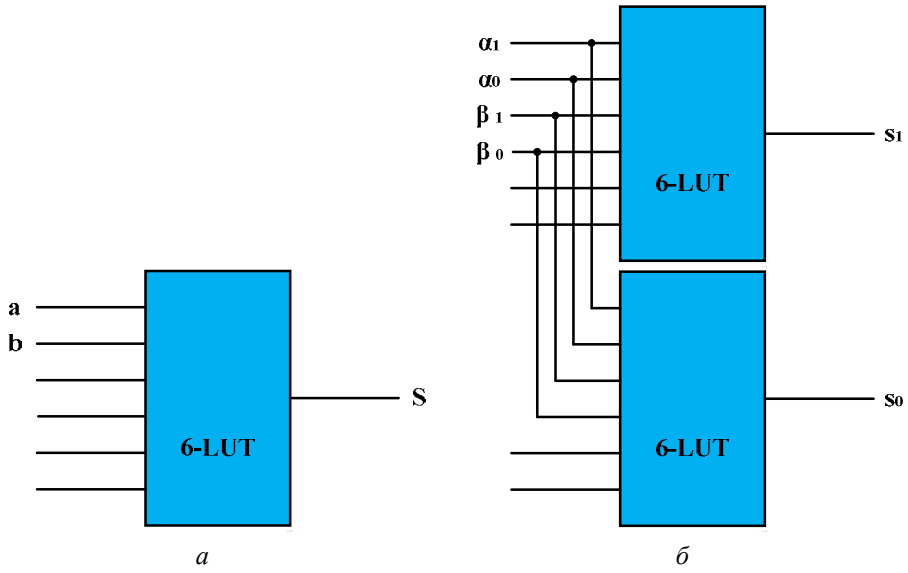

Рис. 3. Реалізація операції додавання двійкових (а) полів Галуа та трійкових (б) полів Галуа

Отже, для виконання операції додавання у трійкових полях Галуа потрібно в 1,26 разу більше апаратних ресурсів, ніж для реалізації операції додавання у двійкових полях Галуа.

Для реалізації помножувачів у двійкових полях Галуа використовуються модифіковані комірки Гілда, які мають три входи і один вихід, тобто їх можна реалізувати за допомогою одного шестивходового елемента LUT. Для трійкових полів використовуються модифіковані комірки Гілда, які мають шість входів і два виходи, тобто для їхньої реалізації потрібно два шестивходових LUT. Також потрібен один елемент LUT, для обчислення кожного коефіцієнта f (рис. 1). У двійкових полях GF(2^n) для реалізації помножувача потрібно $2n^2 - n$ модифікованих комірок Гілда, а у трійкових GF(3^m) – $2m^2 - m$. Відповідно, для двійкового поля потрібно $2n^2 - n$ LUT, а для трійкового – $2(2m^2 - m) + m - 1 = 4m^2 - 2m + m - 1 = 4m^2 - m - 1$. Для двійкових та трійкових полів з однаковою кількістю елементів буде справедливою наближена рівність $\frac{2n^2 - n}{4m^2 - m - 1} = k_{mul}$ – величина, що характеризує співвідношення у використанні елементів LUT для помножувачів. У результаті отримуємо вираз:

$$k_{mul} \approx \frac{2n^2 - n}{4(\log_3 2^n)^2 - \log_3 2^n - 1} \approx \frac{2n^2 - n}{4(n\log_3 2)^2 - n\log_3 2 - 1},$$

$$\lim_{n\to\infty} k_{mul} = \lim_{n\to\infty} \frac{2 - \frac{1}{n}}{4(\log_3 2)^2 - \frac{\log_3 2}{n} - \frac{1}{n^2}} = \frac{2}{4(\log_3 2)^2} = \frac{2}{1.593} = 1.255 .$$

Тобто для реалізації помножувача двійкових полів Галуа з наближенням до нескінченності потрібно приблизно на 1,255 більше апаратних ресурсів, ніж для помножувача трійкових полів Галуа.

Затрати елементів LUT суматора та помножувача (СП) процесора для оброблення елементів полів Галуа, схема якого наведена на рис. 4 [7], для двійкових полів Галуа будуть $n+2n^2-n=2n^2$, а для трійкових – $2m+4m^2-m-1=4m^2+m-1$.

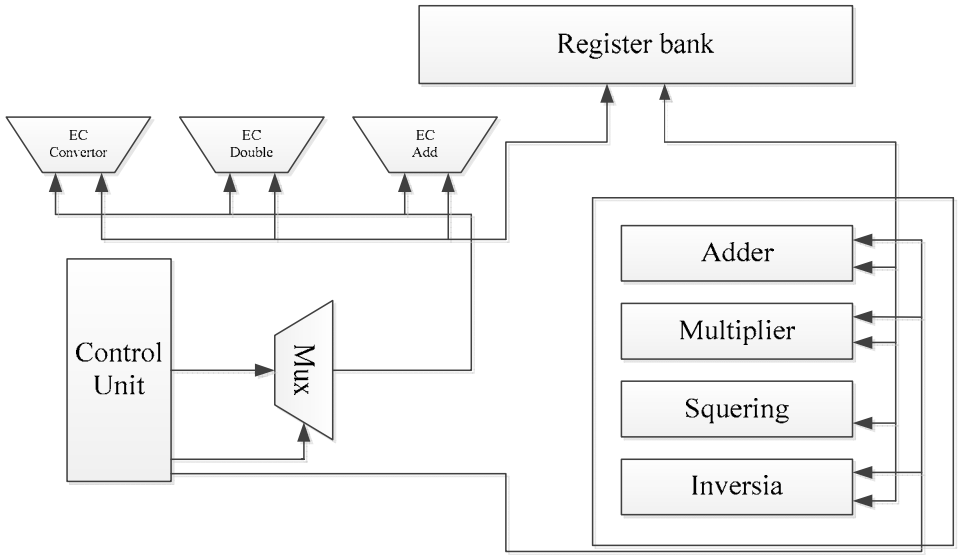

Рис. 4. Процесор для виконання операцій над елементами полів Галуа

Співвідношення витрат для СП процесора:

$$k_{СП} \approx \frac{2n^2}{4m^2+m-1} \approx \frac{2n^2}{4(n\log_3 2)^2+n\log_3 2-1} \approx \frac{2n^2}{4n^2(\log_3 2)^2+n\log_3 2-1},$$

$$\lim_{n\to\infty} k_{СП} = \frac{2}{4(\log_3 2)^2+\frac{\log_3 2}{n}-\frac{1}{n^2}} = \frac{2}{4(\log_3 2)^2} = \frac{2}{1.593} = 1.255.$$

Тобто витрати на реалізацію СП для трійкових полів Галуа в 1,255 разу менші, ніж для реалізації аналогічного вузла СП для двійкових полів Галуа.

Графік функції $k_{СП}$ наведено на рис. 5.

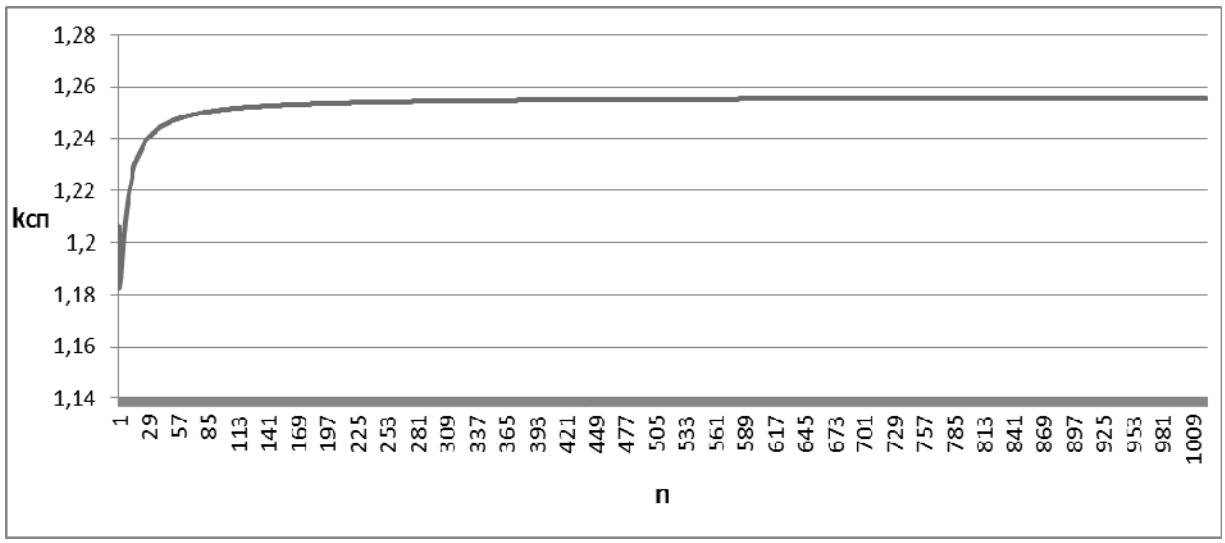

Рис. 5. Графік відношення апаратних затрат операції додавання та множення двійкових полів Галуа до трійкових

Використання трійкових полів Галуа $GF(3^m)$ замість двійкових $GF(2^m)$ дає змогу значно знизити апаратні витрати на реалізацію вузлів криптографічного захисту інформації.

Висновки

У роботі показано використання трійкових полів Галуа та імплементацію їх у сучасній елементній базі. Наведено порівняння реалізації додавання та множення у трійкових та двійкових полях Галуа. Одержано результати порівняння для полів з великими порядками: в разі реалізації додавання у трійкових полях Галуа апаратні витрати приблизно в 1,26 разу більші, ніж за реалізації додавання у двійкових полях; у разі реалізації множення у двійкових полях Галуа апаратні затрати приблизно в 1,255 разу більші, ніж за реалізації множення у трійкових полях; загальні затрати апаратних ресурсів для реалізації обох операцій у двійкових полях Галуа приблизно в 1,255 разу більші, ніж у трійкових.

1. Кушнеров А. Троичная цифровая техника. Перспектива и современность // Университет им. Бен-Гуриона, Беєр-Шева. – Израиль, 2005. – С. 1–7. 2. Arthur W. Burks, Harman H. Preliminary discussion of the logic design of an electronic computing instrument // Institute for Advanced study, Goldstin. – 1946 – P. 10–30 3. Oded Goldrich, Foundations of Cryptography, Volume 1: Basic Tools // Cambridge University Press. – 2014. – P. 7–10. 4. Глухов В. С. Порівняння поліноміального та нормального базисів представлення елементів поля Галуа // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи проектування. Теорія і практика". – 2007. – Вип. 564. – С. 5–6. 5. Добуш А. Р., Костик А. Т. Методи вбудованого контролю виконання операцій у полях Галуа для реалізації в НВІС // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи проектування. Теорія і практика". – 2013. – Вип. 570. – С. 3–7. 6. Проектування 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. 7. Hamid Javashi, Reza Sabbaghi-Nadooshan, A Novel Elliptic curve cryptography Processor using NoC design // Electronic Engineering Department, Islamic Azad University Central Tehran Branch, Tehran. – Iran, 2011. – С. 4.