УДК 004.383
В.С.Глухов, Р. Еліас, А.О.Мельник
Національний університет «Львівська політехніка»

# ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ НА ПЛІС СЕКЦІЙНИХ ПОМНОЖУВАЧІВ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА GF($2^M$) З НАДВЕЛИКИМ СТЕПЕНЕМ

*У роботі розглядаються результати роботи генератора ядра секційних помножувачів елементів полів Галуа GF(2m). Помножувач обробляє m-бітні елементи поля Галуа GF(2m), представлені з використанням гаусівського нормального базису типу 2, і формує m-бітний добуток порціями по n біт (n = 2k, k = 0, 1, …, 5). Кожна секція помножувача формує 1 біт результату. Генератор забезпечує формування помножувачів, які відповідають як стандарту ДСТУ 4145-2002 (m≤509), так і стандарту IEEE 1363-2000 (m≤998). Апаратна складність згенерованих ядер дозволяє їхню імплементацію на ПЛІС для встановлених значень m та n. Але при великих значеннях m та n, імплементація згенерованих ядер стає неможливою з-за їх великої структурної складності.*

*Ключові слова – поле Галуа GF(2m), гаусівський нормальний базис типу 2, секційний помножувач, генератор ядер.*

## Вступ

На сучасному етапі математичною основою цифрових підписів є еліптичні криві. В одному з варіантів реалізації цифрових підписів оброблення точок еліптичних кривих відбувається за правилами оброблення елементів полів Галуа $GF(2^m)$. Розрядність елементів поля $m$ може сягати тисячі біт. Апаратна реалізація помножувача для таких полів вимагає більш ніж мільйона транзисторів. Помножувачі можуть бути паралельними, послідовними та паралельно-послідовними – секційними. У даній роботі розглядаються результати аналізу роботи генератора ядер (описів на мові *VHDL*) секційного помножувача елементів полів Галуа $GF(2^m)$. Помножувач обробляє $m$-бітні елементи поля Галуа $GF(2^m)$, представлені з використанням гаусівського нормального базису типу 2, і формує $m$-бітний добуток порціями по $n$ біт ($1 \le n \le m$). Змінні $m$ та $n$ є параметрами, які може задавати користувач під час генерації ядра. Генератор забезпечує формування помножувачів, які відповідають як стандарту ДСТУ 4145-2002 ($m \le 509$), так і стандарту IEEE1363-2000 ($m \le 998$). Апаратна складність згенерованих ядер помножувачів дозволяє їхню імплементацію на ПЛІС. Але при великих значеннях $m$ та $n$ імплементація стає неможливою з-за великої структурної складності згенерованих ядер.

## 1. Огляд літератури, постановка проблеми

Математичною основою цифрових підписів є еліптичні криві та поля Галуа. Одним з варіантів представлення елементів поля Галуа $GF(2^m)$ є Гаусівський нормальний базис типу 2 [1]. Для даного базису відомий послідовний помножувач Мессі-Омури [2], паралельний помножувач та паралельно-послідовний помножувач (секційний) [3, 4], особливості синтезу помножувальних матриць для них розглянуті у роботі [5]. В Україні діє стандарт цифрового підпису на основі еліптичних кривих [1], який визначає максимальну характеристику поля Галуа $m$=509, у той же час міжнародний стандарт [6] дозволяє працювати з більшими полями ($m \le 998$). У роботах [7, 8] розглядаються особливості генерації *VHDL*-описів (ядер) секційних помножувачів, також наведені кількісні значення апаратної складності згенерованих ядер для значень $m$=515, 519. В обраній для імплементації ПЛІС дані ядра займають до 35% ресурсів. Питання аналізу на початкових етапах проектування потрібних для реалізації ядер апаратних ресурсів ПЛІС розглядається у роботах [9, 10], де для даного класу задач запропоновано розглядати ядра, що генеруються, як багаторівневі системи і застосовувати для аналізу принципи взаємозв'язку відкритих систем.

У даній роботі розглядаються особливості імплементації згенерованих ядер для надвеликих значень $m$ ($m$=998). Показано, що в цьому випадку визначальним для імплементації ядра на ПЛІС стає не апаратна, а структурна складність.

## 2. Мета роботи

Метою роботи є аналіз результатів імплементації на ПЛІС ядер секційних помножувачів елементів полів Галуа $GF(2^m)$, представлених у Гаусівському нормальному базисі типу 2, при надвеликих значеннях степеня поля ($m$=998).

## 3. Реалізація секційного помножувача

Послідовний помножувач Мессі-Омури (рис. 1) складається з двох регістрів циклічного зсуву операндів *RGA* і *RGB* та помножувальної матриці *M*. Секційний помножувач містить декілька помножувальних матриць та конвеєрний регістр для результату множення. На рис. 2

наведено приклад 16-секційного помножувача для $m$ = 515. Додатково помножувачі рис. 1 та рис. 2 містять необов'язкові вузли вбудованого контролю (CED).

Основні етапи роботи генератора ядер помножувача:

ввід параметрів $m$ та $n$;

генерація утворюючого полінома поля $GF(2^m)$ для оптимального нормального базису типу 2;

генерація помножувальної матриці;

генерація секцій помножувача;

генерація вузла вбудованого контролю кожної секції;

об'єднання секцій у єдиний вузол помножувача;

об'єднання секційних вузлів вбудованого контролю в єдиний вузол вбудованого контролю.

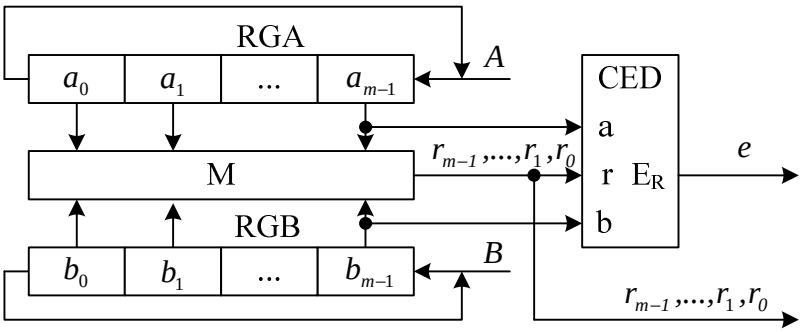


*Рис. 1. Помножувач з вузлом виявленням помилок*

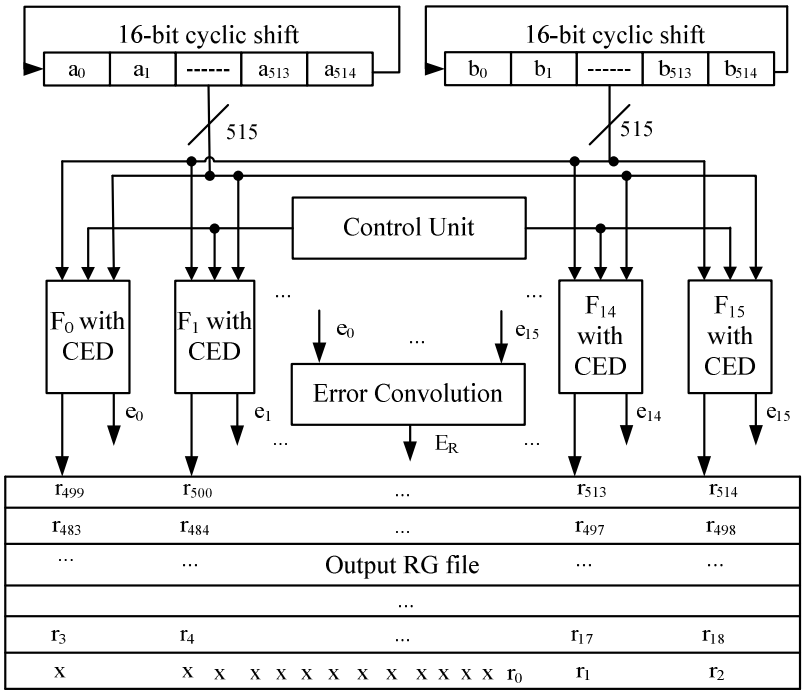


*Рис. 2. 16-секційний помножувач з вбудованим контролем*

## 4. Особливості синтезу помножувальної матриці

Найскладнішою технологічною операцією при синтезі *VHDL*-коду помножувальної матриці є знаходження оберненої матриці ($m$ x $m$) [5]. Час знаходження оберненої матриці для різних полів містить Таблиця 1. Розрахунки для $m$ = 515, 519, 530 проводилися на процесорі з тактовою частотою 2,6 ГГц, 2 ядра (працювало тільки одне ядро), об'єм оперативної пам'яті 4 Гбайта.

*Таблиця 1*

**Час обрахування оберненої матриці**

| m | 515 | 519 | 530 | 998 |
|---|---|---|---|---|
| Час, год. | 1 год. 35 хв. | 1 год. 57 хв. | 1 год. 39 хв. | 50 год. |

Логічна структура згенерованої помножувальної матриці наведена на рис. 3.

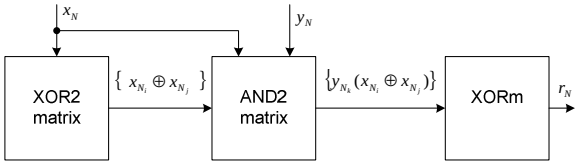


*Рис. 3. Логічна структура помножувальної матриці*

## 5. Результати імплементації та перевіряння роботи помножувачів

Гаусівський нормальний базис типу 2 існує для полів Галуа $GF(2^m)$ для $m$=515, 519, 530, 531, 543, 545, 554, 558, 561, 575, 585, 593, 606, 611, 614, 615, 618, 629, 638, 639, 641, 645, 650, 651, 653, 659, 683, 686, 690, 713, 719, 723, 725, 726, 741, 743, 746, 749, 755, 761, 765, 771, 774, 779, 783, 785, 791, 803, 809, 810, 818, 831, 833, 834, 846, 866, 870, 873, 879, 891, 893, 911, 923, 930, 933, 935, 938, 939, 950, 953, 965, 974, 975, 986, 989, 993, 998 [6] (перераховані тільки поля, для яких $509<m\leq998$).

Результати імплементації деяких ядер для ПЛІС *6vcx130tff1156-2* засобами *Xilinx WebPack12* показує Таблиця 2 та Таблиця 3 (* - синтез попередньо проведений засобами *Synopsys Synplify*).

*Таблиця 2*

**Імплементація помножувача для *m*=515 (без CED)**

| n | 1 | 8 | 16* | 16 | 32 |
|---|---|---|---|---|---|
| Кількість слайсів (%) | 688 (3%) | 1771 (8%) | 1026 (5%) | 2307 (11%) | 7018 (35%) |
| Період синхроімпульсів, нс | 5,523 | 8,5 | 13,1 | 13,8 | 13,8 |
| Час імплементації, хв. | | 5 | 50 | 304 | Немає даних |

*Таблиця 3*

**Імплементація помножувача для *m*=519 (без CED)**

| n | 1 | 8 | 16 | 32 |
|---|---|---|---|---|
| Кількість слайсів (%) | 675 (3%) | 2248 (11%) | 3240 (16%) | 6,112 (30%) |
| Період синхроімпульсів, нс | 6,319 | 13,198 | 12,490 | 14,576 |

Як видно, апаратні витрати на імплементацію ядер складають до 35 % ресурсів ПЛІС і не є визначальними для результатів імплементації. Часова складність ядер, непрямим показником якої є період синхроімпульсів, також не є в даному випадку вирішальним фактором при імплементації.

Сумарна кількість входів операндів та виходів результату одного помножувача дорівнює 3$m$ і для вищезгаданих полів перевищує кількість контактів сучасних ПЛІС. Для перевіряння роботи згенерованих помножувачів використовується спеціально створений *VHDL*-стенд (рис. 4), до складу якого разом з помножувачем входять вхідні *FIFO* із записом по 128 біт і читанням по 1024 біта та вихідний *FIFO* із записом по 1024 біта і читанням по 128 біт. Сумарна кількість входів операндів та виходів результату стенда дорівнює 256, що дозволяє реалізувати його на великому наборі сучасних ПЛІС.

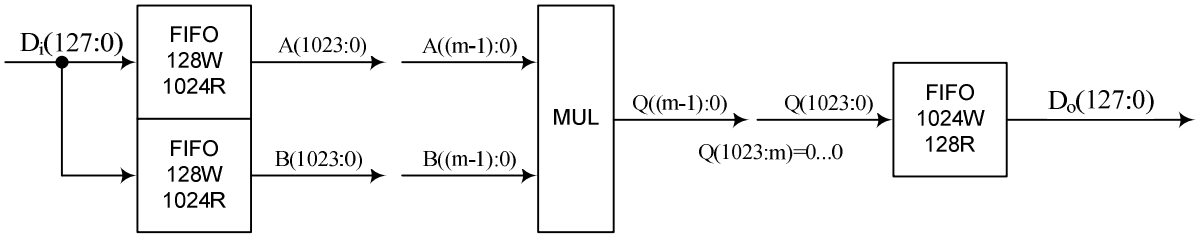


*Рис. 4. Стенд для перевіряння помножувачів*

Таким способом проблема з обмеженою кількістю контактів ПЛІС також не є визначальною для імплементації. Імплементація згаданих ядер пройшла успішно.

Тестові приклади для перевіряння роботи помножувачів утворюють:

множення 1 x 1=1, при цьому у нормальному базисі 1 представляється кодом з $m$ двійкових одиниць (1…1);

множення $a$ x $a = a^2$, при цьому у нормальному базисі результат піднесення до квадрату операнда $a$ дорівнює результату циклічного зсуву цього операнда $a$ на один двійковий розряд (якщо $a=a_0a_1\ldots a_{m-1}$, $a^2=a_1\ldots a_{m-1}a_0$).

За результатами вказаних тестів згенеровані помножувачі працюють правильно.

## 6. Особливості імплементації помножувача для *m*=998

Результати імплементації на ПЛІС *xc6slx150tfgg900-2* ядер для надвеликого значення степеня двійкового поля містить таблиця 4 .

Таблиця 4

**Імплементація помножувача для *m*=998**

| n | 2 | 4 | 8 |
|---|---|---|---|
| Кількість слайсів (%) | 1,323 (5%) | 1,896 (8%) | 3,253 (14%) |
| Період синхроімпульсів, нс | 12.922 | 17.514 | 23.215 |
| Час імплементації, хв. | 1 | 20 | 133 |
| Результат імплементації | успішно | успішно | Не розвелося |

Як видно (таблиця 4), апаратна і часова складність ядер не викликають проблем під час імплементації. Однак, при *n*=8 для ядра не вдалося здійснити імплементацію. Нижче показано процент використання основних елементів ПЛІС для випадку n=8.

Number of Slice Registers: 3,359 out of 184,304 1%
Number of Slice LUTs: 10,720 out of 92,152 11%
Number of occupied Slices: 3,253 out of 23,038 14%
Number of bonded IOBs: 265 out of 540 49%
Number of RAMB16BWERs: 128 out of 268 47%
Number of BUFG/BUFGMUXs: 1 out of 16 6%

Процент використання інших елементів ПЛІС дорівнює 0 %.

Причиною неможливості імплементації може бути недостатня кількість доступних користувачу зв'язків в середині ПЛІС, тобто, структурна складність ядра. Відомі методи визначення можливості імплементації ядер на ПЛІС [9, 10] базуються на оцінці апаратної складності. Розглянуті у даній роботі задачі ставлять проблему оцінки структурної складності проектів на ранніх етапах проектування для визначення можливості їх реалізації на конкретних ПЛІС.

## Висновок

У роботі проведено аналіз результатів імплементації на ПЛІС ядер секційних помножувачів елементів полів Галуа $GF(2^m)$, представлених у Гаусівському нормальному базисі типу 2, при надвеликих значеннях степеня поля ($m$=998). Висловлено припущення, що причиною неможливості імплементації на ПЛІС окремих ядер помножувачів може бути структурна складність ядра, що ставить проблему оцінки структурної складності проектів на ранніх етапах проектування для визначення можливості їх реалізації на конкретних ПЛІС.

*1. 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. 2003.2. J. Omura and J. Massey. Computational method and apparatus for finite field arithmetic. U.S. Patent Number 4,587,627, May 1986. 3. Chanho Lee, Jeongho Lee. Design of an Elliptic Curve Cryptography Processor Using a Scalable Finite Field Multiplier in GF($2^{193}$). Journal of the Korean Physical Society, Vol. 44, No. 1, pp. 39-45. January 2004. 4. Elias Rodrigue. Design of an Elliptic Curve Cryptography Using A Finite Field Multiplier in GF($2^{521}$). Вісник № 658 НУ «ЛП» «Комп'ютерні системи та мережі», Львів, 2009. С. 144 - 149. 5. Глухов В.С. Особливості виконання операцій над матрицями в полях Галуа. Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи проектування. Теорія і практика". Вип. 564. Львів, 2006. С.35-39. 6. IEEE Std 1363-2000 IEEE Standard Specifications for Public-Key Cryptography Sponsor Microprocessor and Microcomputer Standards Committee of the IEEE Computer Society. Approved 30 January 2000. 7. Еліас Р. Генератор ядер секціонованих помножувачів елементів полів Галуа GF($2^m$) для оптимального нормального базису 2-го типу. / Глухов В., Еліас Р. // Комп'ютерні науки та інформаційні технології. / Л. : Вид-во Нац. ун-ту "Львів. політехніка", 2012. – С. 78 - 84. – (Вісник / Нац. ун-т "Львів. політехніка"; № 732. 8. Р. Еліас. Особливості синтезу генератора ядер секціонованих помножувачів елементів полів Галуа GF($2^m$) для пристроїв обробки цифрових підписів. / В. Глухов, Р. Еліас. // І Міжнародна науково-технічна конференція "Захист інформації і безпека інформаційних систем". 31 травня - 01 червня 2012 р. Львів, Україна. 9. Глухов В.С. Вибір багатоядерних структур для пристроїв обробки ЕЦП // Вісник Національного університету "Львівська політехніка" "Комп`ютерні системи та мережі". № 658. Львів, 2009. С.35 – 39. 10. Глухов В.С. Оцінювання апаратних витрат на реалізацію багаторівневої комп'ютерної системи з врахуванням закону Амдаля // Вісник Національного університету «Львівська політехніка» «Комп'ютерні науки та інформаційні технології» № 663. Львів, 2010. С.17 – 23*