

УДК 004.383

**В.С. Глухов, Р. Еліас, А.О. Мельник**  
**ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ НА ПЛІС СЕКЦІЙНИХ ПОМНОЖУВАЧІВ ЕЛЕМЕНТІВ**  
**ПОЛІВ ГАЛУА  $GF(2^m)$  З НАДВЕЛИКИМ СТЕПЕНЕМ**

*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  $GF(2^m)$ . 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 ( $n = 2^k, k = 0, 1, \dots, 5$ ). Кожна секція помножувача формує 1 біт результату. Генератор забезпечує формування помножувачів, які відповідають як стандарту ДСТУ 4145-2002 ( $m \leq 509$ ), так і стандарту IEEE 1363-2000 ( $m \leq 998$ ). 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  $GF(2^m)$ , гаусівський нормальний базис типу 2, секційний помножувач, генератор ядер.

*Рис. 4. Табл. 4. Літ. 10.*

**В.С. Глухов, Р. Элиас, А.А. Мельник**  
**ОСОБЕННОСТИ РЕАЛИЗАЦИИ НА ПЛИС СЕКЦИОННЫХ УМНОЖИТЕЛЕЙ**  
**ЭЛЕМЕНТОВ ПОЛЕЙ ГАЛУА  $GF(2^M)$  С ОЧЕНЬ БОЛЬШИМ СТЕПЕНЬЮ**

*В работе рассматриваются результаты работы генератора ядер секционных умножителей элементов полей Галуа  $GF(2^m)$ . Умножитель обрабатывает  $m$ -битные элементы поля Галуа  $GF(2^m)$ , представленные с использованием гауссовского нормального базиса типа 2, и формирует  $m$ -битное произведение порциями по  $n$  бит ( $n = 2^k, k = 0, 1, \dots, 5$ ). Каждая секция умножителя формирует 1 бит результата. Генератор обеспечивает формирование умножителей, которые соответствуют как стандарту ДСТУ 4145-2002 ( $m \leq 509$ ), так и стандарту IEEE 1363-2000 ( $m \leq 998$ ). Аппаратная сложность сгенерированных ядер позволяет их имплементацию на ПЛИС для установленных значений  $m$  и  $n$ . Но при больших значениях  $m$  и  $n$ , имплементация сгенерированных ядер становится невозможной из-за их большой структурной сложности.*

*Ключевые слова:* поле Галуа  $GF(2^m)$ , гауссовской нормальный базис типа 2, секционный умножитель, генератор ядер.

**V. Hlukhov, R. Elias, A. Melnyk**  
**FEATURES OF THE FPGA-BASED GALOIS FIELD  $GF(2^M)$  ELEMENTS SECTIONAL**  
**MULTIPLIERS WITH EXTRA LARGE EXPONENT**

*Results of work of scalable multiplier for Galois field  $GF(2^m)$  elements core generator are examined. The multiplier uses type 2 Gaussian normal basis for Galois field elements presentation and forms  $m$ -bit result by  $n$ -bit portions. Each section produces 1 bit of result. Core generator satisfies both DSTU 4145-2002 ( $m \leq 509$ ) and IEEE 1363-2000 ( $m \leq 998$ ) standards. Generated cores hardware complexity allows their implementation in FPGA for any  $m$  and  $n$  values. But for big  $m$  and  $n$  values implementation is impossible because of high structural complexity.*

*Keywords:* Galois field  $GF(2^m)$ , Gaussian normal base of type 2, scalable multiplying, core generator.

**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 ( $1 \leq n \leq m$ ). 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 ( $m \leq 509$ ), так і стандарту IEEE 1363-2000 ( $m \leq 998$ ). 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.

**Огляд літератури, постановка проблеми.** 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 ( $1 \leq n \leq m$ ). 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 ( $m \leq 509$ ), так і стандарту IEEE1363-2000 ( $m \leq 998$ ). 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.

**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 ( $m=998$ ).

**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 Рисю 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.

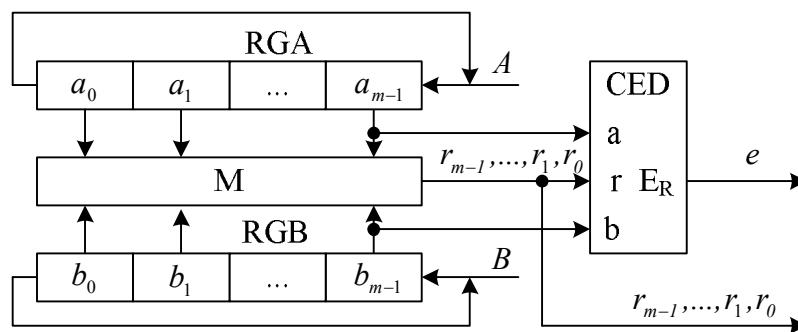


Рис. 1. Помножувач з вузлом виявленням помилок

**Особливості синтезу помножувальної матриці.** Найскладнішою технологічною операцією при синтезі VHDL-коду помножувальної матриці є знаходження оберненої матриці ( $m \times m$ ) знаходження оберненої матриці для різних полів містить. 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.

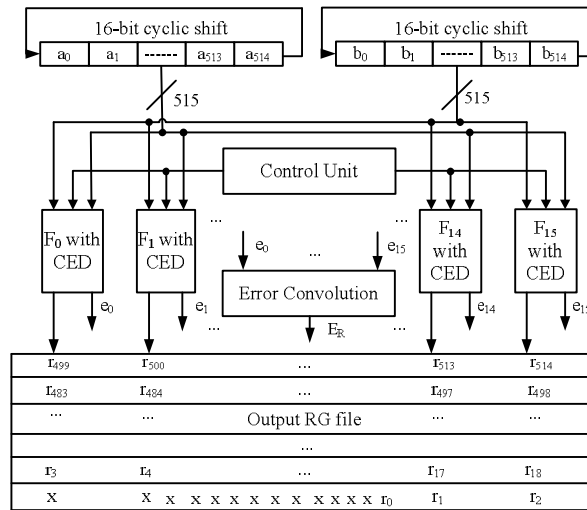


Рис. 2. 16-секційний помножувач з вбудованим контролем

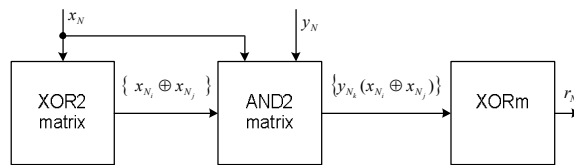


Рис. 3. Логічна структура помножувальної матриці

**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  $509 < m \leq 998$ ).

Результати імплементації деяких ядер для ПЛІС *bvsc130tff1156-2* засобами *Xilinx WebPack12* показує Таблиця 2 та Таблиця 3 (\* – синтез попередньо проведений засобами *Synopsys Synplify*).

Таблиця 2. 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

Таблиця 3. 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, апаратні витрати на імплементацію ядер складають до 35 % ресурсів ПЛІС і не є визначальними для результатів імплементації. Часова складність ядер, непрямым 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  $3m$  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 станда дорівнює 256, що дозволяє реалізувати його на великому наборі сучасних ПЛІС.

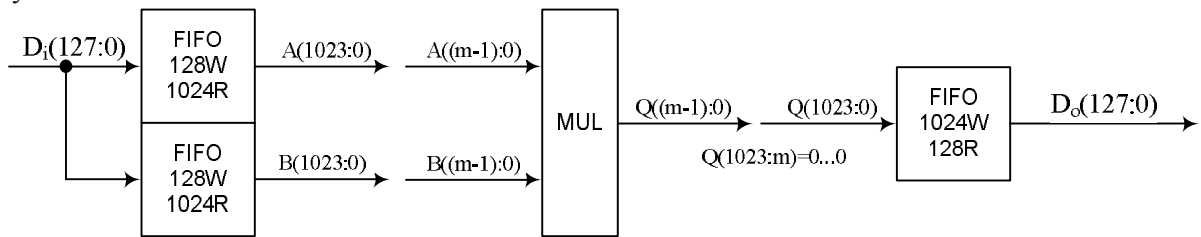


Рис. 4. Стенд для перевірення помножувачів

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

Тестові приклади для перевірення роботи помножувачів утворюють:

- множення  $1 \times 1 = 1$ , при цьому у нормальному базисі 1 представляється кодом з  $m$  двійкових одиниць (1...1);
- множення  $a \times a = a^2$ , при цьому у нормальному базисі результат піднесення до квадрату операнда  $a$  дорівнює результату циклічного зсуву цього операнда  $a$  на один двійковий розряд (якщо  $a = a_0 a_1 \dots a_{m-1}$ ,  $a^2 = a_1 \dots a_{m-1} a_0$ ).

За результатами вказаних тестів згенеровані помножувачі працюють правильно.

**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 розвелось

Як видно (Таблиця 4таблиця 3), 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. // I 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.

Стаття надійшла до редакції 26.05.2013.