УДК 004.032.2

**В. С. Глухов**, д-р техн. наук,
**Р. Еліас**, канд. техн. наук

## ЗМЕНШЕННЯ СТРУКТУРНОЇ СКЛАДНОСТІ БАГАТОСЕКЦІЙНИХ ПОМНОЖУВАЧІВ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА

***Анотація.*** *У статті розглядається підхід до зменшення структурної складності багатосекційних помножувачів елементів довічних полів Галуа. Апаратна складність помножувачів дозволяє реалізувати їх на програмуємих логічних інтегральних схемах, але через структурної комбінаторної складності зробити це неможливо. У роботі пропонується попереднє упорядкування матриці за допомогою змішувача та її реалізація з однотипних матриць логічного множення. Як наслідок, досягається зменшення числа матриць, зниження їх апаратної і структурної складності за рахунок багаторазового використання.*

***Ключові слова:*** *структурна складність, поля Галуа, помножувальна матриця, пам'ять з впорядкованим доступом*

**V. Hlukhov**, DrS.,
**R. Elias**, PhD.

## GALOIS FIELDS ELEMENTS MULTISECTION MULTIPLIERS STRUCTURAL COMPLEXITY REDUCTION

***Abstract.*** *The article discusses the approach to reducing the structural complexity of multi-multipliers binary elements of Galois fields. The hardware complexity of multipliers allows for them to Field-Programmable Gate Array, but due to the structural complexity of combinatorial make it impossible. The paper proposes a preliminary ordering matrix using the agitator and its implementation of the same type of logical multiplication of matrices. As a consequence, achieved by reducing the number of matrices, reducing their hardware and structural complexity due to multiple use.*

***Keywords:*** *structural complex, Galois fields, multiplicative matrix, ordered access memory*

**В. С. Глухов**, д-р техн. наук,
**Р. Элиас**, канд. техн. наук

## УМЕНЬШЕНИЕ СТРУКТУРНОЙ СЛОЖНОСТИ МНОГОСЕКЦИОННЫХ УМНОЖИТЕЛЕЙ ЭЛЕМЕНТОВ ПОЛЕЙ ГАЛУА

***Аннотация.*** *В статье рассматривается подход к уменьшению структурной сложности многосекционных умножителей элементов двоичных полей Галуа. Аппаратная сложность умножителей позволяет реализовать их на программируемых логических интегральных схемах, но из-за структурной комбинаторной сложности сделать это невозможно. В работе предлагается предварительное упорядочение матрицы с помощью перемешивателя и ее реализация из однотипных матриц логического умножения. Как следствие, достигается уменьшение числа матриц, снижение их аппаратной и структурной сложности за счет многократного использования.*

***Ключевые слова:*** *структурная сложность, поля Галуа, умножительная матрица, память с упорядоченным доступом*

### Вступ

У даний час математичною основою опрацювання цифрового підпису є еліптичні криві [3]. Обробка точок еліптичної кривої базується на виконанні операцій у полях Галуа GF(2m), елементи яких можуть бути представлені у поліноміальному та нормальному базисах. Апаратна реалізація помножувача для таких полів вимагає великих витрат обладнання. Помножувачі можуть бути паралельними, послідовними і паралельно-послідовними – секційними, які формують m біт добутку порціями по n біт. Для нормального базису апаратна складність помножувачів дозволяє проводити їхню реалізацію на сучасних програмуємих логічних інтегральних схемах (ПЛІС).

При великих значеннях m і n неможливо реалізувати ядра через їх високу структурну складність [4], методи оцінки якої відомі із літератури [5]. На основі оцінок у статті пропонується метод зменшення структурної складності. Основна увага приділена зменшенню структурної складності помножувальної матриці, яка входить до складу помножувача. У статті пропонується попереднє впорядкування матриці за допомогою спеціального перемішувача. Впорядкування дозволяє реалізувати матрицю з однотипних елементів. Як наслідок, можна зменшити їх кількість, апаратну та структурну складності за рахунок багаторазового використання тільки одного елемента. Це досягається впровадженням конвеєрної структури матриці. Використання пам'яті з впорядкованим доступом [9] як перемішувача повинно за рахунок ре-конфігурованості помножувача забезпечити його роботу з різними полями Галуа.

Для нормального базису відомі послідовний помножувач Мессі-Омури [1], паралельний помножувач і паралельно-послідовний помножувач (секційний). Помножувальні матриці для них досліджувалися в роботі [2]. Перші спроби оцінити структурну складність односекційного помножувача було зроблено у [4; 6; 10]. Аналогічну оцінку для поліноміального базису зроблено у [7 – 8].

Метою роботи є розроблення методу зменшення структурної складності помножувальних матриць помножувача елементів полів Галуа у нормальному базисі.

Структура помножувальної матриці

Головним елементом помножувача [1] елементів поля Галуа GF(2m) у нормальному базисі типу 2 є комбінаційна схема – помножувальна матриця, яка описується математичною матрицею з (m x m) двійкових символів, при цьому у кожному рядку та стовпчику такої матриці міститься тільки дві 1, решта – 0 (за винятком одного рядка та одного стовпчика, які містять одну 1). Матриця симетрична відносно своєї діагоналі. Алгоритм формування матриці для заданого m наведено у [2].

Приклад матриці для $m$=4 наведено на рис. 1.

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_3 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Рис. 1. Помножувальна матриця

Молодший розряд r0 добутку R=A*B обчислюється як

$$r_0 = a_2 b_0 \oplus (a_2 \oplus a_3) b_1 \oplus (a_0 \oplus a_1) b_2 \oplus (a_1 \oplus a_3) b_3,$$

тобто, визначається положенням 1 у матриці. Значення кожного наступного розряду добутку визначається аналогічно після циклічного зсуву операндів A та B на один розряд.

Фрагмент опису формування часткових добутків s0, s1, …, s7, …, s172, з яких формується розряд добутку r0 для матриці з m=173 показано нижче [2]:

$$s_0 = b_0 (a_{21} \oplus a_0);$$
$$s_1 = b_1 (a_{70} \oplus a_{22});$$
$$s_2 = b_2 (a_{59} \oplus a_{44});$$
$$s_3 = b_3 (a_{166} \oplus a_{93});$$
$$s_4 = b_4 (a_{123} \oplus a_{99});$$
$$s_5 = b_5 (a_{104} \oplus a_9);$$
$$s_6 = b_6 (a_{147} \oplus a_{51});$$
$$s_7 = b_7 (a_{117} \oplus a_{87});$$
$$\ldots .$$
$$r_0 = s_0 \oplus s_1 \oplus s_2 \oplus \ldots \oplus s_{172}.$$

Функціональну схему помножувача на основі такої матриці та фрагмент її умовної топології показано на рис. 2. Матриця має нерегулярний характер, що ускладнює її реалізацію і збільшує структурну та апаратну складність.

На рис. 2 регістри Rotation забезпечують циклічний зсув операндів, m-входовий елемент XOR формує значення чергового розряду добутку R=A*B. Чорні цяточки всередині матриці на рис. 2 зображають двовходові елементи I загальною кількістю 2m-1 елементів.

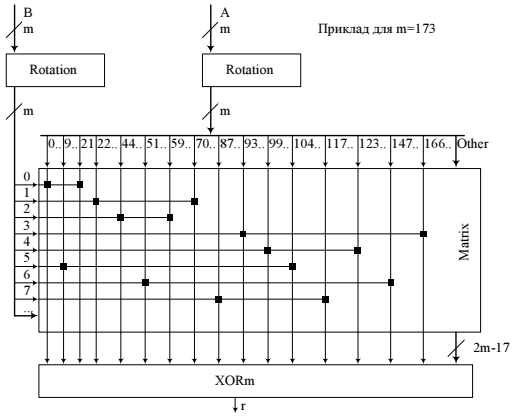


Рис. 2. Помножувач (початковий вигляд)

Модифікація помножувальної матриці.

На першому кроці модифікації помножувальної матриці за допомогою перемішувача Interleaver виконуються перестановлення і дублювання розрядів операнда A на вході помножувальної матриці так, щоб елементи I, зв'язані з одним розрядом операнда B, знаходилися на мінімальній відстані один від одного (рис. 3). Для цього кількість елементів I збільшується до 4m-1. Тоді кожній групі SetA розрядів операнда A буде відповідати своя група SetB розрядів операнда B та своя група елементів I (

рис. 4).

Оскільки підключення розрядів SetA та SetB до елементів I всередині групи всюди однакове (як на рис. 3, то можна замінити велику кількість груп елементів I, що працюють паралельно, на одну групу елементів I, яка буде опрацьовувати сигнали від усіх груп SetA та SetB послідовно (рис. 5).

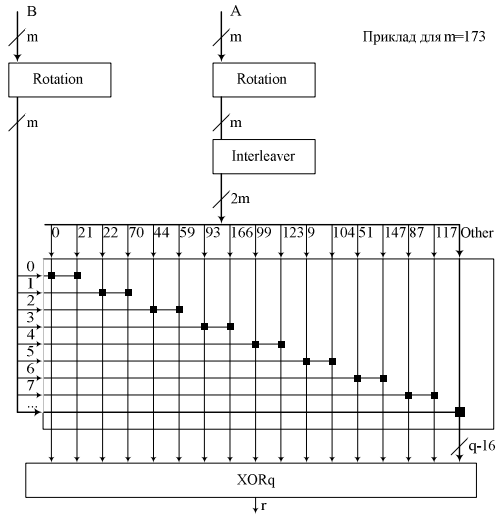


Рис. 3. Переставлені розряди оператора A

Скорочена помножувальна матриця And Set тоді буде мати розмір (k x 2k), де k – розмір групи розрядів SetA.

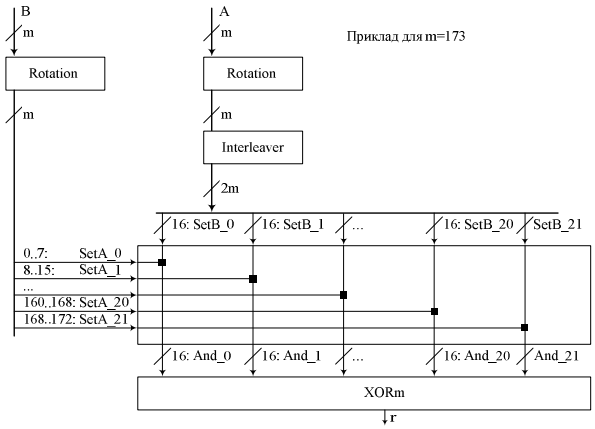


Рис. 4. Паралельне формування часткових добутків

Оцінка структурної складності.

Структурна складність помножувальної матриці оцінюється як O(m2), де m – порядок поля Галуа та кількість рядків і стовпчиків у матриці [10]. Структурну складність скороченої помножувальної матриці можна оцінити як O(k2), а очікуване скорочення структурної складності – як (m/k)2=N2, що для m=173, k=16 буде більше ніж у 100 разів. Зменшення структурної і апаратної складності призведе до збільшення часової складності множення приблизно у m/k =N разів.

Зменшення структурної складності веде до зменшення кількості входів елемента XORn з q=2m-1 (

рис. 2) до 2k (рис. 1), тобто, приблизно у m/k разів (для m=173, k=16 – приблизно у 16 разів).

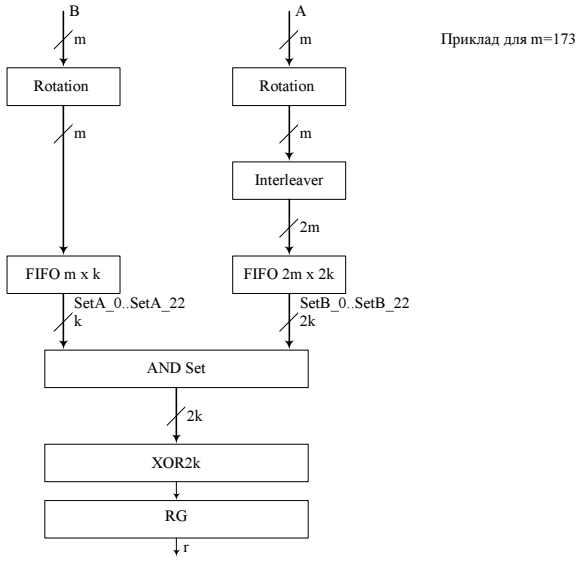


Рис. 5. Послідовне формування часткових добутків

Багатовходові елементи XOR мають пірамідальну структуру (рис. 6). При використання у пірамідальній структурі двовходових елементів (рис. 6) кількість каскадів визначається як $\lceil \log_2 m \rceil$, відповідно, зменшення кількості входів у m/k разів, призводить до зменшення кількості каскадів, а значить і затримки елемента, у $\lceil \log_2 m/k \rceil = \lceil \log_2 N \rceil$ разів (для m=173, k=16 – приблизно у 4 рази). Зменшення затримок комбінаційних елементів дозволяє пропорційно підняти тактову частоту роботи пристрою.

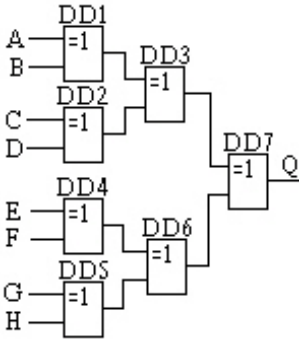


Рис. 6. Пірамідальна структура елемента XORn

Реалізація перемішувача як пам'яті з впорядкованим доступом [9] (рис. 7) дозволить полегшити реконфігурацію запропонованого помножувача для різних полів Галуа GF(2m).

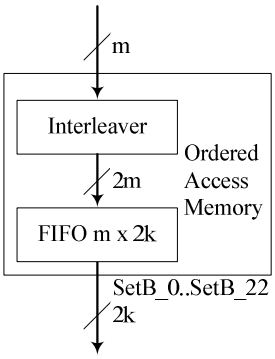


Рис. 7. Пам'ять з впорядкованим доступом

**Висновки**

У статті розглядається підхід до зменшення структурної складності багатосекційних помножувачів елементів двійкових полів Галуа. Елементи полів представлено у нормальному базисі типу 2. Порядок поля сягає 998. Апаратна складність помножувачів дозволяє реалізувати їх на ПЛІС. Але з-за великої структурної складності для деяких комбінацій порядку поля і кількості секцій зробити це практично неможливо. Основна увага приділена зменшенню структурної складності помножувальної матриці, яка входить до складу помножувача. У статті пропонується попереднє впорядкування матриці за допомогою спеціального перемішувача. Впорядкування дозволяє реалізувати матрицю з N однотипних матриць елементів I). Як наслідок, можна зменшити кількість матриць елементів I, апаратну та структурну складності помножувальної матриці за рахунок багаторазового використання тільки однієї матриці I. Очікуване зме-

ншення структурної складності пропорційне N2. Це досягається збільшення часової складності множення в N разів. Використання пам'яті з впорядкованим доступом як перемішувача повинно за рахунок реконфігурованості помножувача забезпечити його роботу з різними полями Галуа.

Список використаної літератури

1. Omura J., and Massey J., (1986), Computational Method and Apparatus for Finite Field Arithmetic. U.S. Patent Number 4, 587, 627, May 1986.

2. Глухов В. С. Особливості виконання операцій над матрицями в полях Галуа / В. С. Глухов // Вісник Національного університету «Львівська політехніка» «Комп'ютерні системи проектування. Теорія і практика». – 2006. – Львів : – Вип. 564. – С. 35 – 39.

3. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К. : Державний комітет України з питань технічного регулювання та споживчої політики. 2003.

4. Глухов В. С. Особливості реалізації на ПЛІС секційних помножувачів елементів полів Галуа GF(2m) з надвеликим степенем / В. С. Глухов, Р. М. Еліас, А. О. Мельник. // Комп'ютерно-інтегровані технології:освіта, наука, виробництво Луцький національний технічний університет. – 2013. – Луцьк : – № 12. – С. 103 – 106.

5. Глухов В. С. Результати оцінювання структурної складності помножувачів елементів полів Галуа / В. С. Глухов, О. В. Глухова // Комп'ютерні системи та мережі. Вісник Національного університету «Львівська політехніка». – Львів : – 2013. – Вип. 773. – С. 27 –29.

6. Глухов В. С. Оцінка структурної складності багатосекційних помножувачів елементів полів Галуа / В. С. Глухов, Г. М. Тріщ // Комп'ютерні системи та мережі. Вісник Національного університету «Львівська політехніка». – 2014.– Львів : – Вип. 806. – С. 27 – 33.

7. Шологон О. З. Обчислення структурної складності помножувачів у поліноміальному базисі елементів полів Галуа GF(2m) / О. З. Шологон // Комп'ютерні системи та мережі. Вісник Національного університету «Львівська політехніка». – Львів : – 2014. – Вип. 806. – С. 284 – 289.

8. Шологон Ю. З. Оцінювання структурної складності помножувачів полів Галуа на основі елементарних перетворювачів / Ю. З. Шологон // Комп'ютерні системи та мережі. Вісник Національного університету «Львівська політехніка». – Львів : – 2014. – Вип. 806. – С. 290 – 295.

9. Мельник А. О. Пам'ять із впорядкованим доступом [Текст] : монографія / А. О. Мельник; Нац. ун-т «Львівська політехніка». – Львів : – 2014. Вид-во Львівської політехніки, – 294 с.: іл. – Бібліогр.: – С. 285 – 291. ISBN 978-617-607-540-0 (у паліт.).

10. Глухова О. В. Аналітична оцінка структурної складності помножувачів елементів полів Галуа / О. В. Глухова, А. Я. Лозинський, Р. І. Яремкевич, А. О. Ігнатович // Матеріали V Всеукраїнської школи-семінару молодих вчених і студентів «Сучасні комп'ютерні інформаційні технології» ACIT'2015. – Тернопіль : ТНЕУ, 22-23 травня 2015. – С. 168 – 169.

Отримано 30.05.2015

References

1. Omura J., and Massey J., (1986), Computational Method and Apparatus for Finite Field Arithmetic. U.S. *Patent Number 4, 587, 627*, May 1986 (In English).

2. Hlukhov V.S. Osoblyvosti vykonannya operatsiy nad matrytsyamy v polyakh Halua [Operations over Matrices in Galois Fields Features], (2006), *"Komp'yuterni Systemy Proektuvannya. Teoriya i praktyka". Visnyk Natsional'noho Universytetu "L'vivs'ka Politekhnika",* Lviv, Ukraine, Vol. 564. pp. 35 – 39 (In Ukrainian).

3. DSTU 4145-2002. Informatsiyni tekhnolohiyi. Kryptohrafichnyy zakhyst informatsiyi. Tsyfrovyy pidpys, shcho gruntuyet'sya na eliptychnykh kryvykh. Formuvannya ta pereviryannya [Information Technology. Cryptographic Techniques. Digital Signatures Based on Elliptic Curves. Generation and Verification], (2003), *Derzhavnyy Komitet Ukrayiny z Pytan' Tekhnichnoho Rehulyuvannya ta Spozhyvchoyi Polityky*, Kiev, Ukraine (In Ukrainian).

4. Hlukhov V.S., Elias R.M., and Mel'nyk A.O. Osoblyvosti realizatsiyi na PLIS sektsiynykh pomnozhuvachiv elementiv poliv Halua GF(2m) z nadvelykym stepenem [Features of the FPGA-based Galois field GF(2m) Elements Sectional Multipliers with Extra Large Exponent], (2013), *Komp'yuterno-intehrovani Tekhnolohiyi:Osvita, Nauka, Vyrobnytstvo – Naukovyy Zhurnal, Luts'kyy Natsional'nyy Tekhnichnyy Universytet.* Luts'k, Ukraine, Vol. 12, pp. 103 – 106 (In Ukrainian).

5. Hlukhov V.S., and Hlukhova O.V. Rezul'taty otsinky strukturnoyi skladnosti pomnozhuvachiv elementiv poliv Halua [Structural Complexity of Galois Field Elements Multipliers Evaluation Results], (2013), *Komp'yuterni Systemy ta Merezhi". Visnyk Natsional'noho Universytetu "L'vivs'ka politekhnika",* Lviv, Ukraine, Vol. 773, pp. 27 – 32 (In Ukrainian).

6. Hlukhov V.S., and Trishch H.M. Otsinka strukturnoyi skladnosti bahatosektsiynykh pomnozhuvachiv elementiv poliv Halua [Structural Complexity of Multisection Galois Field Elements Multipliers Evaluation], (2014), *Komp'yuterni Systemy ta Merezhi". Visnyk Natsional'noho Universytetu "L'vivs'ka politekhnika"*, Lviv, Ukraine, Vol. 806, pp. 27 – 33 (In Ukrainian).

7. Sholohon O.Z. Obchyslennya strukturnoyi skladnosti pomnozhuvachiv u polinomial'nomu bazysi elementiv poliv Halua GF(2m) [Structural Complexity of Galois Field GF(2m) Elements Multipliers in Polynomial Basis Calculation]. *Komp'yuterni Systemy ta Merezhi". Visnyk Natsional'noho Universytetu "L'vivs'ka politekhnika",* Lviv, Ukraine, 2014, Vol. 806, pp. 284 – 289 (In Ukrainian).

8. Sholohon Yu.Z. Otsinyuvannya strukturnoyi skladnosti pomnozhuvachiv poliv Halua na osnovi elementarnykh peretvoryuvachiv [Based on Elementary Transducers Structural Complexity of Galois Field Multipliers Evaluation], (2014), *Komp'yuterni Systemy ta Merezhi". Visnyk Natsional'noho Universytetu "L'vivs'ka politekhnika",* Lviv, Ukraine, Vol. 806, pp. 290 – 295 (In Ukrainian).

9. Mel'nyk A.O. Pam"yat' iz vporyadkovanym dostupom [Tekst]: monohrafiya / [Orderly Access Memory], (2014), *Natsionalnu Universytet "L'vivs'ka Politekhnika" Vyd-vo L'vivska Politekhniky*, 294 p. ISBN 978-617-607-540-0 (In Ukrainian).

10. Hlukhova O.V., Lozyns'kyy A.Ya., Yaremkevych R.I., and Ihnatovych A.O. Analitychna otsinka strukturnoyi skladnosti pomnozhuvachiv elementiv poliv Halua [Galois Field Elements Multipliers Structural Complexity Analytical Evaluation], (2015), *Materialy V Vseukrayins'koyi Shkoly-seminaru Molodykh Vchenykh i Studentiv "Suchasni Komp'yuterni Informatsiyni Tekhnolohiyi" ASIT'2015,* Ternopil, Ukraine, *TNEU,* 2015, May 22-23, pp. 168 – 169.

Глухов
Валерій Сергійович,
д-р техн. наук, проф. каф.
Національного ун-ту «Львівська політехніка»,
м/т.: +38(063)75-72-330.
E-mail:
glukhov@polynet.lviv.ua

Еліас
Родріг Мітрі, канд. техн. наук,
доц. каф. Ліванського міжнародного университету
м/т.: 961.3.492949.
E-mail:
rodrigue.elias@liu.edu.lb