УДК 004.032.2

ОЦІНКА СТРУКТУРНОЇ СКЛАДНОСТІ МОДИФІКОВАНИХ ПОМНОЖУВАЛЬНИХ МАТРИЦЬ ДЛЯ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА $GF(2^m)$

Г. М. Тріщ

Національний університет «Львівська політехніка»
Україна, м. Львів
anya.trisch@gmail.com

Розглядається оцінка нового підходу до зменшення структурної складності багатосекційних помножувачів елементів двійкових полів Галуа $GF(2^m)$. Елементи полів представлено у нормальному базисі типу 2. Порядок поля сягає 998.

Ключові слова: структурна складність, поля Галуа, помножувальна матриця.

В даний час набули актуальності криптографічні методи захисту інформації на основі використання ПЛІС та криптографічних протоколів, побудованих на операціях множення в полях Галуа $GF(2^m)$.

Математичними основами цифрового підпису є еліптичні криві на основі полів Галуа $GF(2^m)$ з використанням гаусівського нормального базису типу 2. Апаратна складність помножувачів є такою, що їх можна реалізувати на сучасних ПЛІС. Але при великих значеннях порядку поля і кількості секцій реалізація на ПЛІС стає неможливою через високу структурну складність проекту (велику кількість внутрішніх зв'язків). Першу спробу оцінити структурну складність односекційного помножувача було зроблено у [1]. У [2] описана програма, яка визначала структурну складність невпорядкованих помножувальних матриць (НПМ) для полів Галуа з великим порядком. У [3] для зменшення структурної складності помножувача в цілому, запропоновано підхід, який полягає у заміні великої НПМ (розміром $m \times m$) на перемішувач та впорядковану модифіковану ПМ (ВПМ) меншого розміру. Структурна складність НПМ оцінюється як $O(m^2)$, де m – порядок поля Галуа. Структурну складність ВПМ можна оцінити як $O(k^2)$ [3], а очікуване скорочення структурної складності – як $(m/k)^2=N^2$, де k – розмір групи розрядів, що обробляються одночасно. Зменшення структурної та апаратної складності призведе до збільшення часової складності множення приблизно у $m/k = N$ разів [3].

Структурну складність помножувача [3] оцінено приблизно та теоретично. Тому для визначення можливості реалізації помножувача на ПЛІС постає задача більш точної її оцінки з врахуванням особливостей топології ПЛІС.

Метою роботи є оцінка структурної складності ВПМ помножувача елементів полів Галуа у нормальному базисі для вибору ВПМ з меншою структурною складністю для її імплементації в складі помножувача у сучасних ПЛІС.

Під час виконання даної роботи на основі запропонованої у [1] та [2] моделі помножувача було вдосконалено програму визначення структурної складності для ВПМ [3] та було проведено перевірку очікуваних теоретичних результатів. Різниця між використанням НПМ розміром ($m \times m$) (рис. 1, *а*) і ВПМ розміром ($k \times 2k$) полягає у тому, що операції, які раніше виконувалися у НПМ паралельно, після модифікації виконуються послідовно у ВПМ меншого розміру.

Декілька (p) ВПМ можна також використовувати паралельно (рис. 1, *б*). Цей підхід дає змогу спростити імплементацію та зменшити структурну складність помножувача (до складу якого входять додаткові вузли, які забезпечують роботу ВПМ – перемішувач, FIFO, вузол згортання). Результати подано на рис. 1, *в*, де за одиницю прийнято складність немодифікованого помножувача з p НПМ, для якого $k=m$.

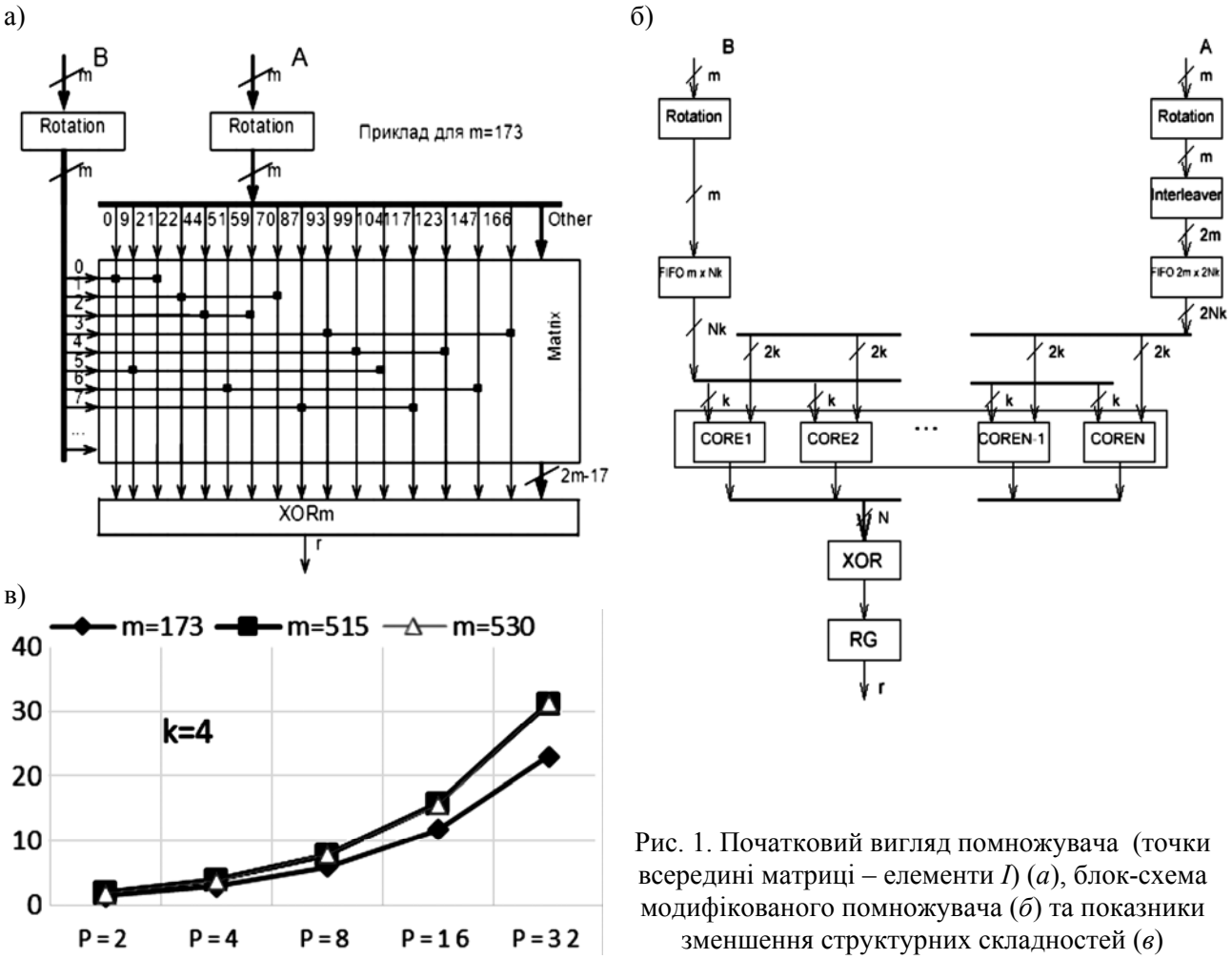

Рис. 1. Початковий вигляд помножувача (точки всередині матриці – елементи *I*) (*а*), блок-схема модифікованого помножувача (*б*) та показники зменшення структурних складностей (*в*)

Проведено уточнену оцінку зменшення структурної складності помножувача елементів полів Галуа $GF(2^m)$ при використанні ВПМ з різними кількостями розрядів k, що обробляються у ВПМ одночасно, кількостями самих ВПМ p, та різним порядком поля m. По відношенню до немодифікованого варіанту зменшення структурної складності може сягати десятків разів, наприклад, для m=530, k=4, p=32 структурна складність зменшується у 31,3 рази.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Hlukhov V., Hlukhova A. Galois field elements multipliers structural complexity evaluation // Proceedings of the 6th International Conference ACSN–2013.– Lviv, Ukraine.– 2013.– P. 18–19.

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

3. Глухов В. С., Еліас Р. М. Зменшення структурної складності багатосекційних помножувачів елементів полів Галуа // Електротехнічні та комп`ютерні системи.– 2015.– № 19 (95).– С. 222–226.

H. M. Trishch

Evaluation of the modified multiplier structural complexity matrixes for elements of Galois fields GF(2^m)

The evaluation of a new approach to reducing the structural complexity of multitapped multipliers of elements of Binary Galois field GF (2^m) is considered. Elements of fields are represented in the normal basis of type 2. The order of the field reaches 998.

Keywords: *structural complexity, Galois field, matrix multiplier.*