УДК 004.032.2

Г. М. Тріщ
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

ХАРАКТЕРИСТИКА СТРУКТУРНОЇ СКЛАДНОСТІ МОДИФІКОВАНИХ ПОМНОЖУВАЧІВ ПОЛІВ ГАЛУА

Розглядається новий підхід зменшення структурної складності багато секційних помножувачів елементів двійкових полів Галуа GF(2^m) та результати його оцінки. Елементи полів представлено у нормальному базисі типу 2. Порядок поля сягає 998.

Ключові слова: структурна складність – поля Галуа – помножувач.

CHARACTERISTICS GALOIS FIELDS STRUCTURAL COMPLEXITY MODIFIED MULTIPLIERS

The article describes the results of evaluation of structural complexity of multisection multipliers elements of Binary Galois field GF (2m) is considered and analysis of multipliers components relative complexity is performed. Elements of fields are represented in the normal basis of type 2. The order of the field <= 998. It is shown that the use of modified matrix multiplier allows to reduce the structural complexity approximately by 30 times.

Key words: structural complexity – Galois Field – Matrix Multiplier.

Вступ

На даний момент набули актуальності і широко використовується математичний апарат еліптичних кривих та криптографічні методи захисту інформації на основі використання ПЛІС та криптографічних протоколів, побудованих на операціях множення в полях Галуа GF(2^m).

Поля Галуа та еліптичні криві на основі полів Галуа GF(2^m) з використанням гаусівського нормального базису типу 2 є математичною основою для побудови пристроїв захисту інформації. Апаратна складність помножувачів є такою, що їх можна реалізувати на сучасних ПЛІС. Але при великих значеннях порядку двійкового поля і кількості помножувачів їхня реалізація на ПЛІС стає неможливою через високу структурну складність проекту (велику кількість внутрішніх зв'язків). Аналіз компонентів помножувальної матриці, яка є основою для побудови помножувачів, допоможе визначити залежності, які впливають на структурну складність помножувачів.

1. Огляд літературних джерел і окреслення проблеми

Перші спроби оцінити структурну складність односекційного помножувача було зроблено у [1]. У роботі [2] описана програма, яка допомагає визначити структурну складність невпорядкованих помножувальних матриць (НПМ) для полів Галуа з великим порядком. Був запропонований підхід [3] для зменшення структурної складності помножувача в цілому,

який полягає у заміні великої НПМ (розміром m x 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. Важливою є також структурна складність кожного компоненту окремо та їх відсоткове співвідношення [4, 5].

2. Мета роботи

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. Також метою є визначення відсоткового внеску компонентів помножувальних матриць у сумарне значення структурної складності.

3. Оцінювання структурної складності ВПМ

Аналіз моделі помножувача на основі запропонованого у роботах [1] та [2] методу дав можливість вдосконалити програму визначення структурної складності ВПМ [3] та здійснити перевірку очікуваних теоретичних результатів. Різниця між використанням НПМ розміром (m x m) (рис.1, 2) і ВПМ розміром (k x 2k) (рис.3) полягає у тому, що операції, які раніше виконувалися у НПМ паралельно після модифікації виконуються послідовно у ВПМ меншого розміру.

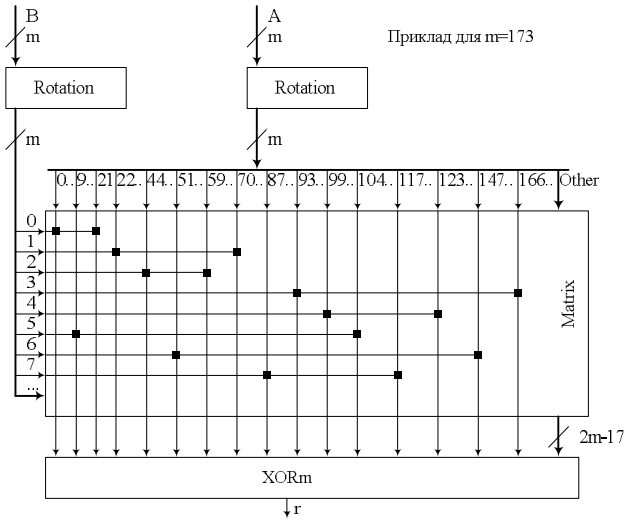

Рис. 1. Помножувач m x m (початковий вигляд, точки всередині матриці – елементи I)

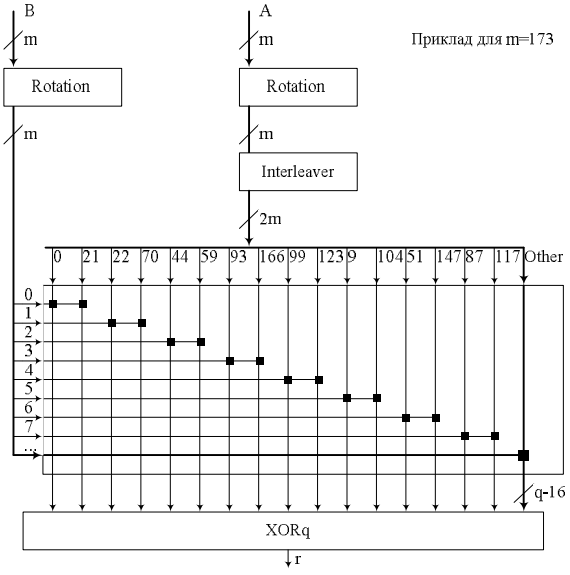

Рис. 2. Помножувач m x m з впорядкованою помножувальною матрицею

Декілька (p) ВПМ можна використовувати паралельно (рис.4). Використання впорядкованих помножувальних матриць дає змогу спростити імплементацію та зменшити структурну складність помножувача (до складу якого входять додаткові вузлів, які забезпечують роботу ВПМ – перемішувач, FIFO, вузол згортання).

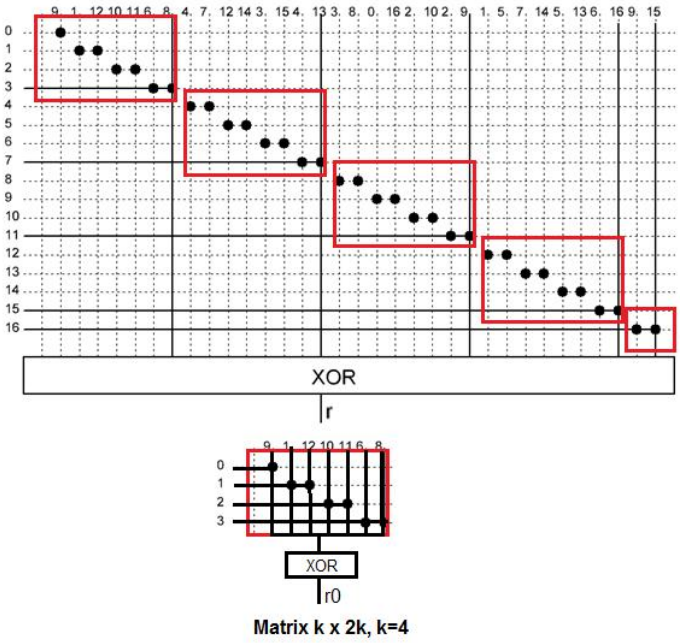

Рис. 3. ВПМ розміром (k x 2k)

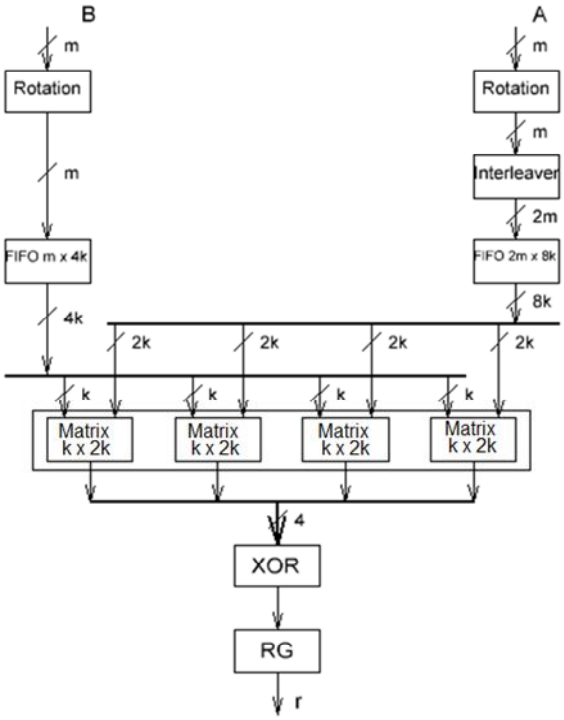

Рис. 4. Модифікований помножувач

Результати оцінювання структурної складності помножувача з ВПМ та порівняння його з помножувачем, який використовує немодифіковану матрицю подано в табл. 1. За одиницю в табл. 1 прийнято складність одного помножувача з p НПМ, яка дорівнює $S_{нр(p=1)}=p*(m*m)$, структурна складність помножувача з модифікованими матрицями $S_{врк}=(m/p)*(k*2k)*p$ + +(m*2m), де (m*m) – структурна складністьНПМ, (m*2m) – структурна складність перемішувача, (m/p)*(k*2k) – складність модифікованої ВПМ, а p – кількість модифікованих ВПМ, що працюють паралельно. На рис. 5 наведено графічні зображення результатів оцінювання структурної складності при даному підході.

Таблиця 1

Показники зменшення структурних складностей

m = 173					m = 515				
p	k	$S_{нр}$	$S_{врк}$	$S_{нр}/S_{врк}$	p	k	$S_{нр}$	$S_{врк}$	$S_{нр}/S_{врк}$
2	4	94254	63297	1.49	2	4	1062788	540387	1.97
4	4	188508	63449	2.97	4	4	2125576	540539	3.93
8	4	377016	63753	5.91	8	4	4251152	540843	7.86
16	4	754032	64361	11.72	16	4	8502304	541451	15.70
32	4	1508064	65577	23.00	32	4	17004608	542667	31.34
2	8	94254	66473	1.42	2	8	1062788	549035	1.94
4	8	188508	67033	2.81	4	8	2125576	549595	3.87
8	8	377016	68153	5.53	8	8	4251152	550715	7.72
16	8	754032	70393	10.71	16	8	8502304	552955	15.38
32	8	1508064	74873	20.14	32	8	17004608	557435	30.51
2	16	94254	73593	1.28	2	16	1062788	567099	1.87

Продовження табл. 1

m = 173					m = 515				
p	k	$S_{нр}$	$S_{врк}$	$S_{нр}/S_{врк}$	p	k	$S_{нр}$	$S_{врк}$	$S_{нр}/S_{врк}$
4	16	188508	75737	2.49	4	16	2125576	569243	3.73
8	16	377016	80025	4.71	8	16	4251152	573531	7.41
16	16	754032	88601	8.51	16	16	8502304	582107	14.61
32	16	1508064	105753	14.26	32	16	17004608	599259	28.38
m = 530					m = 998				
p	k	$S_{нр}$	$S_{врк}$	$S_{нр}/S_{врк}$	p	k	$S_{нр}$	$S_{врк}$	$S_{нр}/S_{врк}$
2	4	1123544	572022	1.96	2	4	1123544	2011122	0.558665262
4	4	2247088	572174	3.93	4	4	2247088	2011274	1.117246084
8	4	4494176	572478	7.85	8	4	4494176	2011578	2.23415448
16	4	8988352	573086	15.68	16	4	8988352	2012186	4.46695882
32	4	17976704	574302	31.30	32	4	17976704	2013402	8.928521974
2	8	1123544	580910	1.93	2	8	1123544	2027498	0.554152951
4	8	2247088	581470	3.86	4	8	2247088	2028058	1.10799987
8	8	4494176	582590	7.71	8	8	4494176	2029178	2.214776624
16	8	8988352	584830	15.37	16	8	8988352	2031418	4.424668877
32	8	17976704	589310	30.50	32	8	17976704	2035898	8.829864757
2	16	1123544	599454	1.87	2	16	1123544	2061018	0.545140314
4	16	2247088	601598	3.74	4	16	2247088	2063162	1.089147629
8	16	4494176	605886	7.42	8	16	4494176	2067450	2.173777359
16	16	8988352	614462	14.63	16	16	8988352	2076026	4.329595101
32	16	17976704	631614	28.46	32	16	17976704	2093178	8.588234732

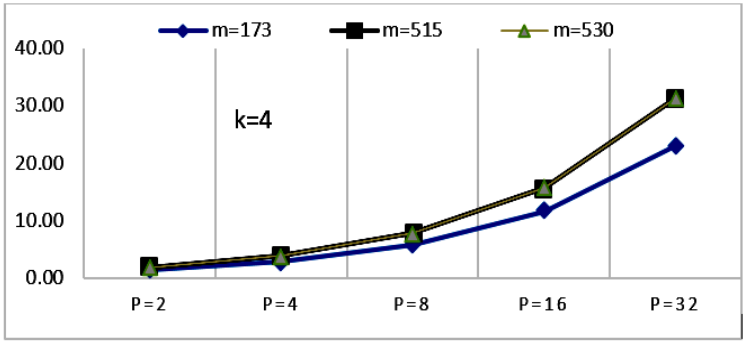

Рис. 5. Показники зменшення структурних складностей

Відношення між структурною складністю ВПМ та перемішувача між собою до загальної структурної складності подано в табл.2 та на рис.6 та рис. 7. На рис.6. подано відсоткове значення складності ВПМ в залежності від кількості ВПМ, що працюють паралельно (p), на рис.7. – відношення складностей перемішувача в залежності від кількості ВПМ, що працюють паралельно (p).

Таблиця 2

Відсоткове співвідношення структурної складності компонентів

m	p	k = 4		k = 8		k =16	
		Перемі-шувач, %	ВПМ p*(k*2k), %	Перемі-шувач, %	ВПМ p*(k*2k), %	Перемі-шувач, %	ВПМ p*(k*2k), %
173	2	90.10	9.90	83.17	16.83	72.08	27.92
173	4	81.99	18.01	71.19	28.81	56.35	43.65
173	8	69.48	30.52	55.27	44.73	39.23	60.77
173	16	53.23	46.77	38.19	61.81	24.40	75.60
173	32	36.27	63.73	23.60	76.40	13.90	86.10
515	2	96.44	3.56	93.64	6.36	88.49	11.51
515	4	93.13	6.87	88.03	11.97	79.35	20.65
515	8	87.14	12.86	78.63	21.37	65.77	34.23
515	16	77.21	22.79	64.78	35.22	49.00	51.00
515	32	62.88	37.12	47.91	52.09	32.45	67.55
530	2	96.54	3.46	93.81	6.19	88.78	11.22
530	4	93.31	6.69	88.33	11.67	79.82	20.18
530	8	87.46	12.54	79.10	20.90	66.42	33.58
530	16	77.71	22.29	65.43	34.57	49.72	50.28
530	32	63.55	36.45	48.62	51.38	33.08	66.92

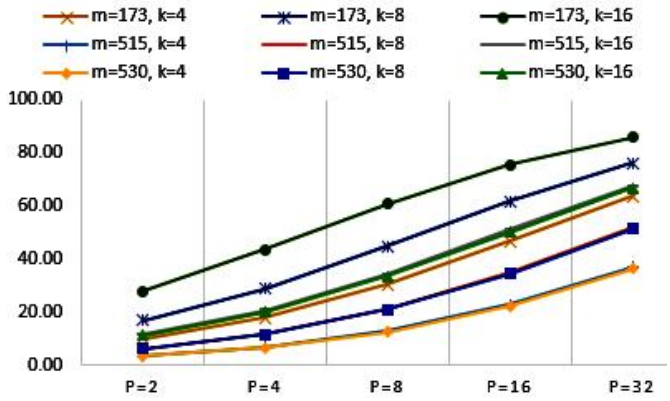

Рис. 6. Відносна складність ВПМ в залежності від кількості (p)

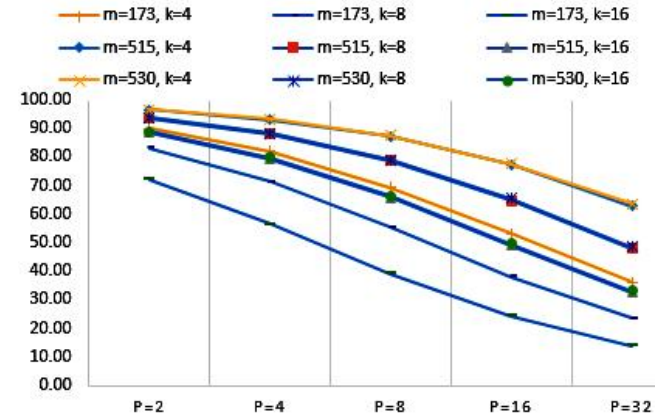

Рис. 7. Відносна складність перемішувача в залежності від кількості (p)

Як бачимо, при малій кількості (p) ВПМ, загальна структурна складність в основному складається зі структурної складності перемішувача (близько 90%). При великій кількості (p) ВПМ видно, що більшу частину структурної складності складає складність безпосередньо самих ВПМ.

Висновки

Проведено уточнену оцінку зменшення структурної складності помножувача елементів полів Галуа GF(2^m) при використанні впорядкованих помножувальних матриць (ВПМ) з різними кількостями розрядів k, що обробляються у ВПМ одночасно, різними кількостями самих ВПМ p, та різним порядком поля m. Відносно немодифікованого варіанту зменшення структурної складності може сягати десятків разів, наприклад, для m=530, k=4, p=32 структурна складність зменшується у 31.3 рази. Проведено аналіз впливу компонентів модифікованої матриці на структурну складність. Результати показали, що при малій кількості (p<32) ВПМ 90% структурної складності припадає на перемішувач, а при великій кількості (p≥32) ВПМ вплив (відсоток) структурної складності перемішувача зменшується до 20-30 %.

1. Глухов В. С., Глухова О. В. Результати оцінювання структурної складності помножувачів елементів полів Галуа [Текст] / В. С. Глухов, О. В. Глухова // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – Львів: – 2013. – Вип. 773. – С. 27 – 32.2. Глухов В. С., Тріщ Г. М. Оцінка структурної складності багатосекційних помножувачів елементів полів Галуа [Текст] / В. С. Глухов, Г. М. Тріщ // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – Львів: – 2014. – Вип. 806. – С. 27 – 33.3. Глухов В.С., Элиас Р. Уменьшение структурной сложности многосекционных умножителей элементов полей Галуа. / В.С.Глухов, Р.Элиас // Электротехнические и компьютерные системы. – 2015. – № 19(95) – С. 222-226. 4. Г. М. Тріщ. Оцінка структурної складності модифікованих помножувальних матриць для елементів полів Галуа GF(2^m) // Матеріали XVII-ої Міжнародної науково-практичної конференції. "Сучасні інформаційні та електронні технології". Одеса: – 2016. 5. Тріщ Г. М. Структурна складність модифікованих помножувальних матриць для елементів полів Галуа GF(2^m)[Текст] / Г. М. Тріщ // Матеріали V міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем". – Видавництво "Львівської політехніки", Львів: – 2016. – С. 80 – 81.

Наукові результати, подані у цій статті, було отримано в рамках дослідницького проекту ДБ/КІБЕР з реєстраційним номером 0115U000446, 01.01.2015 – 31.12.2017, фінансово підтриманим Міністерством освіти та науки України.