УДК 638.322

В.П. ТАРАСЕНКО[1], О.К. ТЕСЛЕНКО[1], А.І. РОГОВЕНКО[2]

[1]Національний технічний університет України «КПІ», Україна
[2] Чернігівський державний технологічний університет, Україна

ОПТИМІЗАЦІЯ АПАРАТНИХ ВИТРАТ НА РЕАЛІЗАЦІЮ ПАРАМЕТРИЧНИХ ЯДЕР (SOFT-CORES) ДЛЯ ВИКОНАННЯ ОПЕРАЦІЙ В СКІНЧЕНИХ ПОЛЯХ

На основі аналізу раніш розроблених апаратних методів виконання операцій в скінчених полях на одновимірному каскаді конструктивних модулів пропонується підхід до мінімізації апаратних ресурсів при реалізації таких операцій на ПЛІС із використанням мови VHDL. Розглянуті структурні методи оптимізації витрат при побудові суматорів по змінному модулю на оптимізованих одновимірних каскадах конструктивних модулів (ОККМ). Експериментальні дані свідчать, що параметричні ядра для операції додавання по змінному модулю ОККМ потребують меншої кількості апаратних ресурсів.

Ключові слова: *скінчені поля, одновимірний каскад однотипних конструктивних модулів, VHDL, ПЛІС, суматор за змінним модулем.*

Вступ

Дедалі частіше для забезпечення гарантоздатності та інформаційної стійкості комп'ютерних систем використовуються операції в скінчених полях. Своє конкретне застосування вони знаходять, наприклад, в криптографічних перетвореннях для захисту від негативних антропогенних впливів, в практиці кодування з метою виявлення та виправлення помилок [1,2] та ін. Технологія ПЛІС, завдяки своєму швидкому розвитку, дає можливість створити гнучкі структури спеціалізованих процесорів для операцій в скінчених полях. Одним з напрямків апаратної реалізації операцій в скінчених полях, що націлений на скорочення апаратних витрат, є використання одновимірних каскадів конструктивних модулів (ОККМ). У роботі [3] обґрунтовано можливість та визначені характеристики реалізації ОККМ будь-якого порядку. У роботі [4] запропонований один з варіантів реалізації ОККМ на основі оптимізованих рішень (softcores) на мові VHDL. Softcores виконують операції додавання та віднімання за модулем і мають параметричний характер, коли користувач шляхом задання відповідних параметрів (наприклад, розрядності даних) визначає конкретну реалізацію. Також були показані можливості мінімізації апаратних витрат за допомогою підбору параметрів кодування класів еквівалентності.

В даній роботі розглянемо структурні методи оптимізації витрат при побудові суматорів по змінному модулю на ОККМ.

1. Основні положення

Аналіз класів еквівалентності, перелічених в [4], показує, що на лівих бокових виходах останнього конструктивного модуля каскаду реалізується функція

$$V_{n-1}(X,Y,P)=\begin{cases} a & \text{при } X+Y<P, \\ b & \text{при } P\le X+Y<2^n, \\ c & \text{при } 2^n\le X+Y<2^n+P, \\ d & \text{при } 2^n+P\le X+Y. \end{cases} \quad (1)$$

На правих бокових виходах першого конструктивного модуля каскаду реалізується функція

$$U_0(X,Y,P)=\begin{cases} k & \text{при } X+Y<P-1, \\ h & \text{при } X+Y=P-1, \\ e & \text{при } X+Y=P, \\ g & \text{при } X+Y>P. \end{cases} \quad (2)$$

В загальному випадку при будь-яких значеннях X,Y та P, на первинних виходах модулів ОККМ буде реалізовуватись основна функція.

Обчислення основної функції може виконуватись з використанням операції віднімання або без такого. Щоб позначити ці два випадки введемо функцію SUB: $SUB_i = 0$, коли віднімання відсутнє, та $SUB_i = 1$ (i = 0,1,…,n-1, n – кількість розрядів суматора), коли віднімання виконується. Позначимо також стани конструктивного модуля, що відповідають різним умовам, за яких віднімання або буде відсутнім, або буде обов'язковим, або буде залежати від сигналів позики та переносу із сусідніх конструктивних модулів:

– Стан 1: $U_{i+1} = h$. У цьому випадку віднімання буде відсутнім незалежно від значень молодших розрядів;

– Стан 2: $U_{i+1} = g$. Віднімання буде в наявності незалежно від значень молодших розрядів;

– Стан 3: $U_{i+1} = k$. У цьому випадку має місце рівність $X_{i+1,n-1}+Y_{i+1,n-1} = P_{i+1,n-1} - 1$. Тобто віднімання можливе, якщо в і-му модулі буде реалізовано перенос при додаванні з відніманням, що відповідає класу d (табл. 1);

– Стан 4: $U_{i+1} = e$. Має місце рівність $X_{i+1,n-1}+Y_{i+1,n-1} = P_{i+1,n-1}$. В цьому випадку віднімання неможливе, якщо в і-му модулі буде реалізовано позику при додаванні з відніманням, що відповідає класу *a* (табл. 1).

Таблиця 1

Визначення функції V_i.

V_{i-1}	v_i							
a	*a*	*b*	*b*	*c*	*a*	*a*	*a*	*c*
b	*b*	*b*	*b*	*d*	*a*	*b*	*b*	*c*
c	*b*	*c*	*c*	*d*	*a*	*c*	*c*	*c*
d	*b*	*d*	*d*	*d*	*b*	*c*	*c*	*d*
x_i	0	1	0	1	0	1	0	1
y_i	0	0	1	1	0	0	1	1
p_i	0	0	0	0	1	1	1	1

Визначені вище стани дозволяють побудувати функцію SUB_i (табл. 2).

Відповідно до табл. 2 обчислення основної функції зводиться до реалізації простого логічного виразу:

$$W_i = \overline{sub} \wedge \left[x_i \oplus y_i \oplus \left((V_{i-1} = c) \vee (V_{i-1} = d) \right) \right] \vee$$
$$\vee\, sub \wedge \left[x_i \oplus y_i \oplus p_i \oplus \left((V_{i-1} = a) \vee (V_{i-1} = d) \right) \right]$$

Таким чином, раніш відома [4] структура конструктивного модуля (КМ) спрощується за рахунок зменшення числа операцій для обчислення основної функції. Натомість, додатково до складу КМ вносяться засоби для обчислення функції SUB. Ці обчислення виконуються за алгоритмом, подібним до обчислення сигналів переносу, тому ускладнення КМ буде не значним. Структура ОККМ, побудованого відповідно до наведених вище положень, показана на рис. 1.

Зауважимо, що суматор на рис.1 має затримку сигналу, пропорційну n+1 , тоді як суматори в [4] мають затримку, пропорційну n.

З аналізу роботи КМ видно, що при об'єднанні КМ в ОККМ можна генерувати сигнали позики та обчислювати функцію SUB тільки у крайніх модулях для старших розрядів, а в модулі для молодших розрядів тільки транслювати. При цьому КМ для старших розрядів (КМ першого типу) будуть мати структуру згідно з рис.1, а модулі для молодших розрядів (КМ другого типу) будуть мати структуру згідно з рис. 2.

Таблиця 2

Визначення функції SUB_i

V_{i-1}	U_{i+1}															
	h	k	e	g	h	k	e	g	h	k	e	g	h	k	e	g
a	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	1
b	0	0	1	1	0	0	1	1	0	1	1	1	0	0	0	1
c	0	0	1	1	0	0	1	1	0	1	1	1	0	0	0	1
d	0	1	1	1	0	1	1	1	0	1	1	1	0	0	1	1
x_i	1				0				1				0			
y_i	0				1				1				0			
p_i	0				0				0				1			
a	0	0	0	1	0	0	0	1	0	0	0	1	0	0	1	1
b	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
c	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
d	0	0	1	1	0	0	1	1	0	0	1	1	0	1	1	1
x_i	0				1				0				1			
y_i	0				0				1				1			
p_i	0				1				1				1			

КМ другого типу, через спрощення за рахунок виключення блоку генерації сигналів U, істотно зменшують апаратні витрати на реалізацію суматора на ОККМ в цілому (рис. 3.). Дійсно, нехай m – номер розряду, починаючи з якого використовуються КМ першого типу, а для розрядів від 0 до m-1 використовуються КМ другого типу (рис. 2). Нехай C1 – складність КМ першого типу, C2 – другого типу. Приймемо $C2 \approx (2/3)C1$. Тоді складність ОККМ

$$C_{оккм} \approx C1_{(n-(1/3)m)}.$$

Необхідно особливо відмітити випадок m=n, коли сигнал SUB відповідає значенню $V_{n-1}(X,Y,P) = a$, що реалізується на лівих бокових виходах останнього КМ каскаду (1), а затрати на реалізацію суматора приблизно на третину менші ніж для суматора на рис. 1. В цьому випадку, нарощування розрядності суматорів можливе тільки в сторону молодших розрядів, що при апаратній реалізації на ПЛІС абсолютно не критично й не накладає ніяких обмежень при реалізації параметричних модулів на мовах опису апаратури (VHDL, Verilog)

Поряд з перевагою таких структур (рис. 3) суматорів по змінному модулю по апаратних затратах є і недоліки, які полягають в порушені регулярності структури та зменшення швидкості за рахунок зворотного проходження сигналу SUB після проходження сигналів V та U до КМ першого

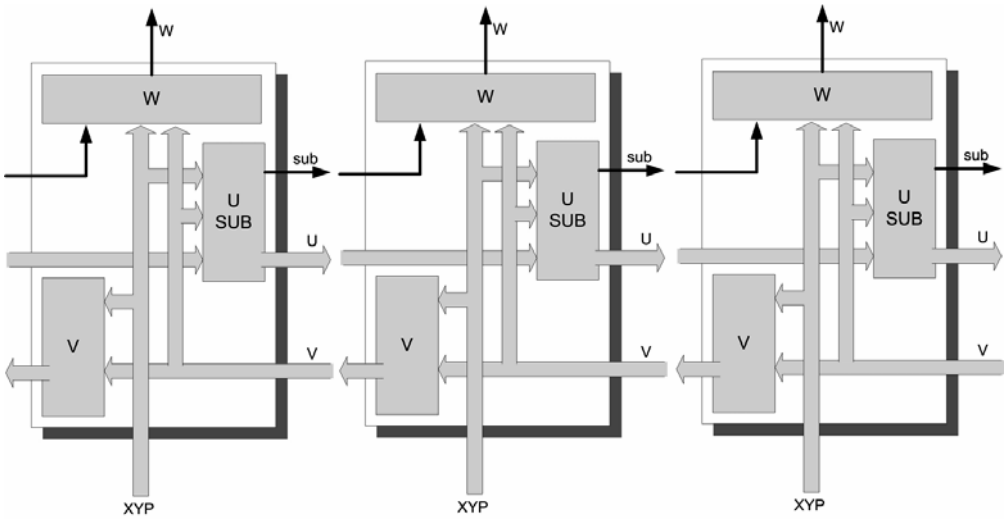

Рис. 1. Структура ОККМ на основі КМ з додатковими лініями SUB.

типу. Нехай, далі, t_1 – затримка сигналів V в КМ обох типів та сигналів U в КМ першого типу, t_2 – затримка сигналу SUB в КМ другого типу, $t_1 > t_2$. Затримка сигналу в сторону старших розрядів – $t_{hight} = nt_1$, затримка сигналу в сторону молодших розрядів $t_{low} = t_1 * max_{(m,n-m)} + mt_2$. Затримка виконання операції - $\approx \max(t_{low}, t_{hight})$. При m=n маємо $t_{low} = nt_1 + nt_2$, що вказує на зменшення швидкості виконання операції порівнюючи з суматором на рис.1 та суматорами, які розглядались в [4]. Але доданок nt_2 (відповідно mt_2) відображає найгірший випадок. Оскільки сигнал SUB в КМ другого типу лише використовується, а не формується, то він може подаватись одночасно на декілька лінійок КМ другого типу по архітектурі «гребінець», що дозволяє вважати $t_{low} \approx t_{hight}$.

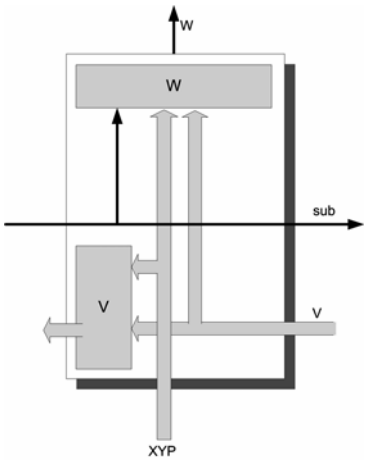

Рис. 2. Структура КМ першого типу для нерегулярного ОККМ.

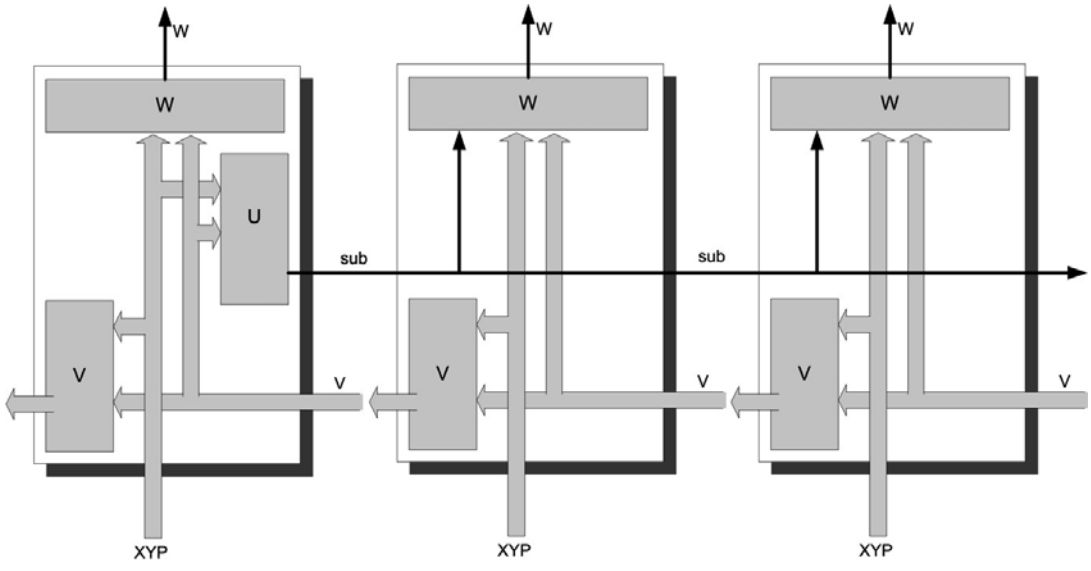

Рис. 3. ОККМ з нерегулярною структурою.

2. Експериментальна частина

У відповідності до запропонованих структур суматорів за змінним модулем було реалізовані параметричні ядра (softcores) на мові VHDL, та проведена кількісна оцінка апаратних затрат. Порівнювалися VHDL реалізації наведених вище структур, та реалізації, які розглядались в [4]. Серія експериментів передбачала проходження операції синтезу та імплементації VHDL рішення у САПР Xilinx ISE 10.1 з оптимізацією по затратах, і з подальшим визначенням кількості необхідних апаратних ресурсів. За основу для реалізації був взята ПЛІС серії Spartan 3E, XC3S500E, у складі засобу проектування та розробки Spartan 3E Starter kit, фірми-виробника Xilinx. Результати експерименту наведені у вигляді графіка залежності кількості slices [4] від розрядності суматора.

Друга серія експериментів проводилася з метою визначення часових характеристик, та ступеню впливу на їх якості структури ОККМ. Перша частина експерименту проводилася аналогічно до попереднього. У другій частині проводилося моделювання на часовому рівні VHDL реалізації кожної з структур при заданих значеннях розрядності. Результати експерименту наведені у табл. 3, у якій показана залежність часової затримки між подачею на інформаційні входи операндів X, Y та P, , та появою дійсного результату обчислення функції (X+Y) mod P на всіх розрядах виходу W.

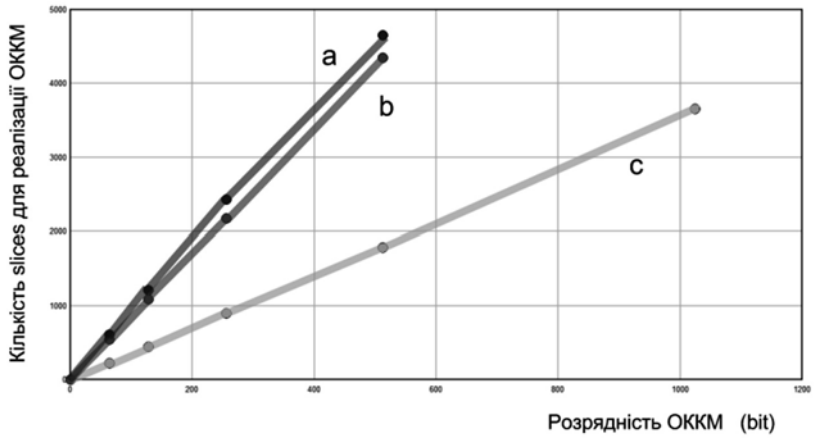

Рис. 4. Графік залежності кількості slices від розрядності ОККМ: a – не оптимізована структура ОККМ; b – оптимізована регулярна структура ОККМ; c – оптимізована нерегулярна структура ОККМ.

Таблиця 3

Часова затримка між подачею операндів на входи ОККМ, та появою дійсного результату на виході

Розрядність ОККМ (bit)	Часова затримка(нс)		
	Оптимізована не регулярна	Оптимізована регулярна	Не оптимізована
4	18.5	13.1	17.5
8	28.6	22	26,8
16	45.3	43.6	43.8
32	86	76.6	81.3
64	165.1	154.2	156.3
128	321.7	285	306.2
256	627.4	565.4	606.1
512	1300	1138	1278
1024	2059	-	-

Висновки

Таким чином, експериментальні дані свідчать, що параметричні ядра для операції додавання по змінному модулю на оптимізованих ОККМ потребують меншої кількість апаратних ресурсів, особливо в випадку ОККМ з нерегулярною структурою (рис. 4), що підтверджує наведені теоретичні результати. Результати моделювання за допомогою САПР затримок між подачею на інформаційні входи операндів та появою результату на виході основної функції, наведені в табл. 3, також підтверджують теоретичні розрахунки. Особливу увагу на використання параметричних ядер на базі оптимізованих ОККМ слід звернути при проведенні обчислень над операндами великої розрядності (від 256 біт), що має велике практичне значення в сучасних криптографічних перетвореннях.

В подальшому необхідно провести вимірювання затрат часу на виконання операцій при безпосередньому фізичному моделюванні в ПЛІС.

Література

1. Харченко В.С. Гарантоздатність комп'ютерних систем: проблеми і результати / В.С. Харченко // Авиационно-космическая техника и технология. – 2005. – № 7 (23). – С. 352-376.

2. Методологічні та термінологічні аспекти інформаційної стійкості освітніх комп'ютерних технологій та мереж / В.П. Тарасенко, А.Ю. Михайлюк, О.К. Тесленко, О.С. Осипов // Радіоелектронні та комп'ютерні системи, 2006. – № 7. – С. 12-17

3. Тарасенко В.П. Реалізація операцій в скінчених полях на одновимірному каскаді конструктивних модулів / В.П. Тарасенко, О.К. Тесленко // Системні дослідження та інформаційні технології. – 2006. – № 2. – С. 56-62.

4. Тарасенко В.П. Створення параметричних ядер (softcores) для виконання операцій в скінчених полях. / В.П. Тарасенко, О.К. Тесленко, А.І. Роговенко // Радіоелектронні і комп'ютерні системи. – 2008. – № 6. – С. 261-264.

Надійшла в редакцію 3.02.2009

Рецензент: д-р техн. наук, проф., завідувач кафедри комп'ютерних систем та мереж В.С. Харченко, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків, Україна.

ОПТИМИЗАЦИЯ АППАРАТНІХ ЗАТРАТ НА РЕАЛИЗАЦИЮ ПАРАМЕТРИЧЕСКИХ ЯДЕР (SOFT-CORES) ДЛЯ ВЫПОЛНЕНИЯ ОПЕРАЦИЙ В КОНЕЧНЫХ ПОЛЯХ

В.П. Тарасенко, А.К. Тесленко, А.И. Роговенко

На основе анализа ранее разработанных аппаратных методов выполнения операций в конечных поля на одномерном каскаде конструктивных модулей предлагается подход по минимизации аппаратных ресурсов при реализации таких операций на ПЛИС с применением языка VHDL. Рассмотрены структурные методы оптимизации расходов при построении сумматоров по переменному модулю на оптимизированных одномерных каскадах конструктивных модулей (ОККМ). Экспериментальные данные свидетельствуют, что параметрические ядра для операции добавления по переменному модулю ОККМ нуждаются в более малом количестве аппаратных ресурсов.

Ключевые слова: конечные поля, одномерный каскад однотипних конструктивних модулей, VHDL, ПЛИС, сумматор по переменному модулю.

OPTIMIZATION OF HARDWARE EXPENSES FOR IMPLEMENTATION OF FINITE FIELD'S CALCULATIONS SOFT-CORES

V.P. Tarasenko, A.K. Teslenko, A.I. Rogovenko

The approach for minimization hardware resources for implementation finite field's calculations in FPGA using VHDL is offered. This approach is based on earlier developed hardware methods for finite field's calculations on one-dimension cascade of constructive units. The structural methods of optimization of charges are considered at the construction of summarizings on the variable module on the optimized one-dimensional cascades of the structural modules (OCSM). Experimental information testify that parametric kernels for the operation of addition on the variable module of OCSM need more a few of resources of vehicles.

Keywords: finite fields, one-dimension cascade of constructive units, VHDL, PLD, adder with variable module.

Тарасенко Володимр Петрович – д-р техн. наук, проф., зав. кафедрою спеціалізованих комп'ютерних систем, Національний технічний університет України «КПІ», Київ, Україна, e-mail: vtarasen@scs.ntu-kpi.kiev.ua.

Тесленко Олександр Кирилович – канд. техн. наук, пров. наук. співр., доц. кафедри спеціалізованих комп'ютерних систем, Національний технічний університет України «КПІ», Київ, Україна, e-mail: teslenko@scs.ntu-kpi.kiev.ua.

Роговенко Андрій Іванович – аспірант, ст. викл. кафедри інформаційних та комп'ютерних систем, Чернігівський державний технологічний університет, Чернігів, Україна, e-mail: arogovenko@gmail.com.