УДК 638.322

К.т.н, доцент Тесленко О. К., магістрант Волік А.С.

**Національний технічний університет України
«Київський політехнічний інститут»**

ОПТИМІЗАЦІЯ АПАРАТНИХ ВИТРАТ НА РЕАЛІЗАЦІЮ СУМАТОРА ПО ЗМІННОМУ МОДУЛЮ НА ПЛІС

Abstract

Olexandr Teslenko, assoc. prof., PhD; Anton Volik, student

Optimization of hardware expenses for implementation of adders with variable module in FPGA

This paper concerns the idea for minimization hardware resources for implementation of adder with the variable module in FPGA using VHDL. Optimal coding of signals method of optimization are considered at the construction of adders with the variable module on the optimized one-dimensional cascades of the structural modules (OCSM). Experimental information testify that there are some variants of coding signals, which minimize hardware resources.

Вступ

В сучасній комп’ютерній криптографії в алгоритмах цифрового підпису [1], обчислення хеш-функцій [2], а також для реалізації ряду криптографічних протоколів [3] та криптографічних перетворень (наприклад, в алгоритмі RSA) застосовуються операції в залишках чисел великої розрядності.

Широке застосування модулярних операцій (операцій в залишках) у засобах захисту інформації з одного боку і розвиток технології ПЛІС з іншого, актуалізують пошук ефективних апаратних реалізацій. Однією з базових операцій у залишках є операція додавання $(X+Y) \bmod P$, де X, Y і P цілі невід'ємні числа, $X, Y < P$. З урахуванням систем команд універсальних ЕОМ обчислення додавання в залишках виконується шляхом застосування наступних трьох операцій (додавання, порівняння та віднімання). Спочатку виконується операція додавання $S = X + Y$, потім результат порівнює з числом P, якщо $S \geq P$, то виконується операція віднімання $S - P$. Однак у випадку створення спеціалізованих обчислювальних пристроїв для криптографічних перетворень, наприклад, на основі ПЛІС, використовувати таку реалізацію не завжди доцільно.

В [4] запропонована реалізація операції додавання по змінному модулю на підставі логічної мережі регулярної лінійної структури - одновимірному каскаді однотипних конструктивних модулів (ОКОКМ), де конструктивні модулі (КМ) і каскад в цілому є комбінаційними схемами. На нижні (первинні) входи КМ подаються і-ті розряди чисел *X*, *Y* і *P*, на верхньому (первинному) виході КМ реалізується і-тий розряд результату. Бічні входи і виходи служать для поширення сигналів переносу як у бік старших так і в бік молодших розрядів. У КМ реалізується одна булева функція від 7 змінних для формування розряду результату і 4 булеві функції від 5 змінних для формування сигналів перенесення - по дві для кожного з напрямків - у бік молодших і у бік старших розрядів.

Шляхом з'єднання КМ створюється ОКОКМ, який реалізує перетворення *F (X, Y, P)* будь-якої необхідної розрядності вихідних чисел:

$$F(X,Y,P) = X + Y \text{ если } X + Y < P,$$

$$F(X,Y,P) = X + Y - P \text{ если } X + Y \geq P.$$

Якщо X, Y <P, то такий ОКОКМ реалізує операцію (X+Y) mod P.

За рахунок одночасного розповсюдження сигналів переносу як в сторону молодших так і в сторону старших розрядів досягається суттєве збільшення швидкості виконання операції.

Постановка задачі

В [4] не визначалися конкретні кодування сигналів переносу у бік старших та молодших розрядів. Можливо 576 варіантів кодування. В зв’язку з цим виникає наступна задача – визначити, чи існує залежність витрат функціональних комірок (*слайсів*) ПЛІС на реалізацію суматора від вибраного кодування і який діапазон можливих значень такої залежності та визачення кодувань, оптимальних по витратах.

САПР ПЛІС, наприклад САПР Xilinx ISE WebPack 9.2, мають режими оптимізації проектів по кількості *слайсів* та зазначають цю кількість у файлі статистики. Почергове виконання проектів «вручну» для всіх варіантів кодувань та різних ПЛІС має значні трудовитрати і не застраховане від помилок, тобто має низьку достовірність. Тому метою даної роботи є забезпечення достовірності результатів визначення оцінок апаратних витрат при реалізації на ПЛІС суматорів в залишках, шляхом створення методики і програми для автоматичного аналізу вказаних оцінок витрат при всіх варіантах кодування сигналів переносу суматора в залишках та різних ПЛІС.

Термінологія

Слайс – деяка кількість комірок в ПЛІС, що мають спільні мультиплексори.

Розв'язок задачі

Для реалізації поставленої задачі на мові VHDL було створено параметричну модель суматора в залишках на ОКОКМ, в якій в якості параметрів задано розрядність суматора та кодування сигналів перенесення. Базуючись на вказаній параметричній моделі було створено методику реалізації інтегрованого середовища, яка полягає в автоматичному виконанні на комп'ютері наступних дій:

1) Автоматичне редагування параметричної моделі на чергові значення кодувань сигналів переносу.
2) Автоматичний запуск САПР Xilinx ISE WebPack 9.2 з вибором типу ПЛІС.
3) Автоматичний запуск програми імплементації відредагованої параметричної моделі в ПЛІС вибраного типу.
4) Автоматичне зчитування з файлу статистик кількісних (в *слайсах*) результатів імплементації та розміщення їх в файлі результату.
5) Аналіз файлу результату для визначення рівня розбіжності (мінімальне та максимальне значення кількості *слайсів*) та перелік кодувань сигналів переносу для мінімальних значень по кожному типу ПЛІС.

Інтегроване середовище було створено на базі Visual C++. Під час тестування розробленого середовища виникали деякі проблеми, зокрема із запуском САПР Xilinx ISE WebPack 9.2. Іноді з невідомих причин (без відповідної діагностики) руйнувався проект для Xilinx ISE WebPack 9.2 і тоді потрібно було відновлювати його і перезапускати все спочатку. Це відбувається через ще не виправленні помилки в програмному забезпеченні САПР.

Експериментальна частина

Після запуску розробленої системи для моделі ОКОКМ із різною кількістю конструктивних модулів для декількох ПЛІС були отримані наступні результати.

Кількість *слайсів*, які займає модель ОКОКМ на ПЛІС дійсно залежить від кодування, причому якщо збільшувати кількість конструктивних модулів в ОКОКМ, то кількість *слайсів* зростає пропорційно.

Було отримано декілька варіантів кодування з мінімальною кількістю *слайсів*, тобто були знайдені оптимальні комбінації кодування.

Для ПЛІС від різних компаній-виробників, у яких однакова кількість входів у таблицях переходів, результат був однаковий. Та якщо кількість входів у таблицях переходів збільшується, то кількість *слайсів*, яку займає модель ОКОКМ – зменшується.

Таблиця 1

Результати для деяких ПЛІС

Найменування ПЛІС		Кількість слайсів	Приклад кодування							
			a	b	c	d	h	k	e	g
Spartan 3AN (64 модулі)	Min	439	10	00	01	11	01	00	10	11
	Max	690	01	10	00	11	11	01	10	00
Spartan 3AN (4 модулі)	Min	19	10	00	01	11	01	00	10	11
	Max	30	01	10	00	11	11	01	10	00
Virtex5 (4 модулі)	Min	14	01	00	10	11	11	10	00	01
	Max	28	01	10	11	00	10	01	11	00

Висновок

Використання розробленої системи показує, що оптимальні реалізації суматорів за змінним модулем залежать від кодування та конкретних ПЛІС. В ході експерименту були знайдені оптимальні кодування.

У подальшому планується розробка конкретних схем на базі одержаних результатів та аналіз їх оптимальності.

Література

1. ГОСТ Р 34.10-94 Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма. Издательство стандартов. М. 1994
2. ISO/IEC 10118 Информационные технологии-Технологии безопасности-Хеш функции, 1994
3. *Диффи У., Хэлмэн М.* Защищенность и имитостойкость. Введение в криптографию.ТИИЭР, том 67, №3, 1979.
4. *Тарасенко В.П., Тесленко О.К.* Реалізація основних арифметичних операцій над залишками на одномірних каскадах конструктивних модулів. Управляющие системы и машины, 2003, № 3(185), С.29-42.