НОВІ ЗАСОБИ
КІБЕРНЕТИКИ, ІНФОРМАТИКИ,
ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ
ТА СИСТЕМНОГО АНАЛІЗУ

УДК 519.6

В.К. ЗАДІРАКА
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *zvk140@ukr.net*.

А.М. ТЕРЕЩЕНКО
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *teramidi@ukr.net*.

ЕФЕКТИВНИЙ АЛГОРИТМ ПІДНЕСЕННЯ ДО КВАДРАТА БАГАТОСЛІВНИХ ЧИСЕЛ

Анотація. Запропоновано метод реалізації операції піднесення до квадрата числа довжиною N слів ($N = 2^n$), який дає змогу обчислювати на основі восьми множень чисел довжиною $N/4$ слів $N \geq 4$. Операція піднесення до квадрата є однією з основних операцій шифрування, дешифрування та верифікації ключів асиметричної криптографії. Від швидкодії цієї операції залежить швидкодія операцій асиметричної криптографії. Згідно з теоремою оцінено складність запропонованого методу для чисел довжиною N слів та показано, що обчислення може бути виконано на основі чотирьох піднесень до квадрата чисел довжиною $N/4$ слів та чотирьох множень чисел довжиною $N/4$ слів. Піднесення до квадрата чотирислівного числа на основі запропонованого методу може бути виконано із застосуванням восьми множень, що на одне множення меньше ніж у методі Карацуби, який використовується рекурсивно. Запропонований метод може бути застосований рекурсивно, що підвищує можливість з розпаралелювання операції піднесення до квадрата великих чисел. Результати роботи можуть бути використані для розроблення швидких алгоритмів багатослівної арифметики та для реалізації операції піднесення до квадрата великих чисел у мікросхемному виконанні.

Ключові слова: багатослівна арифметика, багатослівне множення, багатослівне піднесення до квадрата, піднесення до квадрата за модулем, асиметрична криптографія.

ВСТУП

Сьогодні важко уявити життя без комп'ютерів, смартфонів та інших гаджетів, для виконання програм яких потрібна реалізація операції множення [1–7]. Остання порівняно з реалізацією операції додавання потребує на порядок більше елементів (транзисторів). Час на виконання операцій множення та енергія для роботи транзисторів є значними. До 1962 р. вважалося, що оцінка складності операції множення N^2 є оптимальною, але в публікації А. Карацуби [1] показано, що множення двослівних чисел може бути виконано з використанням трьох множень замість чотирьох. Метод Карацуби був поштовхом для пошуку нових швидких алгоритмів реалізації багатослівної операції множення, які значно прискорювали виконання алгоритмів, спрощували реалізацію на мікропроцесорах та заощаджували використання енергії. Методи оптимізації операції множення можна застосовувати для оптимізації операції піднесення до квадрата, яка є складовою операції піднесення до степеня за модулем, від швидкодії якої залежить швидкодія асиметричних криптографічних програмно-апаратних комплексів [8–11].