СИСТЕМНИЙ АНАЛІЗ

УДК 519.6

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

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

АЛГОРИТМ БАГАТОСЛІВНОГО МНОЖЕННЯ НА ОСНОВІ ПЕРЕТВОРЕННЯ МЕРСЕННА

Анотація. Розглянуто алгоритм реалізації багатослівної операції множення на основі теоретико-числового перетворення Мерсенна. Числа Мерсенна та їхні властивості широко використовують в кібербезпеці, цифровому обробленні сигналів. Алгоритми на основі перетворення Мерсенна можна також реалізувати на квантових комп'ютерах з можливістю суперрозпаралелювання. Операція багатослівного множення є однією з основних операцій шифрування, дешифрування, генерування та верифікації ключів асиметричної криптографії. Від швидкодії цієї багатослівної операції залежить швидкодія операцій асиметричної криптографії. Наведено новий швидкий алгоритм знаходження оберненого числа, яке використовується для обчислення оберненого перетворення Мерсенна, що дає змогу будувати алгоритми реалізації операцій над числами довжиною у мільйон або більше бітів. Отримано оцінку складності алгоритму на основі перетворення Мерсенна для чисел довжиною N слів і зазначено, що такий алгоритм може виконуватися рекурсивно. Проаналізовано межу максимально можливого значення множника в залежності від довжини перетворення Мерсенна p для алгоритму багатослівного множення. Запропоновано новий алгоритм множення за модулем числа Мерсенна на основі двох операцій множення половинної довжини замість трьох множень за методом Карацуби. Здійснено порівняльний аналіз складності за кількістю операцій однослівного множення алгоритму на основі перетворення Мерсенна у комбінації з методом Карацуби та на основі методу Карацуби на прикладі багатослівної операції піднесення до квадрата.

Ключові слова: багатослівна арифметика, багатослівне множення, багатослівне піднесення до квадрата, багатослівне множення за модулем, піднесення багатослівного числа до степеня за модулем, теоретико-числове перетворення, асиметрична криптографія.

DOI 10.34229/KCA2522-9664.26.5.4

ВСТУП

Сучасний науковий світ неможливо уявити без нових технологій, що побудовані на складних або надскладних алгоритмах, реалізація яких потребує використання операцій множення [1–11]. Реалізація операції множення є однією з найскладніших щодо кількості елементів (транзисторів) у порівнянні з реалізацією операцій додавання чи віднімання. До 1962 р. вважалося, що оцінка складності операції множення N^2 є оптимальною у випадку множення двох чисел довжиною N слів. У роботі [1] описано метод множення двослівних чисел з використанням трьох операцій множення замість чотирьох. Метод Карацуби став поштовхом до пошуку нових швидких алгорит-