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.*

ОПТИМІЗАЦІЯ БАГАТОРОЗРЯДНОЇ ОПЕРАЦІЇ МНОЖЕННЯ НА ОСНОВІ ДИСКРЕТНИХ ПЕРЕТВОРЕНЬ (ФУР'Є, КОСИНУСНИХ, СИНУСНИХ) У ПАРАЛЕЛЬНІЙ МОДЕЛІ ОБЧИСЛЕННЯ

Анотація. Розглянуто операцію багаторозрядного множення, від швидкодії якої залежить швидкодія асиметричних криптографічних програмно-апаратних комплексів. Запропоновано алгоритми реалізації операції множення двох N-розрядних чисел на основі дискретних косинусних та синусних перетворень (ДКП та ДСП). За рахунок використання ДКП та ДСП розділено обчислення для дійсної та уявної частин дискретного перетворення Фур'є (ДПФ) дійсного сигналу парної довжини, що дає змогу перевести обчислення з поля комплексних чисел у поле дійсних чисел та зменшити складність багаторозрядної операції множення за кількістю однорозрядних операцій комплексного множення. Проведено заміну операцій алгоритму для збереження симетрії у дійсній або уявній частинах багаторозрядних чисел, що дає змогу використовувати ДКП та ДСП меншої розрядності $N/2+1$ та розширює можливості з розпаралелювання під час реалізації багаторозрядного множення.

Ключові слова: багаторозрядне множення, багаторозрядна арифметика, асиметрична криптографія, дискретне косинусне перетворення, дискретне синусне перетворення, дискретне перетворення Фур'є, швидкий алгоритм обчислення Фур'є.

ВСТУП

Поява нових паралельних обчислювальних систем, як-от багатоядерних процесорів, графічних прискорювачів, кластерів, розподілених систем, систем з розподіленою пам'яттю тощо зумовлена розв'язанням складних прикладних задач у різних галузях. Серед таких задач можна виділити задачі обчислення систем лінійних алгебраїчних рівнянь з кількістю невідомих 33–35 мільйонів, розрахунок оболонок ядерних реакторів, моделювання фізичних і хімічних процесів, аеродинаміки, гідродинаміки, захисту інформації тощо. Це значно розширює використання багаторозрядної арифметики [1–7], оскільки неврахування похибок заокруглення призводить до того, що іноді отримують комп'ютерні рішення, які не відповідають фізичному змісту. Багаторозрядна операція множення є складовою операції піднесення до степеня за модулем, від швидкодії якої залежить швидкодія асиметричних криптографічних програмно-апаратних комплексів.

У роботі Карацуби–Офмана [8] 1962 р. наведено опис алгоритму, який мав складність обчислення багаторозрядного множення за кількістю однорозрядних множень меншу ніж $O^{\text{стовпчик}}(N^2)$, де N — кількість розрядів (слів) багаторозряд-