УДК 004.421

І.О. ПРОЦЬКО
Національний університет «Львівська політехніка», Львів, Україна,
e-mail: *ihor.o.protsko@lpnu.ua*.

О.В. ГРИЩУК
ТОВ «SoftServe», Львів, Україна, e-mail: *ocr@ukr.net*.

РЕАЛІЗАЦІЯ МНОЖЕННЯ МОНТГОМЕРІ ДЛЯ ПРИСКОРЕННЯ ОБЧИСЛЕННЯ МОДУЛЯРНОГО ЕКСПОНЕНЦІЮВАННЯ БАГАТОРОЗРЯДНИХ ЧИСЕЛ

Анотація. Проведено порівняння та аналіз використання розробленої програмної реалізації класу *MontgomeryArithmetic* для обчислення модулярного експоненціювання. Виконано порівняння швидкості виконання розробленого модулярного множення Монтгомері та звичайного модулярного множення для обчислення модулярного експоненціювання на основі методу двійкового піднесення справа наліво для фіксованої основи з попереднім обчисленням скороченого набору залишків. Отримані результати обчислень модулярного експоненціювання з розпаралелюванням на основі багатопотоковості та з використанням розробленого модулярного множення Монтгомері на комп'ютерах загального призначення свідчать про пришвидшення обчислень у середньому в 1.5 раза порівняно з функціями модулярного піднесення до степеня з програмних бібліотек MPIR, OpenSSL, Crypto++.

Ключові слова: модулярне множення, модулярне експоненціювання, паралельні багатопотокові обчислення, передобчислення, багаторозрядні числа.

ВСТУП

Сучасні інформаційні технології надають можливість доступу будь-якому їхньому користувачеві до важливих та значних за обсягом обчислювальних ресурсів і даних. Як наслідок, виникає потреба у застосуванні ефективних програмних засобів захисту на основі багаторозрядних чисел. Найкритичнішими з погляду обчислювальної реалізації теоретико-числових алгоритмів є операції модулярної арифметики над числами великої розрядності [1, 2], яка значно перевищує розрядність процесорів. Зростання розрядності чисел, з якими здебільшого оперують у галузі інформаційної безпеки, призводить до сповільнення реалізації відповідних операцій на комп'ютерах загального призначення. Для досягнення прийнятного рівня захищеності нині використовують великі числа обсягом 1024–2048 розрядів з перспективою зростання розрядності у майбутньому до 4096.

Модулярне множення та модулярне експоненціювання широко застосовують для знаходження дискретного логарифма, в теоретико-числових перетвореннях та у криптографічних алгоритмах з великими числовими даними. Для ефективного обчислення модулярного множення науковці досліджують нові методи, алгоритми та засоби їхньої реалізації. У 1985 р. Пітер Монтгомері [3] запропонував метод модулярного множення, що не потребує виконання операції ділення. Цей метод дає змогу виконувати швидке множення чисел великої розрядності за модулем простих чисел і є загальновживаним у комп'ютерній арифметиці. Модулярне множення Монтгомері забезпечує зменшення часових затримок в обчисленнях у разі його багаторазового використання. Реалізація редукції Монтгомері є найбільш критичним для продуктивності методом у виконанні модулярного експоненціювання у теоретико-числових алгоритмах із застосуванням багаторозрядних чисел.