УДК 004.056

В.Карпінський, Ґ.Літава, І.Якименко
(Тернопільський національний економічний університет),
(Вища державна технічна школа в Новому Сончі (Польща)

РОЗВ'ЯЗАННЯ ПРОБЛЕМИ ДИСКРЕТНОГО ЛОГАРИФМУ ПАРАЛЕЛЬНИМ МЕТОДОМ РО-ПОЛАРДА НА ПІДСТАВІ БІБЛІОТЕК MPI2 І MIRACL

Ключове питання для безпеки криптосистем, що ґрунтуються на еліптичних кривих, зводиться до задачі дискретного логарифму на еліптичній кривій ECDLP (Elliptic Curve Discrete Logarithm Problem), яка полягає в наступному. Задані дана еліптична крива E, визначена над скінченим полем, точка P порядку n та точка Q, що є кратна до точки P. Потрібно знайти ціле число $l \subset <0, n\text{-}1>$ таке, що $Q = l \cdot P$, причому l – це дискретний логарифм Q з основою P. Одним з найефективніших відомих на сьогодні розв'язань дискретного логарифма є паралельна версія алгоритму Ро-Поларда.

Для розв'язання дискретного логарифма невигідно затосовувати багато процесорів, що працюють над однією стежкою блудіння, оскільки це забезпечує дуже малий приріст швидкодії. Суттєво ефективніший підхід для паралельного методу Ро-Поларда полягає у використанні багатьох стежок блудіння. За такого підходу кожний процесор займається обчисленням власної стежки, причому тоді слід знайти колізію двох стежок. Один з методів реалізації паралельного алгоритму, що характеризується високою ефективністю та водночас піддається впровадженню однаковою мірою на багатопроцесорних серверах зі спільноприділеною пам'яттю та комп'ютерних кластрах з розподіленою пам'яттю, полягає у застосуванні стандарту MPI (Message Passing Interface). Згідно з ним можна передавати повідомлення між процесами паралельних програм, що виконуються на одному або більше комп'ютерах. Означення кривих, а також основних операцій над ними сформульовані в багатьох бібліотеках, до яких належить MIRACL. В ній визначені основні дії на еліптичних кривих. Згадана бібліотека відноситься до однієї з найбільш швидкодіючих, зокрема на 64 бітових процесорах. Програма, що базується на бібліотеках MPI2 та MIRACL, взята за основу до вирішення завдання або оцінки потрібного часу для розв'язання дискретного логарифма на кривих $EC(2^m)$ і $EC(p)$ у багатопроцесорному середовищі з розгалуженою та співприділеною пам'яттю з використанням 64 бітових процесорів Itanium 2.

До тестування передбачено застосувати: а) сервер, який обладнаний 128 процесорами типу Intel Itanium 2 з тактовою частотою 1,5 ГГц та обсягом операційної пам'яті 256 ГБ і функціонує під контролем операційної системи SUSE Linux Enterprise Server 9; б) комп'ютерний кластер, що працює під контролем операційної системи Scientific Linux CERN 3 з використанням стандарту MPICH2 та складається з 20 серверів по 2 процесори типу Intel Itanium 2 – 1,3 ГГц, 2 ГБ пам'яті. Одержані результати полягають у визначенні часу виконання поставленої задачі в залежності від кількості задіяних процесорів (кількості стежок блудіння) для архітектур з розподіленою та спільноприділеною пам'яттю, а також порівняльному аналізі швидкодії обох архітектур. Подальшим кроком збільшення прискорення обчислень буде побудова технічного засобу для реалізації основних дій (додавання) на еліптичній кривій $EC(2^m)$, який базуватиметься на програмованих логічних інтегральних схемах FPGA CycloneIII мікроелектронної корпорації Altera, а також застосування його допоміжним компонентом в середовищі з розподіленою пам'яттю (комп'ютерними кластрами) до розв'язання дискретного логарифма.