УДК 681.3.06
А. Хомінчук, І. Якименко
(Тернопільський національний економічний університет)

ПРИСКОРЕННЯ АЛГОРИТМУ ШУФА МЕТОДОМ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ

В зв'язку з стрімким розвитком інформаційних технологій все більше актуальності набуває проблема захисту інформації. Для вирішення її потрібно шукати нові методи. Одним з них і найперспективнішим в даний час є шифрування за допомогою еліптичних кривих (ЕК).

ЕК – це крива третього порядку, яка задається рівнянням

$$y^2 = x^3 + ax + b$$

Для здійснення шифрування, для початку потрібно вирішити низку взаємнопов'язаних задач:

1. Генерування еліптичних кривих, тобто знаходження коефіцієнтів a та b;
2. генерування базових точок на ЕК;
3. пошук порядку ЕК.

Для вирішення задач генерування параметрів та базових точок існують стандартизовані алгоритми. Проте після генерації кривої виникає наступне питання – чи стійка згенерована крива до атак спеціального виду? Показником стійкості ЕК є великий простий порядок кривої. Крім цього, обчислення порядку групи точок на ЕК над кінцевим простим полем має важливе значення як в криптографії, так і в алгоритмах перевірки простоти чисел. Для знаходження порядку можна використати алгоритм Шуфа, який має поліноміальну складність $O(\log^8 p)$ бітових операцій. При дослідженні було виявлено, що основна трудомісткість алгоритму є обчислення великих степенів x^p, y^p по модулю полінома $f_l(x)$, при чому число і степінь – 256-бітні числа (80-90 десяткових знаків), модуль – поліном високого порядку (при експериментах цей модуль сягав тисяч десяткових знаків).

Для збільшення швидкодії роботи алгоритму Шуфа було запропоновано використати технології паралельних обчислень. При цьому розпаралелюється саме піднесення до степеня за модулем. Як відомо, x^P можна розписати наступним чином:

$$x^P = x^{\frac{P}{n}} \cdot x^{\frac{P}{n}} \cdot \ldots \cdot x^{\frac{P}{n}} = \prod_n x^{\frac{P}{n}} \qquad (1)$$

Запис (1) довзоляє розбити підненсення числа до степеня на n незалежних операцій, які можна виконувати паралельно. Проте, як було сказано вище, піднесення до степеня в алгоритмі Шуфа здійснюється за модулем, тоді (1) запишеться в наступному вигляді:

$$x^P = \prod_n x^{\frac{P}{n}} \bmod f \qquad (2)$$

Неважко побачити, що в формулі (2) використання модуля дає додаткове прискорення роботи алгоритму, в якому часткові степені $x^{\frac{P}{n}}$ не перевищують модуль f. Внаслідок цього зменшується розрядність часткових степенів, що дає досить суттєвий виграш в швидкодії.

Отже, для збільшення швидкодії алгоритму Шуфа доцільно використовувати технологію паралельних обчислень.