УДК 003.26.09
Струбицький Р. - ст. гр. ПЗАСм-51
Тернопільський національний економічний університет

РОЗПАРАЛЕЛЕННЯ ЗАДАЧ ДИСКРЕТНОГО ЛОГАРИФМУВАННЯ НА ЕЛІПТИЧНІЙ КРИВІЙ

Науковий керівник: к.т.н., доцент Шпінталь М. Я.

Еліптичні криві – найбільш перспективних інструментів для побудови й аналізу криптографічних алгоритмів, які дозволяють реалізувати широкий спектр криптографічних протоколів. Стійкість яких залежить від пошуку ефективних методів знаходження дискретних логарифмів у групі точок еліптичною кривої.

Нехай F_q - з поля $q = p^n$ елементів, де p - просте і $n \in N$. Еліптичні криві $E(F_q): y^2 = f(x)$ можна представити двояко: геометрично - множина точок з груповим законом і алгебраїчно - в термінах поля функцій $F_q(x)/(y^2 - f(x))$. Число точок еліптичної кривої $E(F_q)$ $\tilde{q}$ близьке до q. Якщо $P \in E(F_q), P \neq E$, де E-нульовий елемент $E(F_q)$, то найменше натуральне число n з умовою $nP = E$ називають порядком точки P. Еліптична крива $E(F_q)$ задана рівнянням Вейєрштрасса

$$y^2 + a_1xy + a_2y = x^3 + a_2x^2 + a_4x + a_6, \quad (1)$$

де похідні по і по поліноми, заданої кривої, не перетворюються в нуль одночасно в жодній точці кривої, навіть при переході до алгебраїчного замкнутого поля, і нехай $Q \in E(F_q)$ - точка порядку t.

Для задачі дискретного логарифмування в групі точок еліптичної кривої потрібно для даної точки $P \in \langle Q \rangle$ знайти l такий, що $P = lQ$. Цю задачу можна вирішити універсальним детермінованими методом узгодження, справедливим для довільної групи обчислювального порядку.

Коли знайдеться елемент ряду $P, P - Q, P - 2Q, P - 3Q, P - 4Q, \ldots, P - RQ$ (2)

який збігається з яким-небудь членом ряду $rQ, 2rQ, 3rQ, 4rQ, \ldots, r^2Q$ (3)

Потрібно відсортувати швидким сортуванням. Після чого впорядковані значення $Z(x)$ та $Z'(y)$, де $x, y \in [0; r)$, доцільно порівнювати бінарним пошуком, який є досить ефективним. При цьому складність наведеного алгоритму узгодження по часі і пам'яті $O(\sqrt{r} \cdot \log r)$. Якщо є два процеси і r велике, то виконувати кроки даного алгоритму можна одночасно.

Якщо є більше 2 процесів, то можна ще прискорити, розподіливши перебір всіх значень x і y по w процесам. Нехай m - власний номер процесу, n_1- нижня, n_2- верхня межі діапазону , де $x \in [0; r)$ для кожного процесу. Тоді можна допустити наступний спосіб розподілу роботи зі складання перших таблиці значень $Z(x), x \in [0; r-1]$ з w процесів: $h = (r - 1 - 0 + 1)/w = r/w$; $ost = r/w - [r/w]$; $n_1 = (m-1) \cdot h = (m-1) \cdot (r/w)$; $n_2 = n_1 + h = (m-1) \cdot (r/w) + r/w$; $if(ost \neq 0)^{m=w}$ $n_2 = n_2 + ost$ Перебір можливих значень здійснюється аналогічним чином.

Позначимо процес обчислення в i-му процесі значень $Z(x), Z'(y)$, де $x, y \in [n_1, n_2 - 1]$, блоками $z(i, x)$ та $z'(i, y)$, де $i \in [1, w]$ відповідно. Тоді паралельне виконання методу узгодження для обчислення дискретного логарифму можна реалізувати за алгоритмом "розподілених узгоджень". Прискорення цього алгоритму буде не менше $w/2$. Можна отримати більш ефективний алгоритм, розподіливши перебір значень x і y узгоджено з часом обчислення початкових значень. Тому доцільно використовувати запропонований метод для розв'язку задачі дискретного логарифмування в кінцевому полі.