УДК 681.3

М.Карпінський[1], докт. техн. наук; І.Якименко[2]
[1]*Університет в Бєльську-Бялей, Польща*
[2]*Тернопільська академія народного господарства*

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОБЧИСЛЕННЯ ТОЧОК НА ЕЛІПТИЧНИХ КРИВИХ НАД ОБМЕЖЕНИМИ ПОЛЯМИ

Розглядається проблема обчислення точок еліптичної кривої з використанням різноманітних підходів: поліноміального алгоритму, алгоритмів "крок гіганта – крок малюка", Корначчі і многочленного детерміністичного алгоритму часу. Проаналізовано існуючі підходи та наведено результати щодо підвищення ефективності знаходження характерних точок еліптичної кривої, що є важливими та актуальними.

Сьогодні питання захисту інформації в комп'ютерних системах є особливо важливими в забезпеченні конфіденційності і автентичності повідомлень державного та комерційного характеру.

Одним із нових і перспективних напрямків для розв'язання задач захисту інформації є побудова стійких криптографічних алгоритмів з використанням математичного апарату еліптичних кривих (ЕК). Основна перевага застосовування ЕК в задачах захисту інформації полягає в значно меншому розмірі ключа для забезпечення високої стійкості. Крім того, застосування еліптичних кривих для криптографічного захисту інформації є перспективним напрямком у практичній криптології, оскільки така криптосистема надійніша за традиційні асиметричні системи, наприклад, алгоритм RSA, за однакових ключів.

В системі з використанням еліптичних кривих застосовують несингулярні криві E над полем F_p, які описуються рівнянням Веєрштраса [1]

$$Y^2 = X^3 + AX + B \qquad (1)$$

для деяких $A, B, \in Fp$, p - велике просте число. Оскільки крива (1) не сингулярна, то $4A^3 + 27B^2 \neq 0 \pmod p$. Отже, необхідно розв'язати задачу обчислення кількості точок на деякій еліптичній кривій.

Для знаходження кількості точок на еліптичній кривій можна застосувати поліноміальний алгоритм, для обмеженого поля малої потужності, що ґрунтується на теорії Шанкса [2]. Суть цього алгоритму полягає у виборі точки $P \in E(F_p)$ та обчисленні цілого числа m на інтервалі $\left(p+1-2\sqrt{p}, p+1+2\sqrt{p}\right)$ такого, щоб $mP=0$. Якщо m є тільки єдиним числом в інтервалі, то з теореми Хассе випливає, що $m = \#E(F_p)$. Число m обчислюється за допомогою „кроку гіганта – кроку малюка". Спершу здійснюються невеликі кроки: складається список перших чисел $s \approx \sqrt[4]{p}$, кратних до P, 2P, 3P,…. Оскільки протилежність точки одержується за допомогою зміни знаку її ординати, то можна насправді взнати координати 2s+1 точок: $0, \pm P, \pm 2P, ..., \pm sP$. На наступному кроці обчислюють $Q = (2s+1)P$, використовуючи двійкове розширення точки $R = (p+1)$, і наприкінці роблять гігантські кроки: за допомогою повторного додавання і віднімання точки Q. Таким чином, обчислюють $R, R \pm Q, R \pm 2Q, ..., R \pm tQ$. Тут $t = \left\lceil 2\sqrt{p} \Big/ (2s+1) \right\rceil$. За теоремою Хассе, точка $R + iQ$ для деякого цілого числа $i = 0, \pm 1, \pm 2, ..., \pm t$ дорівнює одній із точок в списку „невеликих кроків": $R + iQ = jP \quad \forall j \in \{0, \pm 1, \pm 2, ..., \pm s\}$. Підставляючи $m = (p+1)i - j$, отримують mP=0.

Алгоритм приречений на невдачу дуже рідко тому, що для кожної точки P є більш ніж одне число m в інтервалі $\left(p+1-2\sqrt{p}, p+1+2\sqrt{p}\right)$, для якої *mP=0*. Це стається тоді, коли показник степеня групи $E(F_p)$ дуже малий. Для уникнення цих ускладнень використаємо підхід Местре, що опирається на квадратне скручування еліптичної кривої *E*. Якщо еліптична крива E задана рівнянням (1), тоді скручена крива E' має вигляд

$$gY^2 = X^3 + AX + B \tag{2}$$

для деякого неквадратного $g \in F_p^*$. Клас ізоморфізму цієї кривої не залежить від вибору g. Легко побачити, що

$$Y^2 = X^3 + Ag^2X + Bg^3 \tag{3}$$

є рівнянням Веєрштраса для кривої E'. Таким чином, для знаходження #E(F_p) можна обчислити $\# E'(F_p)$.

Означення. j–інваріанта еліптичної кривої E, яка задана рівнянням (1), визначається за формулою

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}. \tag{4}$$

Отже, еліптична крива E та її квадратне скручування E' мають одні і ті ж j–інваріанти.

Морфізми $f : E \to E$, які зберігають точку в нескінченності, утворюють кільце еліптичних кривих $End(E)$ з F_p-ендоморфізмом. Якщо $\Delta \in Z_{<0}$ означає дискримінант степеня, який є в наявності, то

$$End(E) \cong Z\left[\delta\right] = Z + Z\delta, \tag{5}$$

де $\delta = \frac{\sqrt{\Delta}}{2}$ або $\delta = \frac{1+\sqrt{\Delta}}{2}$ в залежності від того, парний чи непарний дискримінант Δ кільця ендоморфізму $End(E)$.

Ендоморфізм Фробеніуса $\varphi \in End(E)$ є ендоморфізмом, якщо подається у вигляді $\varphi(x, y) = (x^p, y^p)$. Це задовольняє квадратне співвідношення

$$\varphi^2 - t\varphi + p = 0 \tag{6}$$

в кільці E. Тут t є ціле число, яке зв'язане з рядом F_p-точок на еліптичній кривій E за допомогою наступного співвідношення

$$\# E(F_p) = p + 1 - t. \tag{7}$$

Група $E(F_p)$ є власним ядром гомоморфізму $\varphi - 1$, який діє на групу точок над алгебраїчним доповненням F_p. Таким чином, показник степеня групи $E(F_p) \in \frac{p+1-t}{n}$, де n - найбільше ціле число, для якого $p = 1(\text{mod } n)$ в $End(E)$.

Тепер візьмемо до уваги теорему 1 /Местре/. Нехай $p > 457$ - просте число та E - еліптична крива над полем F_p. Тоді або еліптична крива E, або її квадратне скручування E' допускають F_p-раціональну точку порядку щонайменше $4\sqrt{p}$.

Щоб переконатися, що алгоритм „кроку гіганта – кроку малюка" справджується для еліптичної кривої E, потрібно знайти раціональну точку на еліптичній кривій порядку щонайменше $4\sqrt{p}$ або знайти таку точку P, яку можна

описати згідно з теоремою 2 Местре: приймемо, що $p > 229$ - просте число та E буде еліптичною кривою над полем F_p. Тоді або еліптична крива E, або її квадратне скручування E' допускають F_p-раціональну точку P з властивістю: єдине ціле число $m \in \left(p+1-2\sqrt{p}, p+1+2\sqrt{p}\right)$, для якого $mP = 0$, є порядком групи точок.

Велика кількість кривих E, для яких теорема 2 не справджується, мають свої j-інваріанти, які дорівнюють 0 або 1728, і таким чином кільце ендоморфізму є ізоморфним до $z\left[\left(1+\sqrt{-3}/2\right)\right]$ або $z[i]$ відповідно. Однак, якщо відоме кільце ендоморфізму E, то тоді можна обчислити F_p, навіть коли p дуже велике. Якщо виключати криві з j-інваріантною 0, тоді теорема 1 є дійсною для $p > 53$.

Застосуємо інший підхід до знаходження кількості точок на еліптичній кривій, що грунтується на алгоритмі Корначчі.

Нехай p - велике просте число та E - еліптична крива над F_p, яка подається рівнянням (1). Тоді щодо кільця C можна записати:

$$\mathrm{End}(\mathrm{E}) \cong \begin{cases} \left[\dfrac{u+v\sqrt{\Delta}}{2} : u,v \in z \;\; i\, u \cong v \pmod{i} \right], \\ \left[u+v\delta : u,v \in z\right] = z + \delta z \end{cases} \tag{8}$$

де $\delta = \sqrt{\dfrac{\Delta}{2}}$ або $\delta = \dfrac{1+\sqrt{\Delta}}{2}$ в залежності від того, дискримінант Δ парний чи непарний. Ендоморфізм Фробеніуса $\varphi \in E \; and \; (E)$ задовольняє співвідношення $\varphi^2 - t\varphi + p = 0$, де $t \in Z$, причому $t^2 < \varphi p$, а також t пов'язане з $\#E(Fp)$ формулою $E(Fp) = p+1-t$. Якщо p ділить Δ, тоді $t = 0 \; i \; \#E(Fp) = p+1$. Тому розглянемо випадок, коли $p = \varphi\overline{\varphi}$. Завдяки цьому побачимо, що ціле число p розбиває $End(E)$ на два ідеали головних простих чисел (φ) і $\overline{(\varphi)}$ з індексом p.

Алгоритм Корначчі полягає в обчисленні генератора простого дільника $p \in Z[\delta]$. Для знаходження генератора головного ідеалу $p \in Z[\delta]$ спочатку обчислимо квадратний корінь b від $b \equiv \Delta(\mathrm{mod}\ 2)$. Змінивши p на $p-b$, можна припустити, що $|b| < p$ і $b \equiv \Delta(\mathrm{mod}\ 2)$. Тоді $p = \left(\left(\dfrac{b+\sqrt{\Delta}}{2}\right), p\right)$ є головним ідеалом з індексом p. Оскільки p є головний, дробовий ідеал, то

$$z + \frac{b+\sqrt{\Delta}}{2p} z \tag{9}$$

дорівнює ідеалу форми $(z+\delta z)\alpha$ для деяких $\alpha \in Z[\delta]$. Іншими словами, існує матриця $\begin{pmatrix} p & g \\ r & s \end{pmatrix} \in SL(Z)$. Перевірка уявних дробових частин показує, що $(r+s\delta)\overline{(r+s\delta)} = p$.

Отже, $r+s\delta$ є генератором для ідеалу p. Для знаходження матриці $\begin{pmatrix} p & g \\ r & s \end{pmatrix}$ розглянемо звичайну дію групи $SL_2(Z)$ на верхній частині залежності $\{z \in C : \mathrm{Im}\, z > 0\}$. Як $\left(b+\sqrt{\Delta}/2\right)$, так і δ належать орбіті $SL_2(Z)$ і містяться в стандартному основному

домені. Поступовим використанням матриць $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} i \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in SL_2(R)$ перетворимо $z + \frac{b+\sqrt{\Delta}}{2p}$ до δ.

Алгоритм Корначчі можна віднести до звичайного алгоритму для зменшення позитивних визначених форматів. Застосуємо теорему 3 Коначчі для спрощення розв'язку розглянутої задачі. Нехай О – комплексний квадратний степінь дискримінанта Δ і p - непарне просте число, для якого дискримінант Δ є ненульовим квадратом за модулем p, а x - ціле число, причому $x^2 \equiv \Delta(\mathrm{mod}\, p)$, $x \equiv \Delta(\mathrm{mod}\, 2)$ і $0 < x < 2p$. Визначимо обмежену послідовність невід'ємних цілих чисел $x_0, x_1, ..., x_t = 0$, причому таких, що $x_0 = 2p$, $x_1 = x$, $x_{i+1} = x_{i-1}(\mathrm{mod}\ x_i)$.

Приймемо за i найменший індекс, для якого $x_i < 2\sqrt{p}$. Якщо Δ ділить $x_i^2 - 4p$ і частка є квадратом υ^2, тоді $\frac{x_i + \upsilon\sqrt{\Delta}}{2}$ є генератором головного ідеалу p від 0.

Розглянемо детермінований многочленний алгоритм часу, для розрахунку ряду точок на еліптичній кривій E над полем F_p. Допускаємо, що еліптична крива E задана рівнянням (1). Тоді можна обчислити $\#E(F_p)$ за модулем 2: потужність групи $E(F_p)$ відома, тільки якщо вона містить точку порядку 2. Оскільки точки порядку 2 характеризуються виглядом (x,0), то многочлен $X^3 + AX + B$ має нуль в F_p, що рівноцінно найбільшому спільному дільнику (НДС)

$$НСД\left(X^p - X, X^3 + AX + B\right) \neq 1 \ в\ кільці\ F_p[X]. \qquad (10)$$

Це можна перевірити ефективніше, а саме – більша частина розрахунків полягає в обчисленні X^p в кільці $F_p[X] \cdot \left(X^3 + AX + B\right)^{-1}$, яке можна здійснити повторним піднесенням до квадрату і множенням, використовуючи двійкове подання показника p.

Узагальнимо це обчислення до інших простих чисел l. При цьому розрахуємо $\#E(F_p)$ за модулем декількох малих простих чисел $l = 3,5,7,....$ За теоремою Хассе,

$$\mathrm{p} + 1 - 2\sqrt{\mathrm{p}} < \#\,\mathrm{E}(\mathrm{F_P}) < \mathrm{p} + 1 + 2\sqrt{\mathrm{p}}, \qquad (11)$$

а це є достатнім для того, щоб

$$\prod_l l > 4\sqrt{p}. \qquad (12)$$

Для визначення потужності звернемося до Китайської залишкової теореми. Слабка сторона теореми для простого числа показує, що цього можна досягти з простими числами не більш як $O(\log p)$ простого числа l, кожне з яких не перевищує $O(\log p)$. Оскільки p велике , то прості числа l є дуже малі щодо p. Зокрема $l \neq p$. Як і для $l = 2$, використовуємо підгрупу $E[l]$ l точок E (Fp):

$$E[l] = \left\{ P \in E\left(\overline{F_p}\right) : l \cdot P = 0 \right\}. \qquad (13)$$

Група $E[l]$ є ізоморфною для $Z/lZ \times Z/lZ$, причому поліноми ділення

$$\psi_l(X) \in F_p[X] \qquad (14)$$

можна розрахувати рекурсивно за допомогою формул доповнення. Їх порядок є $\left(l^2 - 1\right)/2$.

Ендоморфізм Фробеніуса $\varphi : E \to E$ задовольняє квадратне співвідношення (6), в якому для цілого числа t справджується (7). Згідно з алгоритмом перевіряємо, яке із відношень

$$\varphi^2 - t'\varphi + p = 0 \quad t' = 0,1,2,...,l-1 \tag{15}$$

належить групі $E[l]$. Аналіз показує, що відношення може тільки зберігатися для $t' \equiv t(\mathrm{mod}\, l)$, завдяки чому одержуємо значення t за модулем l.

Оскільки відношення можна виразити за допомогою поліномів та ефективно перевірити, то

$$\varphi^2(x,y) + p(x,y) = t'\varphi(x,y) \quad \forall (x,y) \in E[l] \tag{16}$$

тоді і тільки тоді, коли

$$\left(X^{p^2}, Y^{p^2}\right) + p'(x,y) \equiv t'\left(X^p, Y^p\right) \tag{17}$$

за модулем поліномів $\psi_l(X)$ і $Y^2 - X^3 - AX - B$. Тут p' означає ціле число, відповідне до $p(\mathrm{mod} 1)$, що задовольняє $0 \le p' < l$. Слід звернути увагу, що знак "+" відповідає додаванню на еліптичній кривій, причому множення є повторним додаванням.

Більша частина розрахунків полягає в обчисленні показників степеня $X^p, X^{p^2}, \ldots$ в кільці

$$F_p[X,Y] \Big/ \left(\psi_l(X), Y^2 - X^3 - AX - B\right) \tag{18}$$

з подальшим додаванням l разів точки $\left(X^p, Y^p\right)$, яке зводиться до декількох додавань і множень в кільці. Оскільки елементи кільця мають розмір $l^2 \log p$, то кількість витраченої роботи становить $O(\log p(l^2 \log(p)^2)$ і $O(l(l^2 \log p)^2)$ відповідно. Тут прийнято, що множення двох елементів довжини n відбувається за час, який пропорційний до n^2. Беручи до уваги, що $l = O(\log p)$, і здійснивши обчислення для кожного l, остаточно отримуємо вираз для роботи, яка витрачається на повне обчислення: $O(\log^8 p)$.

Многочленний детерміністичний алгоритм часу характеризується високою швидкодією. Однак результати проведеного аналізу свідчать про його малу ефективність на практиці, що викликане звичайними порядками поліномів ділення. Наприклад, при обчисленні для $p=10^{200}$ повинні включати прості числа $l > 250$. Для таких l, які мають один елемент в кільці, вимагається обсягу пам'яті комп'ютера більш ніж 1,5 мегабайта.

Застосуємо твердження 1. Нехай E - еліптична крива, яка є не суперсингуляною над полем F_p з j-інваріантою $j \neq 0$ *або* 1728. Приймемо, що $\Phi_o(j,T) = f_1 \cdot f_2 \cdots f_s$ - розклад на множники $\Phi_o(j,T) \in F_p[T]$ як результат перетворення поліномів. Порядки $f_1, f_2, \ldots f_s$ повинні задовольняти таким властивостям:

а) 1 і l; іншими словами, $\Phi_o(j,T)$ - коефіцієнти як результат перетворення лінійного коефіцієнта l, причому l ділить дискримінант $t^2 - 4p$ та підставляється $r = l$;

б) 1,1,r,r,…,r; інакше $t^2 - 4p$ - квадрат за модулем l, тобто ділиться на l-1 і φ діє на $E[l]$, як матриця $\begin{pmatrix} \lambda & \\ 0 & \mu \end{pmatrix}$, де $\lambda, \mu \in F_l^*$;

в) r,r,r,…,r для деякого r>1; тоді $t^2 - 4p$ не є квадратом за модулем l, степінь r ділить l+1 і φ діє на $E[l]$, як матриця 2×2, що має зміщеного порядку многочлен, який

неможливо перетворювати за модулем l. При цьому r є степенем φ в групі $PGL_2(F_l)$ і слід t для φ задовольняє $t^2 = (\zeta + \zeta^{-1})^2 \, p \pmod{l}$ для деякого r-го кореня $\zeta \in \overline{F}_l$.

Беручи до уваги твердження 2, згідно з яким E - еліптична крива, що не є суперсингуляною над полем F_p з j-інваріантою $j \neq 0$ *або* 1728, та l - непарне просте число, а s є рядом неперетворюваних коефіцієнтів в розкладанні на прості множники $\Phi_o(j,T) \in F_p[T]$. Тоді

$$(-1)^s = \left(\frac{p}{l} \right). \tag{19}$$

Розглянемо особливості удосконалення цього алгоритму, для чого використаємо підхід Еткіна та Еліза [3].

Нехай E - еліптична крива над полем Fp, яка задається рівнянням (1), і $j \in F_p$, причому j-інваріанта, l - просте число. Згідно з Еткіним, спочатку визначається кількість нулів, які має поліном $\Phi_l(j,T)$ в полі F_p. Для цього обчислюємо

$$НСД(T^p - T, \Phi_l(j,T)). \tag{20}$$

Тоді можна побачити, який випадок твердження 1 можна застосувати до головного l. Більша частина розрахунків полягає в обчисленні T^p в кільці $F_p[T]/(\Phi_l(j,T))$. Оскільки $l+1$ є степенем $\Phi_l(j,T)$, то кількість роботи пропорційна до $O(l^2 \log^3 p)$.

Для обчислення точного порядку r ендоморфізму Фробеніуса в $PGL_2(F_l)$ слід знайти

$$НСД(T^{p^i} - T, \Phi_l(j,T)) \tag{21}$$

для i = 2,3,.... Для $i = r$ знаходимо один НСД, який дорівнює $\Phi_l(j,T)$, причому i – найменший індекс з цією властивістю. Відомо за твердженням 1, що r ділиться на $l \pm 1$, і за твердженням 2 знаємо парність $l \pm 1/r$. Цю інформацію можна використати для прискорення обчислень, причому завдяки відомому r суворо обмежуються можливості для $t \pmod 1$. Для знаходження відповідного значення t, слід виконати ці обчислення для декількох малих простих чисел l і тоді знайти за допомогою алгоритму “крок гіганта - крок малюка” між можливими класами залишку за модулем значення простих чисел l. На практиці не використовуються j-інваріанти та модульне рівняння $\Phi_l(X,Y) = 0$, а зв'язані модульні функції, які задовольняють рівнянню (21) з меншими коефіцієнтами. Тоді розглянутий алгоритм є ефективним для помірно великих значень p. Обчислення з модульними поліномами можна зробити в многочленному часі, але кінцевий пошук згідно з „кроком гіганта – кроком малюка” не буде многочленним алгоритмом часу.

Тепер використаємо підхід Елкіза. Якщо ендоморфізм Фробеніуса φ діє на l точки $E[l]$ *як* 2 x 2-матриця з власними значеннями в F_l, то є власний простір C порядку l, який задовольняє дії групи Галуа. Використовуючи твердження 1, це можна ефективно перевірити. Відповідно до власного простору C, існує дільник $F(X) \in F_p[X]$ порядку $(l-1)/2$ від остачі поліноміального виразу $\psi_l(X)$, нулі якого є $(l-1)/2$ і X-координати відмінні від точок у власному просторі C. Тоді обчислюється значення λ, що відповідає простору C. Оскільки результат власних значень дорівнює p, то

$$t \equiv \lambda + p/\lambda \pmod{l}. \tag{22}$$

Для обчислення λ перевіряється, яке із співвідношень

$$\varphi(X,Y) = (X^p, Y^p) = \lambda' \cdot (X,Y) \quad \lambda' = 1,...,l-1 \tag{23}$$

утримується в просторі *C*, за модулем *F(X)*. Маємо, що $\lambda \equiv \lambda' (\mathrm{mod}\, l)$. Більша частина розрахунків зводиться до обчислення X_p і Y_p в кільці

$$F_p[X,Y] / \left(F(X), Y^2 - X^3 - AX - B\right). \tag{24}$$

Беручи до уваги, що *F(X)* притаманніший скоріше порядок $(l-1)/2$, ніж $(l^2-1)/2$, для обчислення беруть тільки дії $O(l^2 \log^3 p + l^3 \log^2 p) = O(\log^5 p)$. Це і є суттєвим щодо значного зменшення часу виконання $O\left(\log^7 p\right)$ відповідної дробової частини алгоритму .

Слід зазначити, що підхід Елкіза справджується та є ефективним лише для простих чисел l, для яких φ має власні значення в F_l. Тобто, для половини простих чисел l, тих, що розпадаються в полі $Q(\sqrt{t^2 - 4p}$. При цьому потрібно обчислити коефіцієнти многочлена $F(X) \in F_p[X]$.

Для підвищення стійкості криптосистеми необхідно використовувати еліптичні криві, для яких число кількості точок було б максимальним та містило б великий простий дільник. Це вимагає знання точної кількості точок еліптичної кривої. На практиці розв'язання задачі обчислення кількості точок на еліптичній кривій значно підвищує рівень криптостійкості системи захисту інформації.

In this paper has been considered the problem of the calculations the points of the elliptic curves within usage of different approaches: polynomial algorithm, "gigantic step – buby step" algorithm, Cornacchia's algorithm, multi deterministic time algorithm. Existed approaches to increase the effectivity of the special-kind points of elliptic curves have been analyzed, as well results have been shown.

Література

1. Beaureal D. Efficient algorithms for implementing elliptic curve public-key schemes //A Thesis submitted to the Faculty of the Worcester Polytechnic Institute. – 1996. – Pp. 190-194.
2. Schoof R. Elliptic curve //Journal de Theorie des Nombres de Bordeaux. –1995. - №7. – Pp. 219-254.
3. Atkin A.O.L. The Number of Points an Elliptic Curve Modulo a Prime. – Chicago:IL, 1988. – 320 p.

Одержано 30.09.2003 р.