А. Г. Ростовцев

Минимизация показателя для эллиптической кривой с комплексным умножением над $\mathbf{F}_p$

При построении криптографических алгоритмов на эллиптических кривых над простыми полями наиболее трудоемкой операцией является умножение точки P на число d. Если кривая обладает комплексным умножением в кольце O_K целых элементов поля $K = \mathbf{Q}(\sqrt{-D})$, то умножение можно ускорить за счет представления $d = c + e\xi$, где $\xi \in O_K$. Пусть q — большой простой порядок группы точек на эллиптической кривой, причем кривая не имеет другой группы порядка q. Предлагаются алгоритмы, вычисляющие разложение $d \equiv c + e\xi \pmod q$ для $D = 1$, $D = 3$, и обеспечивающий минимальное значение $|c|$, $|e|$, не превышающее $q^{1/2}$ для простого порядка q группы точек эллиптической кривой.

1. Эллиптические кривые с комплексным умножением

Эллиптическая кривая $E(\mathbf{F}_p)$ над простым полем $\mathbf{F}_p$ может быть задана уравнением в форме Вейерштрасса

$$y^2 = x^3 + Ax + B, \tag{1}$$

где $4A^3 + 27B^2 \neq 0$. Множество пар (x, y), удовлетворяющих уравнению, совместно с точкой “бесконечность”, образует множество точек кривой. Точки эллиптической кривой образуют абелеву группу с геометрическим законом сложения [1], нулем группы является точка “бесконечность”, точки (x, y) и $(x, -y)$ являются противоположными.

В основу безопасности криптографических протоколов положена задача логарифмирования на эллиптической кривой: для данных точек P, Q найти показатель l такой, что $P = lQ$. Для обеспечения высокой криптографической стойкости число точек кривой должно иметь большой простой делитель q. Кроме того, необходимо, чтобы выполнялось неравенство $q \neq p$ и чтобы q не было делителем чисел $p - 1$, $p^2 - 1$, ..., $p^k - 1$ для некоторого порогового значения k (обычно бывает достаточно обеспечить k = 20÷30). Тогда сложность логарифмирования на эллиптической кривой равна $O\left(\sqrt{q}\right)$ операций сложения точек на кривой, а наилучшим алгоритмом логарифмирования является алгоритм Полларда [2].

Эллиптическая кривая (1) может рассматриваться над алгебраическим замыканием поля $\mathbf{F}_p$. Обозначим такую кривую через $E\left(\overline{\mathbf{F}}_p\right)$. Тогда $E(\mathbf{F}_p)$ является нормальной подгруппой в $E\left(\overline{\mathbf{F}}_p\right)$. Группа точек $E\left(\overline{\mathbf{F}}_p\right)$ обладает эндоморфизмами, заключающимися в умножении каждой точки на произвольное целое число. Эндоморфизмы можно складывать:

$$\varphi(P) + \psi(P) = (\varphi + \psi)P$$

(здесь в левой части равенства используется сложение точек кривой, а в правой части — формальная операция сложения эндоморфизмов). Кроме того, эндоморфизмы можно умножать как отображения. Умножение дистрибутивно относительно сложения, а также коммутативно. Следовательно, эндоморфизмы образуют кольцо. В частности, для любой точки P выполняются равенства $mP + nP = (m + n)P$, $m(nP) = (mn)P$. Поэтому множество эндоморфизмов $E\left(\overline{\mathbf{F}}_p\right)$ всегда содержит кольцо, изоморфное $\mathbf{Z}$.

Если множество эндоморфизмов эллиптической кривой $E\left(\overline{\mathbf{F}}_p\right)$ строго больше $\mathbf{Z}$, то говорят, что кривая обладает *комплексным умножением*. В частности, любая кривая $E\left(\overline{\mathbf{F}}_p\right)$ обладает комплексным умножением на эндоморфизм Фробениуса. Однако на кривой $E(\mathbf{F}_p)$ такое умножение оставляет все точки неподвижными. Если кольцо O_K строго больше $\mathbf{Z}$ и обладает однозначным разложением на множители, то существуют эллиптические кривые, обладающие комплексным умножением, отличным от эндоморфизма Фробениуса. Такое умножение может действовать на кривой $E(\mathbf{F}_p)$.

Характеристика поля p может быть разложена на простые множители в кольце целых элементов O_K некоторого квадратичного расширения $K = \mathbf{Q}\left(\sqrt{-D}\right)$ поля $\mathbf{Q}$. Вид разложения определяется дискриминантом D. Среди значений дискриминанта D, обеспечивающих однозначность разложения в O_K, наиболее просто комплексное умножение реализуется для случая $D = 1$, $D = 3$.

Если $D = 1$, то в уравнении (1) $B = 0$, при этом $O_K = \mathbf{Z}[i]$, где $i^2 = -1$. Тогда существует отображение τ: $(x, y) \to (-x, iy)$. Если рассмотреть эту кривую над простым полем характеристики $p \equiv 1 \pmod 4$, то в поле $\mathbf{F}_p$ существует квадратный корень из -1, то есть $i \in \mathbf{F}_p$. Если число точек кривой свободно от квадратов, то группа точек циклическая. Пусть q — большой простой делитель порядка группы и Q — образующая группы порядка q. В этом случае отображение τ действует на точку как умножение на некоторое целое число j. Поскольку $\tau^2(P) = -P$, то $j^2 \equiv -1 \pmod q$. Ни одна из точек группы порядка q не имеет нулевых координат, следовательно, $q \equiv 1 \pmod 4$ и существует разложение

$$q = \pi\overline{\pi} = (a + bj)(a - bj) = a^2 + b^2,$$

где $a, b \in \mathbf{Z}$. Такое разложение может быть выполнено алгоритмом, приведенным в [3].

Если $D = 3$, то уравнение кривой имеет вид $y^2 = x^3 + B$, при этом $O_K = \mathbf{Z}[\omega]$, где ω — примитивный кубический корень из единицы, удовлетворяющий уравнению $\omega^2 - \omega + 1 = 0$. На этой кривой существует отобра-

жение $\sigma(x,y) = (\omega x, -y)$. При $p \equiv 1 \pmod 6$ имеет место $\omega \in \mathbf{F}_p$ и отображение определено на кривой $E(\mathbf{F}_p)$. Предположим, что число точек на кривой свободно от квадратов. Тогда группа точек циклична и существует образующая Q группы порядка q. В этом случае отображение σ действует на точку как умножение на некоторое целое число v. Поскольку $\tau^3(P) = -P$, то $v^3 \equiv -1 \pmod q$ и $v^2 + v + 1 \equiv 0 \pmod q$, $v = \dfrac{1+\sqrt{-3}}{2}$. Ни одна из точек группы порядка q не имеет нулевых координат, следовательно, $q \equiv 1 \pmod 6$ и существует разложение

$$q = \pi\bar{\pi} = (a + bv)(a - bv^2) = a^2 + ab + b^2,$$

где $a, b \in \mathbf{Z}$. Такое разложение может быть выполнено алгоритмом, приведенным в [3]. Для этого сначала следует найти

$$q = \left(m + n\sqrt{-3}\right)\left(m - n\sqrt{-3}\right) = m^2 + 3n^2,$$

а затем искомое разложение.

Комплексное умножение имеет место и для других значений дискриминанта D, например, $D \in \{2, 7, 11, 19, 43, 67, 163\}$, для которых поле $\mathbf{Q}\left(\sqrt{-D}\right)$ имеет число классов 1. Однако формулы комплексного умножения оказываются более сложными. Так, для $D = 2$ кривая имеет уравнение $y^2 = x(x^2 - 4tx + 2t^2)$, где $t \neq 0$. Комплексное умножение на $\sqrt{-2}$ задается изогенией степени 2 [4] и имеет вид

$$(x,y) \to \left(\frac{-y^2}{2x^2}, \frac{y(x^2 - 2t^2)}{2\sqrt{-2}x^2}\right).$$

2. Минимизация показателя для кривой $y^2 \equiv x^3 + Ax \pmod p$, $p \equiv 1 \pmod 4$

Будем рассматривать показатель d как комплексное число $\lambda = c + ej$, где $j^2 \equiv -1 \pmod q$. В группе порядка q показатель можно представлять с точностью до q. Определим норму комплексного числа $\lambda = (c + ej) \in \mathbf{Z}[j]$ как $N(\lambda) = c^2 + e^2$. Поскольку $q = \pi\bar{\pi}$ — разложение на простые множители, то π — простой элемент в $\mathbf{Z}[j]$, кольцо классов вычетов $\boldsymbol{A} = \mathbf{Z}[j]/\pi\mathbf{Z}[j]$ является полем, которое изоморфно $\mathbf{Z}/q\mathbf{Z}$, и поле $\boldsymbol{A}$ может быть вложено в кольцо $\mathbf{Z}[j]$. Тогда из $\lambda \in \mathbf{Z}[j]$ можно вычесть произвольное число $\beta\pi$, где $\beta \in \mathbf{Z}[j]$, при этом вычет по модулю $\pi\mathbf{Z}[j]$ не изменится.

Алгоритм минимизации показателя $\lambda = c + ej$ предусматривает минимизацию нормы $N(\lambda)$. При этом на каждой итерации выбирается наилучшее из двух направлений, вещественное или мнимое, и из текущего

значения α вычитается кратное π или $j\pi$. Отметим, что знаки коэффициентов c, e в разложении показателя d несущественны, так как $(-c)Q = -(cQ)$.

Для вещественного направления $N(\lambda - n\pi) = (c - na)^2 + (e - nb)^2 = N(\lambda) + n^2q - 2n(ac + be)$. Минимум нормы обеспечивается при $n = \left[\frac{ac+be}{q}\right]$, где $[z]$ означает ближайшее целое к числу z. Для мнимого направления $N(\lambda - nj\pi) = (c + nb)^2 + (e - na)^2$. Минимум нормы обеспечивается при $n = \left[\frac{ae-bc}{q}\right]$. Алгоритм останавливается, если в каждом направлении длина шага равна нулю. При этом наибольшее из двух значений $|c|$, $|e|$ не превышает максимума из $|a|$, $|b|$ и меньше, чем $\sqrt{q}$.

1. Исходное состояние: даны a, b, j. Положить $c = d$, $e = 0$.
2. Метод.
   2.1. Для $\lambda = c + ej$ выбрать оптимальный шаг в вещественном направлении, вычислив $n_1 = \left[\frac{ac+be}{q}\right]$ и $N_1 = (c - na)^2 + (e - nb)^2$. Для $\lambda = c + ej$ выбрать оптимальный шаг в мнимом направлении, вычислив $n_j = \left[\frac{ae-bc}{q}\right]$ и $N_j = (c + nb)^2 + (e - na)^2$.
   2.2. Если $n_1 \neq 0$ или $n_j \neq 0$, то выбрать направление, обеспечивающее наименьшее значение нормы. Если $N_1 < N_j$, то положить $c = c - n_1a$, $e = e - n_1b$, иначе положить $c = c + n_jb$, $e = e - n_ja$. Возврат на шаг 2.1.
   2.3. Если $n_1 = n_j = 0$, то стоп.
3. Выход: $\lambda = c + ej$.

Практически достаточно выбрать оптимальное направление только на первом шаге. На втором и последующих шагах направления чередуются: например, если на первом шаге оптимальное направление вещественное, то на втором — мнимое, на третьем — вещественное и т. д.

Пример минимизации показателя. $q = 269$, $a = 13$, $b = 10$, $j = 187$.
Раскладываемое число: $d = 149$.
Начальные значения: $c = 149$, $e = 0$.
Первая итерация. $\lambda = 149 + 0 \cdot j$. Выбираем направление и длину шага n. Для вещественного направления получаем $n = 7$, $\lambda - n\pi = 58 - 70j$, $N(\lambda - n\pi) = 8264$. Для мнимого направления получаем $n = -6$, $\lambda - nj\pi = 89 + 78j$, $(\lambda - nj\pi) = 14005$.

Оптимальным является вещественное направление.

Вторая итерация. $\lambda = 58 - 70j$. Выбираем оптимальную длину шага n в мнимом направлении. Получаем $n = -6$, $\lambda - nj\pi = -2 + 8j$, $N(\lambda - nj\pi) = 68$.

Третья итерация. $\lambda = -2 + 8j$. Выбираем оптимальную длину шага в вещественном направлении: $n = 0$ для вещественного и для мнимого направления. Стоп.

Разложение: $\lambda = -2 + 8j = -2 + 8 \cdot 187 \equiv 149 \pmod{269}$.

Выход: $c = -2$, $e = 8$.

3. Минимизация показателя для кривой $y^2 \equiv x^3 + B \pmod p$, $p \equiv 1 \pmod 6$

Будем показатель d рассматривать как квадратичное целое число $\lambda = c + ev$, где $v \equiv \frac{1+\sqrt{-3}}{2} \pmod q$. В группе порядка q показатель λ можно представлять с точностью до q. Определим норму комплексного числа $\lambda = (c + ev) \in \mathbf{Z}[v]$ как $N(\lambda) = c^2 + ce + e^2$. Поскольку $q = \pi\bar{\pi}$ — разложение на простые множители, то π — простой элемент $\mathbf{Z}[v]$, и кольцо классов вычетов $\boldsymbol{A} = \mathbf{Z}[v]/\pi\mathbf{Z}[v]$ является полем, которое изоморфно $\mathbf{Z}/q\mathbf{Z}$, и поле $\boldsymbol{A}$ может быть вложено в кольцо $\mathbf{Z}[v]$. Тогда из $\lambda \in \mathbf{Z}[v]$ можно вычесть произвольное число $\beta\pi$, где $\beta \in \mathbf{Z}[v]$, при этом вычет по модулю $\pi\mathbf{Z}[v]$ не изменится.

Алгоритм минимизации показателя $\lambda = c + ev$ предусматривает минимизацию нормы $N(\lambda)$. При этом на каждом шаге выбирается наилучшее направление. Существует три возможных направления: 1, v, v^2, из них только два линейно независимых в силу равенства $v^2 + v + 1 = 0$.. Минимизацию можно проводить по любым двум из этих трех направлений.

Для вещественного направления

$$N(\lambda - n\pi) = (c - na)^2 + (c - na)(e - nb) + (e - nb)^2 = \\ = N(\lambda) + n^2 q - n(2ac + 2be + ae + bc).$$

Минимум нормы обеспечивается при $n = \left[\frac{2ac + 2be + ae + bc}{2q}\right]$, где $[z]$ означает ближайшее целое к числу z.

Для направления v:

$$N(\lambda - nv\pi) = (c + nb)^2 + (c + nb)(e - na - nb) + (e - na - nb)^2 = \\ = N(\alpha) + n^2 q - n(2ae + ac + be - bc).$$

Минимум нормы обеспечивается при $n = \left[\frac{2ae + ac + be - bc}{2q}\right]$.

Для направления v^2:

$$N(\lambda - nv^2\pi) = (c + na + nb)^2 + (c + na + nb)(e - na) + (e - na)^2 = \\ = N(\alpha) + n^2q - n(-ac - 2bc + ae - be).$$

Минимум нормы обеспечивается при $n = \left[\frac{-ac - 2bc + ae - be}{2q}\right]$.

Если выбираются направления 1 и v, 1 и v^2, v и v^2, то показатель имеет представление соответственно $d = c + ev$, $d = c + ev^2$, $d = cv + ev^2$. Алгоритм останавливается, если в обоих направлениях оптимальная длина шага — нулевая. При этом наибольшее из значений $|c|$, $|e|$ не превышает $\sqrt{3q}$.

Для направлений 1 и v алгоритм имеет вид:

1. Исходное состояние: даны a, b, v. Положить $c = d$, $e = 0$.
2. Метод.
   2.1. Для $\lambda = c + ev$ выбрать оптимальный шаг в направлении 1, вычислив: $n_1 = \left[\frac{2ac + 2be + ae + bc}{2q}\right]$, $\lambda - n_1\pi = (c - na) + (e - nb)v$, и норму $N(\lambda - n\pi) = (c - na)^2 + (c - na)(e - nb) + (e - nb)^2$.
   Выбрать оптимальный шаг в направлении v, вычислив $n_v = \left[\frac{2ae + ac + be - bc}{2q}\right]$, $\lambda - n_v v\pi = (c + nb) + (e - na - nb)v$, и норму $N(\lambda - nv\pi) = (c + nb)^2 + (c + nb)(e - na - nb) + (e - na - nb)^2$.
   2.2. Если $n_1 \neq 0$ или $n_v \neq 0$, то выбрать направление, обеспечивающее наименьшее значение нормы. Если $N_1 < N_v$, то положить $c = c - n_1a$, $e = e - n_1b$, иначе положить $c = c + n_vb$, $e = e - n_va - n_vb$. Возврат на п 2.1.
   2.3. Если $n_1 = n_v = 0$, то стоп.
3. Выход: $\lambda = c + ev$.

Практически достаточно выбрать оптимальное направление только на первом шаге. На втором и последующих шагах направления чередуются: например, если на первом шаге оптимальное направление 1, то на втором – v, на третьем – 1 и т. д.

Пример минимизации показателя. $q = 331$, $a = 11$, $b = 10$, $v = 32$.
Раскладываемое число: $d = 250$.
Начальные значения: $c = 250$, $e = 0$.
Первая итерация. $\lambda = 250 + 0 \cdot v$. Выбираем направление и длину шага n. Для направления 1: $n = 12$, $\lambda - n\pi = 118 - 120v$, $N(\lambda - n\pi) = 14164$. Для направления v: $n = 0$,

$\lambda - n\nu\pi = 250 + 0\cdot v$, $N(\lambda - n\nu\pi) = 62500$.
Лучшее направление — 1.

Вторая итерация. $\lambda = 118 - 120v$. Для направления v получаем
$n = -6$, $\lambda - n\nu\pi = 58 + 6v$, $N(\lambda - n\nu\pi) = 3748$.

Третья итерация. $\lambda = 58 + 6v$. Для направления 1 получаем: $n = 3$,
$\lambda - n\pi = 25 - 24v$, $N(\lambda - n\pi) = 601$.

Четвертая итерация. $\lambda = 25 - 24v$. Для направления v получаем
$n = -1$, $\lambda - n\nu\pi = 15 - 3v$, $N(\lambda - n\nu\pi) = 189$.

Пятая итерация. $\lambda = 15 - 3v$. Для направления 1 получаем $n = 1$,
$\lambda - n\pi = 4 - 13v$, $N(\lambda - n\pi) = 133$.

Шестая итерация. $\lambda = 4 - 13v$. Для направления v получаем $n = -1$,
$\lambda - n\nu\pi = -6 + 8v$, $N(\lambda - n\nu\pi) = 52$.

Седьмая итерация. $\lambda = -6 + 8v$. Для направления 1 получаем $n = 0$,
$\lambda - \alpha\pi = -6 + 8v$, $N(\lambda - n\nu\pi) = 52$.
Стоп.

Итоговое разложение: $\lambda = -6 + 8v = -6 + 8 \cdot 32 \equiv 250 \pmod{331}$.
Выход: $c = -6$, $e = 8$.

Предложенный способ минимизации показателя d можно использовать и для других типов кривых с комплексным умножением, например, для кривых с $D \in \{2, 7, 11, 19, 43, 67, 163\}$ и для кривых над конечным расширенным полем с комплексным умножением на собственное значение эндоморфизма Фробениуса.

Литература

1. N. Koblitz. A course in number theory and cryptography. — Springer-Verlag, 1987.
2. J. Pollard. A Monte Carlo method for index computation (mod p) // Math. Comp., v. 32, 1978, pp. 918–924.
3. J. Pollard, C. Schnorr. An efficient solution of the congruence $x^2 + ky^2 = m \pmod{n}$ // IEEE Transactions on Information Theory, v. IT–33, 1987, pp. 702–709.
4. D. Husemöller. Elliptic curves. — Graduate texts in mathematics, v. 111, Springer-Verlag, 1986.