А. Г. Ростовцев

Арифметика эллиптических кривых над простыми полями без удвоения точек

Эллиптические кривые над конечными полями являются наиболее перспективной структурой для построения криптографических алгоритмов. Длительность выполнения криптографического примитива определяется длительностью умножения точки на число. Традиционно эта процедура выполняется путем сложений и удвоений точек. Для умножения точки P на число k последнее представляется в двоичном виде: $k = \sum_{i=0}^{n-1} k_i 2^i$, цепочки из нескольких стоящих подряд единиц заменяются в соответствии с формулой $1 + 2 + 2^2 + ... + 2^m = -1 + 2^{m+1}$, вычисляются точки 2^iP и складываются с учетом коэффициентов k_i. При этом число удвоений примерно в три раза превосходит число сложений, и вклад длительности удвоений в длительность умножения точки на число является определяющим.

Использование комплексного умножения, например, для кривых со значениями j-инварианта 0 или 1728, позволяет вдвое сократить число удвоений [1] и за счет этого примерно в 1,5 раза увеличить скорость выполнения криптографических примитивов по сравнению с кривыми общего вида.

Эллиптические кривые над полем характеристики 2, имеющие коэффициенты из поля $\mathbf{F}_2$, позволяют заменить операцию удвоения операцией комплексного умножения на собственное значение эндоморфизма Фробениуса: $(x, y) \to (x^2, y^2)$. Однако арифметика поля характеристики 2 неудобна для программной реализации (операцию умножения многочленов нужно задавать с использованием многочисленных сложений и сдвигов). Кроме того, число кривых с хорошими криптографическими свойствами очень невелико и стойкость криптоалгоритмов на таких кривых несколько ниже, чем на кривых над простыми полями близкого размера. Эти обстоятельства ограничивают возможное применение таких кривых.

Существует многочисленный класс эллиптических кривых над конечными полями, обладающий комплексным умножением, в котором можно отказаться от удвоения точек, заменив его другой более простой операцией. Это эллиптические кривые с комплексным умножением, для которых порядок подгруппы, образованной операцией комплексного умножения, не фиксирован [2]. Наиболее простой вид комплексное умножение имеет для кривой вида

$$y^2 = x^3 - 4tx^2 + 2t^2x \pmod{p}, \qquad (1)$$

здесь переход к скрученной кривой задается умножением коэффициента t на квадратичный невычет. Обычно можно положить $t = \pm 1$. Число точек на этой кривой равно $p + 1 \pm 2a$, где $p = a^2 + 2b^2$. Умножение на мнимое число $\varphi = \sqrt{-2}$ задается рациональным отображением:

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

В случае проективной кривой $Y^2Z = X^3 - 4tX^2Z + 2t^2XZ^2$ формулы комплексного умножения примут вид:

$$\varphi(X_1, Y_1, Z_1) = \sqrt{-2}(X_1, Y_1, Z_1) = (X_2, Y_2, Z_2),$$

где

$$X_2 = Y_1^2 Z_1,\ Y_2 = Y_1 \sqrt{-2}^{-1} (X_1^2 - 4t^2 Z_1^2),\ Z_2 = 2X_1^2 Z_1.$$

Умножение точки на число φ требует выполнения 7 умножений в поле $\mathbf{F}_p$, тогда как удвоение точки требует выполнения 12 таких умножений.

Пусть r — большой простой порядок группы точек кривой (1). Для того чтобы исключить операцию удвоения, показатель d нужно представить как многочлен степени не более $\log_2 r$ от переменной φ с коэффициентами из множества (0, 1, –1). Покажем как это можно сделать.

Сначала найдем представление порядка группы как многочлена указанного вида. Поскольку в кольце классов вычетов $\mathbf{Z}/r\mathbf{Z}$ определено умножение на φ, существует разложение числа r на простые множители в кольце $\mathbf{Z}[\varphi]$:

$$r = c^2 + 2d^2 = (c + d\sqrt{-2})(c - d\sqrt{-2}) = \rho\bar{\rho} \qquad (2)$$

и существует вычислимый гомоморфизм из $\mathbf{Z}[\varphi]$ в $\mathbf{Z}/r\mathbf{Z}$ путем подстановки φ вместо числа $\sqrt{-2}$. Это разложение может быть вычислено с кубической сложностью от $\log_2 r$, длина каждого из чисел c, d менее $0{,}5\log_2 r$, а их суммарная длина — менее $\log_2 r$. При гомоморфизме один из комплексных сомножителей в (2) дает 0 (mod r). Предположим, что это ρ. Выстроим поочередно двоичные коэффициенты при c, d в цепочку справа налево:

$$\ldots, d_3, c_3, -d_2, -c_2, -d_1, -c_1, d_0, c_0,$$

получим искомое представление длины не более $\log_2 r$ бит.

Имеет место следующее утверждение.

Теорема. Любой показатель k такой, что $0 < k < r$, можно представить как многочлен от φ такой, что степень многочлена не более $\log_2 r$, а коэффициенты равны 0, 1 или –1.

Доказательство. Значение $k \pmod r$ не изменится, если к нему прибавить число $n\rho$ или $m\varphi\rho$ для произвольных целых m, n. Для комплексных чисел $k = k_0 + k_1\varphi$ и начального значения $k_0 = k$, $k_1 = 0$, находим вычет по модулю решетки с базисом $(c, d\varphi)$ такой, что норма $k_0^2 + 2k_1^2$ комплексного числа k минимальна. Для этого на каждом шаге находим такие m, n, для которых норма числа $k - n\rho$, $k - m\varphi\rho$ минимальна. Число шагов алгоритма в среднем равно 2. Алгоритм останавливается, когда число $k_0 + k_1\varphi$ попадает внутрь параллелограмма с r точками, концентрично вписанного в эллипс $u^2 + 2v^2 = r$. Очевидно, что при этом суммарная длина коэффициентов k_0, k_1 не превышает $\log_2 r$. Теорема доказана. ■

Следствие. При замене операции удвоения в процедуре умножения точки на число операцией комплексного умножения суммарное число комплексных умножений не превышает число удвоений.

Построение некоторых криптографических алгоритмов (цифровой подписи на основе протокола Эль-Гамаля, бесключевого шифрования Месси — Омуры и др.) требует выполнения операции обращения по модулю порядка группы.

Для чисел, представленных по основанию φ как многочленов над $\mathbf{F}_2$ от φ, существует φ-арный аналог бинарного алгоритма Евклида. При нахождении наибольшего общего делителя многочленов A и B, представленных как многочлены над $\mathbf{F}_2$ от φ, если хоть один из них имеет нулевой младший коэффициент, то происходит деление этого многочлена на φ (сдвиг вектора коэффициентов), в противном случае из большего многочлена вычитается меньший. Для того чтобы сохранить коэффициенты из $\mathbf{F}_2$, полученная разность рассматривается как комплексное число, которое переводится в пару двоичных чисел, а затем — в φ-адическое число. Далее процедура рекурсивно повторяется.

Расширенный φ-арный аналог бинарного алгоритма Евклида также аналогичен расширенному бинарному алгоритму Евклида.

Таким образом, операцию умножения точки на число для эллиптической кривой (1) можно реализовать без удвоения точек, то есть так же, как и для кривых над полем характеристики 2 с комплексным умножением на собственное значение эндоморфизма

Фробениуса. Кроме того, операцию модульного обращения можно выполнять, не выходя за рамки φ-адического представления. Это позволяет примерно в 1,5 раза повысить скорость программно реализованных криптографических алгоритмов по сравнению с кривыми без комплексного умножения. В отличие от кривых со значениями $j = 0$, 1728, также обладающих комплексным умножением, и кривых над расширенными полями с умножением на собственное значение эндоморфизма Фробениуса, орбита циклической группы, образованной автоморфизмом φ в кольце эндоморфизмов кривой (1), не является перечислимым множеством. Поэтому наличие комплексного умножения не снижает сложность вычисления логарифма в группе точек кривой (1), в отличие указанных выше кривых.

Литература

1. Ростовцев А. Г. Алгебраические основы криптографии. — СПб., Мир и Семья, 2000.
2. Ростовцев А. Г., Маховенко Е. Б. Введение в криптографию с открытым ключом. — СПб., Мир и Семья, 2001.