XXXIII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V: С.138-140, 2005.
© Санкт-Петербургский государственный политехнический университет, 2005.

УДК 50.41.00, 50.37.23

О.В.Шемякина (4 курс, каф. ИБКС), А.Г.Ростовцев, д.т.н., проф.

ИСПОЛЬЗОВАНИЕ КОММУТАТИВНОСТИ ИЗОГЕНИЙ В КРИПТОГРАФИИ С ОТКРЫТЫМ КЛЮЧОМ

Эллиптические кривые – одни из самых перспективных инструментов для построения криптографических алгоритмов. Криптографические алгоритмы, действующие на группе точек эллиптических кривых, являются наиболее стойкими алгоритмами криптографии с открытым ключом. Однако криптографические алгоритмы можно строить и на отображениях эллиптических кривых. Криптосистемы, основанные на вычислении алгебраических отображений (изогений) эллиптических кривых, представляются стойкими по отношению к квантовому компьютеру. Кроме того, использование изогений позволяет реализовать принципиально новые протоколы (например, протокол упорядоченной подписи).

Эллиптическая кривая $E(K)$ над полем K характеристики, отличной от 2 и 3, задается уравнением $y^2 = x^3 + Ax + B$, где полином в правой части не имеет кратных корней в K. Инвариант эллиптической кривой равен $j = \frac{12^3 4A^3}{4A^3 + 27B^2}$. Эллиптическая кривая задается своим j-инвариантом с точностью до изоморфизма.

Пусть E_1 и E_2 – эллиптические кривые. Изогенией называется отображение (задаваемое парой рациональных функций), переводящее бесконечно удаленную точку кривой E_1 в бесконечно удаленную точку кривой E_2. Если такое отображение существует, кривые называются изогенными.

Эллиптические кривые являются изогенными над алгебраически замкнутым полем тогда и только тогда, когда они имеют одинаковое число точек.

Ядро изогении – множество точек на кривой, которые переходят в бесконечно удаленную точку.

Композиция изогений определяется как композиция отображений.

Для каждой изогении $\varphi: E_1(K) \to E_2(K)$ существует дуальная изогения $\hat{\varphi}: E_2(K) \to E_1(K)$. При этом $\hat{\varphi}\ (\varphi) = [l]$ – оператор умножения точки на целое l на кривой E_2, $\varphi\ (\hat{\varphi}) = [l]$ – оператор умножения точки на целое l на кривой E_1, а число l является степенью изогении.

Точки из ядра изогении при отображении φ перейдут в бесконечно удаленную точку кривой E_2, которая при дуальном отображении $\hat{\varphi}$ по определению изогении перейдет в бесконечно удаленную точку кривой E_1. С другой стороны, как было сказано выше, композиция этих отображений является умножением точек на число l. Таким образом, ядро изогении состоит из точек конечного порядка l (точек кручения).

Справедлива следующая теорема.

Теорема. Мощность ядра изогении равна ее степени: $\#\mathrm{Ker}(\varphi) = l$, если $\deg(\varphi) = l$.

Пусть E_1 и E_2 – эллиптические кривые. Изогения $E_1 \square E_2$ является алгебраическим гомоморфизмом эллиптических кривых как абелевых групп, который определяется ядром, мощность которого равна степени изогении. Если порядок r подгруппы $E_1(K)$ взаимно прост со степенью изогении, то изогения задает изоморфизм групп порядка r.

Хотя нас интересуют эллиптические кривые над конечными полями, необходимо рассмотреть свойства кривых над полем комплексных чисел. При этом все факты остаются справедливыми и для других полей.

Эллиптическая кривая над полем комплексных чисел определяется решеткой, которая (с учетом масштабирования, если потребуется) задается парой комплексных чисел $(1, \tau)$. Кривые, изоморфные данной, задаются парами $(1, \gamma\tau)$, где γ – матрица с единичным определителем. При этом j-инвариант кривой является функцией от τ, т.е. $j = j(\tau)$, обладающей следующими свойствами:

$$j(\tau) = j(\tau + 1), \tag{1}$$

$$j(\tau) = j(-1/\tau). \tag{2}$$

j-инварианты (l+1) кривой, l-изогенной данной, выражаются через j-инвариант исходной кривой следующим образом:

$$j(l\tau), j(\frac{\tau + k}{l}), \text{ где } k = 0, 1, \ldots l - 1. \tag{3}$$

Можно определить l-й модулярный полином $\Phi_l(X, j(\tau))$ как

$$\Phi_l(X, j(\tau)) = (X - j(l\tau)) \prod_{k=0}^{l-1} (X - j(\frac{\tau + k}{l})).$$

Для данной эллиптической кривой с j-инвариантом $j(\tau)$ корни полинома $\Phi_l(X, j(\tau))$ являются j-инвариантами всех кривых, l-изогенных данной.

Далее рассматриваются эллиптические кривые над конечными полями, поскольку именно они имеют практическое применение в криптографии. Введем понятия следа и дискриминанта Фробениуса.

Пусть кривая E задана над полем $\mathbf{F}_p$, и число точек на кривой равно $\#E(\mathbf{F}_p)$. Тогда след эндоморфизма Фробениуса определяется как $t = p + 1 - \#E(\mathbf{F}_p)$, а дискриминант эндоморфизма Фробениуса $D = t^2 - 4p$.

Над полем $\mathbf{F}_p$ может существовать 0, 1, 2 или $l + 1$ кривая, l-изогенная данной в зависимости от символа Лежандра $\left(\frac{D}{l}\right)$:

если $\left(\frac{D}{l}\right) = -1$ (D является квадратичным невычетом по модулю l), то не ни одного корня;

если $\left(\frac{D}{l}\right) = 1$ (D является квадратичным вычетом по модулю l), то существует 2 корня;

если $\left(\frac{D}{l}\right) = 0$ (D делится на l), то существует либо один, либо l + 1корень.

Композиция изогений ассоциативна как композиция отображений. Для построения многих протоколов на изогениях эллиптических кривых обычно требуется коммутативность изогений разных степеней.

Теорема. Композиция изогений двух простых степеней коммутативна.

Для доказательства используются формулы (3), а также свойство (1) модулярной функции $j(\tau)$.

Следствие 1. Композиция изогений произвольного числа простых степеней коммутативна.

Доказательство проводится по индукции. Базой индукции является доказанная теорема.

Данная теорема позволяет использовать циклы изогенных эллиптических кривых для построения криптографических алгоритмов, а также определяет изогении составных степеней как композицию изогений простых степеней.

Коммутативность композиции изогений позволяет строить криптографические протоколы — аналоги протоколов Диффи-Хеллмана, Эль-Гамаля.

Следствие 2. Если порядок r подгруппы $E(K)$ взаимно прост со степенью каждой изогении, то композиция изогений задает изоморфизм групп порядка r эллиптических кривых над алгебраически замкнутым полем. Этот факт может быть использован в криптоанализе, когда соответствующая задача решается на любой из изогенных кривых.