Защита информации

Павел Юдаев

МГТУ им. Баумана, Кафедра ИУ-9

Москва, 2014

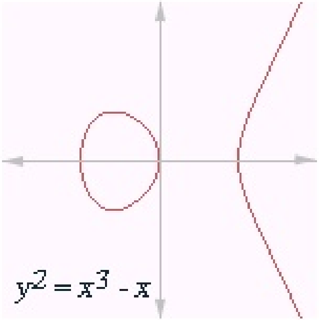
Раздел 20 - Криптография на эллиптических кривых

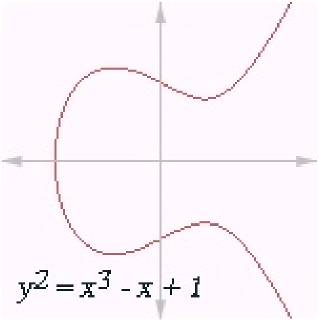
Эллиптическая кривая (над полем F) - гладкая кривая, зад. ур-ем вида
$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in F$

Гладкая - в $F \times F$ нет точек кривой (x, y), где равны нулю обе частные производные.

Если хар-ка поля F не равна 2 или 3, то заменой коорд. приходим к выражению (встречается деление на 2 и на 3)
$y^2 = x^3 + ax + b$

Условие гладкости превращается в условие, что куб. мн-н справа не имеет кратных корней.





над $\mathrm{R}x\mathrm{R}$
слева - Дискриминант > 0, две непр. компоненты;
справа - Д < 0, одна компонента.

Дискриминант эл.кривой опр-ся для ур-я кривой в общем виде; при хар-ке поля не равной 2 или 3 он равен дискр-ту правой части
$\Delta = -4a^3 - 27b^2$. Условие гладкости эквив. тому, что $\Delta \neq 0$.

(Дискр-т многочлена равен $a_n^{2n-2} \cdot \prod(\alpha_i - \alpha_j)^2$ для всех корней α_i, α_j.)

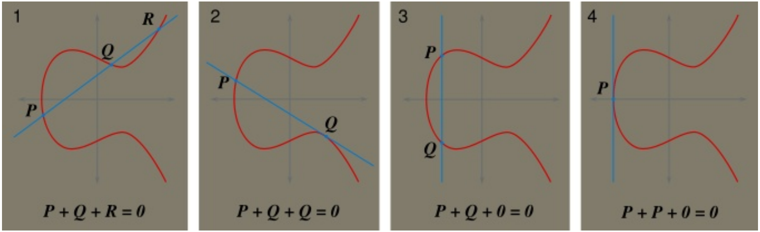
При хар-ке 2, либо
$y^2 + y = x^3 + ax + b$ (суперсингулярные) либо
$y^2 + xy = x^3 + ax + b$ (несуперсингулярные).

Структура группы точек эл. кривой

Рассм. эл. кривую над $K = F_q$:
$E(K) = \{(x, y) \in F_q \times F_q : y^2 = x^3 + ax + b\} \cup \{0\}$

Определим груповую операцию (наз. ее сложением):
1) P = 0 => -P = 0, P + 0 = P.
2) P = (x,y) => -P = (x, -y). Это согласуется с тем, что в F_q у любого эл-та либо есть два кв. корня (два корня у y^2), либо ни одного.
3) прямая PQ пересекает кривую в точке R, => P + Q = -R.
4) прямая PQ - касательн. в т. P (или Q) => P + Q = 2P = -R
R - единств. другая точка пересечения или 0, если таких нет.

Рисунок: сложение точек на эл. кривой



Формула сложения, $Char(F) \neq 2, 3$:
$P = (x_1, y_1), Q = (x_2, y_2), P + Q = (x_3, y_3)$:

Пусть ур-е прямой PQ: $y = \lambda x + \beta$. Тогда все (x_i, y_i) уд. ур-ю $x^3 - (\lambda x + \beta)^2 + ax + b = 0$. Сумма корней мн-на равна коэфф. при второй старшей степени (здесь - при x^2), значит
$x_3 = \lambda^2 - x_1 - x_2$,
$y_3 = \lambda(x_1 - x_3) - y_1$,

угол наклона прямой PQ
$\lambda = (y_2 - y_1)/(x_2 - x_1)$, $P \neq Q$
$\lambda = (3x_1 + a)/(2y_1)$, $P = Q$.

В случае наличия у кривой особых точек (обе част. пр-е = 0) понятие касательной в них не опр. и операция сложения не им. смысла.

Для полей хар. 2 - другие ф-лы: (хар. 3 - не рассм. в этом курсе)
Несуперсингулярная кривая

$$x_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a_2,$$
$$y_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1 + x_3) + x_3 + y_1,$$

при сложении различных точек и

$$x_3 = x_1^2 + a_6/x_1^2,$$
$$y_3 = -x_1^2 + \left(\frac{x_1+y_1}{x_1}\right)x_3 + x_3,$$

при удвоении.

Суперсингулярная кривая

$$x_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + x_1 + x_2,$$
$$y_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1 + x_3) + y_1 + a_3,$$

при сложении различных точек и

$$x_3 = \frac{x_1^4+a_4^2}{a_3^2},$$
$$y_3 = \left(\frac{x_1^2+a_4}{a_3}\right)(x_1 + x_3) + y_1 + a_3,$$

при удвоении.

Задача

Пусть P = (0,0) на э.к. над R $y^2 + y = x^3 - x^2$.
Найти 2P, 3P.

Решение.
Сначала преобразуем к каноническому виду:
Л.ч. должна быть y^2. Ищем линейную замену пер-й: $y \mapsto t$.
$y^2 + y \mapsto t^2 + 0 \cdot t + c$
$\Rightarrow y = t - 1/2$.
Аналогично для п.ч., $x = u + 1/3$.

Канонич. вид:
$y^2 = x^3 - 1/3 * x + (1/4 - 2/27)$

P $\mapsto$ Q = (-1/3, 1/2). 2Q = (2/3, -1/2). 3Q = 2Q + Q = (2/3, 1/2). Заодно заметим, что 2Q = -3Q,
значит точка Q имеет порядок 5: 5Q = 0.

Возвр. к исходной кривой:
2P = (1, -1), 3P = (1, 0) = -2P. Заметим, что при неканонич. уравнении кривой, не вып. правило -(x, y) = (x, -y).

Теорема 1

Мн-во точек эл. кривой - абелева группа.

Док-во

0 - нейтр. элемент. Коммутативность - очевидно из опр. групповой операции. Ассоциативность - сложно, без док-ва.

Очевидно, каждая точка P э.к. порождает циклическую подгруппу $< P >$.

Теорема 2 (Теорема Хассе)

$\big||E(F_p)| - p\big| < 2\sqrt{p} + 1$, p - порядок поля.

Без док-ва.

Задача

найти порядок точки P = (2,3) на $y^2 = x^3 + 1$ над R.

Решение: Находим 2P = (0,1); 4P = 2·2P = (0,-1) = -2P. След., 6P = 0.

Значит, порядок P - делитель числа 6. Известно, что 2P $\neq$ 0. Прямой проверкой убежд., что 3P = 2P + P $\neq$ 0. Значит, порядок P равен 6.

Как искали 2P: угол наклона касательной в точке P есть
$\lambda = \frac{dy}{dx}\Big|_P = \frac{2y}{3x^2}\Big|_P = \frac{6}{12} = \frac{1}{2}$

Значит, точка пересечения касательной и кривой есть точка вида
R = (2,3) + (d, 2d). Подставляем в ур-е кривой,
находим d = -2, R = (0, -1). Значит 2P = -R = (0,1).

Раздел 20 - Криптография на эллиптических кривых

Для суперсингулярных кривых точно известен их порядок. Более того, для $GF(2^n)$ при n - нечет., сущ. 3 класса неизоморфн. с/с кривых:

$$E_1: \; y^2 + y = x^3$$
$$E_2: \; y^2 + y = x^3 + x$$
$$E_3: \; y^2 + y = x^3 + x + 1$$

При нечетном n группы циклические.

Для криптографии представляют интерес, в частности, кривые E_2 и E_3 и такие n, при которых порядок группы $E(K)$ в качестве сомножителя содержит большое простое число (макс. простой сомножитель определяет сложность задачи дискр. логарифмирования в конечном поле).

Вообще, RSA опубликовала список эл. кривых, рекомендованных к использованию в криптографии. (Обесп. приемлемую стойкость и допускают быструю реализацию операций.)

Пример: (не обяз. из списка RSA)

n	Кривая	Порядок группы
173	$\mathcal{E}_2$	$5 \cdot 13625405957 \cdot P42$
173	$\mathcal{E}_3$	$7152893721041 \cdot P40$
191	$\mathcal{E}_2$	$5 \cdot 3821 \cdot 89618875387061 \cdot P40$
191	$\mathcal{E}_3$	$25212001 \cdot 5972216269 \cdot P41$
239	$\mathcal{E}_2$	$5 \cdot 77852679293 \cdot P61$
239	$\mathcal{E}_3$	$P72$
323	$\mathcal{E}_3$	$137 \cdot 953 \cdot 525313 \cdot P87$

Для задачи дискр. логарифмирования в конечном поле $GF(p) = \mathbb{Z}_p$ не изв. полиномиальных алгоритмов, изв. субэксп. алгоритмы.
В группе точек эл. кривой не изв. субэксп. алгоритма дискр. логарифма для больших показателей. Только эксп. сложность.

Это позволяет уменьшить размер ключа по сравнению с системами, использующими операции в $GF(p) = \mathbb{Z}_p$, при той же криптостойкости.

Раздел 20 - Криптография на эллиптических кривых

Оптимизация операций в группе точек суперсингулярной э.к. над $GF(2^n)$

Как известно, при сложении точек вып. операция обращения. Она медленная в конечном поле. Надо минимизировать кол-во сложений. Зато операция удвоения обходится без обращения.

Решение: вместо выч. kP "в лоб" , разложить натур. число k в сумму степеней двойки. Таким образом, даже в худшем случае $(k = 2^t - 1)$ число сложений будет не $k - 1$, а $log(k)$.

Ускорим операцию сложения.

Проективные координаты.

Позволяет исключить операцию инверсии при сложении.

Подстановка X = x/z, Y = y/z. Переход от пар (x, y) к тройкам (x, y, z).

=> ур-я $E_2: \ y^2z + yz^2 = x^3 + xz^2$
$E_3: \ y^2z + yz^2 = x^3 + xz^2 + z^3$

Проективные координаты считаются эквивалентными, если $\exists t \neq 0 : (x, y, z) \sim (tx, ty, tz)$.

След., имеем класс эквивалентности $(x : y : z)$. Мн-во всех кл-в экв-тей наз. проективными координатами. Геометрически (двумерное) проективное пространтсво можно предст. себе как мн-во прямых в обычном 3-мерном пр-ве, прох. через начало координат.

Теперь рассм E(K) - мн-во точек проективной плоскости, уд. ур-ю э.к. Единств. точкой с нулевой коорд. z явл. O = (0, 1, 0) - соотв. беск. уд. точке, 0 группы точек э.к.

Для ост. точек $(x : y : z) \sim (x/z : y/z : 1)$, откуда следует вз. одн. соотв-е (x:y:z) и (x/z, y/z).

Тогда можно вывести ф-лу сложения для точек E_2 или E_3:
$P = (x_1 : y_1 : 1),\ Q = (x_2, y_2, z_2), R = P + Q = (x_3, y_3, z_3)$.

Пусть $P \neq Q, P \neq 0, Q \neq 0$. Тогда (вывод опустим)
$x_3 = a^2 b z_2 + b^4$,
$y_3 = (1 + y_1) z_3 + a^3 z_2 + a b^2 x_2$,
$z_3 = b_3 z_2$

По сравнению с исп. аффинных (обычных) коорд. увеличилось число умножений, зато ни одного обращения.

Алгоритм: при выч. kP раскладываем k в сумму степеней 2, вычисляем эти точки (вида $2^t P$), затем складываем их с исп. проективных координат. Окончат. рез-т преобр. в аффинные делением на z_3 - одна инверсия в самом конце.

Раздел 20 - Криптография на эллиптических кривых

Э. к. над конечными полями используются в некоторых криптографических приложениях и факторизации.

Основная идея, заложенная в этих приложениях, заключается в том, что известный алгоритм, используемый для конкретных конечных групп переписывается для использования групп рациональных точек эллиптических кривых

1. RSA, DSA, DH с эллиптическими кривыми

2*. ЭЦП - ГОСТ Р 34.10-2001

3*. Факторизация с помощью эллиптических кривых Ленстры

Модификации существующих криптосистем

Большинство криптосистем современной криптографии естественным образом можно "переложить" на эллиптические кривые.

- Э.к. рассм. над кольцом вычетов по составному модулю $n = pq$.
- Порядок группы точек э.к. для спец. кривых равен $(p + 1)(q + 1)$.
- Случайный выбор э.к. - пар-ры э.к. a, b не зад-ся польз-лем, а зависят от выбранного польз-лем случ. числа y.
- Параметр a легко находится с помощью расширенного алгоритма Евклида по одной заданной точке (x, y) из э.к.
- Для операций с точками кривой знать пар-р кривой b не нужно.

Аналог RSA на э.к.

В варианте RSA на эллиптических кривых есть ограничения на вид э.к. и вид чисел p, q.

Шаг алг-ма	Исх. алг-м	Алг-м на э.к.
опред модуля, n	A выбир. простые p,q, выч. n = pq	так же
Генерация случайным образом открытого ключа e. Алиса отправляет всем пару (n,e)	e вз. простое с $(p-1)(q-1)$, $1 < e < n$	e вз просто с $(p+1)(q+1)$, $1 < e < n$
A выч. з.к. d	$d \equiv e^{-1} \bmod ((p-1)(q-1))$	$d \equiv e^{-1} \bmod ((p+1)(q+1))$
B выч. шифротекст C, отпр. его A	$C \equiv M^e \bmod (n)$	C=e(M,y), (M, y)-точка э.к.
A расш.шифротекст	$M \equiv C^d \bmod (n)$	$(M, y) = dC$

Аналог с-мы D-H на э.к.

Шаг алг-ма	Исх. алг-м	Алг-м на э.к.
Определение группы (кривой) и базового эл-та. A отпр. B:	Большое простое p и случайное g: 1<g<p	Э. к. и случайную точку G на ней
A выбирает случ. число a и отправляет B:	Число $g_a \equiv g^a \bmod (p)$	Точку $G_a = aG$
B выбирает случ. число b и отправляет A:	Число $g_b \equiv g^b \bmod (p)$	Точку $G_b = bG$
A выч.	Секретное число $k \equiv g_b^a \bmod (p)$	Секретную точку $K = aG_b$
B выч.	Секретное число $k \equiv g_a^b \bmod (p)$	Секретную точку $K = bG_a$
A, B обл. одним секретом (проверка тривиальна)		

EC DSA

Параметры алгоритма

1. хэш-функции H(x). (SHA-256 и т.д.)
2. q - число эл-в поля
3. a,b - эл-ты поля, опр. ур-е э.к.
4. G - базовая точка э.к.
5. n - порядок G (простое число), L - его длина в битах

d - с.к. А, случ. целое из [1 .. n-1]
Q - о.к. А, Q = dG

А подписывает сообщ. М:
1. e = H(M), z - его левые L бит
2. А выбир. случ. секр. k из [1 .. n-1] - nonce
3. А выч $(x_1, y_1) = kG$, $r \equiv x_1 \bmod n$. если r=0, возвр. на шаг 2
4. А выч. $s \equiv k^{-1}(z + rd) \bmod n$. Если s=0, возвр. на шаг 2
5. подпись - это пара (r,s)

Необходимость секретности k очевидна. Уникальность?

Пусть были генерир. две подписи (r,s) and (r,s'), с исп. одного и того же неизв. k для разных изв. сообщ. M and M'. Злоумыш. может выч-ть z and z'.
Т.к. $s - s' \equiv k^{-1}(z - z') \bmod n$ то злоумыш. находит $k \equiv z - z's - s'^{-1} \bmod n$.

Т.к. $s \equiv k^{-1}(z + rd) \bmod n$, злоумыш. выч-ет с.к. $d \equiv sk - zr^{-1} \bmod n$.

Этот прием был использ. для взлома с.к., исп. в Sony PlayStation 3.

Проверка подписи

В может проверить, допустим ли о.к. Q:
1. пров., что $Q \neq O$
2. что Q лежит на кривой
3. что $nQ = O$

Сама проверка подписи:

1. r и s должны быть из [1,n - 1].
2. e = H(M), z равно L самых левых битов e.
3. $w \equiv s^{-1} \bmod n$.
4. $u_1 \equiv zw \bmod n$ и $u_2 \equiv rw \bmod n$.
5. $(x_2, y_2) = u_1 G + u_2 Q$.
6. Подпись верна, если $r \equiv x_2 \bmod n$, иначе не верна.

Корректность подписи

$(x_2, y_2) = u_1 G + u_2 Q = (s^{-1}z + s^{-1}rd)G$
По построению, $k \equiv s^{-1}(z + rd) \bmod n$, $ord(G) = n$
$\Rightarrow (x_2, y_2) = kG = (x_1, y_1)$.

Литература к лекции

1. Болотов, *Алгоритмические основы эллиптической криптографии*, 2000, главы 3,4

2*. Болотов, *Алгоритмические основы эллиптической криптографии*, 2004, параграф 1.3

3*. Левин, Носов, *Анализ повышения криптографической сложности систем при переходе на эллиптические кривые*