

---

---

# ЛЕКЦИЯ 7

---

## ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

**Эллиптические кривые** — это математический аппарат, который часто используется в различных алгоритмах шифрования. Он имеет ряд преимуществ: при использовании эллиптических кривых повышается защищённость на ключа один бит по сравнению с обычными алгебраическими операциями (например, вычисление вычетов по какому-нибудь большому модулю). Также эллиптические кривые хорошо реализуются при аппаратной и программной реализации. Поскольку множества, построенные на эллиптических кривых, являются группой, то эти множества можно использовать, не меняя алгоритм в таких шифрах, как RSA и Elgamal.

### 1. Группы

Понятие групп играет важную роль в этой теме. **Группа** — это множество точек с определённой операцией. Эти операции обладают важными свойствами: замкнутостью, ассоциативностью. В этом множестве существует единичный элемент (или нейтральный элемент). Каждый ненулевой элемент этого множества имеет обратный по отношению к себе.

Важной характеристикой группы является её порядок. **Порядок** — это количество элементов в данной группе.

Также важным подмножеством групп являются группы, которые являются циклическими. **Циклической группой** называется такая группа, которая состоит из степеней одного элемента. При этом наименьшее число  $m$  такое, что какой-то элемент в степени  $m$  равняется единичному элементу, является **порядком элемента**.

### 2. Множество точек эллиптической кривой

Эллиптическая кривая задаётся аналитическим уравнением, имеющим общий вид:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Будут рассматривать только те кривые, которые приводимы к **канонической форме**.



Конспект не проходил проф. редактуру, создан студентами и, возможно, содержит смысловые ошибки. Следите за обновлениями на [lectoriy.mipt.ru](http://lectoriy.mipt.ru).

ме (forme Вейерштрасса):

$$y^2 = x^3 + ax + b.$$

Можно вычислить дискриминант от параметров  $a$  и  $b$ . Введём дополнительное ограничение на отсутствие особых точек: если  $x_1, x_2, x_3$  — корни уравнения

$$x^3 + ax + b = 0,$$

то потребуем:

$$D = (x_1 - x_2)^2(x_1 - x_3)^2(x_3 - x_2)^2 \neq 0,$$

$$D = -16(4a^3 + 27b^2) \neq 0.$$

Если дискриминант больше нуля, множество изображается графиком, состоящим из двух частей. Есть область, в которой содержится разрыв.

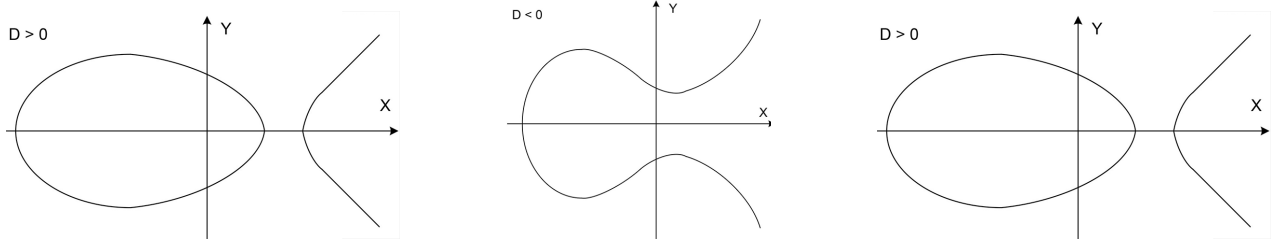


Рис. 7.1

Если дискриминант меньше нуля, то график состоит из одной части. Если дискриминант равен нулю, то у графика появляются особые точки (этот случай рассматривать не будем, также, как и случай, когда дискриминант больше нуля).

Практикам интересен случай, когда дискриминант меньше нуля, то есть когда кривая состоит из одной части.

Рассмотрим частный случай такой кривой. Пусть эллиптическая кривая  $E$  задаётся уравнением:

$$y^2 + y = x^3 - x^2.$$

Будем брать точки, координаты которых являются целыми числами. Тогда получим 4 точки (эти 4 точки равнозначны между собой).

В качестве **нулевого элемента** берётся точка в бесконечности. Считается, что её координаты:  $(\infty, \infty)$ .

Более того, для этой точки вводится **аксиома**: любая вертикальная прямая где-то в бесконечности будет пересекать эту точку.

Также вводится ещё одна **аксиома**: касательная к кривой пересекает данную кривую в точке касания два раза.

### 3. Операция сложения

На кривой выбраны точки  $P$  и  $Q$ .

Сумму можно найти следующим образом: пусть  $S$  — точка пересечения прямой, которая проходит через точки  $P$  и  $Q$ . Но точка пересечения  $S$  с эллиптической кривой — это третья точка.



Для подготовки к экзаменам пользуйтесь учебной литературой. Об обнаруженных неточностях и замечаниях просьба писать на [pulsar@phystech.edu](mailto:pulsar@phystech.edu)

**!** Конспект не проходил проф. редактуру, создан студентами и, возможно, содержит смысловые ошибки. Следите за обновлениями на [lectoriy.mipt.ru](http://lectoriy.mipt.ru).

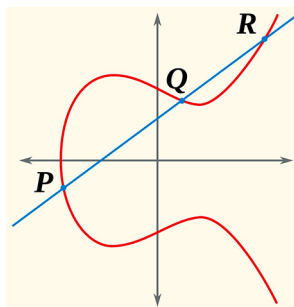


Рис. 7.2

Проведем прямую через два слагаемых (две точки) и найдём пересечение. Далее проведем через точку  $S$  вертикальную прямую. Эта вертикальная прямая пересечёт кривую в четвёртой точке, которая и считается суммой.

Эта операция является коммутативной: две точки создают одну прямую, в результате чего получается всегда одна и та же точка  $S$ , а дальше построения аналогичны.

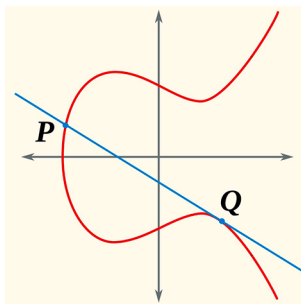


Рис. 7.3

Рассмотрим точки  $P$  и  $Q$ , расположенные на эллиптической кривой. Чтобы найти их сумму, нужно провести прямую. Если эта прямая больше нигде не пересекает эллиптическую кривую, то тогда сумма точек будет равна нулевому элементу  $(\infty, \infty)$ .

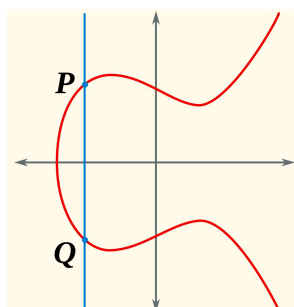


Рис. 7.4

Если точка  $P$ , расположенная так, что проведенная через нее прямая будет являться касательной к эллиптической кривой, то результатом её сложения с точкой  $O(\infty, \infty)$  будет эта же точка  $P$ .

В качестве упражнения читателю предлагается подумать, что произойдёт, если сложить точку  $P$  с элементом  $O(\infty, \infty)$ .

**!** Для подготовки к экзаменам пользуйтесь учебной литературой. Об обнаруженных неточностях и замечаниях просьба писать на [pulsar@phystech.edu](mailto:pulsar@phystech.edu)



Конспект не проходил проф. редактуру, создан студентами и, возможно, содержит смысловые ошибки. Следите за обновлениями на [lectoriy.mipt.ru](http://lectoriy.mipt.ru).

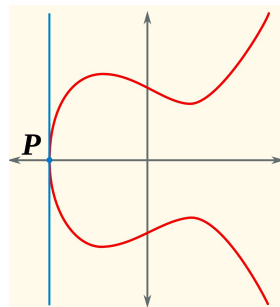


Рис. 7.5

Вернемся к рассмотрению эллиптической кривой, которая задаётся следующей формулой:

$$y^2 + y = x^3 - x^2.$$

Точку  $A$  будем прибавлять к самой себе. Видно, что  $A + A = B$ . Продолжая суммирование, будем получать точки  $C$ ,  $D$  и нулевой элемент. Видно, что в данном случае такая группа является циклической, причём порядок группы равен пяти.

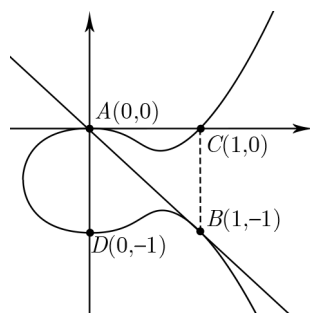


Рис. 7.6

В точке  $A$  касательная будет лежать на оси абсцисс, пересекая точку  $C$ . Далее проводим вертикальную прямую и попадаем в точку  $B$ , тем самым графически показывая, что  $A + A = C$ .

Сумма точек  $A$  и  $B$  даст  $C$ . Прямая  $AB$  будет проходить через точку  $B$  по касательной (касательная пересекает кривую в двух точках). Проводим вертикальную и попадаем в точку  $C$ .

Прямая, проведённая через точки  $A$  и  $C$ , будет пересекать кривую в трёх точках: два раза  $A$  и один раз  $C$ . Проведённая вертикальная прямая приводит к точке  $D$ .

#### 4. Аналитические формулы для вычисления координат суммы точек эллиптической кривой

Будем обсуждать только реальные криптосистемы: в них используются уравнения кривой с отрицательным дискриминантом.

Возьмём точки  $P(x_1, y_1)$  и  $Q(x_2, y_2)$ . Сумма этих двух точек есть точка с координатами  $(x_3, y_3)$ , причём эти координаты определяются аналитически уравнениями, в которых фигурирует параметр  $\lambda$ .



Для подготовки к экзаменам пользуйтесь учебной литературой. Об обнаруженных неточностях и замечаниях просьба писать на [pulsar@phystech.edu](mailto:pulsar@phystech.edu)

**!** Конспект не проходил проф. редактуру, создан студентами и, возможно, содержит смысловые ошибки. Следите за обновлениями на [lectoriy.mipt.ru](http://lectoriy.mipt.ru).

Часто требуется найти  $R(x_R, y_R)$ :

$$P + Q + R = 0,$$

или  $T(x_T, y_T)$ :

$$P + Q = T.$$

Уравнения возникают из рассмотрения коэффициента наклона касательной. Могут возникнуть 4 случая.

1. Точки не совпадают.

Тогда коэффициент наклона находится уравнением:

$$s = \frac{y_2 - y_1}{x_2 - x_1}.$$

Для координат точек  $R$  и  $T$  можно получить формулы:

$$x_R = s^2 - x_P - x_Q, \quad y_R = y_P - s(x_P - x_R);$$

$$x_T = s^2 - x_P - x_Q, \quad y_T = -y_P + s(x_P - x_T).$$

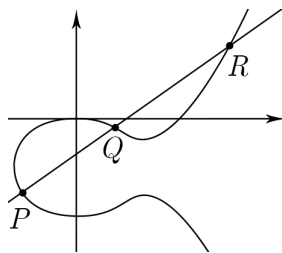


Рис. 7.7

2. Одна из точек является точкой касания прямой, соединяющей две точки.

Тогда:

$$s = \frac{3x^2 + a}{2y}, \quad s = \frac{3x^2 - p}{2y}.$$

$$s = \frac{3x^2 + a}{2y}, \quad s = \frac{3x^2 - p}{2y};$$

$$x_R = s^2 - x_P - x_Q, \quad y_R = y_P - s(x_P - x_R);$$

$$x_T = s^2 - x_P - x_Q, \quad y_T = -y_P + s(x_P - x_T).$$

3. Ни одна из двух точек не является точкой касания.

Тогда

$$x_P = x_Q, \quad y_P \neq y_Q;$$

$$s = \infty;$$

$$T = P + Q = \langle 0 \rangle;$$

$$R = -T = \langle 0 \rangle.$$

**!** Для подготовки к экзаменам пользуйтесь учебной литературой. Об обнаруженных неточностях и замечаниях просьба писать на [pulsar@phystech.edu](mailto:pulsar@phystech.edu)

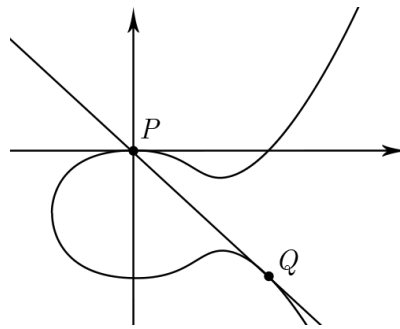


Рис. 7.8

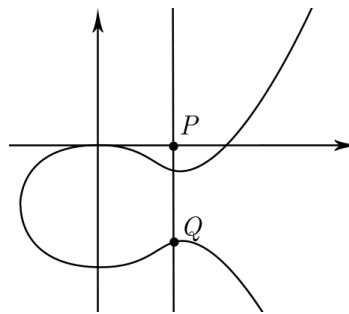


Рис. 7.9

4. В сумме участвует лишь точка касания.

$$x_P = x_Q, \quad y_P = y_Q = 0;$$

$$s = \infty;$$

$$T = P + Q = \langle 0 \rangle;$$

$$R = -T = \langle 0 \rangle.$$

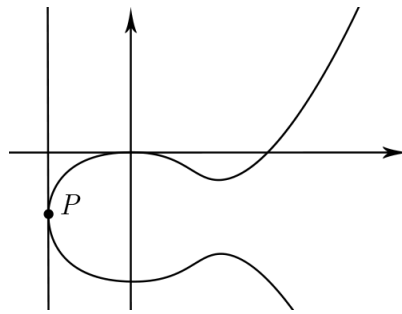


Рис. 7.10

## 5. Использование эллиптических кривых в шифровании

При взломе алгоритма RSA злоумышленнику приходится решать задачу факторизации. Если используют эллиптическую кривую, то проблема злоумышленника обычно приводится в следующий вид: ему известны точки  $P$  и  $Q$ , причём  $Q$  является элементом, который нужно много раз просуммировать, чтобы получить все точки, относящиеся к данной группе. И злоумышленнику надо узнать, сколько раз нужно подействовать операцией на элемент  $Q$ , чтобы получить  $P$ .

Впервые на практике в качестве стандарта шифросистема на эллиптической кривой была принята в Германии, и она использовала алгоритмы электронно-цифровой подписи. Алгоритм состоит из трёх этапов: алгоритм генерации, алгоритм подписывания и алгоритм проверки подписи. Алгоритм генерации состоит из следующих 5 шагов.

1. Выбираем эллиптическую кривую. Число точек в этой кривой должно делиться на большое целое число  $N$ . Коэффициенты, которые используются в эллиптической кривой, будут в итоге защиты либо представлены либо в аппаратном средстве, либо в программном средстве. И в случае, если злоумышленник каким-то образом узнает эту кривую, то нужно будет менять весь алгоритм в системе. Поэтому обычно параметры алгоритма не считают секретными, секретным считают только ключ.

На алгоритме генерации выбирают точку и случайное число  $D$  от 1 до  $(N-1)$  и проводят вычисления по вычислению точки  $Q$ . Точка  $Q$  есть точка  $P$ , сложенная сама с собой  $(D-1)$  раз. Секретным ключом объявляем  $D$ , открытым ключом — параметры кривой, точку  $P$ , точку  $N$  и точку  $Q$ .

2. Второй этап — это этап формирования подписи. При формировании выбирается случайное число  $K$ . Вычисляется  $K$  раз точка  $P$ , вычисляется число  $R$ , которое зависит от координаты точки  $P$ . Если  $R$  — ненулевое, то переходим к шагу 3, если  $R$  — нулевое, то возвращаемся к шагу 1.
3. Вычисляется обратный элемент  $K$  по модулю  $N$ .
4. Вычисляется число  $S$ . Если  $S$  — нулевое, то повторяем шаги с 1-го по 4-й. Если  $S$  — ненулевое, то для сообщения  $M$  подписью является набор чисел  $R$  и  $S$ , и тогда можно передавать числа  $M$ ,  $R$  и  $S$  по каналу связи в открытом виде.





*Конспект не проходил проф. редактуру, создан студентами и, возможно, содержит смысловые ошибки. Следите за обновлениями на [lectoriy.mipt.ru](http://lectoriy.mipt.ru).*

Чтобы убедиться, что сообщение имеет нужного автора, проводится проверка: если  $R$  и  $S$  находятся в допустимых пределах и ненулевые, то тогда осуществляется переход к следующему шагу. Если же  $R$  и  $S$  вылетают за пределы, то считаем, что само сообщение повреждено, и объявляем подпись некорректной. Вычисляем число  $W$  — обратное  $S$  по модулю  $N$  и хеш-функцию (ставим в соответствие сообщению какое-то число).

5. Вычисляется число  $V$ . Если  $V = R$  то сообщение не сменило владельца и не изменилось в процессе передачи.

## 6. Стандарты электронно-цифровой подписи

В качестве хеш-функции на шаге 4 подпись вычисляется по стандартам ANSI X9F1 и IEEE P1364. Там использовался алгоритм SHA-1.

В России также был принят стандарт электронно-цифровой подписи, который использовал эллиптические кривые со следующими параметрами: размер подписи равен 512 бит, а число, по которому считают модуль, должно быть больше, чем  $2^{255}$ .

Сама эллиптическая кривая задаётся в виде инварианта. Также в этом стандарте используется своя хеш-функция и ограничения на инвариант.

## 7. Заключение

Эллиптические кривые — это множество с определённой операцией. По сравнению с обычным вычислением по модулю, то есть нахождением вычетов, в системах с эллиптическими кривыми обнаруживается большая криптостойкость (больше на один бит ключа по сравнению с RSA), то есть злоумышленнику нужно решать более сложные уравнения, которые не описываются какими-то простыми арифметическими операциями.

При проектировании шифросистемы обычно смотрят на точку времени, когда эта система была спроектирована, потому что она ограничена, с одной стороны, мощностями реализации этого алгоритма, а с другой стороны, она ограничена возможностями криптоаналитика. Если у криптоаналитика нет готового математического аппарата, по которому он может находить коэффициент, то можно считать, что таких алгоритмов не существует. Естественно, как только математика развивается, и находятся теоремы или утверждения, которые позволяют за меньшее время найти ответ, то тогда говорят, что данный алгоритм не подходит, и приходится искать что-то новое.



*Для подготовки к экзаменам пользуйтесь учебной литературой. Об обнаруженных неточностях и замечаниях просьба писать на [pulsar@phystech.edu](mailto:pulsar@phystech.edu)*