ТЕМА 8. Криптография с использованием эллиптических кривых

8.1. Математические понятия

Преимущество подхода на основе *эллиптических кривых* в сравнении с задачей факторизации числа, используемой в RSA, или задачей целочисленного логарифмирования, применяемой в алгоритме Диффи-Хеллмана и в DSS, заключается в том, что в данном случае обеспечивается эквивалентная защита при меньшей длине ключа.

В общем случае уравнение *эллиптической кривой* E имеет вид:

$y^2 + axy + by = x^3 + cx^2 + dx + e$

В качестве примера рассмотрим *эллиптическую кривую* E, уравнение которой имеет вид: $y^2 + y = x^3 - x^2$

На этой кривой лежат только четыре точки, координаты которых являются целыми числами. Это точки

A (0, 0), B (1, -1), C (1, 0) и D (0, -1)

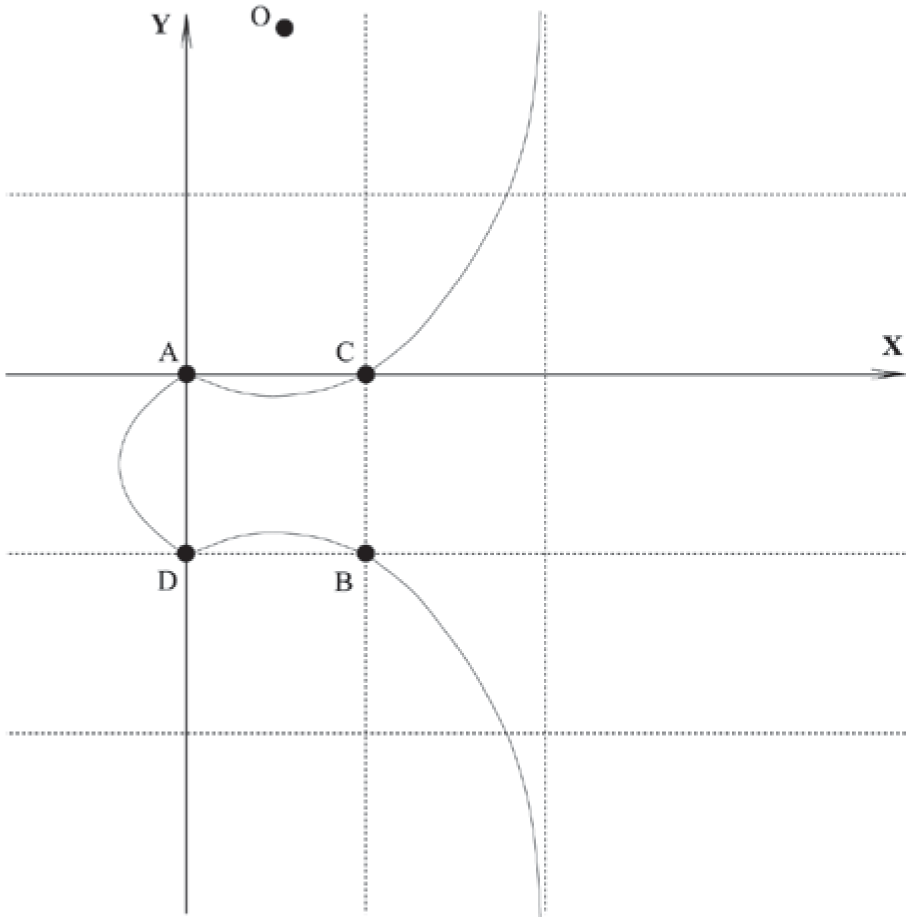

Рисунок 8.1 – Пример эллиптической кривой с четырьмя точками

Для определения *операции сложения для точек на эллиптической кривой* сделаем следующие предположения:

- На плоскости существует бесконечно удаленная точка $0 \in E$, в которой сходятся все вертикальные прямые.

- Будем считать, что касательная к кривой пересекает точку касания два раза.
- Если три точки *эллиптической кривой* лежат на прямой линии, то их сумма есть 0.

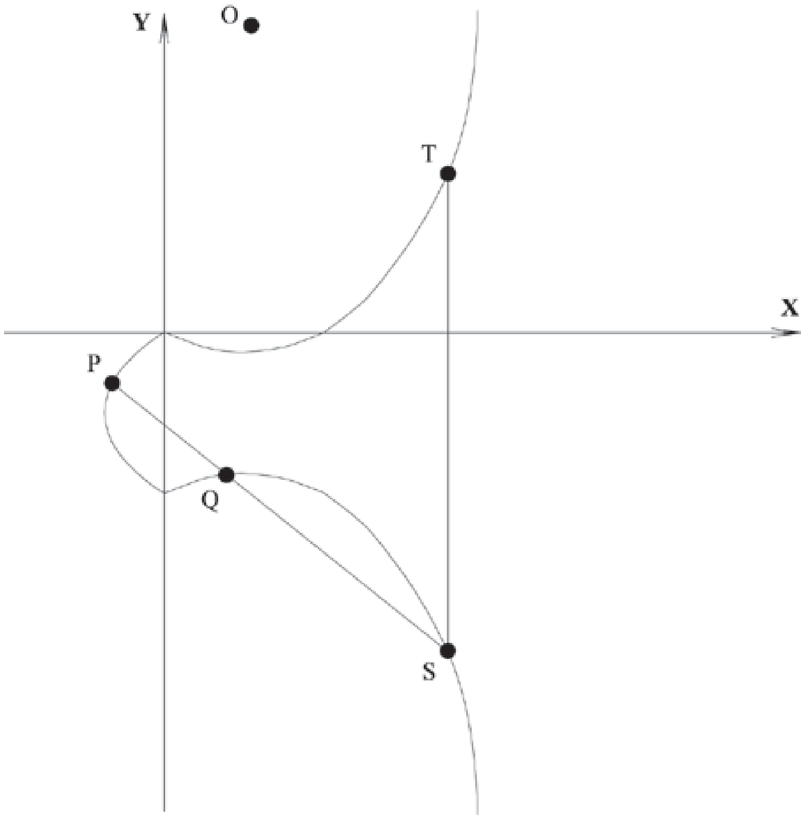

Рисунок 8.1 – Сложение точек на эллиптической кривой

Введем следующие правила сложения точек на *эллиптической кривой*:

- Точка 0 выступает в роли *нулевого элемента*. Так, 0 = -0 и для любой точки P на *эллиптической кривой* P + 0 = P.
- Вертикальная линия пересекает кривую в двух точках с одной и той же координатой x - скажем, S = (x, y) и T = (x, -y). Эта прямая пересекает кривую и в бесконечно удаленной точке. Поэтому $P_1 + P_2 + 0 = 0$ и $P_1 = -P_2$.
- Чтобы сложить две точки P и Q (см. рисунок 11.2) с разными координатами x, следует провести через эти точки прямую и найти точку пересечения ее с *эллиптической кривой*. Если прямая не является касательной к кривой в точках P или Q, то существует только одна такая точка, обозначим ее S. Согласно нашему предположению P + Q + S = O

  Следовательно, P + Q = -S или P + Q = T.

  Если прямая является касательной к кривой в какой-либо из точек P или Q, то в этом случае следует положить S = P или S = Q соответственно.
- Чтобы удвоить точку Q, следует провести касательную в точке Q и найти другую точку пересечения S с *эллиптической кривой*. Тогда Q + Q = 2 × Q = -S.

Введенная таким образом *операция сложения* подчиняется всем обычным правилам сложения, в частности коммутативному и ассоциативному законам. Умножение точки P *эллиптической кривой* на положительное число k определяется как сумма k точек P.

В криптографии с использованием *эллиптических кривых* все значения вычисляются по модулю p, где p является простым числом. Элементами данной *эллиптической кривой* являются пары неотрицательных целых чисел, которые меньше p и удовлетворяют частному виду *эллиптической кривой*:

$y^2 \equiv x^3 + ax + b \pmod{p}$

Такую кривую будем обозначать $E_p(a,b)$. При этом числа a и b должны быть меньше p и должны удовлетворять условию $4a^3 + 27b^2 \pmod{p} \neq 0$. Множество точек на *эллиптической кривой* вычисляется следующим образом.

Для каждого такого значения x, что $0 \le x \le p$, вычисляется $x^3 + ax + b \pmod{p}$.

Для каждого из полученных на предыдущем шаге значений выясняется, имеет ли это значение квадратный корень по модулю p. Если нет, то в $E_p(a,b)$ нет точек с этим значением x. Если корень существует, имеется два значения y, соответствующих операции извлечения квадратного корня (исключением является случай, когда единственным значением оказывается y = 0). Эти значения (x,y) и будут точками $E_p(a,b)$.

Множество точек $E_p(a,b)$ обладает следующими свойствами:

1. P + 0 = P
2. Если P = (x,y), то P + (x,-y) = 0. Точка (x,-y) является отрицательным значением точки P и обозначается -P. Заметим, что (x,-y) лежит на *эллиптической кривой* и принадлежит $E_p(a,b)$.
3. Если $P = (x_1,y_1)$ и $Q = (x_2,y_2)$, где $P \neq Q$, то $P + Q = (x_3,y_3)$ определяется по следующим формулам:
4. $x_3 \equiv \lambda^2 - x_1 - x_2 \pmod{p}$
5. $y_3 \equiv \lambda (x_1 - x_3) - y_1 \pmod{p}$

где

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1), & \text{если } P \neq Q \\ (3x_1^2 + a)/2y_1, & \text{если } P = Q \end{cases}$$

Число λ есть угловой коэффициент секущей, проведенной через точки $P = (x_1, y_1)$ и $Q = (x_2, y_2)$. При P = Q секущая превращается в касательную, чем и объясняется наличие двух формул для вычисления λ.

Задача, которую должен решить в этом случае атакующий, есть своего рода задача ***"дискретного логарифмирования на эллиптической кривой"***, и формулируется она следующим образом. Даны точки P и Q на *эллиптической кривой* $E_p(a,b)$. Необходимо найти коэффициент k < p такой, что

$P = k \times Q$

Относительно легко вычислить P по данным k и Q, но довольно трудно вычислить k, зная P и Q.