信息安全数学基础

第七章 椭圆曲线

熊 虎

信息与软件工程学院

xionghu.uestc@gmail.com

第七章 椭圆曲线

7.1 椭圆曲线密码体制

7.1.1 实数域上的椭圆曲线

7.1.2 有限域上的椭圆曲线

7.1.3 椭圆曲线上的ElGamal加密体制

7.1.1实数域上的椭圆曲线

由于椭圆曲线是双线性配对的理论基础,因此本节首先对其进行介绍。

椭圆曲线并非椭圆,之所以称为椭圆曲线是因为它的曲线方程与计算椭圆周长的方程相似。一般的,椭圆曲线指的是由维尔斯特拉斯(Weierstrass)方程

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

所确定的曲线,它是由方程的全体解(x, y)再加上一个无穷远点O构成的集合,其中a, b, c, d, e是满足一些简单条件的实数,x和y也在实数集上取值。上述曲线方程可以通过坐标变换转化为下述形式:

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

7.1.1实数域上的椭圆曲线

由它确定的椭圆曲线常记为$E(a,b)$,简记为E。

当 $4a^3+27b^2\neq 0$时,称$E(a,b)$ 是一条非奇异椭圆曲线。对于非奇异椭圆曲线,可以基于集合$E(a,b)$ 定义一个群。

这是一个Abel群,具有重要的“加法规则”属性。下面,首先给出加法规则的几何描述,然后给出加法规则的代数描述。

1)加法的几何描述

椭圆曲线上的加法运算定义如下:如果椭圆曲线上的3个点位于同一直线上,那么它们的和为O。从这个定义出发,可以定义椭圆曲线的加法规则:

7.1.1实数域上的椭圆曲线

(1) O 为加法的单位元,对于椭圆曲线上的任何一点 P ,有 $P+O=P$。

(2)对于椭圆曲线上的一点$P=(x,y)$，它的逆元为 $-P=(x,-y)$。注意到$P+(-P)=P-P=O$。

(3)设 P和 Q是椭圆曲线上x 坐标不同的两点, $P+Q$的定义如下:作一条通过P 和Q 的直线l 与椭圆曲线相交于R (这一点是唯一的,除非这条直线在 P点或Q 点与该椭圆曲线相切,此时于分别取 $R=P$ 或 $R=Q$),然后过R 点作y 轴的平行线 l', l'与椭圆曲线相交的另一点 S就是 $P+Q$,如图7.1所示。

7.1.1实数域上的椭圆曲线

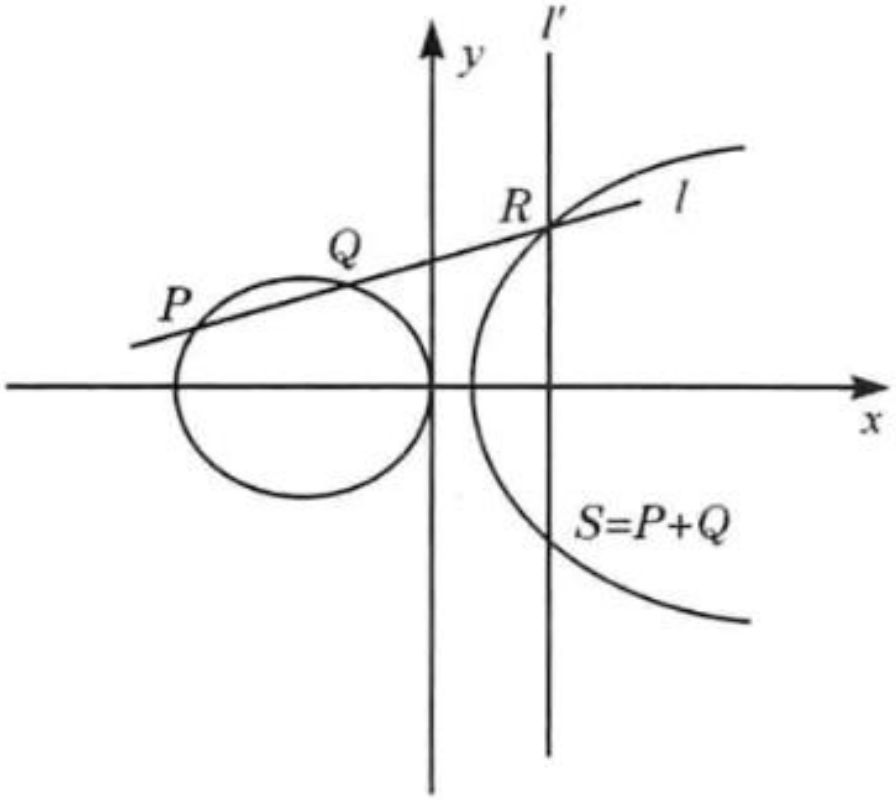

图7.1 椭圆曲线上点的加法的几何解释

7.1.1实数域上的椭圆曲线

(4)上述几何解释也适用于具有相同 x 坐标的两个点 P 和 $-P$ 的情形。用一条垂直的线连接这两个点,可看做是在无穷远点与椭圆曲线相交,因此有 $P+(-P)=O$ 。这与上述第(2)条叙述是一致的。

(5)为计算点 Q 的两倍,在 Q 点作一条切线并找到与椭圆曲线的另一个交点 T ,则 $Q+Q=2Q=-T$ 。

以上定义的加法满足加法运算的一般性质,如交换律、结合律等。

7.1.1实数域上的椭圆曲线

2) 加法的代数描述

对于椭圆曲线上不互为逆元的两点 $P=(x_1,y_1)$和 $Q=(x_2,y_2)$，$S=P+Q=(x_3,y_3)$由以下规则确定:

$$x_3=\lambda^2-x_1-x_2$$

$$y_3=\lambda(x_1-x_3)-y_1$$

式中

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}, P\neq Q\\ \dfrac{3x_1^2+a}{2y_1}, P=Q\end{cases}$$