# 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

# 7.1.1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

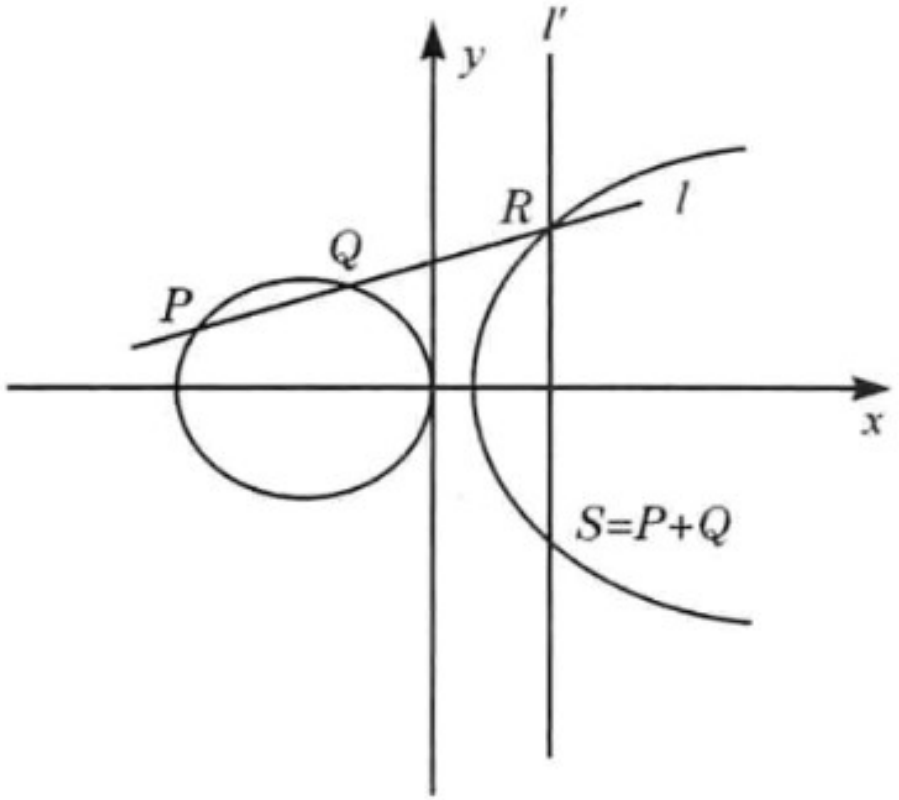


图7.1 椭圆曲线上点的加法的几何解释

# 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

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

# 第七章 椭圆曲线

# 7.1.2有限域上的椭圆曲线

椭圆曲线密码体制使用的是有限域上的椭圆曲线,即变量和系数均为有限域中的元素。有限域 $GF(p)$ 上的椭圆曲线是指满足方程

$$y^3 \equiv x^3 + ax + b(\mathrm{mod}\ p)$$

的所有点$(x, y)$再加上一个无穷远点$O$构成的集合,其中, $a, b, x$ 和 $y$ 均在有限域 $GF(p)$ 上取值, $p$ 是素数。这里把该椭圆曲线记为$E_p(a, b)$ 。该椭圆曲线只有有限个点,其个数$N$由 Hasse定理确定。

# 7.1.2有限域上的椭圆曲线

**定理7.1** (Hasse定理) 设$E$是有限域$GF(p)$上的椭圆曲线,$N$是$E$上点的个数,则

$$p+1-2\sqrt{p} \leq N \leq p+1+2\sqrt{p}$$

当$4a^3+27b^2 (\mathrm{mod}\ p) \neq 0$时,基于集合$E_p(a,b)$可以定义一个Abel群,其加法规则与实数域上描述的代数方法一致。设$P,Q \in E_p(a,b)$, 则

(1) $P+O=P$。

(2)如果$P=(x,y)$, 那么$(x,y)+(x,-y)=O$,即点$(x,-y)$是$P$的加法逆元,表示为$-P$。

(3)设$P=(x_1,y_1)$和$Q=(x_2,y_2)$,$P \neq -Q$,则$S=P+Q=(x_3,y_3)$由以下规则确定:

# 7.1.2有限域上的椭圆曲线

$$x_3 \equiv \lambda^2 - x_1 - x_2 (\mathrm{mod}\ p)$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p)$$

式中

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

(4)倍点运算定义为重复加法,如 $4P = P + P + P + P$ 。

# 7.1.2有限域上的椭圆曲线

例**7.1** 设 $p=11, a=1, b=6$ ,即椭圆曲线方程为

$$y^2 \equiv x^3 + x + 6 (\text{mod } 11)$$

要确定椭圆曲线上的点,对于每个 $x \in GF(11)$ ,首先计算 $z \equiv x^3 + x + 6 (\text{mod } 11)$ , 然后再判定 $z$ 是否是模11的平方剩余(方程 $y^2 \equiv z \bmod 11$ 是否有解),若不是,则椭圆曲线上没有与这一 $x$ 相对应的点;若是,则求出 $z$ 的两个平方根。该椭圆曲线上的点如表7.1所示。

# 7.1.2有限域上的椭圆曲线

表7.1 椭圆曲线 $y^2 \equiv x^3 + x + 6 (\mathrm{mod}\ 11)$ 上的点

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $x^3+x+6(\mathrm{mod}\ 11)$ | 6 | 8 | 5 | 3 | 8 | 4 | 8 | 4 | 9 | 7 | 4 |
| 是否是模 11 的平方剩余 | 否 | 否 | 是 | 是 | 否 | 是 | 否 | 是 | 是 | 否 | 是 |
| $y$ | | | 4 | 5 | | 2 | | 2 | 3 | | 2 |
| | | | 7 | 6 | | 9 | | 9 | 8 | | 9 |

# 7.1.2有限域上的椭圆曲线

只有$x=2,3,5,7,8,10$时才有点在椭圆曲线上,$E_{11}(1,6)$是由表7.1中的点再加上一个无穷远点$O$构成,即

$$E_{11}(1,6)=\{O,(2,4),(2,7),(3,5),(3,6),(5,2),(5,9),(7,2),(7,9),(8,3),(8,8),(10,2),(10,9)\}$$

设 $P=(2,7)$，计算 $2P=P+P$ 。首先计算

$$\lambda\equiv\frac{3\times2^2+1}{2\times7}(\text{mod }11)=\frac{2}{3}(\text{mod }11)\equiv8$$

于是

$$x_3\equiv8^2-2-2(\text{mod }11)\equiv5$$

$$y_3\equiv8\times(2-5)-7(\text{mod }11)\equiv2$$

所以 $2P=(5,2)$ 。同样可以算出

# 7.1.2有限域上的椭圆曲线

$3P=(8,3), 4P=(10,2), 5P=(3,6), 6P=(7,9),$

$7P=(7,2), 8P=(3,5), 9P=(10,9), 10P=(8,8),$

$11P=(5,9), 12P=(2,4), 13P=O$ 。

由此可以看出, $E_{11}(1,6)$是一个循环群,其生成元是 $P=(2,7)$。

# 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

# 7.1.3椭圆曲线上的 ElGamal加密体制

为了使用椭圆曲线来构造密码体制,需要找到类似大整数因子分解或离散对数这样的困难问题。

**定义7.1** 椭圆曲线 $E_p(a,b)$ 上点 $P$ 的阶是指满足

$$nP = \underbrace{P + P + \cdots + P}_{n} = O$$

的最小正整数,记为 $ord(P)$ ,其中 $O$ 是无穷远点。

# 7.1.3椭圆曲线上的 ElGamal加密体制

定义**7.2** 设$G$是椭圆曲线$E_p(a,b)$上的一个循环子群，$P$是$G$的一个生成元，$Q \in G$。已知$P$和$Q$，求满足

$$mP = Q$$

的整数$m, 0 \le m \le ord(P)-1$，称为椭圆曲线上的离散对数问题( elliptic curve discrete logarithm problem, ECDLP)。计算$mP$的过程称为点乘运算(Point multi-plication)。

# 7.1.3椭圆曲线上的 ElGamal加密体制

在使用一个椭圆曲线密码体制时,首先需要将发送的明文 $m$ 编码为椭圆曲线上的点 $P_m=(x_m,y_m)$,然后再对点 $P_m$ 做加密变换,在解密后还得将 $P_m$ 逆向译码才能获得明文。下面对椭圆曲线上的 ElGamal密码体制做一介绍。

1)密钥生成(KeyGen)

在椭圆曲线 $E_p(a,b)$ 上选取一个阶为 $n$ ( $n$ 为一个大素数)的生成元 $P$ 。随机选取整数 $x(1<x<n)$ ,计算 $Q=xP$ 。公钥为 $Q$ ,私钥为 $x$ 。

2)加密(Encrypt)

为了加密 $P_m$ ,随机选取一个整数 $k,1<k<n$ ,计算

$$C_1=kP,C_2=P_m+kQ$$

则密文 $c=(C_1,C_2)$ 。

# 7.1.3椭圆曲线上的 ElGamal加密体制

3)解密(Decrypt)

为了解密一个密文 $c=(C_1,C_2)$ ,计算

$$C_2-xC_1=P_m+kQ-xkP=P_m+kxP-xkP=P_m$$

攻击者要想从 $c=(C_1,C_2)$计算出 $P_m$ ,就必须知道 $k$ 。而要从$P$ 和$kP$ 中计算出 $k$ 将面临求解椭圆曲线上的离散对数问题。