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

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$P=(2,7)$。