椭圆曲线密码

Elliptic Curve Cryptography

刘卓

由 Miller 和 Koblitz 在 20 世纪 80 年代中期提出。大约在同一时间，Lenstra 开发了一种使用椭圆曲线的分解算法。近年来，椭圆曲线在密码学中的应用得到了迅速的发展。其主要优点是利用椭圆曲线，我们可以用比 RSA 和其他现代密码系统所需要的数目小得多的数字来实现安全性。

1 椭圆曲线

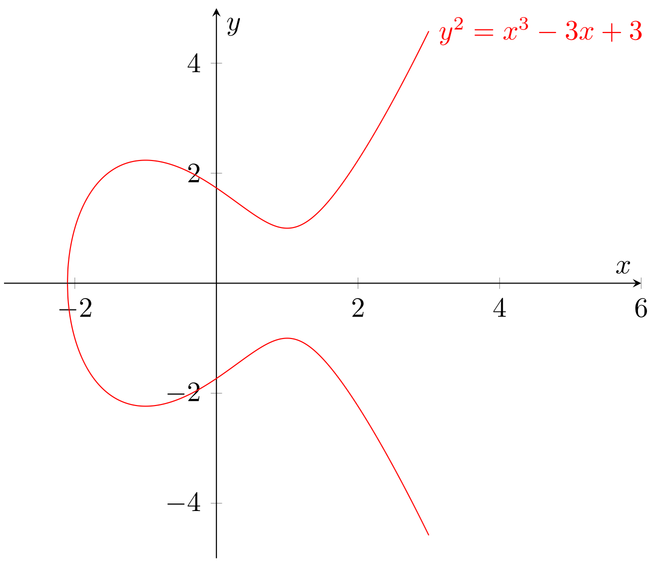
定义 1 (椭圆曲线)**.** 实数上的椭圆曲线是满足方程的点 (x, y) 的集合

$$E : y^2 = x^3 + Ax + B, A, B \in \mathbb{R}$$

要求曲线是非奇异 (non-singular) 的 (即无尖端、无自交、无孤立点)。这个条件等价于

$$4A^3 + 27B^2 \neq 0$$

例 1. 椭圆曲线 $y^2 = x^3 - 3x + 3$:



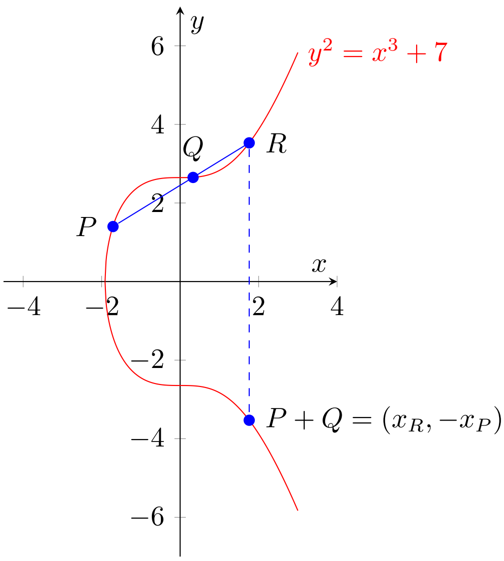
$$4A^3 + 27B^2 = 4 \cdot (-3)^3 + 27 \cdot 3^2 \neq 0$$

□

点 $P=(x_P,y_P)$ 和点 $Q=(x_Q,y_Q)$ 是在椭圆曲线 $E:y^2=x^3+Ax+B$ 上的两个点。则 $P+Q=(x_R,-y_R)$，其中

$$
\begin{aligned}
\alpha &= \frac{y_Q-y_P}{x_Q-x_P} \\
x_R &= \alpha^2-x_P-x_Q \\
y_R &= y_P+\alpha\left(x_R-x_P\right)
\end{aligned}
$$

例 2.



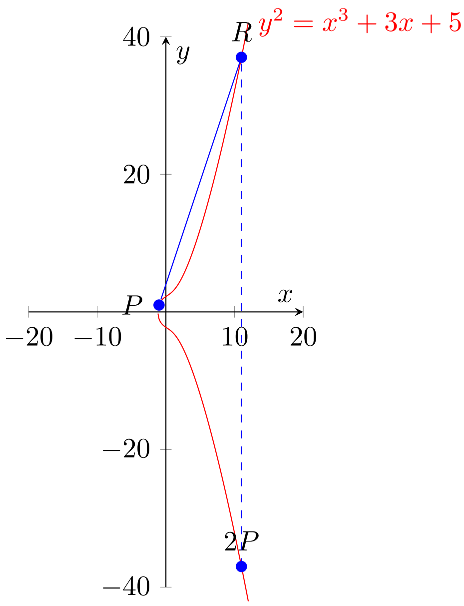
□

定义 2. 如果点 $P=(x_P,y_P)$ 在椭圆曲线 $E:y^2=x^3+Ax+B$ 上，$2P=(x_R,-y_R)$，其中

$$
\begin{aligned}
\alpha &= \frac{3x_P^2+A}{2y_P} \\
x_R &= \alpha^2-2x_P \\
y_R &= y_P+\alpha\left(x_R-x_P\right)
\end{aligned}
$$

例 3. $y^2=x^3+3x+5; P=(-1,1),$ 计算$2P$

$$
\begin{aligned}
\alpha &= \frac{3x_P^2+A}{2y_P}=\frac{3(-1)^2+3}{2(1)}=3 \\
x_R &= \alpha^2-2x_P=3^2-2(-1)=11 \\
y_R &= y_P+\alpha\left(x_R-x_P\right)=1+3(11-(-1))=37 \\
2P &= (x_R-y_R)=(11,-37)
\end{aligned}
$$



□

定义 3. 给定一个质数 p，一个 (离散的) 椭圆曲线并 mod p 是满足方程的所有整数点 (x, y) 的集合，该方程表示为：

$$E : y^2 = x^3 + Ax + B \pmod p$$

$$A, B \in [0, p-1], 4A^3 + 27B^2 \neq 0 \pmod p$$

例 4. $y^2 = x^3 + 16x + 14 \pmod{23}$

$$\left(\begin{array}{c|cccccccccccccccccccccc} x & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 \\ y^2 \pmod{23} & 8 & 8 & 20 & 4 & 12 & 4 & 9 & 10 & 13 & 1 & 3 & 2 & 4 & 15 & 18 & 19 & 1 & 16 & 1 & 8 & 20 & 20 \end{array}\right)$$

比如 $\underbrace{y^2 = 10^2 = 8 = 1^3 + 16 \cdot 1 + 14 = x^3 + 16x + 14}_{\pmod{23}}$，所以 $(1, 10)$ 为一个解

再者 $\underbrace{y^2 = 13^2 = 8 = 2^3 + 16 \cdot 2 + 14 = x^3 + 16x + 14}_{\pmod{23}}$，所以 $(2, 13)$ 为一个解

所有 32 个解的集合为

$$\begin{aligned} &\{\{1,10\},\{1,13\},\{2,10\},\{2,13\},\{4,2\},\{4,21\},\{5,9\},\\ &\{5,14\},\{6,2\},\{6,21\},\{7,3\},\{7,20\},\{9,6\},\{9,17\},\\ &\{10,1\},\{10,22\},\{11,7\},\{11,16\},\{12,5\},\{12,18\},\\ &\{13,2\},\{13,21\},\{15,8\},\{15,15\},\{17,1\},\{17,22\},\\ &\{18,4\},\{18,19\},\{19,1\},\{19,22\},\{20,10\},\{20,13\}\} \end{aligned}$$

```
def Elliptic_Curve_points(A,B,p):
    """
    求解满足椭圆曲线y^2 = x^3 + Ax + B
    所以整数点的几何
    但对于大质数运算时间过长
```

```
    p : int
        质数，求余.
    A : int
        椭圆曲线A.
    B : int
        椭圆曲线B.

    返回所有点

    """
    return [(x, y) for x in range(p) for y in range(p) if (y*y - (x**3 + A*x + B)) % p == 0]

print(Elliptic_Curve_points( A=16, B=14, p=23))
```

□

以下算式都适用于实数上的椭圆曲线和 mod p 的椭圆曲线:

- 加法结合律:$(P_1+P_2)+P_3=P_1+(P_2+P_3)$;
- 加法交换律:$P_1+P_2=P_2+P_1$;
- 如果 $P=(x,y)$ 并有一个整数 k，则:

$$kP=\underbrace{P+P+\cdots+P}_{\text{k 个}}$$

- 对于任意两个整数 k,h，则

$$h(kP)=(hk)P=k(hP)$$

定义 4 (椭圆曲线加法)**.** 让 $P=(x_P,y_P)$ 和点 $Q=(x_Q,y_Q)$ 是在椭圆曲线 $E: y^2=x^3+Ax+B \pmod p$ 上的两个点。则 $P+Q=(x_R,-y_R)$, 其中

$$\begin{aligned}
\alpha &= (y_Q-y_P)\cdot(x_Q-x_P)^{-1} \pmod p\\
x_R &= \alpha^2-x_P-x_Q \pmod p\\
y_R &= y_P+\alpha\,(x_R-x_P) \pmod p
\end{aligned}$$

定义 5 (椭圆曲线点倍增)**.** 让 $P=(x_P,y_P)$ 是在椭圆曲线 $E: y^2=x^3+Ax+B \pmod p$ 上的两个点。则 $2P=(x_R,-y_R)$, 其中

$$\alpha = \left(3{x_P}^2+A\right)\cdot(2y_P)^{-1} \pmod p$$

$$
\begin{aligned}
x_R &= \alpha^2 - 2x_P \pmod p \\
y_R &= y_P + \alpha\,(x_R - x_P) \pmod p
\end{aligned}
$$

例 5. 让 $p = 23, y^2 = x^3 + 13x + 7 \pmod{23}$, 点 $P = (14, 9)$, 点 $Q = (17, 14)$

1. 点 P, Q 是否在曲线上?

解.

$$A = 13; B = 7; p = 23$$

$$4A^3 + 27B^2 \pmod{23} = 4 \cdot (13)^3 + 27 \cdot (7)^2 \pmod{23} \neq 0$$

$$P = (14, 9)\text{代入}y^2 = x^3 + 13x7$$

满足等式即可 □

2. 计算 $P + Q$

解.

$$
\begin{aligned}
\alpha &= (y_Q - y_P) \cdot (x_Q - x_P)^{-1} \pmod p \\
&= (14 - 9)(17 - 14)^{-1} \pmod{23} \\
&= (5)(3)^{-1} \pmod{23} \\
&= (5)(8) \pmod{23} \\
&= 17 \pmod{23}
\end{aligned}
$$

$$
\begin{aligned}
x_R &= \alpha^2 - x_P - x_Q \pmod p \\
&= 17^2 - 17 - 14 \pmod{23} \\
&= 5 \pmod{23}
\end{aligned}
$$

$$
\begin{aligned}
y_R &= y_P + \alpha\,(x_R - x_P) \pmod p \\
&= 9 + 17(5 - 14) \pmod{23} \\
&= 17 \pmod{23} \\
-y_R &= -17 \pmod{23} \\
&= 6 \pmod{23}
\end{aligned}
$$

$$P + Q = (x_R, -y_R) = (5, 6)$$

□

3. 如果 $S = (9, 5)$,$T = (9, 18)$, 计算 $S + T$

解. 因为 $y_T + y_S = 0 \pmod{23}$, 所以 $S+T$ 无解 □

例 6. 让 $p=23, y^2 = x^3+5x+8 \pmod{23}$, 点 $P=(3,2)$, 计算 $2P$

解. $A=5; B=8; p=23$

$$\begin{aligned}
\alpha &= \left(3{x_P}^2 + A\right)\cdot(2y_P)^{-1} \pmod{p}\\
&= (3(3)^2+5)\cdot(2(2))^{-1} \pmod{23}\\
&= (32)\cdot(4)^{-1} \pmod{23}\\
&= 9\cdot 6 \pmod{23}\\
&= 8 \pmod{23}
\end{aligned}$$

$$\begin{aligned}
x_R &= \alpha^2 - 2x_P \pmod{p}\\
&= 64 - 2(3) \pmod{23}\\
&= 12 \pmod{23}
\end{aligned}$$

$$\begin{aligned}
y_R &= y_P + \alpha\,(x_R - x_P) \pmod{p}\\
&= 2 + 8(12-3) \pmod{23}\\
&= 5 \pmod{23}\\
-y_R &= -5 \pmod{23}\\
&= 18 \pmod{23}
\end{aligned}$$

$$2P = (x_R, -y_R) = (12, 18)$$

□

2 椭圆曲线迪菲-赫尔曼密钥交换

1. *Alice* 和 *Bob* 决定一个质数 p，并在曲线 $E_p: y^2 = x^3 + Ax + B \pmod{p}$ 上选择一个点 Q，并公开；
2. *Alice* 随机选择一个整数 N_A，*Bob* 随机选择一个整数 N_B，并自己保留，不公开；
3. *Alice* 计算 $Q_A = N_A \cdot Q$ （这里 $N_A \cdot Q$ 是指 N 倍的 Q，方法与求 $2P$ 相同）然后发送给 *Bob*；
4. *Bob* 计算 $Q_B = N_B \cdot Q$ 然后发送给 *Alice*；
5. *Alice* 计算 $N_B \cdot Q_A$；*Bob* 计算 $N_A \cdot Q_B$；

6. 因此他们得到公钥:

$$N_AQ_B = N_A(N_BQ) = (N_AN_B)Q = (N_BN_A)Q = N_B(N_AQ) = N_BQ_A$$

其思想就是:

- 用曲线加法代替模乘 p;
- 用曲线上点的整数倍来代替模幂 p;
- 暂时没有已知算法可以分解攻击曲线密码;
- 椭圆曲线的模可以用来分解 N;
- 离散对数的改版;

例 7. *Alice* 和 *Bob* 想要交换一个密钥，因此他们共同决定了一个质数 $p = 7211$ 和椭圆曲线 $E_{7211}: y^2 = x^3 + x + 7206 \pmod{8831}$。并公开点 $P = (3, 5)$

1. *Alice* 选择一个整数 $N_A = 12$, 然后计算 $Q_A = N_A \cdot P = (1794, 6375)$;
2. *Bob* 选择一个整数 $N_B = 23$, 然后计算 $Q_B = N_B \cdot P = (3861, 1242)$;
3. 保留 N_A, N_B, 公开 Q_A, Q_B
4. *Alice* 拿到了 Q_B 后计算 $N_AQ_B = 12(1794, 6375) = (1472, 2098)$
5. *Bob* 拿到了 Q_A 后计算 $N_BQ_A = 23(3861, 1242) = (1472, 2098)$

因为 $N_AQ_B = N_A(N_BQ) = (N_AN_B)Q = (N_BN_A)Q = N_B(N_AQ) = N_BQ_A$，因此他们成功交换了密钥。

□

2.1 发布明文

现在 *Alice* 和 *Bob* 决定一个质数 p，并使用曲线 $E_p: y^2 = x^3 + Ax + B \pmod{p}$ 进行加密。
明文转化为整数 $M \in [1, p-1]$

1. 选择一个大整数 k, 计算
$$x_j = M \cdot k, j \in 1, 2, \cdots, k-1$$
2. 每次计算 x_j，我们测试 $x^3 + Ax + B$ 是否二次剩余 $\bmod p$
3. 当第一次 $x^3 + Ax + B$ 二次剩余 $\bmod p$，使用点 U 加密明文 M，其中
$$U = \left(x_j, \sqrt{x_j^3 + Ax_j + B}\right) \pmod{p}$$

3 椭圆曲线 El Gamal

1. *Bob* 决定一个质数 p 和一个椭圆曲线 $E_p: y^2 = x^3 + Ax + B \pmod p$。然后再选择一个点 P 和一个正整数 k。计算 $Q = k \cdot P$;
2. *Bob* 公开 E_p, P, Q。保留 k 不公开;
3. *Alice* 使用 E_p 加密信息 M 为点 U。然后选择一个正整数 h, 计算 $Y_1 = h \cdot P$ 和 $Y_2 = U + h \cdot Q$;
4. *Alice* 将 (Y_1, Y_2) 发送给 *Bob*;
5. *Bob* 进行解密。计算

$$Y_2 - kY_1 = U + hQ - k(hP) = U + hQ - h(kP) = U + hQ - hQ = U$$

   得到 U;

例 8. *Alice* 和 *Bob* 共同决定了一个质数 $p = 8831$ 和椭圆曲线 $E_{8831}: y^2 = x^3+3x+45 \pmod{8831}$。并公开点 $P = (4, 11)$

假设 *Alice* 想发送明文 $m = \textbf{THE}$ 给 *Bob*

解. 那么 $m = \textbf{T} \cdot 26^0 + \textbf{H} \cdot 26^1 + \textbf{E} \cdot 26^2 = 19 + 7 \cdot 26 + 4 \cdot 26^2 = 2905$,$x_U = 2905$。这里编码方式可以选择其他的方法。

$$y^2 = {x_U}^3 + 3x_U + 45 \pmod{8831} = 8187$$

, 只需要找到 $y^2 \pmod{8831} = 8187$ 即可，通过列表很容易可以找到。有 $(2905, 1898), (2905, 6933)$ 两个点，随机选择一个作为 U。在这里令 $U = (2905, 1898)$，*Alice* 想把它发给 *Bob*，他们应该怎么做呢?

Bob 假设选择一个整数 $k = 3$, 接着他计算 $Q = kP = 3(4, 11) = (413, 1808)$，发送给 *Alice*。

Alice 得到点 Q 后，选择一个整数 $h = 8$，计算

$$Y_1 = h \cdot P = 8(4, 11) = (5415, 6321)$$

和

$$Y_2 = U + h \cdot Q = (2905, 1898) + 8(413, 1808) = (323, 1743)$$

然后将 (Y_1, Y_2) 发送给 *Bob*

Bob 进行解密。计算

$$U = Y_2 - kY_1 = (323, 1743) - (673, 146) = (323, 1743) + (673, 8685) = (2905, 1898)$$

得到 U，再用约定好的方式对其进行解密即可; □

4 与 RSA 的比较

	RSA	椭圆曲线
密钥长度	长	相同加密强度时更短
速度	快	相同加密强度时更快
安全性	高	相同密钥长度时更高
破解方法	大数分解	离散对数

在继承关系上，可以说 ECC 是 RSA 的继承者。