网络安全数学基础(二)

沈佳辰
jcshen@sei.ecnu.edu.cn

華東師範大學
EAST CHINA NORMAL UNIVERSITY

网络安全数学基础

第九章 椭圆曲线

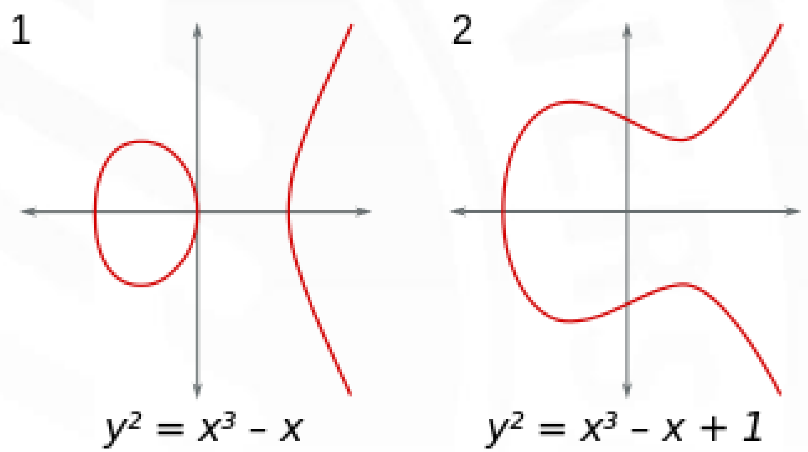
§9.1 椭圆曲线

- 定义9.1.1 令F为一个域，$a, b \in F$，则方程

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

称为域F上的椭圆曲线。上式称为维尔斯特拉斯（Weierstrass）方程。

- 例 实域上的椭圆曲线



- 定义9.1.2 令F为一个域，$a, b \in F$，令

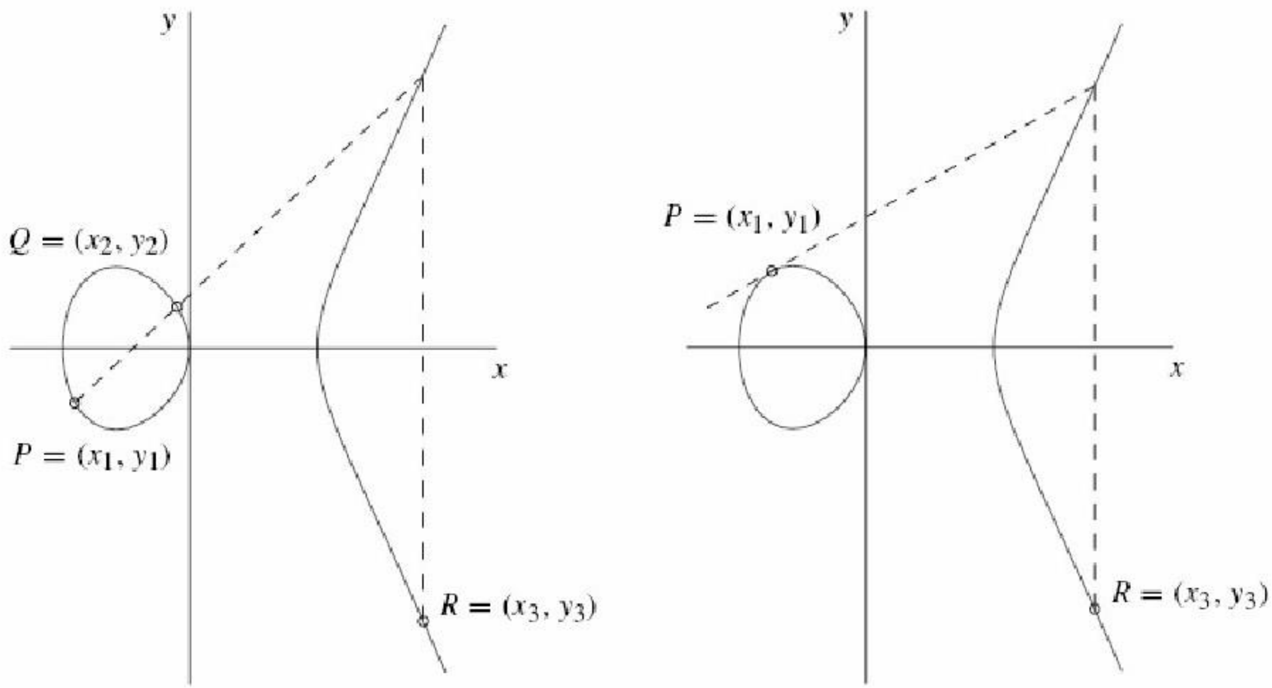
$$E = \{(x, y) | y^2 = x^3 + ax + b\} \cup \{\infty\},$$

设$P_1, P_2 \in E$，令R为过P_1, P_2的直线与E的第三个交点关于X轴的对称点，并记$P_1 + P_2 = R$。

- 定义9.1.2 令F为一个域，$a, b \in F$，令
$$E = \{(x, y) | y^2 = x^3 + ax + b\} \cup \{\infty\},$$
设$P_1, P_2 \in E$，令R为过P_1, P_2的直线与E的第三个交点关于X轴的对称点，并记$P_1 + P_2 = R$。

- $2P = P + P$为过P的E的切线与E的另一个交点关于X轴的对称点。

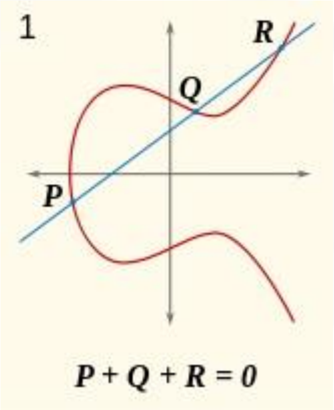
- 椭圆曲线上的加法



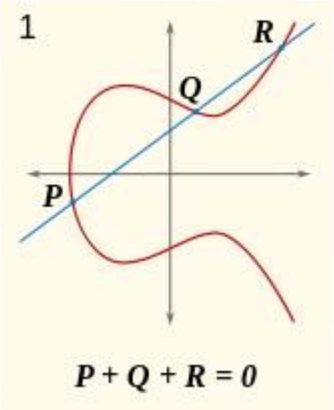
(a) 相加： $P + Q = R.$　　(b) 倍点： $P + P = R.$

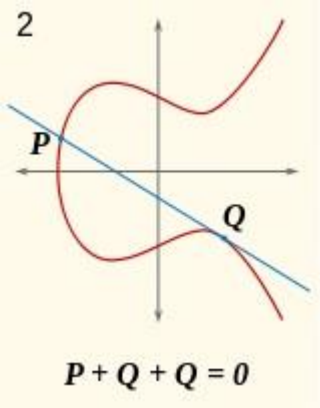
- 椭圆曲线上加法的性质

- 椭圆曲线上加法的性质

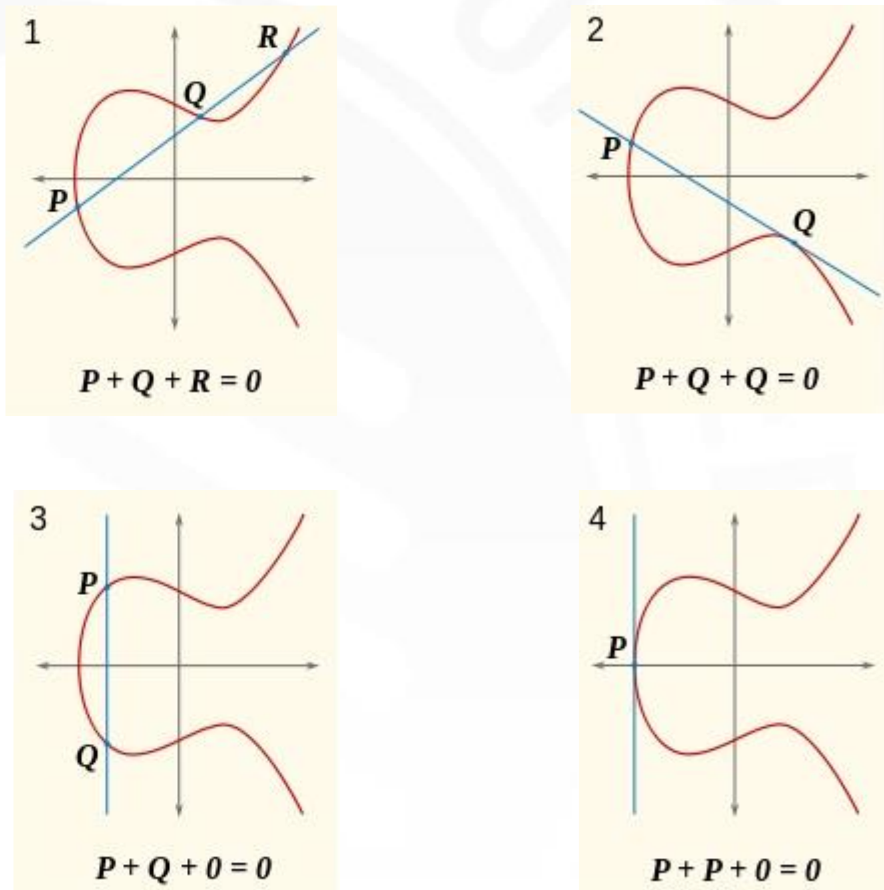


- 椭圆曲线上加法的性质





- 椭圆曲线上加法的性质



- 定理9.1.1 若规定$\infty + \infty = \infty$，则$(E, +)$构成一个阿贝尔群（交换群），其中∞为单位元，记作O， $P = (x, y)$的逆元为$Q = (x, -y)$。

- 例 设实域上椭圆曲线E: $y^2 = x^3 + 73$。令$P = (2,9)$和$Q = (3,10)$，求$R = P + Q$和$2R$。

- 例 设实域上椭圆曲线E: $y^2 = x^3 + 73$。令$P = (2,9)$和$Q = (3,10)$，求$R = P + Q$和$2R$。

解：易知过P, Q的直线为$y = x + 7$，代入椭圆曲线方程得$(x + 7)^2 = x^3 + 73$，可求得直线与椭圆曲线的第三个交点为$(-4,3)$，因此$R = (-4, -3)$。

- 例 设实域上椭圆曲线E: $y^2 = x^3 + 73$。令$P = (2,9)$和$Q = (3,10)$，求$R = P + Q$和$2R$。

解：易知过P, Q的直线为$y = x + 7$，代入椭圆曲线方程得$(x+7)^2 = x^3 + 73$，可求得直线与椭圆曲线的第三个交点为$(-4,3)$，因此$R = (-4,-3)$。

对椭圆曲线求微分可知$2ydy = 3x^2dx$，因此E在R的斜率为$\left.\frac{dy}{dx}\right|_{\substack{x=-4\\y=-3}} = -8$，因此过$R$的$E$的切线为$y = -8(x+4) - 3$，代入椭圆曲线并求解可得另一个交点为$(72,-611)$，因此$2R = (72,611)$。

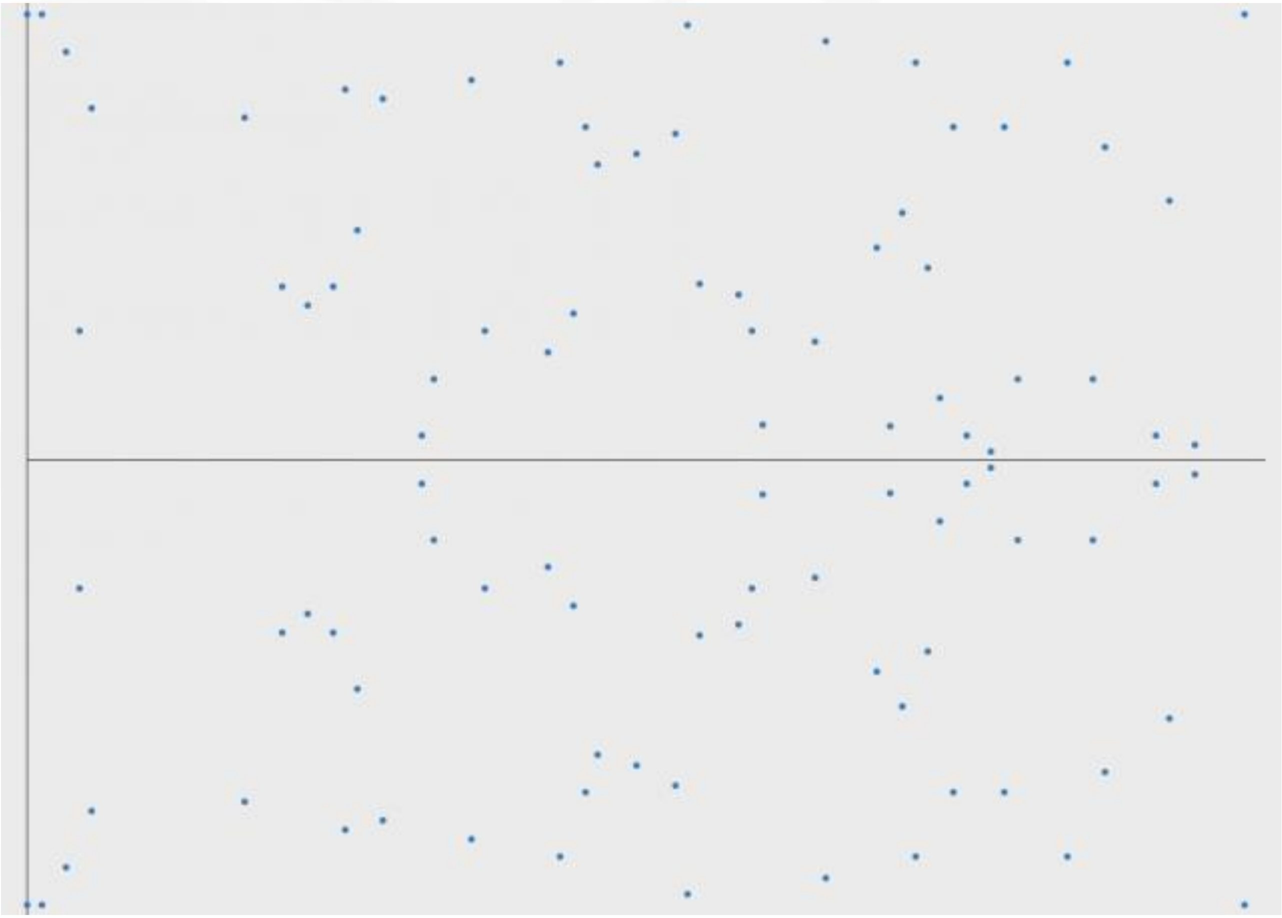
§9.2 椭圆曲线密码

- 以下三类公钥系统被认为是安全有效的
  - 基于大整数分解问题的RSA 型公钥密码；
  - 基于有限域上离散对数问题的ElGamal 型公钥密码；
  - 基于椭圆曲线离散对数问题的椭圆曲线公钥密码。

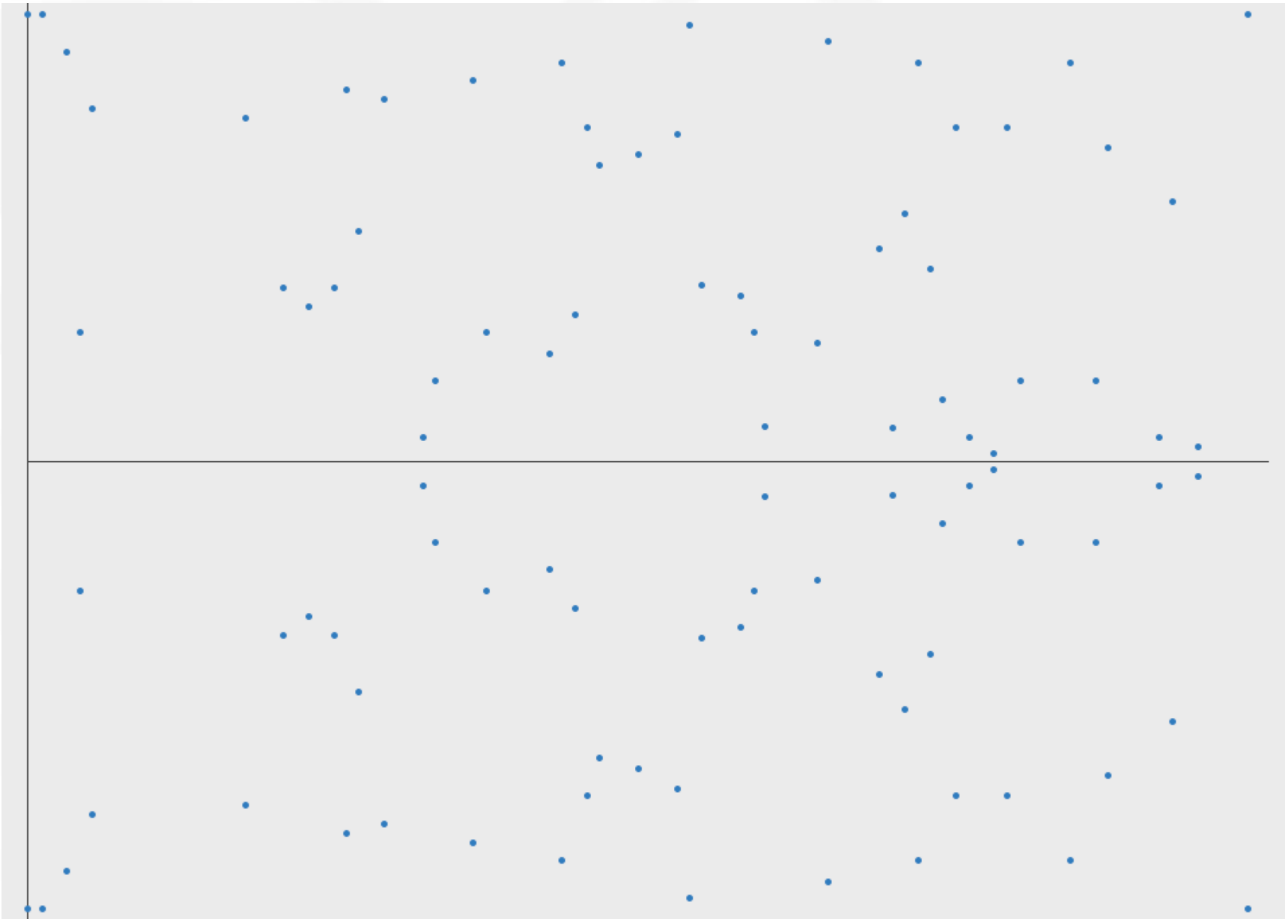
- 椭圆曲线公钥密码优势：对于椭圆曲线离散对数问题，目前不存在亚指数时间算法，从而为达到相同安全性所需的密钥尺寸更小
  - RSA 密码体制：2048比特；
  - 椭圆曲线密码体制：224-255比特。

- 椭圆曲线密码体制适用于计算、存储、带宽受限，但又要求高速实现的应用领域，例如智能卡、无线通讯等。

- 有限域上椭圆曲线



- 有限域上椭圆曲线加法



- El'Gamal密码方案的椭圆曲线形式

  - 设E为F_q上的椭圆曲线，一般记为$E(F_q)$，设$P=\left(x_p,y_p\right)\in E(F_q)$，且$P$的次数足够大，任取$1<s<ord\ (P)$，令$Q=\left(x_q,y_q\right)=sP$，则$E\left(F_q\right),P,Q$为公钥，$s$为私钥。
  - 消息m满足$m\in F_q^*$，任取$1<r<ord\ (P)$，计算$(x_1,y_1)=rP,(x_2,y_2)=rQ,c=m\cdot x_2$，则密文为$(x_1,y_1,c)$。
  - 解密时，计算$(x',y')=s(x_1,y_1)$，再计算$m'=c\cdot x'^{-1}$，解得明文。

- 方案的正确性

证明：因为$(x',y') = s(x_1,y_1) = srP = rsP = rQ = (x_2,y_2)$，因此$x' = x_2$，故$m' = c \cdot {x'}^{-1} = c \cdot x_2^{-1} = m$，得证。

- 方案的正确性

证明：因为$(x',y') = s(x_1,y_1) = srP = rsP = rQ = (x_2,y_2)$，因此$x' = x_2$，故$m' = c \cdot {x'}^{-1} = c \cdot x_2^{-1} = m$，得证。

- 方案的安全性依赖于椭圆曲线上的离散对数问题。

实验5

- El’Gamal密码方案的椭圆曲线形式
  - 令$E: y^2 = x^3 + x + 6$为F_{11}上的一条椭圆曲线，求E上的所有点。
  - 令$P = (2,7)$，取$s = 5$，求公钥。
  - 设消息$m = 3$，取r =7，求m的密文(x_1, y_1, c)。
  - 对(x_1, y_1, c)做解密运算，求(x', y')，并进一步求其明文m'。
- 要求：输出中间结果和最终结果
- 语言：C/C++或Python
- 使用头歌平台搭建环境并提交作业