椭圆曲线密码体制(ECC)

- ECC 因**密钥长度短、计算速度快**而迅速爆红，成为公钥密码的主流之一，是设计大多数**计算能力和存储空间有限**、**带宽受限**又要求**高速实现**的安全产品的首选。
  - 智能卡
  - 无线网络
  - 手持设备

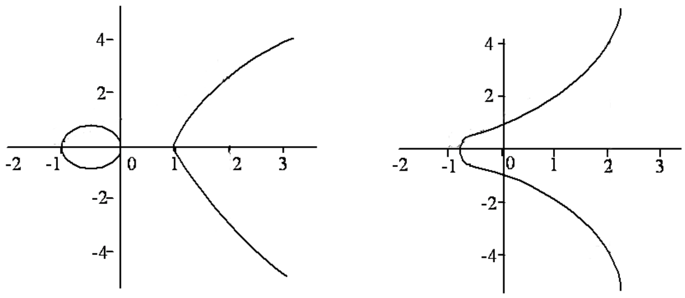
- 非奇异椭圆曲线

设a,b∈R，且 $4a^3+27b^2\neq 0$，方程 $E: y^2 = x^3 + ax + b$

的所有解(x,y)，连同一个无穷远点O组成集合E称为非奇异椭圆曲线。

- $4a^3+27b^2\neq 0$ 是保证方程有三个不同解(实数或复数)的充要条件

- 如果 $4a^3+27b^2=0$，则对应的椭圆曲线称为奇异椭圆曲线



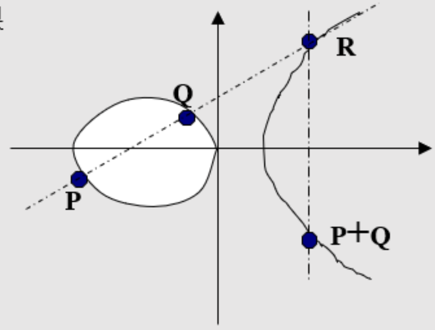
(a) $y^2=x^3-x$　　　　(b) $y^2=x^3+x+1$

非奇异椭圆曲线可构成加法交换群

- 若 E 是非奇异椭圆曲线，可在该集合上定义一个二元运算，通常用加法表示，使之成为交换群(E,+)。
- 加法交换群(E,+)的特性
  - 单位元：无穷远点 O
    - 对于任意 P∈E，有 P+O=O+P=P
  - 逆元：设 P=(x,y)∈E，则 P 的逆元定义为-P=(x,-y)
    - 于是，P+(-P)=(x,y)+(x,-y)=O
  - 对任意 P,Q∈E，设 $P=(x_1,y_1)$,$Q=(x_2,y_2)$，计算 P+Q 时考虑以下三种情况：

① $x_1 \neq x_2$ 时

– 画一条通过P、Q的直线与椭圆曲线交于R，R的逆元便是P+Q的结果

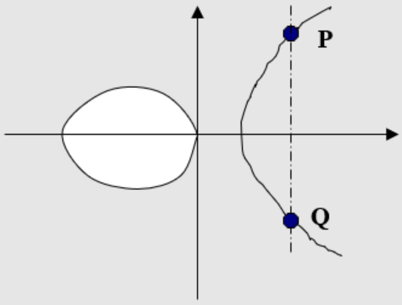


设$P+Q=(x_3,y_3)$，则

$$x_3=\lambda^2-x_1-x_2, y_3=\lambda(x_1-x_3)-y_1, \text{其中}\lambda=\frac{y_2-y_1}{x_2-x_1}$$

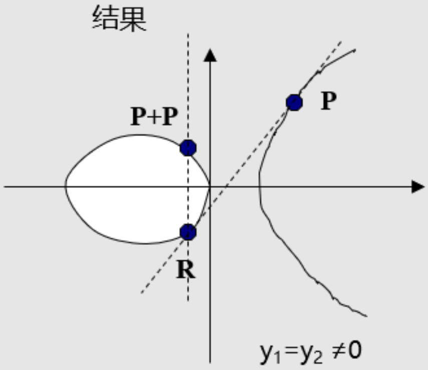
② $x_1=x_2$ 且 $y_1=-y_2$ 时，P与Q互为逆元

此时，P+Q=O

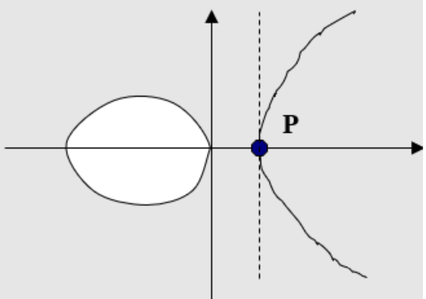


③ $x_1=x_2$ 且 $y_1=y_2$ 时，则P=Q (点P与自己相加)

– 画一条通过P的切线，与椭圆曲线交于R，R的逆元便是P+P的结果



$y_1=y_2 \neq 0$



$y_1=y_2=0$ P+P=O

设$P+P=(x_3,y_3)$，则

$$x_3=\lambda^2-2x_1, y_3=\lambda(x_1-x_3)-y_1, \text{其中}\lambda=\frac{3x_1^2+a}{2y_1}$$

- 令 P 为椭圆曲线 E 上一点。对正整数 n，若点 P 自加 n 次，即 P+P+…+P，可简写成 **nP**
- P 的阶：满足 nP=O 的最小正整数 n

有限域上的 ECC

- 密码学中使用的是**有限域上的椭圆曲线**，是由方程
  $E: y^2 \equiv x^3+ax+b \pmod p$
  定义的曲线(包括无穷远点 O)
  其中 $a,b \in F_p$，且满足 $4a^3+27b^2 \neq 0 \pmod p$
  - E 上点的坐标 x 和 y 都是 F_p 中的元素，即属于{0,1,…,p-1}
  - **注意：**前面介绍的椭圆曲线方程的系数是实数(连续的)，而有限域上的椭圆曲线方程的系数属于 F_p(离散的，整数)

- 有限域 F_p 上的椭圆曲线，通常记为 $E(F_p)$，简记为 E （F_p 称为 E 的基域)
- $E(F_p)$在加法定义下形成交换群，简记为(E,+)
  - 单位元：无穷远点 O
  - 加法运算与实数上的曲线加法相同，只是所有的坐标运算都是模 p 的

椭圆曲线上的困难问题

- 椭圆曲线密码体制(ECC)建立在椭圆曲线上的困难问题之上
- 基于离散对数、Diffie-Hellman 问题的密码方案均可用椭圆曲线实现
  - Diffie-Hellman 密钥交换协议（椭圆曲线版）
  - ElGamal 密码体制（椭圆曲线版）

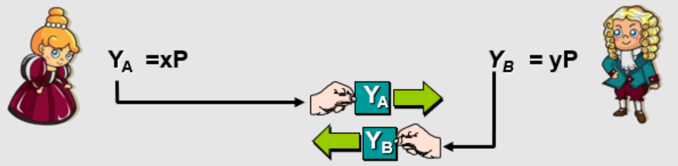
  ……
- 设 $P \in E(F_p)$, P 的阶是一个非常大的素数，则有如下两个困难问题：
  - **椭圆曲线上的离散对数问题(DL)**

 令 Q=kP，则给定 P、Q，求 k 是计算上不可行的
  - **椭圆曲线上的计算 Diffie-Hellman 问题(CDH)**

 给定 aP、bP，求 abP 是计算上不可行的

椭圆曲线版 Diffie-Hellman 密钥交换协议

- **系统建立：**
  - 选择椭圆曲线$E(F_p)$，及其上一点P，设P的阶是一个非常大的素数
  - $E(F_p)$和P是公开的系统参数
- **密钥交换如下图：**



$xY_B = K$　　　$yY_A = K$

$(xyP = K)$　　　$(xyP = K)$

椭圆曲线概述　ECC 的优点小结

① **安全性高**
- 比基于传统离散对数问题的公钥体制更安全

② **灵活性好**
- F_p上的椭圆曲线可通过改变参数得到不同的曲线

③ **密钥长度更短**
- 使用更短的密钥长度提供相同的安全强度

ECC	**160 bit**	**224 bit**
RSA	**1024 bit**	**2048 bit**
密钥长度比	**6:1**	**9:1**

SEC（高效密码学标准）
提出者：Certicom Corp
比特币中使用 ECDSA/secp256k1 曲线

双线性映射技术（Bilinear Pairing）

- **超奇异椭圆曲线**是有限域上一种特殊的椭圆曲线
- 在该类曲线上，存在一种被称为**双线性映射**(bilinear pairing)的有效算法，可以**将曲线上两个点映射到基域上的一个元素**
- 如今，基于超奇异椭圆曲线和双线性映射的密码体制变得炙手可热，成为当今密码学研究的热点。

双线性映射技术　　描述

- 设 p 是大素数，加法群 G_1 和乘法群 G_2 都是 p 阶群。双线性映射 $e:G_1 \times G_1 \to G_2$ 满足以下条件：
  - ① **双线性**：对任意 $P,Q,R \in G_1$ 和 $a,b \in Z^*_p$ 有
    $e(P, Q+R)=e(P, Q)\ e(P, R)$
    $e(P+Q, R)=e(P, R)\ e(Q, R)$
    $e(aP, bQ)=e(P, Q)^{ab}$
  - ① **非退化性**：存在 $P \in G_1$,有 $e(P, P) \neq 1$
  - ② **可计算性**：对于所有 $P,Q \in G_1$, $e(P, Q)$可有效计算
- 通常，取 G_1 为有限域上超奇异椭圆曲线，G_2 为 G_1 的基域（椭圆曲线所基于的有限域）

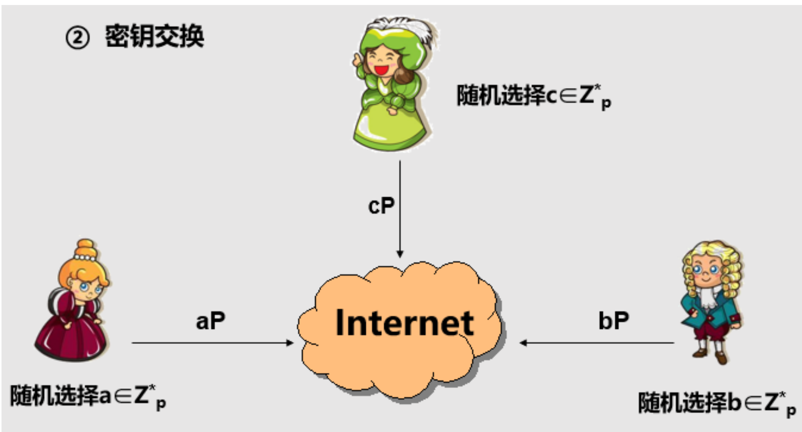
双线性映射技术　　超奇异椭圆曲线上的困难问题

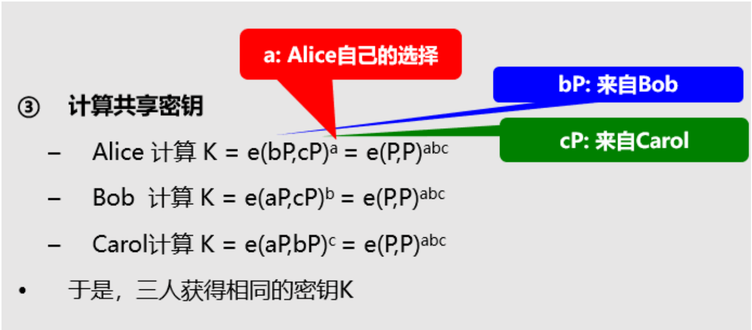
① 离散对数问题(DL)
② 计算 Diffie-Hellman 问题(CDH)
③ 双线性 Diffie-Hellman 问题(BDH)
　设 $a, b, c \in Z^*_p$，给定 $P, aP, bP, cP \in G_1$
　求 $e(P,P)^{abc}$ 是计算上不可行的

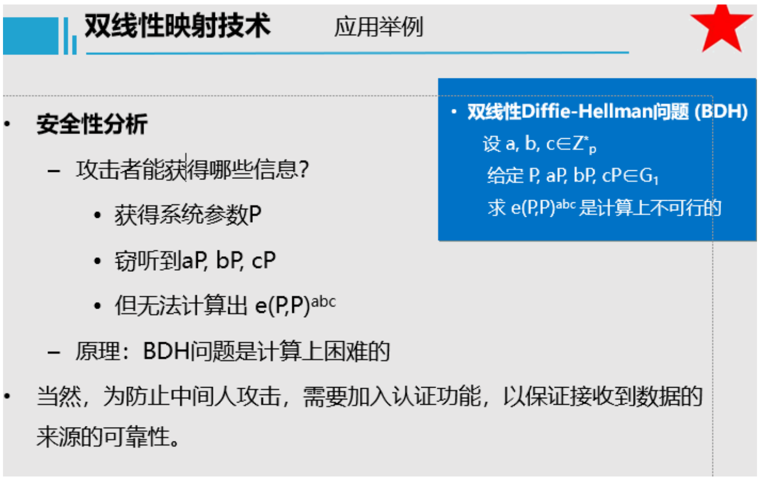
双线性映射技术　　应用举例

三方 Diffie-Hellman 密钥交换协议

① **系统建立**
- 随机选择大素数 p，生成 p 阶加法群 G_1 和乘法群 G_2
- 随机选择阶足够大的元素 $P \in G_1$
- $e:G_1 \times G_1 \to G_2$ 是双线性映射







双线性映射技术 优缺点

- **优点**

  提供了丰富的运算性质，可以满足以前难以满足的安全需求

- **缺点**

  目前广泛应用的算法(Weil pairing, Tate pairing)计算速度相对较慢

8.2 基于身份的密码学(IBC)

- 传统公钥密码体制存在的问题：

  公钥杂乱无章，随机的，不可识别。

- **如何确保公钥的真实性？**
  - 需要将所有者的身份和公钥绑定
    - 公钥证书，PKI
    - 但 PKI 的运行和维护代价很大

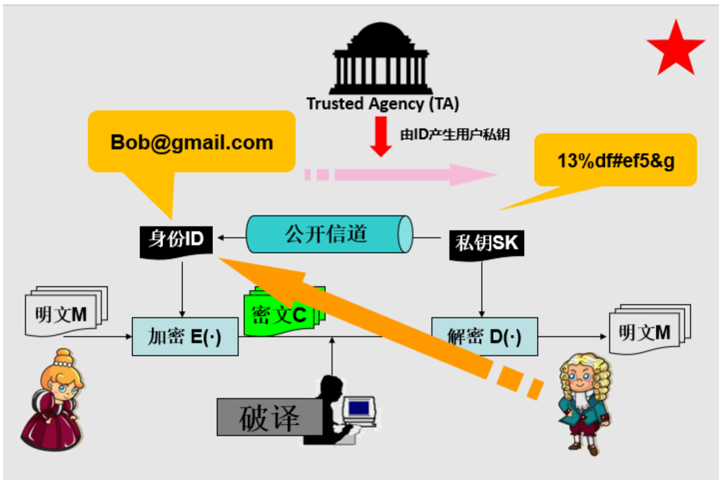
- **Q: 是否有另一种解决该问题的方法？**

  A:基于身份的密码学 (IDENTITY-BASED CRYPTOGRAPHY)

IBC 的提出：ADI SHAMIR　1984 年

IBC 的原理

- 传统公钥密码中公钥的产生
  - 先选择私钥，再计算公钥，公钥必然显得 “一片混乱”
- IBC 产生公钥的原理
  - 先选择公钥，再计算私钥
  - 公钥可选择 email 地址、身份证号等，称之为用户的身份，记为 ID
    (注意：公钥就是 ID，或从 ID 直接推导而来)
  - 私钥看起来杂乱无章，没关系，反而有利



IBC下的秘密通信模型

- **ID 必须是每个用户唯一确定的信息**，比如身份证号、电子邮箱等。
- 需要注意的是
  - ID 并没有任何特殊的数学意义，它所具有的是特殊的社会意义。
  - 因为，数学上可以用任何串做公钥，于是我们选择了具有特殊社会意义的串作为 ID。

Trusted Agency (TA)

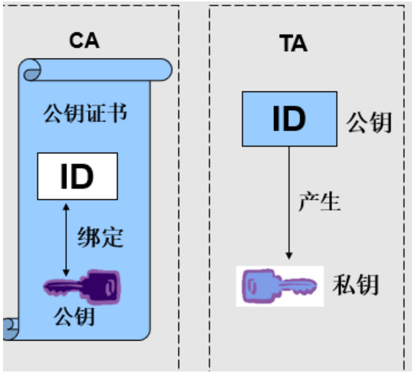
- 我们依然需要一个可信第三方，用以帮助用户产生私钥，称之为
  Trusted Agency (TA)
  也即，用户选择自己的 ID 作为公钥
  TA 根据 ID 产生相应的私钥（用户的私钥从 TA 那里获得）
- **注意**
  - **IBC 中的 TA 与 PKI 中的 CA 职能不同**
  - **TA 的任务简单很多**

CA 与 TA 的区别

- **CA 的任务**

  绑定 ID 和公钥 (ID 不是公钥)
- **TA 的任务**

  由 ID 计算出私钥 (公钥就是 ID，或从 ID 直接推导而来)



IBC 的优缺点

- **优点**
  - 避免使用复杂的 PKI 系统
- **缺点**
  - 私钥泄露以后，相应的 ID 也就无法使用
    - 密钥撤销问题是影响 IBC 发展的主要桎梏
  - 密钥托管问题（Key-escrow）
    - 私钥由 TA 产生，一旦 TA 被攻破，所有用户信息将受到严重威胁