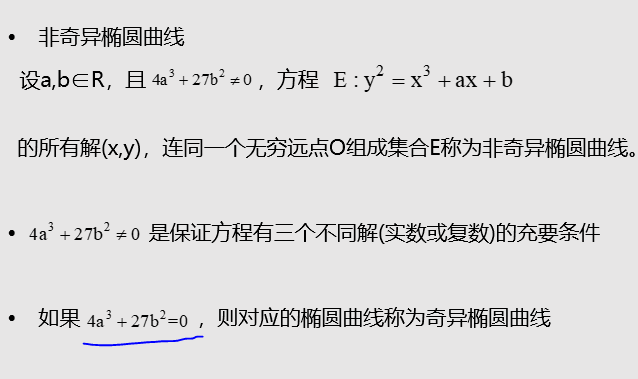
椭圆曲线密码体制(ECC)

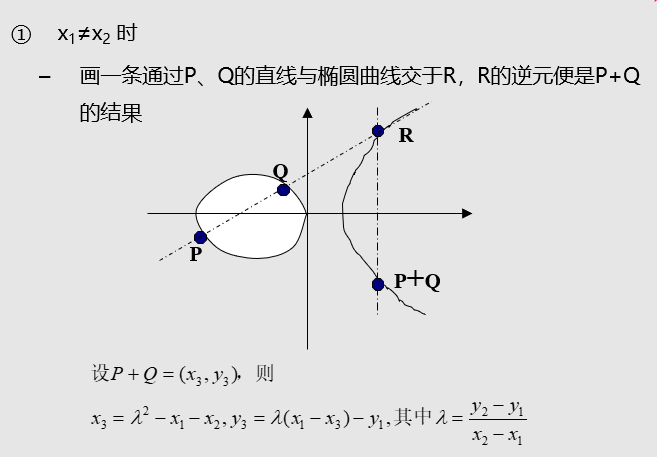
* ECC因**密钥长度短、计算速度快**而迅速爆红，成为公钥密码的主流之一，是设计大多数**计算能力和存储空间有限**、**带宽受限**又要求**高速实现**的安全产品的首选。
  + 智能卡
  + 无线网络
  + 手持设备

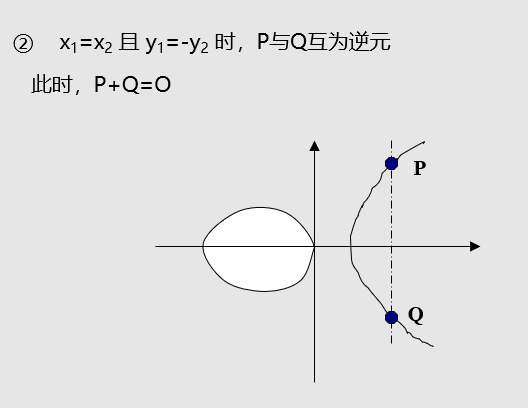


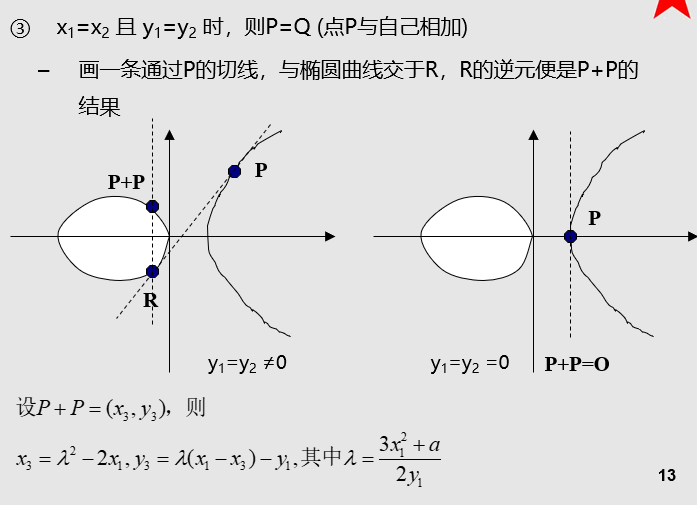


**非奇异椭圆曲线可构成加法交换群**

* 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=(x1,y1),Q=(x2,y2)，计算P+Q时考虑以下三种情况：







* 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: y2≡x3+ax+b (mod p)

定义的曲线(包括无穷远点O)

其中 a,b∈Fp，且满足4a3+27b2 ≠0 (mod p)

* + E上点的坐标 x 和 y 都是Fp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Fp(离散的，整数)
* 有限域Fp上的椭圆曲线，通常记为E(Fp)，简记为E (Fp 称为E的基域)
* E(Fp)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）

……

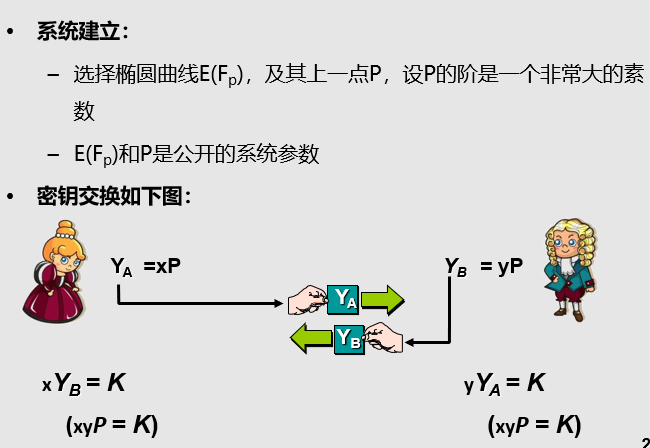
* 设P∈E(Fp), P的阶是一个非常大的素数，则有如下两个困难问题：
  + **椭圆曲线上的离散对数问题(DL)**

令Q=kP，则给定P、Q，求k是计算上不可行的

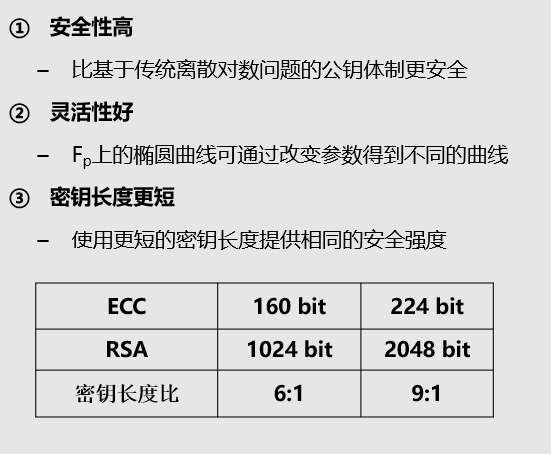
* + **椭圆曲线上的计算Diffie-Hellman问题(CDH)**

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**



**椭圆曲线概述** ECC的优点小结



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G1和乘法群G2都是p阶群。双线性映射e:G1×G1→G2满足以下条件：
  1. **双线性**：对任意 P,Q,R∈G1 和 a,b∈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∈G1,有e(P, P)≠1
  2. **可计算性**：对于所有P,Q∈G1, e(P, Q)可有效计算
* 通常，取G1为有限域上超奇异椭圆曲线，G2为G1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)

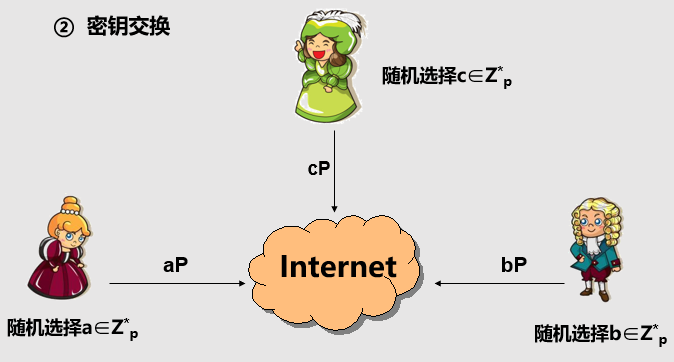
设 a, b, c∈Z\*p，给定 P, aP, bP, cP∈G1

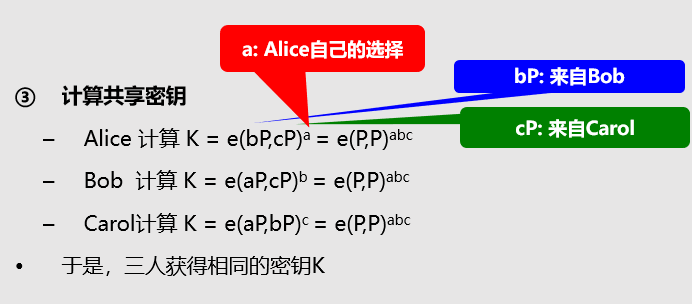
求e(P,P)abc 是计算上不可行的

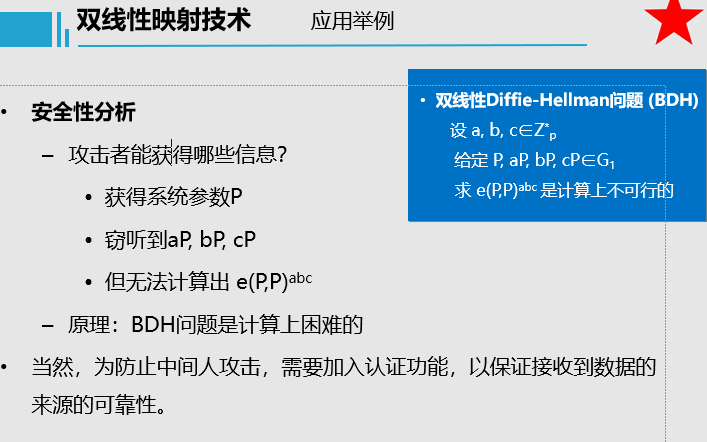
**双线性映射技术** 应用举例

**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G1和乘法群G2
     + 随机选择阶足够大的元素P∈G1
     + e:G1×G1→G2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)

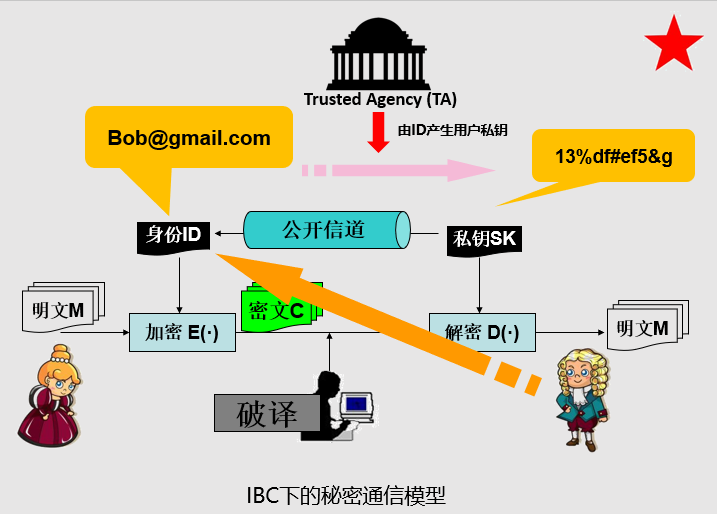
IBC的提出：Adi Shamir 1984年

### 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



* **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**

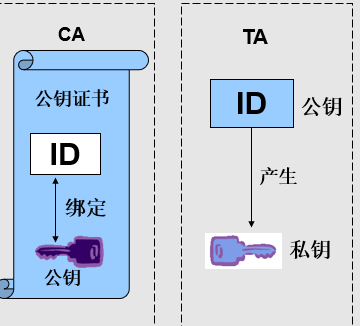
**CA 与 TA 的区别**

* **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