现代密码学

中国海洋大学　信息安全实验室

第8章

椭圆曲线与基于身份的密码学

本章内容

8.1 椭圆曲线概述

8.2 基于身份的密码学(IBC)

8.1 椭圆曲线概述

- 1985年，N.Koblitz(华盛顿大学) 和 V.Miller(IBM)分别独立提出了椭圆曲线密码体制(ECC)的思想

Neal Koblitz

- 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

  ……

椭圆曲线的曲线方程

- 一般来讲，椭圆曲线的曲线方程是以下形式的三次方程：

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

其中，$a_1,a_2,a_3,a_4,a_5,a_6 \in R$

- **满足该方程的(x,y)称为椭圆曲线E上的点，通常用大写字母P、Q或R表示。**

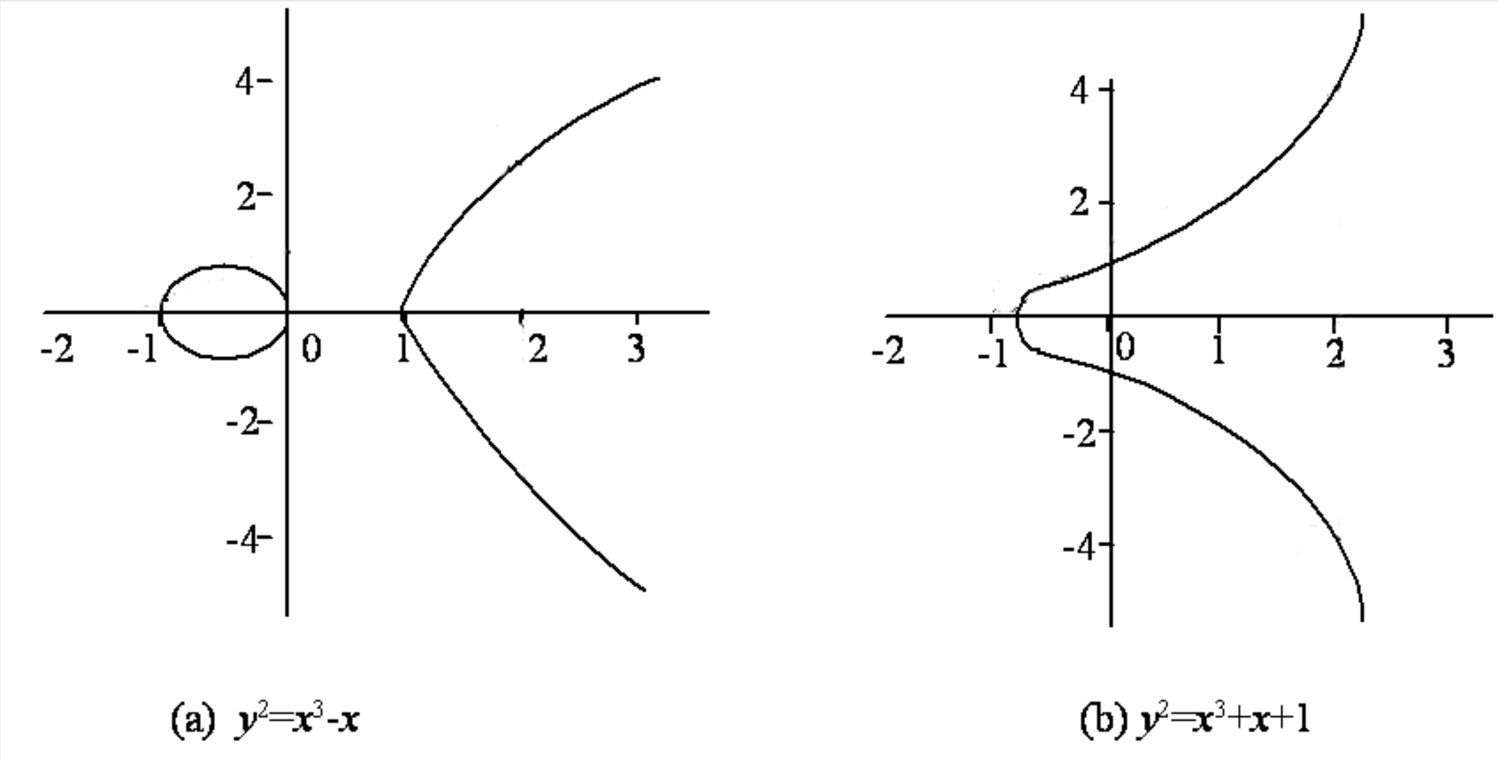
- 非奇异椭圆曲线

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



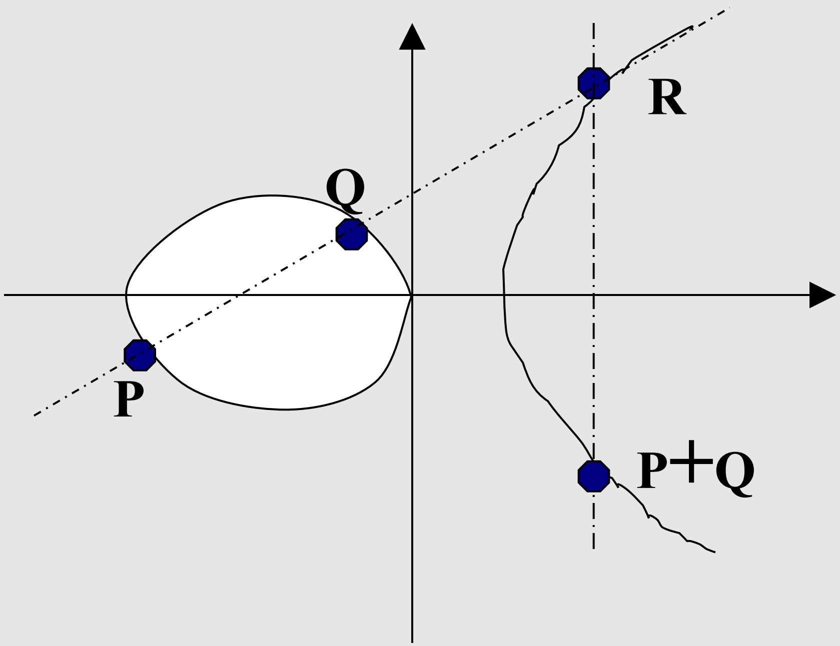
非奇异椭圆曲线的两个例子

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

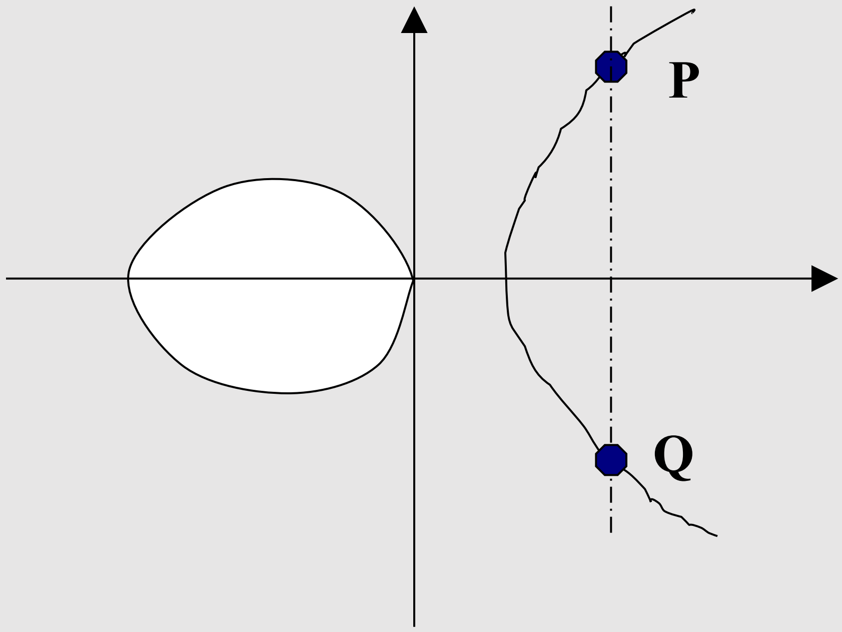


设$P+Q=(x_3, y_3)$，则

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

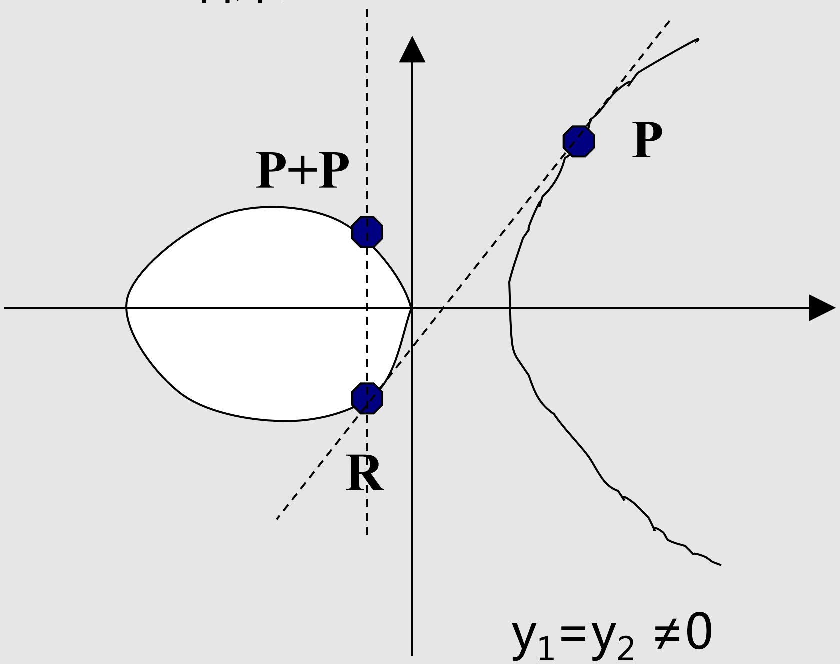
② $x_1=x_2$ 且 $y_1=-y_2$ 时，P与Q互为逆元

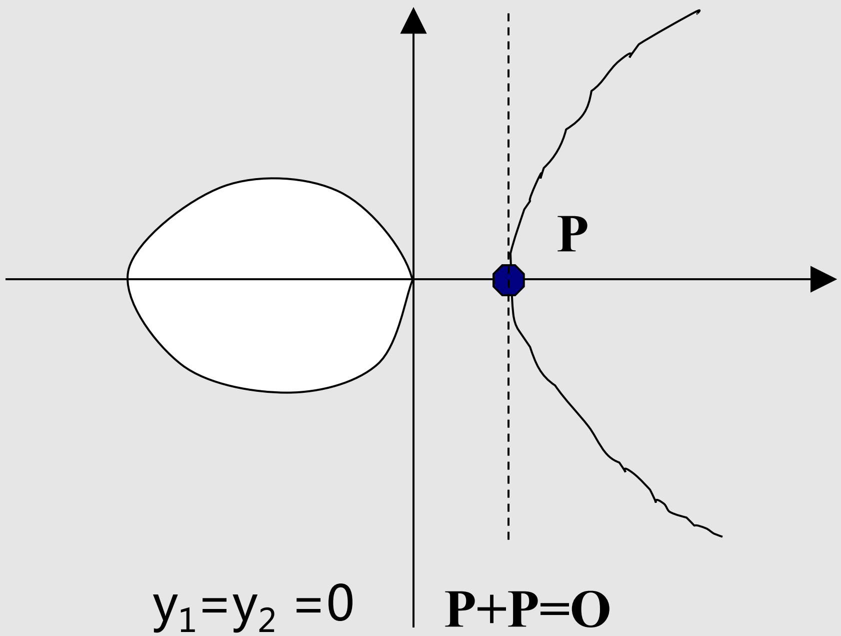
此时，P+Q=O



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





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)

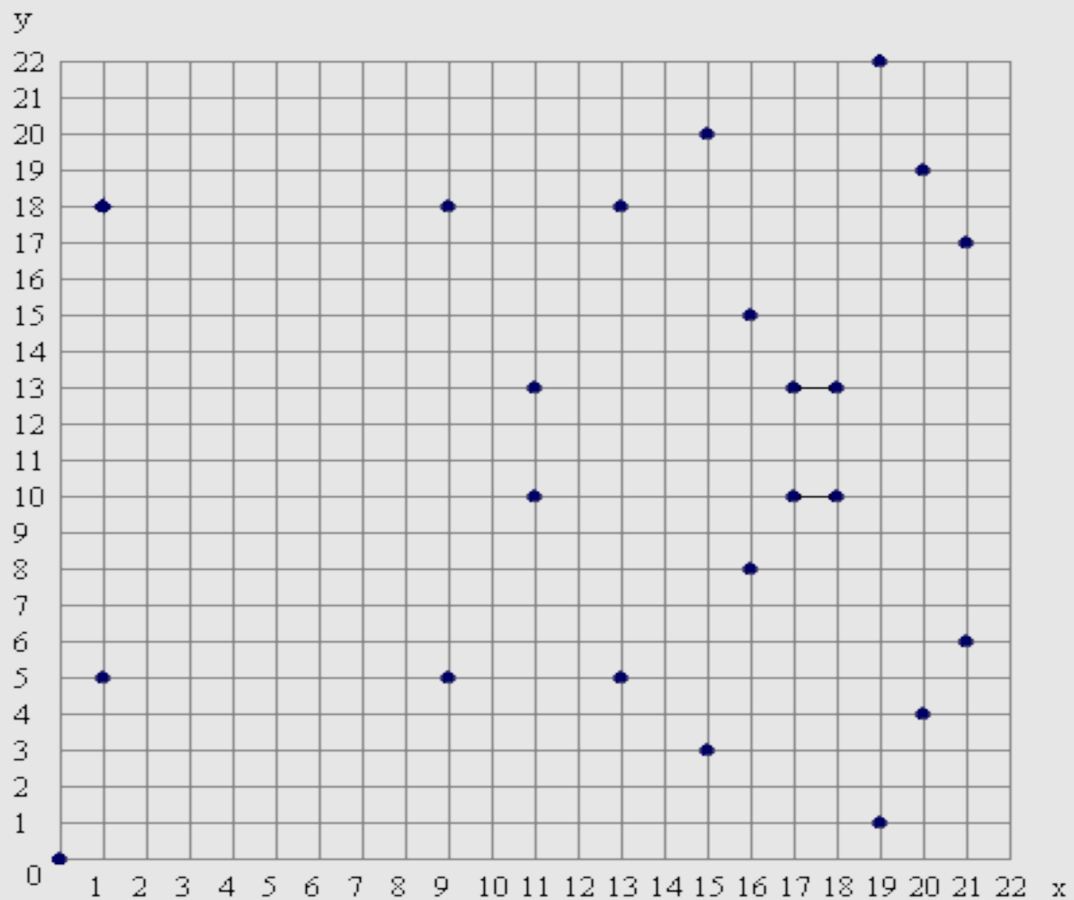
  其中 $a,b \in F_p$，且满足$4a^3+27b^2 \neq 0 \pmod p$
  - E上点的坐标 x 和 y 都是F_p中的元素，即属于{0,1,…,p-1}
  - **注意**：前面介绍的椭圆曲线方程的系数是实数(连续的)，而有限域上的椭圆曲线方程的系数属于F_p(离散的，整数)

F_p 称为E的基域

- 有限域F_p上的椭圆曲线，通常记为$E(F_p)$，简记为E
- $E(F_p)$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

举例

- $y^2 = x^3 + x \bmod 23$



Elliptic curve equation: $y^2 = x^3 + x$ over F_{23}

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）

  ……

椭圆曲线上的困难问题

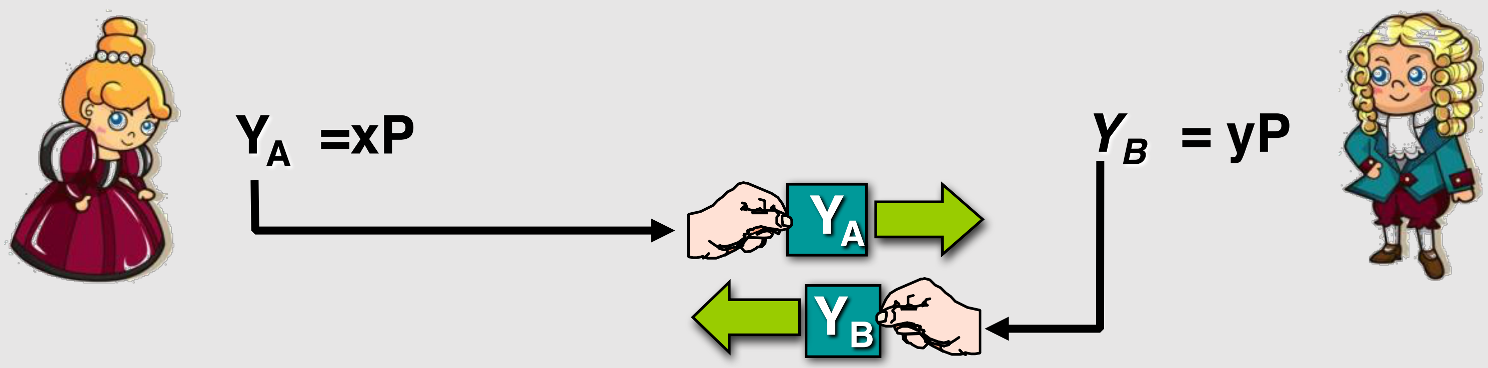
- 设P∈E(F_p), P的阶是一个非常大的素数，则有如下两个困难问题：
  - **椭圆曲线上的离散对数问题(DL)**

    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：**



$xY_B = K$

$(xyP = K)$

$yY_A = K$

$(xyP = K)$

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**

- 国外已有用ECC进行加解密的产品出现在市场上
  - 美国NeXT Computer公司开发快速椭圆曲线加密(FEE)算法
  - 加拿大Certicom公司开发出实用的ECC集成电路
  - 3COM/Palm Computing、Motorala、日本Mitsushita及NTT实验室、法国Thompson、德国Siemens、加拿大Waterloo大学等也都实现这一体制 (包括软件和硬件实现)
- 目前，ECC标准化正在进行中。虽然还没有统一的标准方案，但已有一些较为成熟的标准出现
  - IEEE（P1363）
  - ANSI X9F1工作组（X9.42，X9.62和X9.63）
  - ISO/IEC

……

SEC Standards for Efficient Cryptography

- **Recommended Elliptic Curve Domain Parameters**
  - 提出者：Certicom Corp.

拥有超过500个关于ECC的专利

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 $e:G_1\times G_1\rightarrow G_2$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

$$e(P, Q+R)=e(P, Q)\, e(P, R)$$

$$e(P+Q, R)=e(P, R)\, e(Q, R)$$

$$e(aP, bQ)=e(P, Q)^{ab}$$

② **非退化性**：存在$P\in G_1$,有$e(P, P)\neq 1$

③ **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)

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

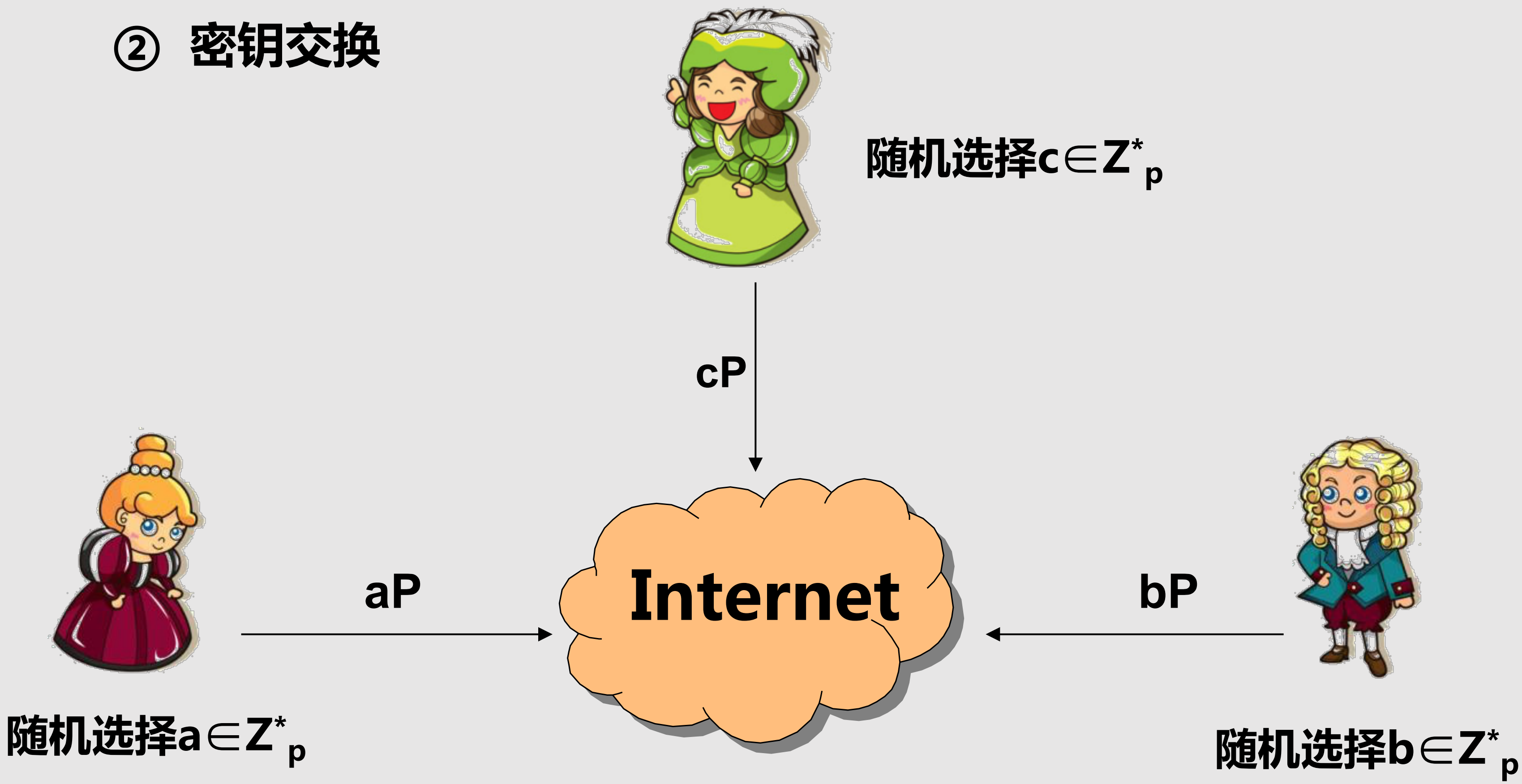
- **三方Diffie-Hellman密钥交换协议**

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$P \in G_1$
- $e: G_1 \times G_1 \rightarrow G_2$是双线性映射

双线性映射技术　应用举例

② 密钥交换



a: Alice自己的选择

bP: 来自Bob

cP: 来自Carol

③ **计算共享密钥**

- Alice 计算 $K = e(bP,cP)^a = e(P,P)^{abc}$
- Bob 计算 $K = e(aP,cP)^b = e(P,P)^{abc}$
- Carol计算 $K = e(aP,bP)^c = e(P,P)^{abc}$

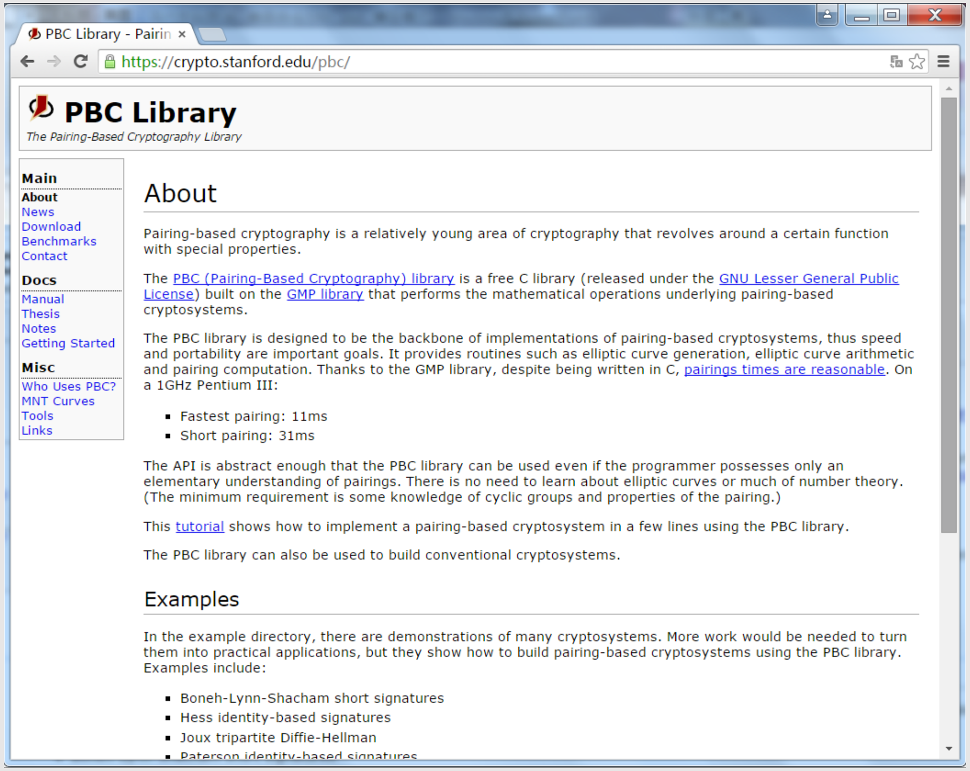
• 于是，三人获得相同的密钥K

- **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

- **安全性分析**
  - 攻击者能获得哪些信息？
    - 获得系统参数P
    - 窃听到aP, bP, cP
    - 但无法计算出 $e(P,P)^{abc}$
  - 原理：BDH问题是计算上困难的
- 当然，为防止中间人攻击，需要加入认证功能，以保证接收到数据的来源的可靠性。

双线性映射技术　支持双线性映射的软件包

- **PBC-library**
  - 开发者：Ben Lynn
  - 注：需要另一个软件包GMP的支持



- **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

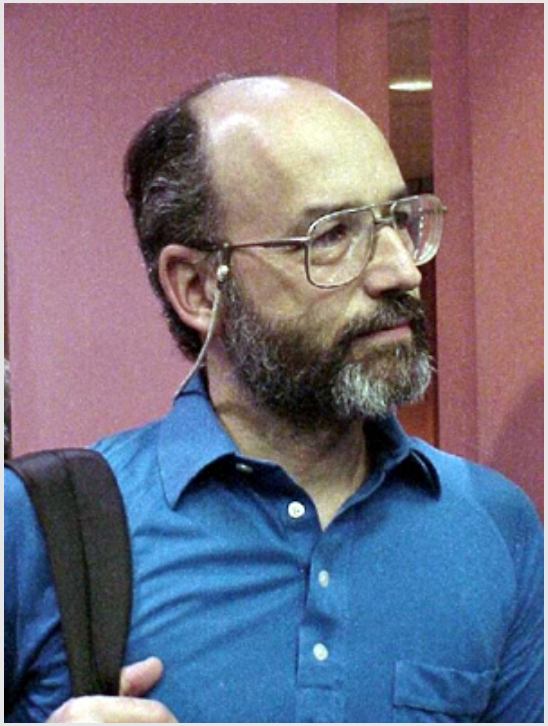
Q: 是否有另一种解决该问题的方法？

基于身份的密码学 (Identity-Based Cryptography)

- IBC 的提出

  Adi Shamir

  1984年

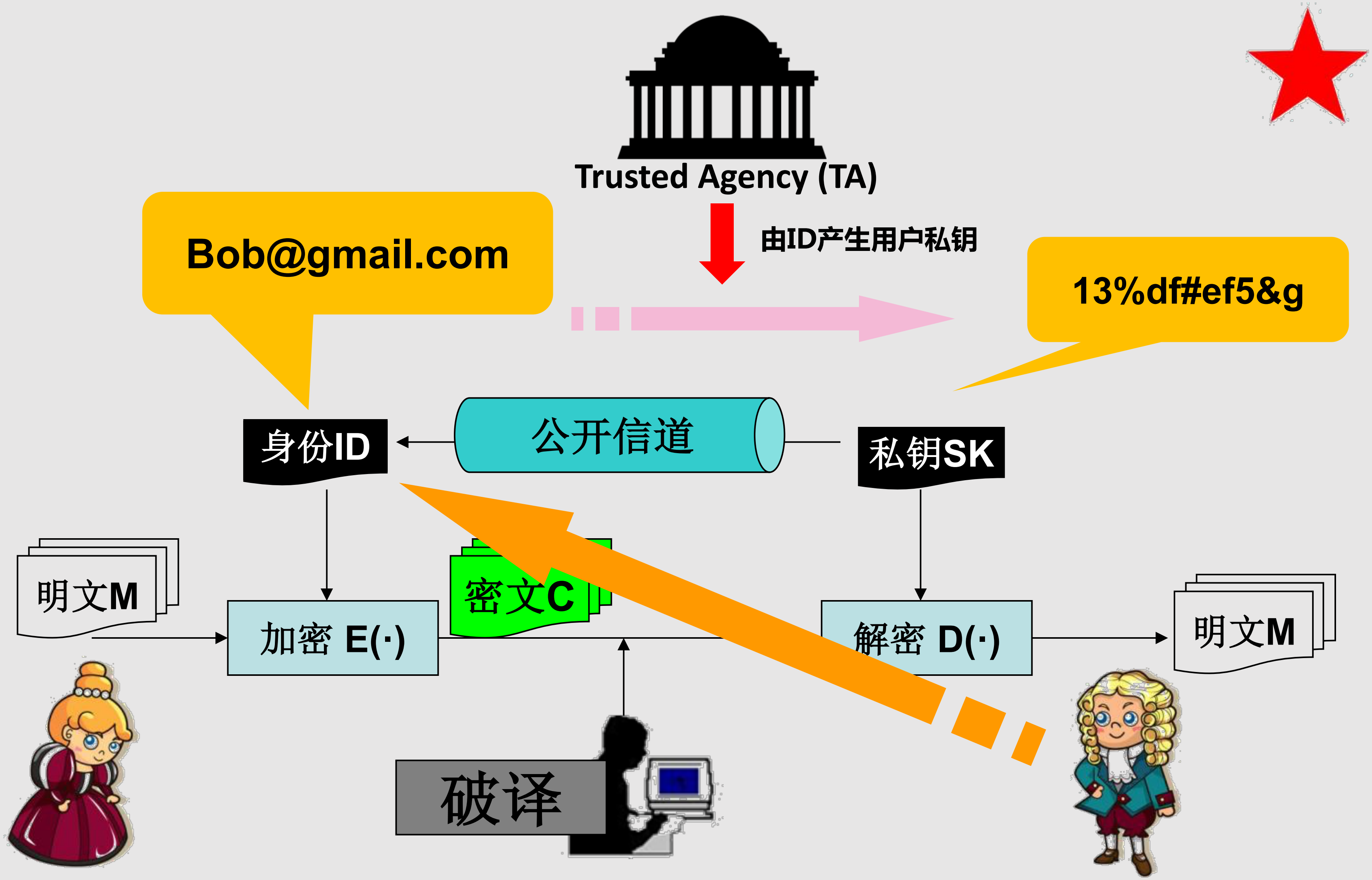


相关文献： Identity-Based Cryptosystems and Signature Scheme

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)

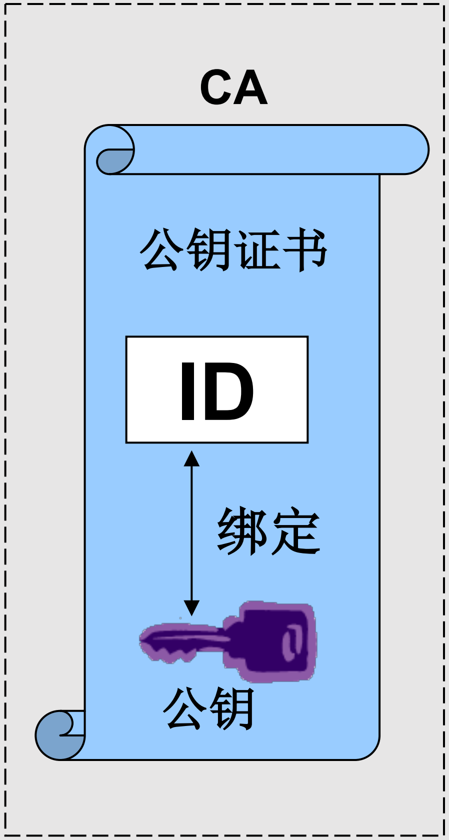
  也即，用户选择自己的ID作为公钥

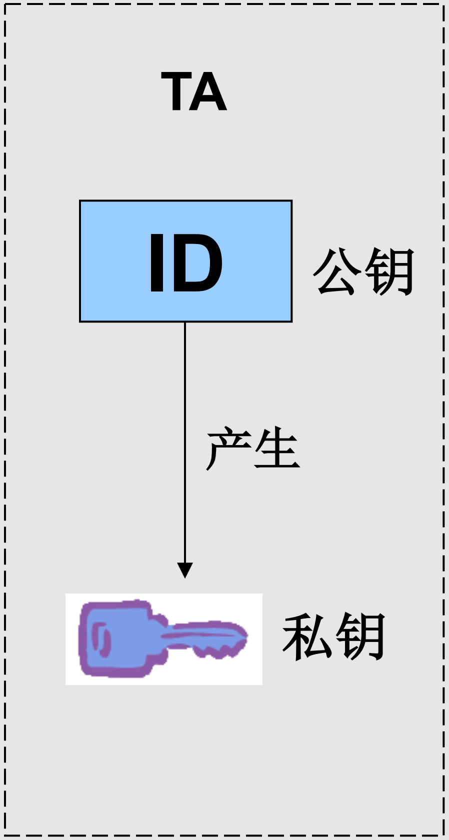
  TA根据ID产生相应的私钥（用户的私钥从TA那里获得）

- **注意**
  - **IBC中的TA 与 PKI中的CA 职能不同**
  - **TA的任务简单很多**

Trusted Agency (TA)

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**
  - ① 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
  - ② 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

私钥泄露了

怎么办

扩展阅读

IBS
基于身份的
签名方案

IBE
基于身份的
加密方案

本章小结

1. 掌握ECC的优势
2. 掌握椭圆曲线加法群的几何性质
3. 掌握双线性映射技术的描述
4. 掌握IBC的基本概念、优缺点、TA和CA的区别
5. 了解椭圆曲线版Diffie-Hellman密钥交换协议

练习题

1. **与传统公钥密码相比，ECC的优点是 (　　D　　)**

   A. 安全性高　B. 灵活性好　C. 密钥长度更短　D. 以上都对

2. **不属于双线性映射特性的是 (　　D　　)**

   A. 双线性　B. 非退化性　C. 可计算性　D. 差分性

3. **TA的主要任务是 (　　B　　)**

   A. 签发证书　B. 产生用户私钥

   C. 作废过期证书　D. 以上都不对

练习题

4. IBC中的密钥托管问题是指（ C ）

A. ID如果发生泄露，其安全性会受到威胁

B. 私钥泄露以后，相应的ID也就无法使用

C. 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

D. 以上都不对

练习题

5. 双线性映射技术作用于（ C ）

A. 奇异椭圆曲线　B. 非奇异椭圆曲线

C. 超奇异椭圆曲线　D. 以上都不对

6. 双线性映射技术可以（ B ）

A. 将曲线上一个点映射到其基域的一个元素

B. 将曲线上两个点映射到其基域的一个元素

C. 将基域的一个元素映射到曲线上的一个点

D. 以上都不对