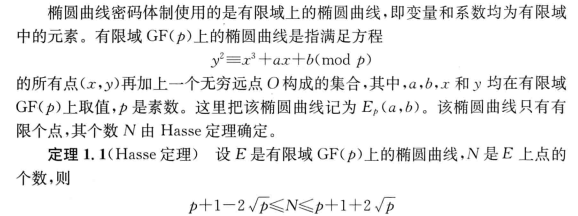
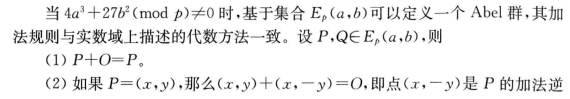
# 基于配对的密码学

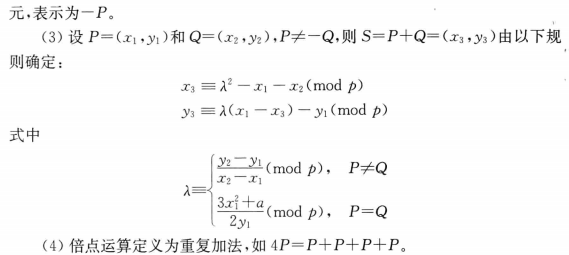
近年来，利用椭圆曲线构造的双线性配对(bilinear pairings)称为密码学领域的焦点。双线性配对，即代数曲线上的Weil配对和Tate配对，研究代数几何的重要工具。他们在密码学上的早期应用主要是攻击椭圆曲线或超椭圆曲线密码体制，即将椭圆曲线或超椭圆曲线上的离散对数问题归纳为有限域中乘法群上的离散对数问题。他们是构造短签名体制、基于身份的加密体制、基于身份的签名体制、无证书加密体制、无证书签名体制、一轮三方密钥协商铁艺·协议的重要工具。基于配对的密码学(pairing-based cryptography)就是研究双线性配对理论、配对的快速实现、密码体制的设计与安全性证明的学科。

## 有限域上的椭圆曲线

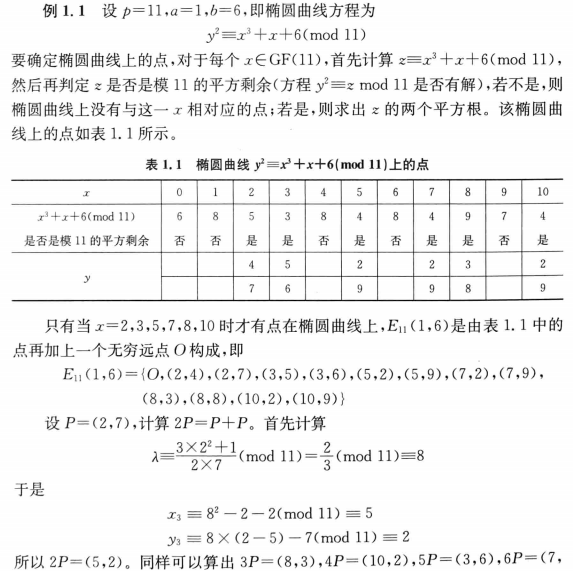


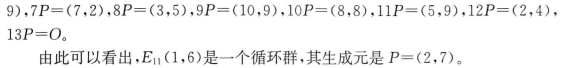
有限域上的椭圆曲线，即变量和系数均为有限域中的元素



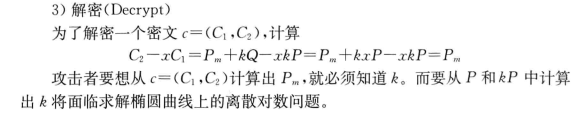
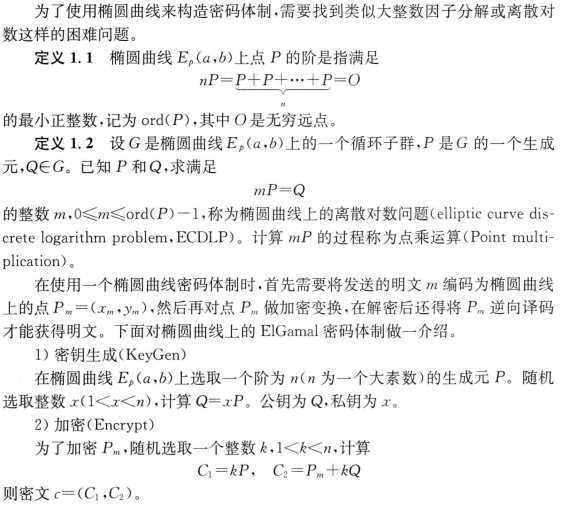


这里(x,-y),-y实际上是y在p上的逆元！！

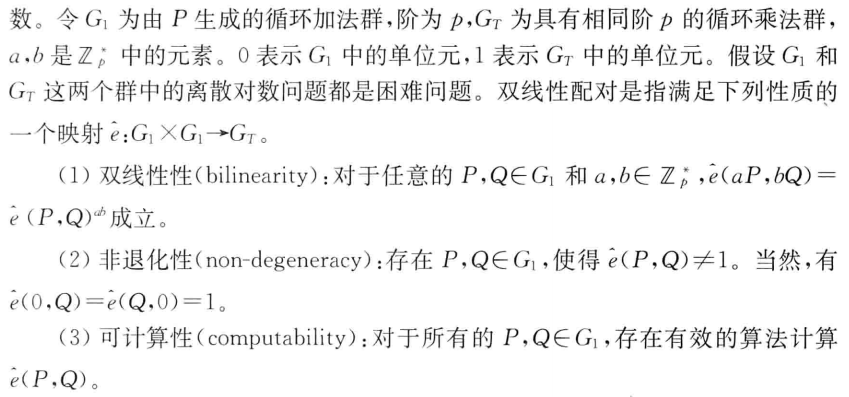


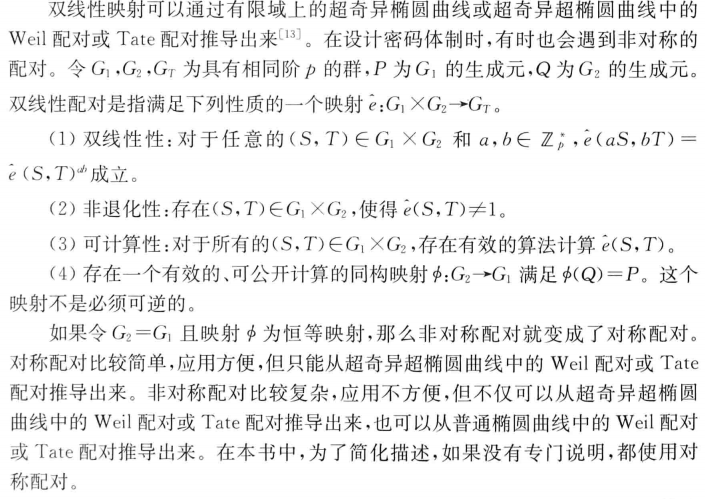


## 椭圆曲线上的EIGamal加密体制



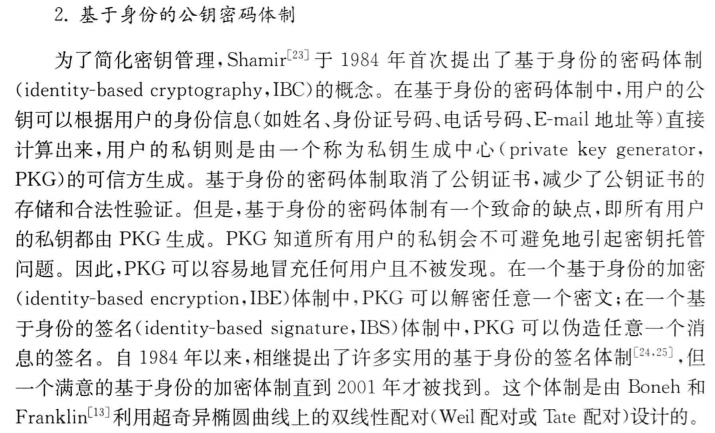
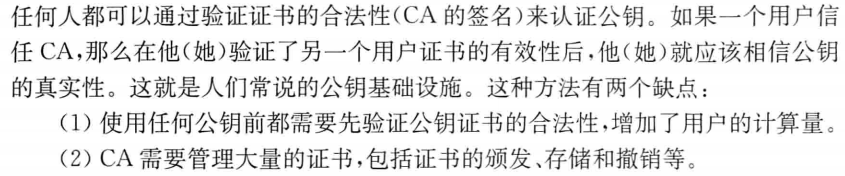
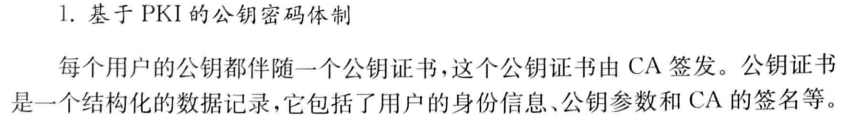
## 双线性配对理论



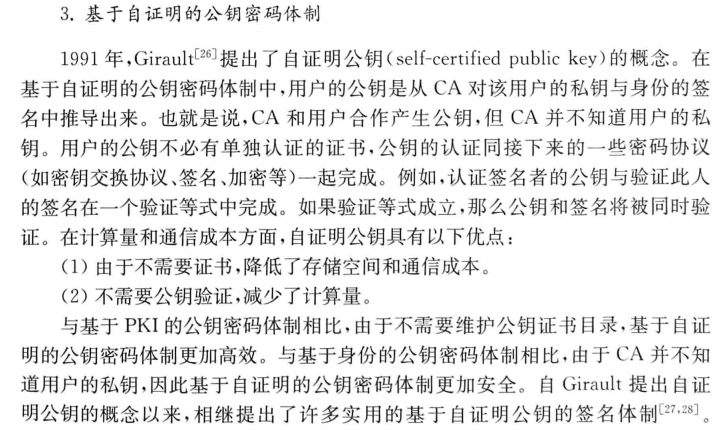


## 公钥认证方法

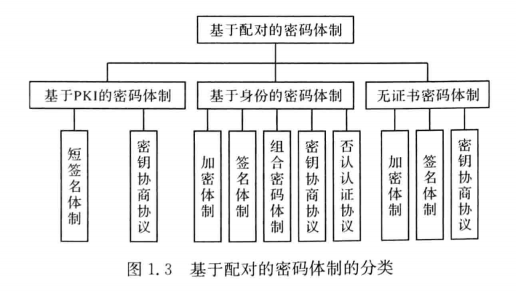
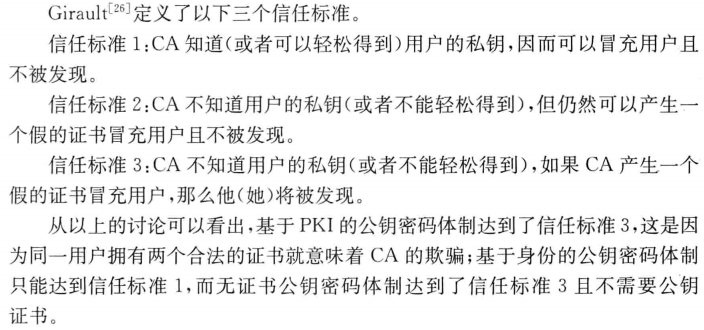
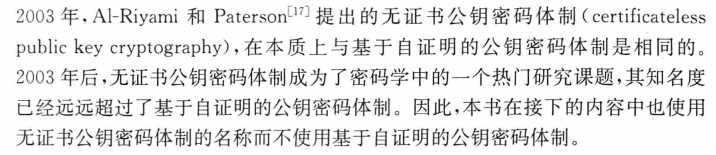
在公钥密码体制中，每个用户拥有两个密钥：私钥和公钥。其中只有私钥有用户秘密保存，公钥可以有一个整数权威(certificate authority,CA)保存在一个公钥目录中。然而，公钥密码体制易受到“公钥替换”攻击，即攻击者用自己选定的假公钥替换公钥目录之中正是的密钥。当一个用户用着个加密要加密一个消息时，这个攻击者就可以争取解密。为了抵抗公钥替换攻击，需要让用户的公钥可以以一种可验证和可行的方式与用户的身份信息关联起来。目前，认证用户的公钥有三种不同的方法：基于公钥基础设施(public key infrastructur) KPI的方法、基于身份的方法、和基于自证明的方法。



用户的公钥根据用户的身份信息直接计算出来，而用户的私钥有密钥生成中心生成。



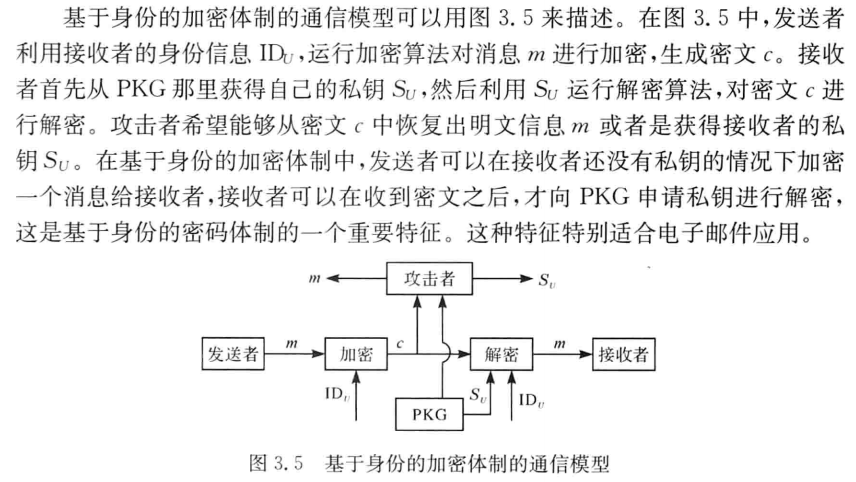
自证明中，CA与用户合作产生公钥，CA不知道用户的私钥。公钥的认证同接下下来的密码协议一同完成。



## 3.3 基于身份的加密体制

### 算法框架：

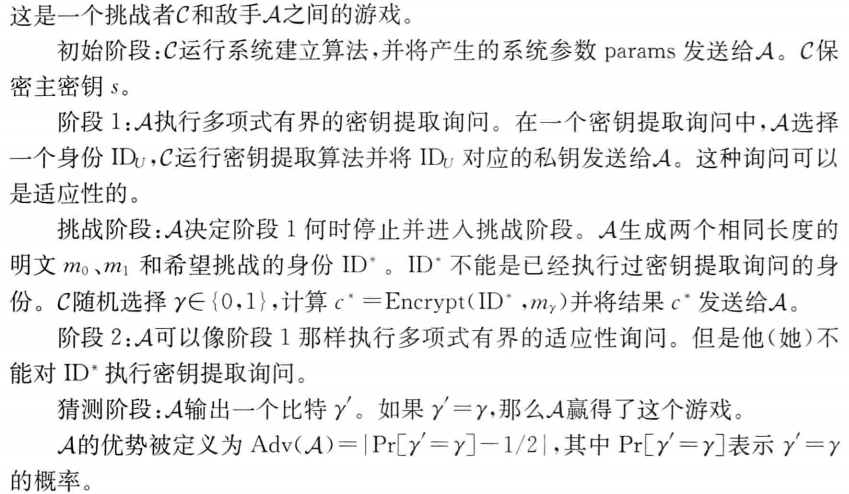
这里PKG保密了主密钥S，显然密钥提取过程中是通过主密钥S对IDu进行加密从而得到Su。



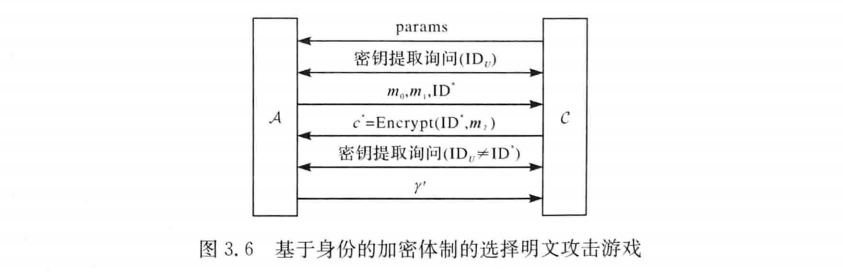
再给予身份的加密体制中，发送者可以在接收者还没有私钥的情况下加密一个消息给接收者，接收者可以在接受密文之后才向PKG(Private key Generation)申请私钥进行解密，这是基于身份的密码体制的一个重要特征。这种特征特别适合用于电子邮件应用。

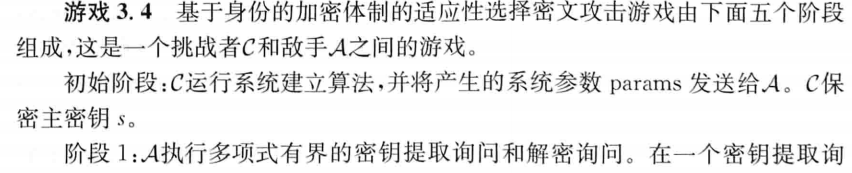
### 可证明安全性

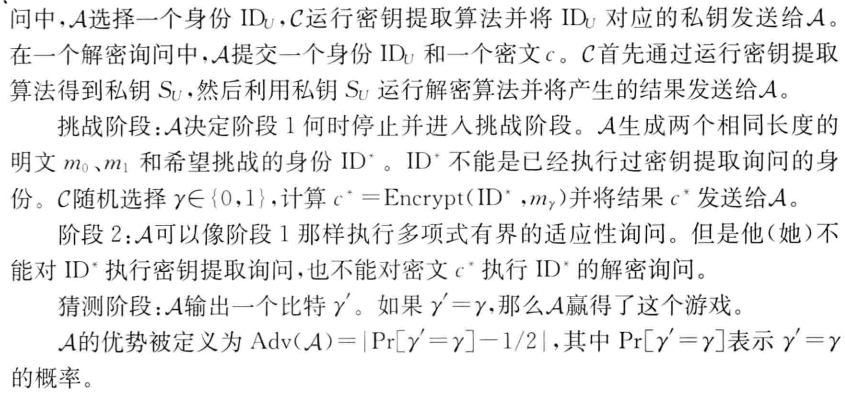
在证明安全性时，需要注意的是当一个敌手攻击一个公钥ID时，这个敌手可能已经拥有了其他用户的私钥。



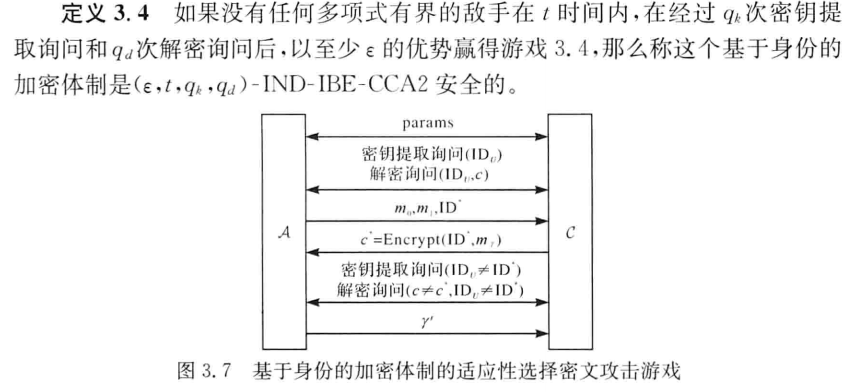
这个过程中选择明文攻击主要是攻击的是从公钥到私钥的加密过程。即IDu经过主密钥S的加密过程得到Su的过程。







在使用主密钥S对IDU进行加密但是却没有反向的对私钥Su的解密过程。所以这里的选择密文攻击是对消息的机密攻击。即A提交一个身份IDu和一个密文c,C解密在返回给敌手A。



思想：我们知道加密算法的基础就是数学，尤其是数论知识。因为对于攻击者来说，加密算法是不可破解这个命题必然对应着某个核心的数学问题对他来说是不可解的。所以在证明一个加密算法是否安全的时候，就可以将这个加密算法规约到某个具体的数学难题上。如今公认的数学难题有数论离散对数问题、大素数分解问题等。

如果你坚信你的算法是安全的，那么就可以给出认为安全的定理，这个定理的形式是这样的：如果解答某个数学难题是困难的，那么破解这个算法就是困难的。证明思路是一种反正法思路：假设破解这个算法不困难，那么推到出解决某个数学难题不困难。这就与给定的条件：加大某个数学难题是困难的相矛盾，那么这个假设就不成立。

具体设计：设计四种角色1、算法敌手，目的是破解加密算法 2、算法挑战者，代表加密算法接受算法敌手的挑战，职责是应答算法敌手的询问 3、难题敌手目的是破解数学难题，手段是假装成算法挑战者，通过与算法敌手的互动借助其实力破解数学难题。4、难题挑战者，代表数学难题接接受敌手的挑战，职责是为算法挑战者提供难题实例让其破解。

互动流程：1、难题挑战者首先生成难题的参数(难题实例)并发给难题敌手，难题敌手伪装成算法挑战者，根据数学难题参数进一步构造算法的公钥参数(算法实例)并发给算法敌手；2、算法敌手发起询问，这个询问更具不同的安全级别(选择明文攻击/选择密文攻击)包括密钥生成询问、加密询问、解密询问。这些询问结果可能是真实的，可能是随机的，但算法绝对分辨不出来。3、算法敌手发起挑战，发送两端等长的明文给难题敌手，难题敌手随机选择其中一段明文，进行加密并返回给算法敌手；4、算法敌手猜测密文加密的明文是哪一个，或者直接计算出明文是什么，随后难题敌手录用算法的截获做出难题的解答，并给出难题的最终挑战结果。

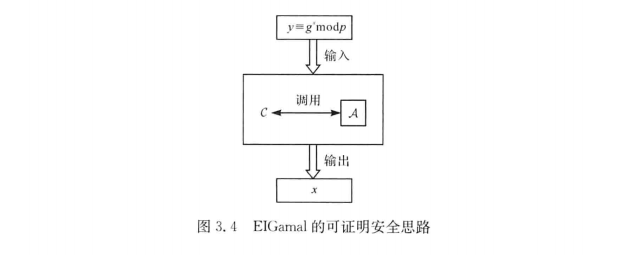


图3.4中，C是难题挑战者，A是算法挑战者。算法C需要应对下面几个问题：

