1. 绪论
   1. 研究背景

当今的社交网络平台大都基于服务器-客户端的架构，当用户需要在自己的朋友圈中分享一个文件的时候，用户首先必须将文件上传至服务器，并设定一个访问策略，由服务器来执行访问策略来决定某一个用户是否具有访问权限。这种架构模式下限定了某些应用场景，例如当用户需要分享一个比较隐私的文件时，出于安全的考虑，用户肯定不会将其上传至服务器来进行共享，即便服务器是可信的，若被恶意用户攻破的时候，用户的隐私信息也将被泄露。2011年CSDN等大型网站的密码等隐私信息被泄露很好地说明了这点。

随着社交网络应用的发展，用户在社交网络中的好友数量急剧增加，与此同时，用户在社交网络中扮演的角色也出现多样化。当今社交网络平台对用户上传的文件能够执行一些比较简单的访问控制，例如具备好友关系的用户能够访问该文件，反之则不能。但这种简单的访问控制往往满足不了用户的需求。一般而言用户会将自己的好友按照关系分为同学，同事，朋友，家人等类别，若用户需要在同学和朋友中分享某个文件时，上述简单的访问控制则无法实现。

* 1. 国内外研究现状
  2. 本文工作

基于上述提出的问题，本文设计并实现了一个面向p2p社交网络的自主授权CP-ABE的原型系统。

1. 预备知识
   1. P2p网络
   2. 属性加密

属性加密的概念来源于身份加密，1984年Shamir在文献中首次提出身份加密的概念。身份加密也属于公钥加密的一种，其提出用用户的身份来作为公钥，例如用户A的身份为IDA，用户B要向用户A发送秘密消息m时，只需要将用户A的身份IDA作为密钥，执行加密算法获取密文发送给用户A即可。从加密的过程来看身份加密的减少密钥管理的工作量，在身份加密方案中，不需要像其他公钥加密方案一样需要有一个权威的第三方来认证某个公钥是属于某个用户的。在身份加密的基础上Sahai, Waters提出了模糊的身份加密，在模糊的身份加密方案中，将用户的身份用一些离散的值（属性）来刻画，若加密过程中使用的身份和解密过程中使用的身份相同的值（属性）超过某个阈值时，则认为这两组值所代表的是同一个身份，从而可以进行解密操作获取明文信息。Sahai, Waters等人在论文中引出了属性加密的概念，在属性加密方案中，加密的密文和用户的密钥都由一组属性来进行刻画，只有当密钥中的属性和密文中的属性相匹配时才能够进行解密操作获取明文。由此引出了属性加密的两种构造方案：密文策略属性加密和密钥策略属性加密。在密文策略属性加密方案中，用户的密钥中包含了标识用户特征的一些属性集合，密文中包含了一个访问策略，当用户密钥中的属性满足明文中定义的访问策略时则可以进行解密获取明文。而密钥策略属性加密则是相反的过程，加密的密文使用一些属性集合进行标识，用户的密钥中包含了一个访问策略，只有加密的密文中的属性满足密钥中定义的访问策略时才能够进行解密操作获取明文。

* + 1. 秘密共享
    2. 双线性