面向关系隐私保护社交网络的匿名访问控制机制的研究

1.功能简介

本机制是针对社交网络中，在好友互相访问时，隐藏请求者的身份，使得用户可以匿名访问朋友发布的内容，从而达到对用户关系隐私进行保护的目的。

程序的运行过程可以分为以下5个步骤，分别是初始化，颁发凭证，制定策略，出示凭证并提出访问请求，访问控制。各个过程实现的功能如图所示。

以CL签名为基础，使用承诺方案，交互式零知识证明协议。最后得到的结果是true或者false，分别对应着允许访问和拒绝访问。



2.程序简介

程序的源代码共分为4个包，下面分别介绍这4个包。

(1) initialization包

这个包主要是系统初始化，为后续步骤的实现提供参数。

KeyGen类，系统运行的第一步，初始化，也是CL签名的KeyGen算法，生成公私钥对，这里是生成SNSP和Bob的公私钥。生成的公私钥在xml\_file包中，以key.xml文件形式存在。该类包含main()方法。

Method类提供一些共用的方法，得到系统时间的getTime()，得到随机大整数的方法，和安全哈希方法。

SetUp类，主要用于设置一些参数的长度，这些参数的长度和系统的安全性息息相关。

(2) issue\_credential包

这个包的主要功能有为用户颁发凭证。

Issue类，颁发凭证。该类包含main()方法。

CLSigner类，CL签名的sign()方法和verify()方法。以及得到签名时所需的一些参数。

ZKP\_Sign类，对用户的身份信息做一个承诺，并用零知识证明。

(3) access\_control包

PolicyGenerator类，选取代表用户的素数，制定访问控制策略。该类包含main()方法。

RequestGenerator类，对凭证随机化处理，匿名提出访问请求。该类包含main()方法。

ResponseGenerator类，对提出的请求进行决策。该类包含main()方法。

ZKP\_verify类，采用零知识证明对整个过程进行证明。

(4) create\_xml包

主要用于生成相应的xml文件，和对xml文件中的内容进行读取。该过程需要用到jar包里的，dom4j-1.6.1.jar，jdom.jar。

