**北京科技大学实验报告**

学院：计通学院 专业：信息安全 班级：信安182

姓名： 梁逸飞 学号：41824141 实验日期： 2020年 12月 8日

**实验名称：基于java实现群签名过程**

**实验目的：**深入理解群签名的内容和实现原理，分析群签名过程和原理，实现群签名

**实验原理：**在一个群签名方案中，一个群体中的任意一个成员可以以[匿名](https://baike.baidu.com/item/%E5%8C%BF%E5%90%8D" \t "https://baike.baidu.com/item/%E7%BE%A4%E7%AD%BE%E5%90%8D/_blank)的方式代表整个群体对消息进行签名。与其他[数字签名](https://baike.baidu.com/item/%E6%95%B0%E5%AD%97%E7%AD%BE%E5%90%8D" \t "https://baike.baidu.com/item/%E7%BE%A4%E7%AD%BE%E5%90%8D/_blank)一样，群签名是可以公开验证的，而且可以只用单个群[公钥](https://baike.baidu.com/item/%E5%85%AC%E9%92%A5" \t "https://baike.baidu.com/item/%E7%BE%A4%E7%AD%BE%E5%90%8D/_blank)来验证。也可以作为群标志来展示群的主要用途，种类等。

**实验环境：**eclipse、java1.8、jd-gui

**实验内容与步骤：**

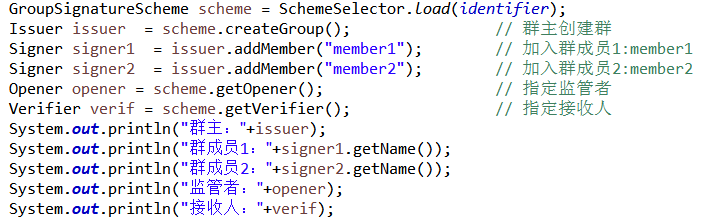
一、了解群签名的定义、过程以及特性

此部分单独制作了说明文档，详请请见“群签名说明文档.docx”说明文档。

二、基于java实现群签名

1、群的创建以及成员添加

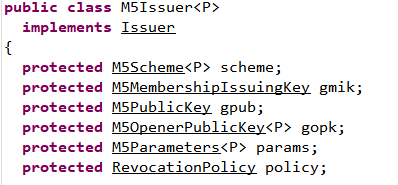
实现的主要代码如下。



scheme为签名机制，根据此机制群主issuer调用createGroup创建群，通过调用addMmeber加入新的群成员，通过调用getOpener以及getVerifier指定监管者和接收人。

由于具体的实现部分都在jar包中封装起来了，在执行调用createGroup创建群时，已经自动完成了生成群主私钥、群参数的过程，同样群成员加入后将会自动完成对成员分配私钥和颁发证书的过程。

具体信息可以利用jd-gui工具对jar包进行反汇编查看具体的实现代码，以生成群主时为例，生成的群密钥、群参数等如下图所示。



同样加入新成员后群成员也拥有密钥等相关私有信息，同样可以对其jar包进行反汇编查看。

2、群成员签名

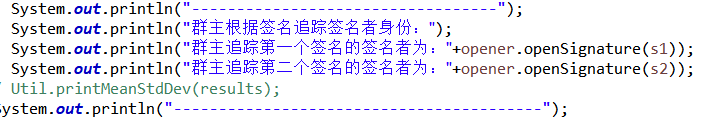
调用群成员signMessage函数对消息进行签名。让群成员1对消息1进行签名产生签名s1，群成员2对消息2进行签名差生签名s2，然后再让接收人分别就签名s1和s2进行验证。

代码实现如下。



3、追踪群成员身份

由于之前指定了监管者，所以在监管者介入的情况下，群主可以通过签名信息追踪签名者的身份。因此就签名s1和s2进行身份追踪，并比较与之前的签名对象是否相符合。



4、测试运行代码

运行结果如下图所示。



根据运行结果可以查看群主、群成员、监管者和接收人的一些身份信息，以及群成员的签名信息，并且通过接收人均能验证成功。群主通过对s1和s2签名进行追踪到的成员为member1和member2，对应群成员1和群成员2，与之相符合。说明代码实现成功。

**实验结果与分析：**

上述代码能够较好地实现群签名的功能，实现了群签名的整个流程。除此之外还对群签名的特性进行了验证，提高了对数字认证技术的认识，加深了对群签名的了解。

实现的具体代码详见GroupSignature.java文件。