# 群签名

一、概念

所谓群[签名](https://baike.baidu.com/item/%E7%AD%BE%E5%90%8D" \t "https://baike.baidu.com/item/%E7%BE%A4%E7%AD%BE%E5%90%8D/_blank)（group signature）就是满足这样要求的签名：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。

二、过程

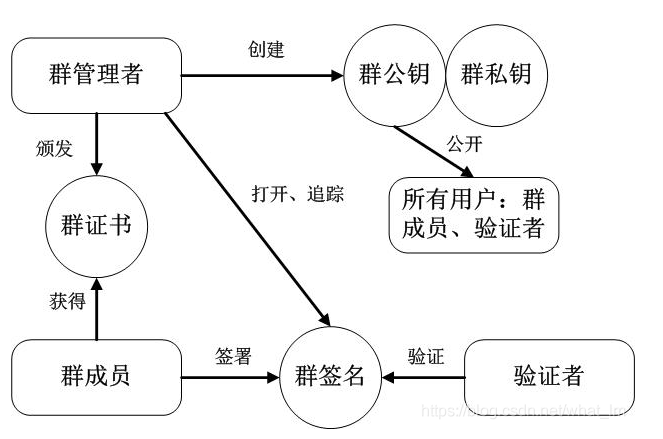
1、生成群：生成群公钥(gpk)，群主私钥(gmsk)和群参数。

2、加入群：群主为群成员产生私钥（gsk）和证书（cert）

3、生成群签名：群成员用私钥和证书对消息进行签名。

4、群签名验证：接收人通过群公钥、群参数验证群签名信息的有效性（此时接收人只知道签名属于哪个群，但无法获取签名者的身份信息）。

5、追踪签名者信息：在监管介入的情况下，可以通过群签名信息追踪签名者的身份。



三、特性

1、群特性：只有群中成员能够代表群体签名。

2、验证简单性：接收者可以用公钥验证群签名。

3、匿名性：群成员用群参数产生签名，其他人仅可验证签名的有效性，并通过签名知道签名者所属群组，却无法获取签名者身份信息。   
 4、可追踪性: 在监管介入的场景中，群主可通过签名获取签名者身份。

四、代码实现

见GroupSignature.java。