|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 部门名称 | 文档编号 |  | 版本 |  | 密级 |  |
| 项目名称 |  | | | | |
| 项目来源 |  | | | | |

**BBS群签名算法实现说明书**

编 写： \_\_\_\_ 日 期：

检 查： \_\_\_\_ 日 期：

审 核： \_\_\_\_ 日 期：

批 准： \_\_\_\_ 日 期：

文档变更记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 变更(+/-)说明 | 作者 | 版本 | 日期 | 批准 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |

目录

[1. 引言 2](#_Toc526004142)

[1.1 背景 2](#_Toc526004143)

[1.2 术语和缩略语 2](#_Toc526004144)

[1.3 参考资料 2](#_Toc526004145)

[2. 总体设计 2](#_Toc526004146)

[2.1 需求 2](#_Toc526004147)

[2.2 架构设计目标和约束 2](#_Toc526004148)

[2.2.1 运行环境 2](#_Toc526004149)

[2.2.2 开发环境 2](#_Toc526004150)

[2.3 设计思想 3](#_Toc526004151)

[2.4 软件架构 3](#_Toc526004152)

[2.5 重要业务流程 3](#_Toc526004153)

[2.5.1 流程1 3](#_Toc526004154)

[2.5.2 流程2 3](#_Toc526004155)

[2.6 模块划分 3](#_Toc526004156)

[3. 接口设计 3](#_Toc526004157)

[3.1 外部接口 3](#_Toc526004158)

1. 引言
   1. 背景

群签名是一种具有特殊性质的数字签名，它允许一个群体中的任意一个成员可以以匿名的方式代表整个群体对消息进行签名，从而为群成员提供了匿名保护。与其他数字签名一样，群签名是可以公开验证的，而且可以只用单个群公钥来验证。在需要确定是哪一个群成员进行的签名时，群主可以利用追踪密钥获取签名成员的真实身份。

在公共资源的管理，重要军事情报的签发，重要领导人的选举，电子商务重要新闻的发布，金融合同的签署等事务中，群签名都可以发挥重要作用。

* 1. 术语和缩略语

p:阶数。

:阶数为的整数群。

G1:椭圆曲线上的阶数为p的加法循环群。

G2:椭圆曲线上的阶数为p的加法循环群。

GT:椭圆曲线上的阶数为p的乘法循环群。

g1:G1的生成元。

g2:G2的生成元。

（双线性对运算）

GPK:群公钥，。

TK:追踪密钥，。

SK:用户密钥，。

:群签名，。

* 1. 参考资料

1. 总体设计
   1. 需求
   2. 架构设计目标和约束
      1. 运行环境

Go 1.9.2

* + 1. 开发环境

Go 1.9.2

* 1. 设计思想

群签名方案包含以下组成部分：

群主（Group master）：产生群公开密钥，主密钥，以及追踪密钥；

群管理员（Group manager）：一旦发生争端，利用群追踪密钥追踪签名者的身份信息；

私钥生成中心（Private key generator）：利用主密钥产生用户的签名密钥；

签名者（Signer）：利用签名密钥产生一个群签名；

验证者（Verifier）：利用群公钥对群签名进行验证。

一个群签名方案包含以下过程：

系统建立：群主产生群公开密钥，主密钥，以及追踪密钥，群公开密钥用于验证群签名的有效性，主密钥用于生成用户签名密钥，追踪密钥由群管理员保管；

成员加入：用户可以进行注册，私钥生成中心产生用户的签名密钥；

签名：用户利用签名密钥可以产生消息或文件的群签名；

验证：验证者利用公钥可以对群签名进行验证；

追踪：给定一个群签名，群管理员利用追踪密钥可以从中恢复出签名者的身份信息。

针对群签名的特点，群签名方案应满足以下几点安全性质：

完整性（Soundness and completeness)：群成员产生的有效的群签名可以通过验证，无效的签名不能通过验证；

不可伪造性（Unforgeability）：只有群内成员可以产生有效的群签名；

匿名性（Anonymity）：给定一个消息和对应的群签名，除了群管理员，任何人无法追踪签名者的身份；

可追踪性（Traceability）：给定一个有效的群签名，群管理员可以利用追踪密钥恢复出签名者的身份；

无关联性（Unlinkability）：给定两个消息及对应的群签名，无法判断是否由同一个签名者产生；

无框架（No framing）：即使所有群成员相互勾结，也无法产生非群内用户产生的有效群签名；

防陷害性（Exculpability）：没有群成员或相互勾结的群成员能够产生代表他人的群签名；

抗联合攻击（Coalition resistance）：相互勾结的群成员不能产生一个无法追踪的群签名。

* 1. 软件架构
  2. 重要业务流程
     1. 流程1
     2. 流程2
  3. 模块划分
     1. 模块1
     2. 模块2

1. 接口设计
   1. 外部接口

本算法对外有哪些接口，逐一详细说明参数、返回值、调用约束（如能否并发调用）等

1. 生成群公钥和追踪密钥：func NewGroupKey(rng \*amcl.RAND) (\*GroupKey,error)
2. 传入参数：
3. rng:随机数。
4. 传出参数：
   1. GroupKey:群公钥，其中群密钥包括主密钥MSK，追踪密钥TK和群公钥GPK。
   2. error:错误类型。
5. 生成用户私钥：func Registration(gmsk \*GroupMasterKey,rng \*amcl.RAND) (\*UserKey,error)
6. 传入参数：
7. gmsk:群公钥。
8. rng:随机数。
9. 传出参数：
10. UserKey:用户私钥
11. Error:错误类型
12. 生成群签名：func NewGroupSig(rng \*amcl.RAND,gpk \*GroupPublicKey,uk \*UserKey, message []byte)(\*GroupSignature,error)
13. 传入参数：
    1. rng:随机数。
    2. gpk:群公钥。
    3. uk:用户私钥。
    4. message:待签名消息。
14. 传出参数：
15. GroupSignature:群签名
16. Error:错误类型
17. 验证群签名：func GroupVerify(GroupSig \*GroupSignature,gpk \*GroupPublicKey, message []byte) error
18. 传入参数：
    1. GroupSig:群签名。
    2. gpk:群公钥。
    3. message:签名消息。
19. 传出参数：
20. Error:错误类型
21. 追踪签名者身份：func Tracing(GroupSig \*GroupSignature, tk \*TracingKey) (\*K,error)
22. 传入参数：
    1. GroupSig:群签名。
    2. tk:追踪密钥TK。
23. 传出参数：
24. K:用户私钥
25. Error:错误类型