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

**Mp环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

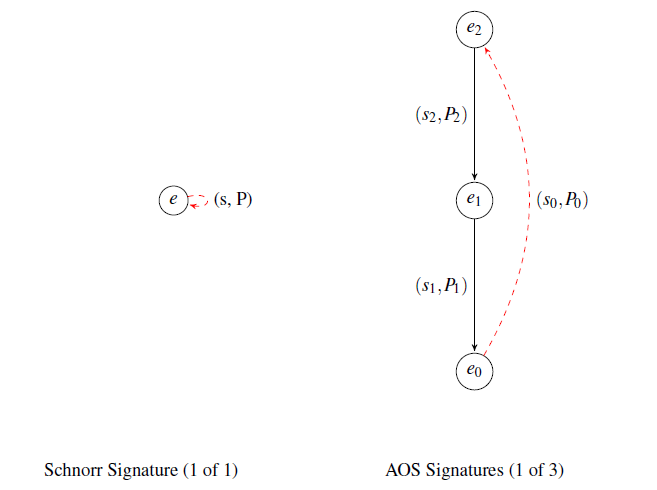
环签名可理解为一种知识证明，即证明n个公钥对应一个相应的签名密钥，也可表述为“签名者知道私钥或或…”。相应的，Borromean 环签名则可表述为“签名者知道私钥{}中的一个和{}中的一个”。Borromean 环签名主要基于AOS环签名和变色龙哈希技术构造。

1. 变色龙哈希

带陷门信息的哈希函数，掌握陷门信息，就可以找到哈希函数的碰撞。设和为生成元，陷门信息为，且有，H为一个标准哈希函数，一个变色龙哈希函数可定义为

若，则有，即可在不知道e的情况下计算h。

1. AOS环签名



假设有n个用户，签名时，可从任意下标j开始计算，首先选择随机整数，计算，然后随机选择，计算，依次计算…，，…，，，其中为随机整数。，则对应，最终签名为。

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

环签名算法包括签名密钥生成、签名、验证等三个算法。签名密钥生成算法输入安全参数，输出若干用户的密钥对。签名算法输入签名者的私钥，若干用户的公钥，输出一个环签名。验证算法输入若干公钥，验证环签名是否有效。

* 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. 生成签名者密钥对：func NewSignKey(round int, rng \*amcl.RAND) (\*SignKey,error)
2. 传入参数：
3. round:多个环的个数。
4. rng：随机数。
5. 传出参数：
   1. SignKey:签名者密钥，包括私钥SK和公钥PK。
   2. error:错误类型。
6. 生成环成员公钥：func NewPubKey(rng \*amcl.RAND, round int, num int) (\*RingPK,error)
7. 传入参数：
8. rng:随机数。
9. round：多个环的个数。
10. num：每个环的成员个数。
11. 传出参数：
    1. RingPK：环成员公钥（不包括签名者公钥）。
    2. error:错误类型。
12. 签名公钥加入公钥环中：func NewSignPubKey(ringPK \*RingPK,signKey \*SignKey, startIndx int) (\*RingPK,error)
13. 传入参数：
14. ringPK:环成员公钥。
15. signKey：签名者密钥。
16. startIndx：签名公钥在环中的位置（环签名起始位置）。
17. 传出参数：
    1. ringPK:环成员公钥，包括签名者的公钥。
    2. error:错误类型。
18. 计算哈希值，func BorromeanHash(m []byte, G1 \*SECP256K1.ECP, i int, j int) \*SECP256K1.BIG
19. 传入参数：
20. m:待签名消息。
21. G1:椭圆曲线上的一个点。
22. i：整数下标。
23. j：整数下标。
24. 传出参数：
25. SECP256K1.BIG: 哈希值，类型为大整数。
26. 环签名：func NewRingSig(signPubKey \*RingPK,signKey \*SignKey, rng \*amcl.RAND,m []byte, round int,num int, startIndx int) (\*RingSig,error)
27. 传入参数：
    1. signPubKey:环成员公钥。
    2. signKey:签名者密钥。
    3. rng:随机数。
    4. m:待签名消息。
    5. round：多个环的个数。
    6. num：每个环的成员个数。
    7. startIndx：签名起始位置。
28. 传出参数：
29. RingSig:环签名。
30. error:错误类型。
31. 环签名验证：func RingSigVerfy(ringSig \*RingSig, signPubKey \*RingPK,m []byte) error
32. 传入参数：
    1. ringSig:环签名。
    2. signPubKey:环成员公钥。
    3. m：签名消息。
33. 传出参数：
34. Error:错误类型