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

**rangeproof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

Rangeproof基于Borromean 环签名构造，可证明整数v在一定范围内。记，将v表示为长度为n的m进制数，则rangeproof可证明经Pedersen承诺加密过的数值v的范围为，或m进制每位的数字范围为。设和为生成元，为阶整数循环群，为一个安全的哈希函数。

Rangeproof包括以下过程。

证明：

* 对于，

1. 若，随机选择整数，计算；
2. 若，随机选择整数，计算承诺值；

随机选择，计算；

对于，随机选择，计算；

计算；

* 计算；
* 对于，

1. 若，对于，随机选择，计算，记；

计算；

对于，计算；

1. 若，对于，随机选择，计算

；

计算；

* 计算，最终输出

验证：

* 对于，

1. 设置；
2. 对于，计算；
3. 计算；

* 计算；

若和成立，则通过验证。

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

rangeproof算法包括生成范围证明、验证算法。生成范围证明算法输入一个之间的整数，产生一个范围证明，验证算法输入范围证明，输出验证结果。

* 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. 产生范围证明，func NewProof(value int, rng \*amcl.RAND) (\*Proof,error)
2. 传入参数：
3. value:待证明的值。
4. rng:随机数。
5. 传出参数：
6. proof:范围证明。
7. error：错误类型。
8. 验证范围证明：func Verify(proof \*Proof) error
9. 传入参数：
   1. proof:范围证明。
10. 传出参数：
11. error:错误类型。