|  |
| --- |
| 基于安全多方计算和安全门限密钥共享技术的  锁定账户生成方案  Version 0.0.0 |

**目录**

基于安全多方计算和安全门限密钥共享技术的 1

锁定账户生成方案 1

1 安全多方计算介绍 3

1.1 安全多方计算提出背景 3

1.2 拉格朗日插值公式 3

2 门限密钥共享技术介绍 3

3 锁定账户 3

3.1 锁定账户生成方案 3

3.2 锁定账户签名方案 3

3.3 锁定账户密钥更新方案 3

# 安全多方计算介绍

## 安全多方计算提出背景

## 拉格朗日插值公式

# 门限密钥共享技术介绍

# 锁定账户

## 锁定账户生成方案

万维链上的validator（编号为……）生成门限锁定账户过程如下：

1. 选择随机数，将广播全网（为椭圆曲线基点）
2. 选择次多项式：，将通过安全信道传输给，同时将……广播全网
3. 到信息之后，进行验证：，如果验证不通过，则拒收，请求重新发送信息
4. 待所有信息都发送完毕且验证通过后，每个用户的密钥份额为，
5. 门限锁定账户地址为，其中，对应私钥为，这个私钥只有通过份以上密钥份额才能够恢复

## 锁定账户签名方案

## 锁定账户密钥更新方案