|  |
| --- |
| 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 3

1.1 安全多方计算提出背景 3

1.2 安全多方计算的基础运算 3

2 门限密钥共享技术 4

2.1 线性密钥共享机制 4

2.2 Shamir多项式插值密钥共享方案 4

3 锁定账户 4

3.1 锁定账户生成方案 4

3.2 锁定账户签名方案 5

3.3 锁定账户密钥更新方案 5

# 安全多方计算

## 安全多方计算提出背景

随着互联网的迅速发展，越来越多的应用场景需要网络用户之间进行协作运算。但是出于隐私保护和数据安全的考虑，参与协作运算的用户并不想和其他用户进行计算数据的分享，这一问题导致协同计算无法执行，从而导致网络资源并不能够高效分享利用和一些应用场景难以实现。安全多方计算（secure multi-party computation）让这一问题迎刃而解，它为解决数据隐私保护和协同计算之间的矛盾提供了理论基础。

安全多方计算是分布式密码学的理论基础，也是分布式计算研究的一个基本问题。安全多方计算是指在一个互不相信的多用户网络中，两个或多个用户能够不泄漏各自私有输入信息，协同合作执行某项计算任务。简单地说，安全多方计算是指一组人，比如……，共同安全地计算函数。其中这个函数的个输入分别由这个参与者秘密掌握的，设的秘密输入是，并且在计算结束后，得到输出。这里的安全性是要求即使在某些参与者有欺骗行为的情况下，保证计算结果的正确性，即计算结束后每个诚实的参与者都能得到正确的输出，同时还要求保证每个参与者输入的保密性，即每个参与者除了外，得不到任何其他信息。

安全多方计算已经有了丰富的理论成果和强有力的工具，虽然它的实际应用还处于起步阶段，但终将成为计算机安全一个不可缺少的部分。

## 安全多方计算的基础运算

# 门限密钥共享技术

## 线性密钥共享机制

## Shamir多项式插值密钥共享方案

# 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