|  |
| --- |
| 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。

## 安全多方计算协议的分类

目前安全多方计算协议根据实现方式的不同，可以分为四类：

* 基于VSS子协议的安全多方计算协议

现存的大部分安全多方计算协议都采用了可验证密钥分享VSS（Verifiable Secret Sharing）子协议作为协议构造的基础，这类协议适合计算任意有限域上的函数。有限域上任意函数均可表示成域中定义加法和乘法的有向图，因此只要可以安全计算加法和乘法，就可以计算每一个加法和乘法来完成有限域上任意函数的计算。

* 基于Mix-Match的安全多方计算协议

基于VSS子协议的安全多方计算协议能够计算任意函数，但是不能高效计算布尔函数，为此提出了另一种安全多方协议——Mix-Match。这种协议的基本思路是参与者使用秘密分享方案分享系统的私钥，系统的公钥公开。协议过程中，参与者将自己输入使用的公钥y随机加密，然后将自己的加密结果公布，最后通过Mix-Match使得所有参与者获得共同输出。

* 基于OT的安全多方计算协议

基于OT的安全多方计算协议用于计算任意比特运算函数。它利用OT子协议实现“与（and）”、“或（or）”、“非（not）”三种基础运算，再将任意比特运算函数分解为三种基础运算的组合，最后通过迭代的方式计算出任意比特运算函数。

* 基于同态加密的安全多方计算

基于同态加密的安全多方计算能够抵抗主动攻击，它的思路是选定原子计算，使得任意函数计算均可分解为原子计算的序列，同时原子计算的输入和输出均使用同态加密算法加密，在加密状态下得到最终的计算结果，只有特定的参与者集合才能够将计算结果解密得到明文。

## 安全多方计算的基础运算

# 门限密钥共享技术

## Shamir门限密钥共享概念

门限密钥共享技术（threshold key sharing scheme）解决的是密钥安全管理问题。现代密码学体制的设计是使得密码体制的安全性取决于密钥的安全，密钥的泄露就意味着体制失去了安全性，因此密钥管理在密码体制的安全性研究和设计中占有重要的地位。特别是多方利益体共同管理一个账户时，账户的密钥如何可信安全地分配给多方参与者就变得非常棘手。针对这一问题，以色列密码学家Shamir提出了Shamir门限密钥共享的概念：密钥被分为份分配给个参与者，每个参与者掌握一个密钥份额（key sharing），只有集齐超过个密钥份额，才能够将密钥恢复。

## 线性密钥共享机制

线性密钥共享是Shamir门限密钥共享的推广，它的本质是要求主密钥空间、子密钥空间和随机输入集合都是线性空间，并且密钥重构函数是线性的。形式化定义如下：

设是一个有限域，是实现存取结构的一个密钥共享体制，是主密钥空间。我们说是上的一个线性密钥共享体制，如果满足以下条件：

1. 子密钥是上的线性空间，即对于，常数，使得子密钥空间。记为收到空间的向量的第个分量，这个分量依赖于主密钥和随机数。
2. 每个授权集都可以通过线性组合子密钥的方式得到主密钥，即对于任意一个授权集，常数，使得对任意主密钥和随机数，都有

## 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