2.1陈莉，林柏钢[11]的基于分布式线性方程组的安全多方计算协议

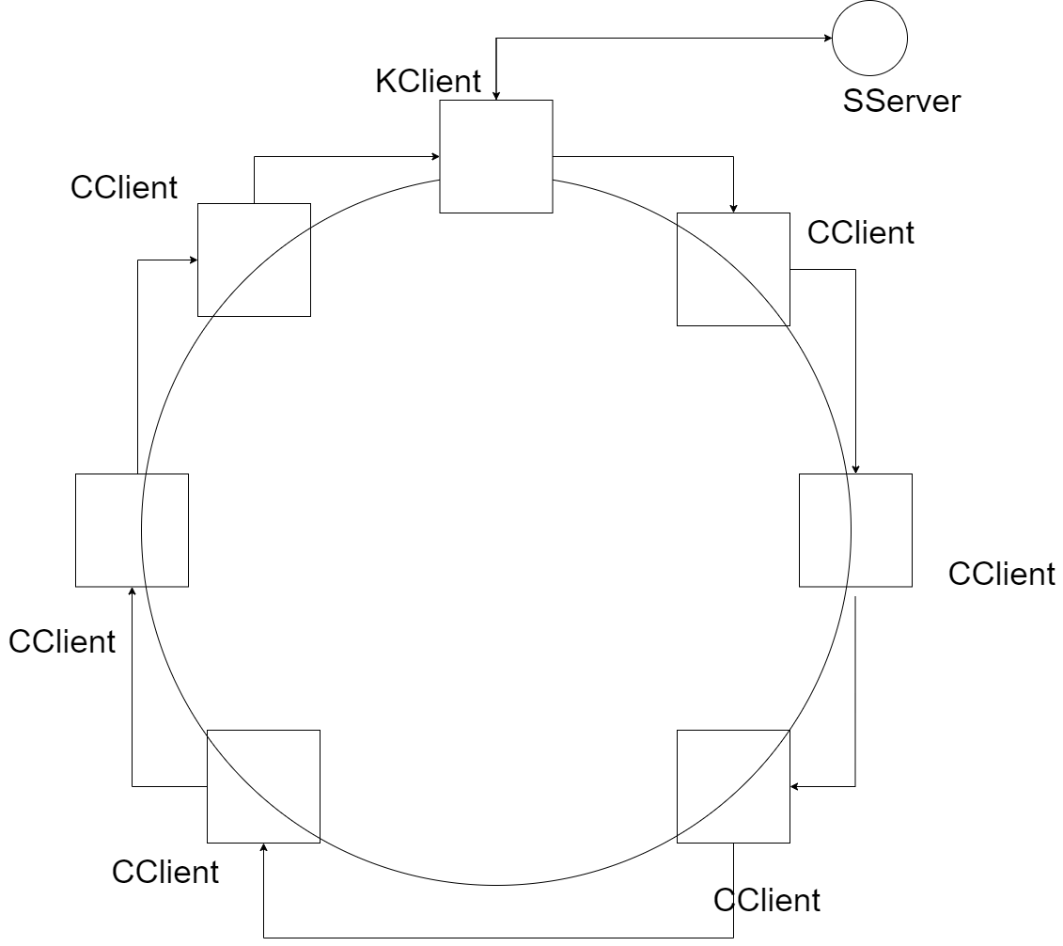
协议模型通过参与方使用的公钥加密明文矩阵，并发送给，接着随机生成可逆矩阵，用其与密文相乘并发送给，通过解密密钥对接受的数据解密，求解线性方程组，将结果发送给各参与方。

|  |
| --- |
| 输入：拥有维矩阵和维向量 |
| 1) 用的公钥加密矩阵和，并将他们发送给。  2）用的公钥计算加密矩阵和。根据加密的同态性，计算和，接着随机生成一个阶可逆矩阵计算和并将它们发送给。  3）利用解密密钥对接收到的和进行解密。解密可获得和的值。求解线性方程组。  4）将发送给其余参与方 |
| 输出：得到，满足线性方程组。 |

当协议模型处于理想模型时，数据不会被破坏，隐私性完全得到保护，但现实中不存在此模型。当所有参与方都是半诚实时，而加密方法时安全的，因而当攻击者的支撑结构为S(A)={{2,…,s},{1,…,s-1}}时，协议时安全的。而此协议也存在致命缺陷。在协议中，ps拥有解密密钥，p1拥有其他参与方的加密后的密文，一旦这两方合谋，那么数据就会完全泄露。

2.2马飞，蒋建国[7]基于环形拓扑CClient-KClient-SServer的计算协议

如图所示，方案采用环形拓扑结构，参与统计计算的用户数据采用单项传递。结构中有3种不同类型的节点：CClient，KClient，SServer。



[11] 陈莉,林柏钢.基于分布式线性方程组求解的安全多方计算协议[J].信息网络安全,2013(09):2-5.

2.2Asharov基于云服务器的TFHE安全外包计算方案

Asharov等人基于文献[9-10]中的FHE方案给出了相对比较高效的TFHE方案。

|  |
| --- |
| TFHE安全外包计算方案 |
| 1）各参与方运行TFHE密钥生成协议的第一轮并产生公共的公钥。  2）各方运行TFHE密钥生成协议的第二轮。产生公共的计算密钥。并利用第一轮的公共公钥将各自的输入加密，广播出去。  3）云服务器拿到方案的公钥、计算密钥以及所有的密文之后自行算出计算结果的密文然后将此密文广播。  4）各参与方拿到计算结果的密文后运行解密协议即可得到真正的计算结果。 |

在上诉过程中，各参与方仅需要执行与TFHE相关的计算，而真正的计算任务则在云服务器进行。因此对各参与方来说。计算量不是很大。

该协议可以被证明在半恶意模型下安全。即模型中敌手基本遵照协议进行，但是可能会根据自己的试图恶意地产生运算中使用地随机数。因此，云服务器可以仅利用简明非交互零知识论证系统，而不是用掷币协议来证明它在诚实地执行协议。从而将其转化为恶意敌手模型下安全地协议，转化后地协议仍然可以在四轮内完成。

## 通用安全多方计算

安全多方计算（Secure Muti-party Computation ，简称MPC，也称为SMC或SMPC）问题是由中国计算机科学家、图领奖获得者姚启智教授于1982年首先提出的，即著名的百万富翁问题：两个胜负欲极强的有钱人Alice和Bob街上相遇。 如何在不暴露财富的情况下比较谁更富有？

后经Goldreich、Micali以及Wigderson等人的发展，成为现代密码学中非常活跃的研究领域，即安全多方计算，其数学描述为，“ 有个参与者，要以一种安全的方式共同计算一个函数，这里的安全是指输出结果的正确性和输入信息、输出信息的保密性。具体地讲，每个参与者，有一个自己的保密输入信息，个参与者要共同计算一个函数



计算结束时，每个参与者Pi只能了解,不能了解其他方的任何信息。” 简单来说，安全多方计算协议作为密码学的一个子领域，其允许多个数据所有者在互不信任的情况下进行协同计算，输出计算结果，并保证任何一方均无法得到除应得的计算结果之外的其他任何信息。换句话说，MPC技术可以获取数据使用价值，却不泄露原始数据内容。

# 安全的计算协议

本节分析参考文献中外包计算协议的好坏，然后选择适合于分布式统计的协议，设计出方案，使分布式统计的数据得到隐私保护。

## 刘锵，唐春明[8]基于多租赁用户模型下的安全外包计算

当数据拥有者选择一个不受信任的第三方服务计算商时，称为单租赁用户模型，也可以选择多个不受信任的第三方服务计算商时，称为多租赁用户模型。文献[8]在Kamara和Raykova结合门限密钥共享方案的安全协议上，提出了基于非门限存取结构的安全外包计算协议，原理如下。

对于任意函数，假设能被个值线性计算，即，则函数。因此，按照文献[11]中所得到的密钥共享方案，可以把分成个秘密分块，对于任意的，个秘密分块都可以线性计算。因此，我们能把函数转换为一个方函数



且任意的都能计算该函数。下面给出计算的外包计算协议。

假设用户和每个至今啊都存在一条秘密通道，任意可计算函数在个租赁用户中存在一个安全多方计算协议以及基于线性的线性密钥共享方案，则我们为计算提出一个外包计算协议，该协议首先的时非门限存取结构。

图表 2 安全的非门限外包计算协议

|  |
| --- |
| 1）用户根据算法把输入分成个秘密分块，每个秘密分块通过秘密通道发送给服务器，需要强调的是也许是一个向量。因为对于任意存取结构，不一定存在理想的密钥共享方案（若的秘密分块具有相同的长度，则他们是理想的密钥共享方案）。  2）计算参与方执行安全多方计算协议计算。执行的结果是每个得到输出的秘密分块。同理，也许是一个向量。  3）把秘密分块通过秘密通道发送给用户后，用户再使用算法从恢复出。 |

如果计算协议在动态和主动攻击者下是安全的，是一个安全的密钥共享方案，则协议在动态和主动攻击者下是安全的。其中中攻击者与协议中攻击者是一样的。

* + - 1. 马飞,蒋建国.具有隐私保护的分布式协作统计计算方案[J].计算机工程与设计,2015,36(09):2383-2387.DOI:10.16208/j.issn1000-7024.2015.09.013.
      2. 刘镪,唐春明,胡杏,张永强.多租赁用户模型下有效安全外包计算[J].信息网络安全,2013(09):17-21.
      3. Brakerski Z, Vaikuntanathan V. Effieient fully homomorphic eneryption from (standard) LWE [J]. SIAM Journal on Computing. 2014.43(2):831-871
      4. Brakerski Z, Gentry C. Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping [C]//Proc of the 3rd Innovations in Theoretical Computer Science Conf.
      5. Tang CM, Gao SH, Zhang CL. The Optimal Linear Secret Sharing Scheme for Any Given Access Structure[EB/OL]. http://eprint.iacr.org/2011/147.ps,2011.