概念：

半诚实模型：假设敌手会按照协议规则进行计算，但会通过分析协议消息来获得诚实方的隐私输入，又称为诚实但好奇模型

恶意模型：敌手不会按照协议准确执行，并且可通过发送任意特定消息来试图使其他参与方在无察觉情况下泄露隐私输入。

* **背景原因**

360网络安全相应中心定期发布的安全报告，汇总了大量网络安全时间，其中数据泄露事件占云安全事件的比重为37.9%。一些重大的数据泄露事件包括1600万巴西COVID-19患者的详细信息在网上曝光，埃隆马斯克等人Twitter账号被盗并发布欺诈信息，奥迪、大众330万客户遭遇数据泄露等。由此可知，数据在隐私保护条件下安全、有效地协作处理和利用，使数据产生应有价值，正在成为社会信息化发展的迫切要求。

* **定义及性质**

安全多方计算，研究一组互不信任的参与方，在不借助第三方的情况下，如何在保护各自输入数据的隐私性的同时，共同完成某种多输入计算，并保证输出结果的正确性，是实现隐私保护科学计算的关键技术，亦是填补密码学“密文计算“版图的重要备选技术之一。

安全多方计算模型中蕴含着三个基本规则：

1. 参与方拥有相近的计算资源和对等的角色；
2. 不借助参与方之外的第三方；
3. 所有参与方都知道被计算的功能函数f。

具有以下两个方面的特性:

1. 输入隐私性：从协议执行中所暴露出来的信息不能推导出任意参与方的隐私输入，除去那些可以通过计算结果反推出的部分。

两个变量来衡量：协议能够接受的作恶参与方数，作恶参与方的行为模型。

1. 鲁棒性:任何协议能容忍的敌对合谋参与方子集都不能通过分享信息或者篡改指令来使得诚实方输出一个错误结果。

* **发展历程**

安全多方计算问题首先由YAO于1982年提出，首先将安全多方计算的功能函数转化为抽象的电路，然后对电路的每个门进行某种混淆，最后通过逐次计算每个混淆门的方式来计算整个电路，从而实现对任意功能函数的安全多方计算。5年后，O.Goldreich、S.Miclai和A.Wigderson三位学者提出了密码学安全的可以计算任意函数的安全多方计算协议。他们证明了在被动情况下，n-private协议是存在的，在主动攻击情况下，n-resilient协议是存在的，并展示了如何构造这些协议。

1988年，M.Ben-Or、S.Goldwasse和A.Wigderson，以及D.Chaum、C.Crepeau和I.Damgard几乎同时证明了在信息论安全模型中，被动攻击情况下当串通攻击者数t<n/2、主动攻击情况下t<n/3、网络非同步情况下当串通攻击者数t<n/4时，任意函数都可以被安全计算。

众多密码学家致力于此方向的研究，研究内容主要包括以下几个维度：参与方数量上包括两方计算和多方计算；攻击者模型包括半诚实模型和恶意模型；研究问题包括安全模型建立、可行性分析、通用协议设计、具体问题的计算协议、实际应用和安全多方计算扩展问题等。这些研究直到21世纪，算法改进和计算消耗才达到可以开始考虑实际应用的节点。

* **通用vs特定**

通用的安全多方计算协议试图计算满足一定条件的任意函数，从实现手段上可以分为:混淆电路、秘密共享、不经意传输、同态加密以及最新的不经意随机访问存储五种实现方式。Fairplay是第一个著名的通用安全多方计算实现，它证明了一个隐私计算协议可以通过高级语言描述并编译成可执行文件来在数据拥有方之间执行。通用协议的执行效率往往比较低，故需正对具体的计算问题设计专门的协议。

针对特定的问题，安全比较、隐私集合交集、保密排序和安全投票等等，所设计的协议具有很强的应用性，其运算优化和安全性适配能够达到非常理想的效果。

* **实际应用**

安全多方计算的应用研究包括隐私保护数据挖掘、隐私保护电子投票、隐私保护模式匹配、隐私保护信息检索等。与追求最高安全性的学术研究不同，实际应用会选取相对较弱的安全假设，以及较少的参与方数目，来提高整体系统的运行效率。

* **原理及核心原理**

急急急

* **最新技术**

近年来，安全多方计算仍旧是密码学界研究的热点。

在通用的安全多方计算协议方面，Geoffroy给出了相关随机性模型下计算s层的安全多方计算，电路计算复杂度可以降低到O(s/loglogs)。Elette，Geoffroy，Yuval等提出了伪随机相关生成器PGG的概念，并基于PGG设计了不经意传输协议、一次真值表和Beaver乘法元组等，极大的降低了随机数生成过程的通信复杂度。Ran，Abhi和Daniel给出了适应性安全的多方安全计算协议构造方法。无条件安全的通信复杂度的界限也有新的进展。

恶意模型下复杂度理论的完备性和轮次复杂度有了新的研究成果。Garg，Goel和Jain给出了具有广播信道的安全多方计算的轮复杂度最新研究成果Morgan，Pass和Rafael提出了第一个允许恶意敌手存在的情况下，简介非交互式安全两方计算协议。对于高延迟网络，降低通信复杂度能够提高很大的通信效率，节约计算时间。

* **未来展望**

早期的研究工作仅仅解决了安全多方计算协议理论上存在性的问题，其效率低下，并不能用于解决实际问题。而近年来，随着云计算的发展，对于安全多方计算实用化的要求越来越迫切，实用化的安全多方计算协议得到飞速发展，到目前为止，基于Cut-and-Choose技术的Yao安全两方计算协议、基于Beaver三元组和GMW的SPDZ类的安全多方计算协议，已经成为真正可实用的安全多方计算协议，并广泛用于隐私保护机器学习等实际应用中。

随着这些年云计算的发展，目前安全多方计算协议已能实用落地，然安全多方计算还有许多待解决的问题。

1. 安全多方计算的定义

由于安全多方计算协议的构造形式多种多样，而各研究者基于的安全模型不一致，而得出的应用条件也是不一样的，这种不同会影响到协议的具体应用，故而一个大家认同的、完备的定义一直是研究热点。

2.新的安全多方计算协议构造方法

目前大部分研究者在设计安全多方计算协议时，基本都以VSS的子协议为构造基石，设计出的协议在答题结构上都是类似的，这样在解决通信效率和安全性上没有实质性突破。是否存在新的构造方法来设计高效安全多方计算协议，是研究者们一直在探索的问题之一。

3.恶意模型下的安全多方计算

现在对安全多方计算问题的研究主要基于密码学和信息轮等安全模型，尽管从理论上说，任何通用模型下的SMC协议都可以转换成恶意模型下的SMC协议，但这种理论转换在效率上是不可行的。因此，恶意模型下的安全多方计算问题需要得到进一步的研究。