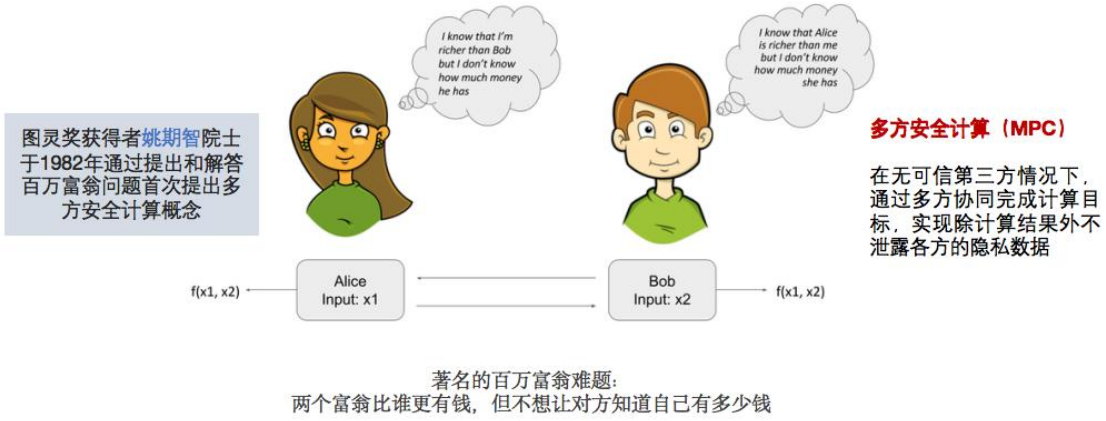
多方安全计算

Secure Multiparty Computation

多方安全计算是指在无可信第三方情况下，通过多方共同参与，安全地完成某种协同计算。即在一个分布式的网络中，每个参与者都各自持有秘密输入，希望共同完成对某个函数的计算，但要求每个参与者除计算结果外均不能得到其他参与实体的任何输入信息。也就是参与者各自完成运算的一部份，最后的计算结果由部分参与者掌握或公开共享。也就是说多方安全计算技术可以获取数据使用价值，却不泄露原始数据内容，保护隐私。因此在大数据发展并立法保护的今天，多方安全计算技术从多年的学术研究，变得具有巨大的商业价值。

多方安全计算是由一系列密码学安全计算协议组成，常采用的技术有秘密共享(Secret Sharing)、不经意传输(Oblivious Transfer)、混淆电路(Garbled Circuit)、同态加密(Homomorphic Encryption)等。安全多方计算技术在需要隐私保护的场景中具有重要意义，其主要适用的场景包括联合数据分析、数据安全查询、数据可信交换等。



著名的百万富翁难题：
两个富翁比谁更有钱，但不想让对方知道自己有多少钱

多方安全计算框架可以让多方安全地计算任何函数或某类函数的结果。自 1986 年姚期智提出第一个通用的多方安全计算框架以来，30 多年间已经有 BMR、GMW、BGW、SPDZ 等多个多方安全计算框架陆续提出。多方安全计算具有很高的安全性，要求敏感的中间计算结果也不能泄露，在近几十年的发展中，其各种核心技术和构造方案不断接受学术界和工业界的检验，具有很高的可信性，其性能在各种研究中也不断提升，现在在很多场景下已经达到了产业能实际应用接受的程度。