**一次多项式安全多方计算通信协议**

# 场景描述

对于一组参与实体*p*1, *p*2, …, *pn*，每个实体有一个秘密**整数**数据，分别是*x*1, *x*2, …, *xn*，参与实体希望共同计算出一个公共函数*f*(*x*1, *x*2, …, *xn*)，同时保持其秘密数据的私密性。准确来说，就是不存在超过*t*个实体勾结的情况下，任意实体的秘密数据不会被其他实体所知晓。

本文所描述的通信协议针对函数*f*是一次多项式的情形，即：

*f*(*x*1, *x*2, …, *xn*) = *c*1*x*1 + *c*2*x*2 + … + *cnxn*，其中*c*1, *c*2, …, *cn*为公共整数常数。

在实际应用场景中，其中一个参数实体将作为计算发起者，负责选择计算参数并发送给其他的参与实体。最后的计算结果归属存在以下两种情形：

1. 只有计算发起者需要知晓计算结果；
2. 所有参与者均需要知晓计算结果。

上述两种情形在通信协议上略有不同。

# 安全多方计算通信协议

假定参与计算的实体总数为*n*，一次完整的安全多方计算过程均包含以下阶段：

## 准备阶段

该阶段由计算发起者选择计算参数，并发送给其他参与实体，参数包含以下内容(见《安全多方计算算法》文档的第2.1节)：

1. 素数*p*；
2. 随机数。

注：准备阶段对于每次安全多方计算均需要运行一次，而不是运行一次可进行多次计算。



图1. 准备阶段通信示意图

## 输入阶段

该阶段每个参与实体将秘密信息分散至*n*个分片中，给其他每个参与实体发送其对应的分片。

实体*pi*发送给实体*pk*的分片为*qi*(*ak*) (见《安全多方计算算法》文档的第2.2节)。



图2. 输入阶段通信示意图

## 输出阶段

该阶段每个参与实体计算一个输出数据*βi* (见《安全多方计算算法》文档的第2.3节)。该阶段因计算结果的归属不同而有所不同

1. 计算结果仅归属计算发起者

对于这种情形，除计算发起者之外的其他参与实体将输出数据发送给计算发起者。



图3. 输出阶段通信示意图1

1. 所有参与者均需要知晓计算结果

对于这种情形，每个参与实体均需将其计算得出的输出数据发送给其他参与实体。



图4. 输出阶段通信示意图2

# 通信协议评估

## 通信复杂度

准备阶段*n* – 1条消息，输入阶段*n*(*n* - 1)条消息，输出阶段根据计算结果归属的不同而异，分别是*n* – 1和*n*(*n* - 1)条消息，故总体通信复杂度为O(*n*2)。

## 工作量证明

在计算结果仅归属计算发起者的情形，可能存在计算发起者需要向其他参与实体付费的问题，此时有可能需要考虑工作量证明问题。

1. 在输出阶段，如果全体参与实体均向计算发起者发送了输出数据，显然所有的参与实体均为安全多方计算做出了足额的贡献；
2. 在输出阶段，如果某个参与实体*u*没有向计算发起者发送输出数据，这里有两种可能：
   1. *u*收到了来自所有其他实体的输入数据，但没有完成输出数据的计算或发送，此时责任在*u*；
   2. *u*没有收到某个参与实体发送的输入数据，此时*u*无法计算输出数据，责任应该在没有发送输入数据的实体。