**安全多方计算算法**

# 场景

对于一组参与实体*p*1, *p*2, …, *pn*，每个实体有一个秘密数据，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，即秘密数据不被其他实体所知晓。

# 一次多项式计算

指*f*(*x*1, *x*2, …, *xn*) = *c*1*x*1 + *c*2*x*2 + … + *cnxn*，*c*1, *c*2, …, *cn*为公共常数。

## 准备阶段

1. 各实体共识一个素数*p*，以及一组随机数
2. 每个实体*pi*(1≤*i*≤*n*)随机选择一个*t*次多项式*qi*(*x*) = *xi* + *qi*1*x + qi*2*x*2+…+ *qitxt* mod *p*，其中。

## 输入阶段

每个实体计算*qi*(*a*1)，*qi*(*a*2)，…，*qi*(*an*)，并将*qi*(*ak*)发给实体*pk*(1≤*k*≤*n*)；

此时每个实体*pi*拥有的信息是*q*1(*ai*), *q*2(*ai*), …, *qn*(*ai*)。

## 输出阶段

每个实体*pi*计算：*βi = c*1*q*1(*ai*) + *c*2*q*2(*ai*) +, …, + *cnqn*(*ai*)，并将*βi*发送给每个实体*pk*(1≤*k*≤*n*)。

此时每个实体拥有的信息是*q*1(*ai*), *q*2(*ai*), …, *qn*(*ai*)；*β*1, *β*2 ,…, *β*n。

计算*f*(*x*1, *x*2, …, *xn*)如下：

因为*β*i *= c*1*q*1(*ai*) + *c*2*q*2(*ai*) +, …, + *cnqn*(*ai*) *mod p*

= *c*1(*x*1+*q*11 *ai+q*12 *ai*2+,…,+*q*1*t ait*) + *c*2(*x*2+*q*21 *ai+q*22 *ai*2+,…,+*q*2*t ait*) + … + *cn*(*xn*+*qn*1 *ai+qn*2 *ai*2+,…,+*qnt ait*) *mod p*

对应次数项系数相加，得：

= (*c*1*x*1 + *c*2*x*2 + … + *cnxn*) + (*c*1*q*11 + *c*2*q*21 + … + *cnqn*1)*ai* + … + (*c*1*q*1*t* + *c*2*q*2*t* + … + *cnqnt*)*ait* *mod p*

= (*c*1*x*1 + *c*2*x*2 + … + *cnxn*) + *mod p*

*β*1, *β*2 ,…, *β*n可视为*n*个方程，其中未知数一共*t* + 1个，分别是：

*s*0 = *c*1*x*1 + *c*2*x*2 + … + *cnxn*

*s*1 =

*s*2 =

……

*st* =

选择*t* + 1个方程，即可得解，*s*0就是所求的*f*(*x*1, *x*2, …, *xn*)。

## 非模*p*上的计算

需知晓*c*1*x*1 + *c*2*x*2 + … + *cnxn*的上限，然后有两种做法：

1. 让*p*大于上述上限；
2. 使用中国剩余定理：选择多组素数*p*，以及随机数；重复上述2.1 ~ 2.3过程，然后将各解通过中国剩余定理求得实际值。此时要求所选素数的乘积大于上述上限。

# 基于Shamir秘密分享的计算

本质上第2节中的算法利用了Shamir的秘密分享方案。

## Shamir的秘密分享方案

Shamir的秘密分享方案是一个(*k*, *n*)门限秘密分享方案，即将秘密*D*分解为*n*个分片，使得：

1. 拥有任意*k*个或更多的分片，可以快速计算*D*；
2. 仅拥有*k* - 1个或更少的分片，*D*完全不可判断，对于所有取值概率相同。

方案描述如下：

1. 方案基于一个*k* – 1次一元多项式，该多项式在有限域*Fp*上，其中*p*是素数，且*p* > *D*，多项式如下：

*q*(*x*) = *d*0 + *d*1*x* + … + *dk*-1*xk*-1 mod *p*

1. 分享秘密：
   1. 随机选择*k*-1个随机数*d*1, *d*2, …, *dk*-1*Fp*，令*d*0 = *D*，构建上述多项式；
   2. 计算*q*(1), *q*(2), …, *q*(*n*)，构造*n*个分片(*i*, *q*(*i*))，其中1≤*i*≤*n*。
2. 通过*k*个分片还原秘密：*k*个分片，就有*k*个线性方程，未知数是*d*0, *d*1, …, *dk*-1，通过解方程可得所有未知数，其中*d*0就是还原出来的秘密*D*。

## 利用Shamir秘密分享完成一次多项式安全多方计算

1. 准备阶段

每个参与实体使用素数*p，t*+1作为门限*k*，以及自身的秘密数据*xi*构建Shamir秘密分享多项式。

1. 输入阶段

每个参与实体使用随机数作为多项式的输入，构造n个分片(*ai*, *q*(*ai*))。

1. 输出阶段

参与实体计算自身的*βi*，发送并获得*β*1, *β*2 ,…, *β*n后，选择其中*t*+1个值，假定为*β*1, *β*2 ,…, *βt*+1，构建*t*+1个分片(*ai*, *βi*)，其中1≤*i*≤*t*+1。将这*t*+1个分片通过Shamir秘密分享的还原算法获得所需计算的一次多项式结果。