MPC的算法最终目的：将**一份权限**打散到**多个参与者**中。通过对每个人拥有的密钥片段进行整合，最终恢复出一个完整的密钥，使用该密钥对消息进行签名。

1. 密码学核心技术：分布式密钥生成DKG

2.DKG简介

DKG通过多方参与，计算共享的公钥与私钥集，解决上述问题， 分布式秘钥产生不依赖任何可信的第三方。在(n,t)-DKG中， n为节点数量，t为阈值， DKG协议允许n个节点共同产生秘钥，使得任何数量**大于阈值t**的节点子集都能使用该共享秘钥，然而任何数量**少于阈值t**的节点子集都没有对该共享秘钥的任何知识。

1. DKG的基本构造块：可验证秘钥共享VSS

(n,t+δ,t)-秘密共享：假设整数n, t ,δ 满足 n>=t+δ>t>=0 ,一个(n,t+δ, t) 秘密共享协议是被用于一个交易方 在n个节点之间共享一个秘钥，使得其中任何t+δ或者更多的节点能够计算密钥s, 但是t个或更少的节点没有关于s的任何信息。

3.算法实现的简易数学模型

假设：M 当前需要加密消息

P 一个随机数（①P是质数②M/2<P<M）

m 当前系统节点总数

n 可解密的最少节点数

Node k 第k个可解密节点

加密阶段：

（1）构造加密方程：axn-1+bxn-2+...+cx2+dx+M

方程系数a,b,...,c,d由系统自动生成，但要满足a,b,...,c,d,e < P

1. 计算生成各个节点的密钥片段

对于节点Node k：**（akn-1+bkn-2+...+ck2+dk+M）mod P**

1. 将根据节点编号生成的**密钥片段**、**随机数P**发送给对应节点

解密阶段：

注意：目前每个节点掌握三个信息：①密钥片段②节点编号③随机数P

（1）设方程式**axn-1+bxn-2+...+cx2+dx+M**

（2）节点将自己的信息代入方程式，得到一个方程组，对方程组进行求解

（3）求解得到方程组的常数项即为恢复后的消息

示例：

假设：当前需要加密消息M=8

随机数P=7

可解密的最少节点数n=3，分别为Node 1、Node 2、Node 3

加密阶段：

构造方程：4x2+3x+8

|  |  |  |
| --- | --- | --- |
| 节点编号 | 计算过程 | 密钥片段 |
| Node 1 | 4\*1+3\*1+8=15 mod 7 | 1 |
| Node 2 | 4\*4+3\*2+8=30 mod 7 | 2 |
| Node 3 | 4\*9+3\*3+8=53 mod 7 | 4 |

解密阶段：

已知P=7

|  |  |  |
| --- | --- | --- |
| 节点 | 节点编号 | 密钥片段 |
| Node 1 | 1 | 1 |
| Node 2 | 2 | 2 |
| Node 3 | 3 | 4 |

假设存在方程式：ax2+bx+M

得到方程组：

a+b+M=1 mod 7

4a+2b+M=2 mod 7

9+3b+M=4 mod 7

解之，得：a=4 , b = 3

还原方程：4x2+3x+M

任选Node 1、Node 2、Node 3代入原方程：  
4+3+M=1 mod 7

解之，得：M=8