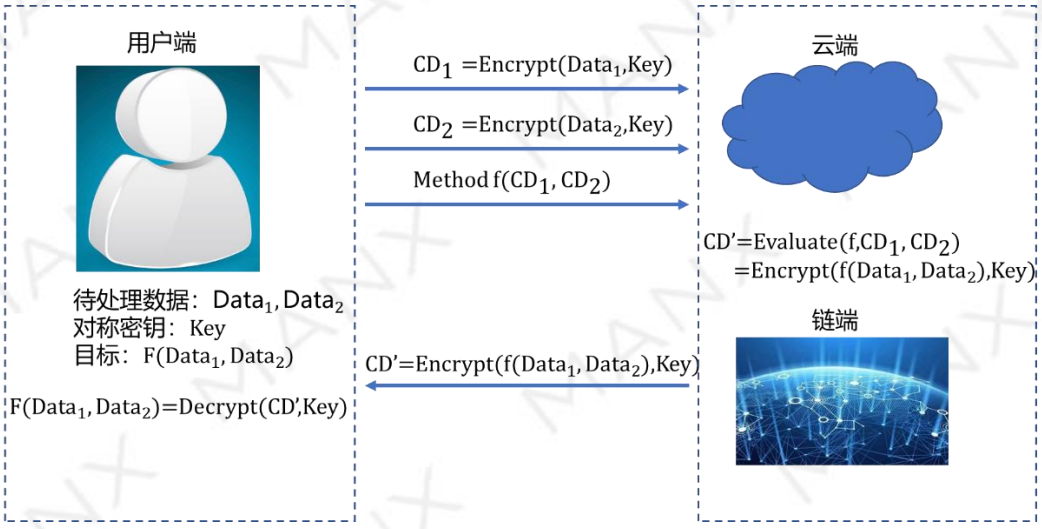
MANX 同态加密技术

课题 **1**：**MANX** 同态加密设计概念：

区块链和云技术促进了全球数据共享，但也引发了人们对隐私安全的担忧。幸运的是，随着技术的进步，引入“同态加密”技术，该技术提供了一种对加密数据进行处理的功能，即加密数据在传输过程中，无需密钥进行解密就能对加密数据进行处理，而且处理过程不会泄露任何原始内容，同时，拥有密钥的用户解密后可以得到处理后的结果，由此大幅度提高了数据的安全隐私保护。对于区块链来说，同态加密是一种先进的隐私保护机制。

课题 **2**：同态加密流程：



数据同态加密

1. 用户对 Data1 和 Data2 进行加密，将加密后的数据 CD1 和 CD2 发送到云端；

2. 用户向云端提交数据处理方法 f()；

3. 云端和链端使用方法 f()对密文数据 CD1 和 CD2 进行处理；

4. 云端和链端将处理后的结果发送给用户；

5. 用户对数据进行解密，得到相应原始数据处理后的结果。

课题 **3**：同态加密的功能和方法：

在同态加密过程中我们具体需要以下几个主要方法：

- GenerateKey 方法：用来生成密钥
- Encrypt 方法：用来进行同态加密
- Evaluate 方法：在用户给定的数据处理方法 f()下，对密文进行操作
- Decrypt 方法：用来解密密文

定义 3 基于公钥密码体制的安全同态加密方案由一组概率多项式时间（PPT）算法 (Setup, Encrypt, Circuit, Decrypt)组成：

- $\mathrm{Setup}(1^n 1^l)$：输入安全参数n及最大用户数l，输出用户私钥sk和公钥pk；
- $\mathrm{Encrypt}(\mathrm{id}, \mathrm{pk}, m_i)$：给定数据标识id，用户公钥pk与明文$m_i$，输出密文$c_i$；
- $\mathrm{Circuit}(\mathrm{id}, \{\alpha_i, c_i\}_{i=1}^{l})$:输入数据标识id，密文$c_1$,...,$c_l$,及相应权值$\alpha_1$,...,$\alpha_l$,输出运算结果$c = \sum_{i=1}^{l} \alpha_i c_i$;
- $\mathrm{Decrypt}(\mathrm{id}, \mathrm{sk}, c)$:已知数据标识id，用户私钥sk与密文$c_{Cir}$，输出明文$m = \sum_{i=1}^{l} \alpha_i m_i$。

课题 **4**：**MANX** 选用的同态加密方案

基于 **R-LWE** 的线性同态加密方案

- $\mathrm{Setup}(1^n 1^l)$:输入安全参数$n = 2^k (k \in Z)$，最大用户数l及正整数，$p < q = 1 \bmod 2^n$, q为素数。随机选取$s \in R_q = Z_q[x]/< f(x) > (f(x) = x^n + 1 \in Z[x])$作为私钥，公钥为$(a, b = a \times s + pe)$，其中$a \leftarrow R_q$是均匀随机选取的，误差项e从误差分布$\gamma \subset R_q$中独立选取；

- $\mathrm{Encrypt}(\mathrm{id}, \mathrm{pk}, m_i)$：给定数据标识id及用户公钥$(a, b)$，为了加密一n比特的明文消息$m_i \in \{0,1\}^n \subset R_q$，均匀随机选取$t_i \in R_q$。输出密文$\left(c_i^{(1)}, c_i^{(2)}\right) = \left(a \times t_i + pe_i^{(1)}, b \times t_i + pe_i^{(2)} + m_i\right)$其中$e_i^{j} (j = 1,2)$从分布$\gamma$中独立选取，其中$R_q$中多项式加法为普通多项式相加，乘法为普通多项式相乘模$x^n + 1$；

- $\mathrm{Circuit}(\mathrm{id}, \{\alpha_i, c_i\}_{i=1}^{l})$：输入数据标识id，权值为$\alpha_1$,..., α_l的密文$\left(c_1{}^{(1)}, c_1{}^{(2)}\right)$,..., $\left(c_l{}^{(1)}, c_l{}^{(2)}\right)$输出密文；$\left(c^{(1)}, c^{(2)}\right) = \left(\sum_{i=1}^{l} \alpha_i c_i{}^{(1)}, \sum_{i=1}^{l} \alpha_i c_i{}^{(2)}\right) = \left(\sum_{i=1}^{l} \alpha_i \left(a \times t_i + pe_i{}^{(1)}\right), \sum_{i=1}^{l} \alpha_i \left(b \times t_i + pe_i{}^{(2)} + m_i\right)\right)$
- $\mathrm{Decrypt}(\mathrm{id}, \mathrm{sk}, c)$：收到数据标识id，用户私钥sk及密文$(c_1, c_2)$后，计算$(c_2 - c_1 \times s) \bmod p$可得明文$m = \sum_{i=1}^{l} \alpha_i m_i$。