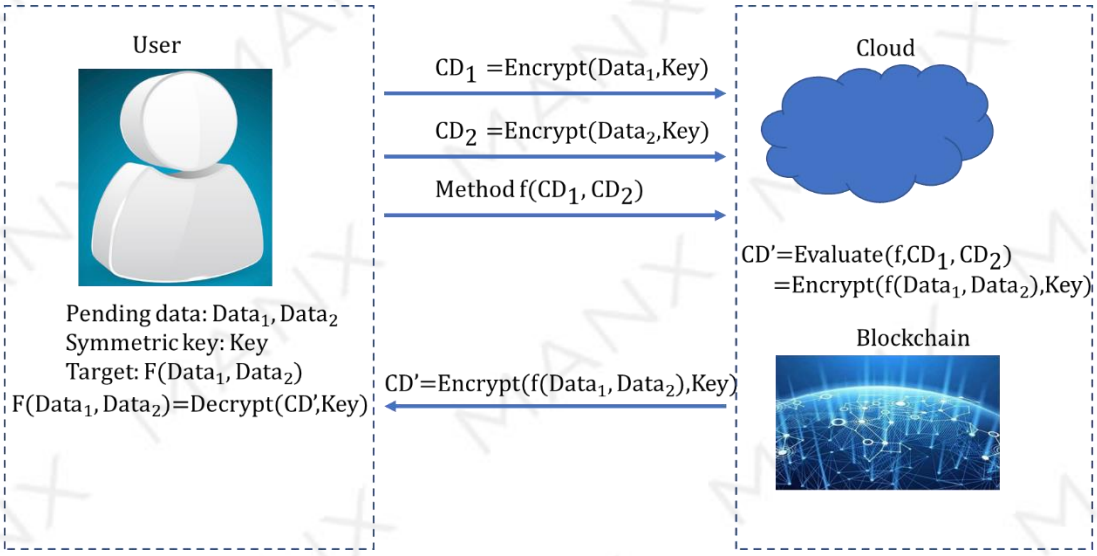
MANX Homomorphic Encryption Technique

Topic 1: Design Concept of MANX Homomorphic Encryption:

Blockchain and cloud technologies have promoted global data sharing, but they have also raised concerns about privacy and security. Homomorphic encryption technology has been introduced so that the encrypted data can be processed without the need to decrypt data before processing. No original content is revealed during the entire process. After the blockchain or the cloud has finished processing and returned the encrypted result, the user can decrypt the encrypted result with their secret key. The homomorphic encryption mechanism is an advanced privacy protection mechanism that greatly improves data security.

Topic 2: MANX Homomorphic Encryption Procedure:



Data Homomorphic Encryption

The procedure is as follows:

1. The user encrypts Data1 and Data2 and sends the encrypted data CD1 and CD2 to the cloud.
2. The user submits data processing method f()to the cloud.
3. The cloud uses method f() to process CD1 and CD2 directly and then encrypts the result.
4. The cloud returns the encrypted result to the user.
5. The user decrypts the encrypted result to obtain the real result.

Topic 3: Homomorphic Encryption Functions and Methods:

Several methods need attention during the homomorphic encryption process:

- GenerateKey(): used to generate key
- Encrypt(): used to do homomorphic encryption
- Evaluate(): used to process the encrypted data given f()
- Decrypt(): used to decrypt the encrypted data

Definition: Public key cryptography-based fully homomorphic encryption scheme consists of 4 probabilistic polynomial time algorithm (Setup, Encrypt, Circuit, Decrypt)

- $\text{Setup}(1^n 1^l)$: Enter security parameter n and maximum user number l, Return secret key sk and public key pk;
- $\text{Encrypt}(\text{id}, \text{pk}, m_i)$: Given data id, user public key pk and plaintext m_i, return ciphertext c_i;
- $\text{Circuit}(\text{id}, \{\alpha_i, c_i\}_{i=1}^l)$: Enter data id, cipher text c_1,...,c_l, and corresponding weight α_1,...,α_l, return $c = \sum_{i=1}^l \alpha_i c_i$;
- $\text{Decrypt}(\text{id}, \text{sk}, c)$: given data id, user secret key sk and ciphertext c_{Cir}, Return plaintext $m = \sum_{i=1}^l \alpha_i m_i$

Topic 4: MANX Selected Encryption Scheme:

Linear Homomorphic Encryption Scheme based on R-LWE

- $\text{Setup}(1^n 1^l)$:Enter security parameter $n = 2^k (k \in Z)$, maximum user number l and positive integer p, $p < q = 1 \bmod 2^n$, q is prime number. Randomly sample $s \in R_q = Z_q[x]/< f(x) >$ $(f(x) = x^n + 1 \in Z[x])$ as the secret key, $(a, b = a \times s + pe)$ is the public key, where $a \leftarrow R_q$ is randomly sampled, error term e is independently sampled from error distribution $\gamma \subset R_q$;

- Encrypt(id, pk, m_i)：Given data id and user public key (a, b)，encrypt n-bit plaintext message $m_i \in \{0,1\}^n \subset R_q$，Randomly sample $t_i \in R_q$. Return ciphertext $\left(c_i^{(1)}, c_i^{(2)}\right) = \left(a \times t_i + pe_i^{(1)}, b \times t_i + pe_i^{(2)} + m_i\right)$, where $e_i^j (j = 1,2)$ is independently sampled from distribution γ. In R_q, add is ordinary polynomial add，multiply is ordinary polynomial multiply mod $x^n + 1$；

- Circuit$(id, \{\alpha_i, c_i\}_{i=1}^l$：Enter data id，weights are α_1 ,..., α_l, ciphertext are $\left(c_1^{(1)}, c_1^{(2)}\right)$,..., $\left(c_l^{(1)}, c_l^{(2)}\right)$. Return $\left(c^{(1)}, c^{(2)}\right) = \left(\sum_{i=1}^l \alpha_i c_i^{(1)}, \sum_{i=1}^l \alpha_i c_i^{(2)}\right) = \left(\sum_{i=1}^l \alpha_i \left(a \times t_i + pe_i^{(1)}\right), \sum_{i=1}^l \alpha_i \left(b \times t_i + pe_i^{(2)} + m_i\right)\right)$;

- Decrypt(id, sk, c)：given data id，user private key sk and ciphertext (c_1, c_2)，calculate $(c_2 - c_1 \times s) \bmod p$, Return plaintext $m = \sum_{i=1}^l \alpha_i m_i$。