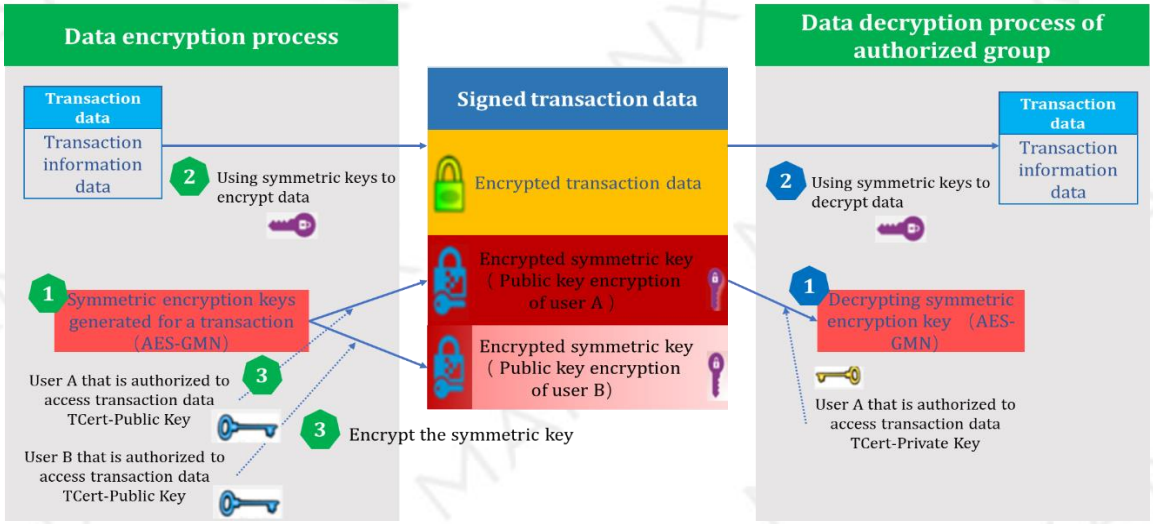
MANX Post-Quantum Encryption Technique

Topic 1: Encryption Module is the Fundamental Technology to Achieve Authorized Data Sharing:

Authorized data sharing is implemented through a combination of symmetric and symmetric keys. Specific steps are as follows:

1) The data sharing initiator generates a symmetric encryption key for the transaction;
2) Using this symmetric encryption key to encrypt the transaction data and other data on the chain to obtain ciphertext information;
3) Select the data authorization object or set of objects and query the public key information of the authorization object;
4) Encrypt the symmetric encryption key through the public key information of the authorization object and send it to the authorization sharing object;
5) The authorization object decrypts its symmetric encryption key through its own private key;
6) The authorization object finds the corresponding ciphertext information at the corresponding storage path by decrypting the key and decrypting the original data that is authorized for sharing.



Data Authorization Sharing

Topic 2: Versatile Use of MANX Encryption Module

The MANX encryption module implements pluggable encryption/decryption and can support seamless switching between the international encryption standard AES and the

national standard cipher system SM4 at any time; the signature and verification module supports the elliptic curve ECC, the national standard SM2 signature algorithms and the verification algorithm, so the pluggable encryption module can be used under all circumstances which follows the same encryption protocol; the blockchain's bottom layer protocol co-processing module supports the transaction packaging, sending and verification of the existing mainstream public chain platform.

Topic 3: Threats Posed by Quantum Computing to Traditional Encryption Algorithms

In the past three decades, encryption methods represented by public-key cryptosystems such as RSA, ECC, Diffie-Hellman, and algebraic homomorphism have become core security protocols for the internet and information infrastructure. They have wide-ranging and critical applications in military, politics, economics and life. Moreover, they play a crucial role in the secure communication of individuals, businesses and governments. The theoretical threats to traditional cryptography by quantum computing, the rapid development of quantum computer-related technologies, and the initiation and promotion of national quantum strategies and policies by various countries have given today's information society an unprecedented sense of urgency. IBM and Google have successfully developed a quantum computing prototype with 50 and 72 qubits, taking the first step of quantum computing from theory to application. With quantum computers as the operating environment, quantum algorithms can easily solve the aforementioned security system. The security of RSA and ECC public key cryptosystems are based on the assertion that large integer factorization and discrete logarithm are NP hard problems. However, Shor's algorithm shows that large integer factorization and discrete logarithm problems are solvable problem in the quantum machine environment. With the rapid growth of quantum computing capabilities, quantum computing is a serious threat to the once unbreakable security defenses in the fields of the state, finance, society and individuals. It poses a huge threat to almost all areas involved in information security. MANX core development member Dr. Jack Chiu has had in-depth discussions Professor Vladan Vuletic concerning these topics of quantum computing and post-quantum algorithms.

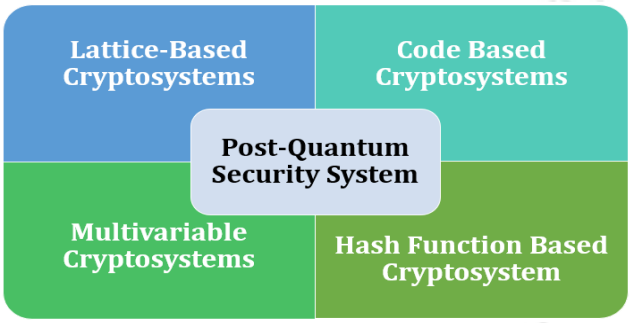
The blockchain puts almost all of the digital currency's security on the public key security system—elliptic curve public key cryptography ECC. However, once quantum computers become practical, they can crack almost all of the Bitcoin, Ethereum, etc. within seconds, and make the value of the digital currency collapse in an instant. Therefore, we have proposed a cryptographic security system against quantum computing and software solutions to ensure the basic security of the next generation of digital currency in the post-quantum era.

Topic 4: Structure of MANX Post-Quantum Encryption Security System

MANX carried out research on post-quantum cryptosystems in four areas:

(1) lattice-based cryptography;
(2) code-based cryptography;
(3) multi-variable public key cryptography;
(4) hash-function-based cryptography

Considering the controllability of public key and cyphertext and the efficiency of signatures, we will create post-quantum public-key encryption and signature standards based on hash functions and lattice ciphers for different ecosystems and applications.



Post-quantum Security System

Topic 5: MANX Signature Scheme based on Lattice Cryptography

The safety of lattice-based cryptography is based on lattice problems such as the shortest vector problem and the nearest vector problem in the lattice. Theoretically, lattice problems can't be solved by existing quantum algorithms including Shor's algorithm and Grover's algorithm, so unlike more widely used and known public-key schemes such as the RSA, ECC which are easily attacked by a quantum computer, lattice-based constructions appear to be resistant to attack by both classical and quantum computers. Furthermore, many lattice-based constructions are known to be secure under the assumption that certain well-studied computational lattice problems cannot be solved efficiently.

1) Parameter Selection

Construct an $m \times k$ matrix S with integer entries randomly selected from $\{-d, \dots, 0, \dots, d\}$ as the private key, i.e., the signature key. Similarly, construct an $n \times m$ matrix A with integer entries randomly selected from Z_q, computing $T = AS \in Z_q^{m \times k}$ as the public key, i.e., the verification key. The hash function in the lattice signature scheme is assumed to be $H: \{0,1\}^* \to \{v: v \in \{-1,0,1\}^k, \|v\|_1 \leq \kappa\}$. To sign the message μ, the signature first randomly

selects an m-dimensional vector y in the discrete uniform distribution D_σ^m, where σ is the standard deviation of D_σ^m, namely, the relevant parameters of the lattice signature scheme are obtained.

2) Key Generation

Key signing. Randomly select S from $\{-\mathrm{d}, \ldots, 0, \ldots, \mathrm{d}\}$;

Key verification. Randomly select A from $Z_q^{n\times m}$ and calculate $T = AS \in Z_q^{m\times k}$; random oracle model:

$$H: \{0,1\}^* \to \{v: v \in \{-1,0,1\}^k, \|v\|_1 \le \kappa\}$$

3) Signing process

Step 1: Randomly select the m-dimensional vector y from the discrete uniform distribution D_σ^m;

Step 2: Calculate Ay, then calculate $c = H(Ay, \mu)$, where μ is the signed message;

Step 3: Calculate $z = Sc + y$;

Step 4: Output the signature result (z, c) according to the probability $\Pr = \min\left(\frac{D_\sigma^m(z)}{MD_{Sc,\sigma}^m(z)}, 1\right)$, and reject sampling theorem is adopted in the signature process.

4) Verification Process

After the signature pair (z, c) is received, $\|z\|$is calculated. If $\|z\| \le 2\sigma\sqrt{m}$ and $c = H(Az - Tc, \mu)$ are satisfied, the signature is accepted.

Topic 6: MANX Signature Scheme based on Merkel Tree

Step 1:Generate the random parameters of the hash function through the PN256 generation module;

Step 2:Use a seed to generate a signature and verification key sequence by pseudo-random number generator PRNG;

PRNG：$\{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n$

Step 3:Use the signature and verification key sequence to generate the root node value of the Merkel tree as the public key of the signature system;

$v_{0,j}= \text{hash}(Y_j)$, $v_{h,j}= \text{hash}(v_{h-1,2j} || v_{h-1,2j+1})$, $1 \le h \le H$, $0 \le j < 2^{H-h}$

Step 4: Query the counter module to obtain the coordinate value of this signature key.

Step 5: Calculate the signature key, the verification key and the node value of the Merkel tree verification path used for this signature according to the coordinate value of this signature key.

Step 6: Process the message to be signed through the message digest generation module to generate a message digest;

Step 7: A one-time signature is made for message digest of step 6 by using the signature key, verification key and node value of the Merkel tree verification path generated in step 5:

$$e_s = (e_{s,n-1}, e_{s,n-2}, \dots, e_{s,0}) = \left(f^{d_{n-1}}(x_{s,n-1}), f^{d_{n-2}}(x_{s,n-1}), \dots, f^{d_1}(x_{s,1}), f^{d_0}(x_{s,0})\right)$$

Step 8: Add 1 to the counter module and point to the next signature key.

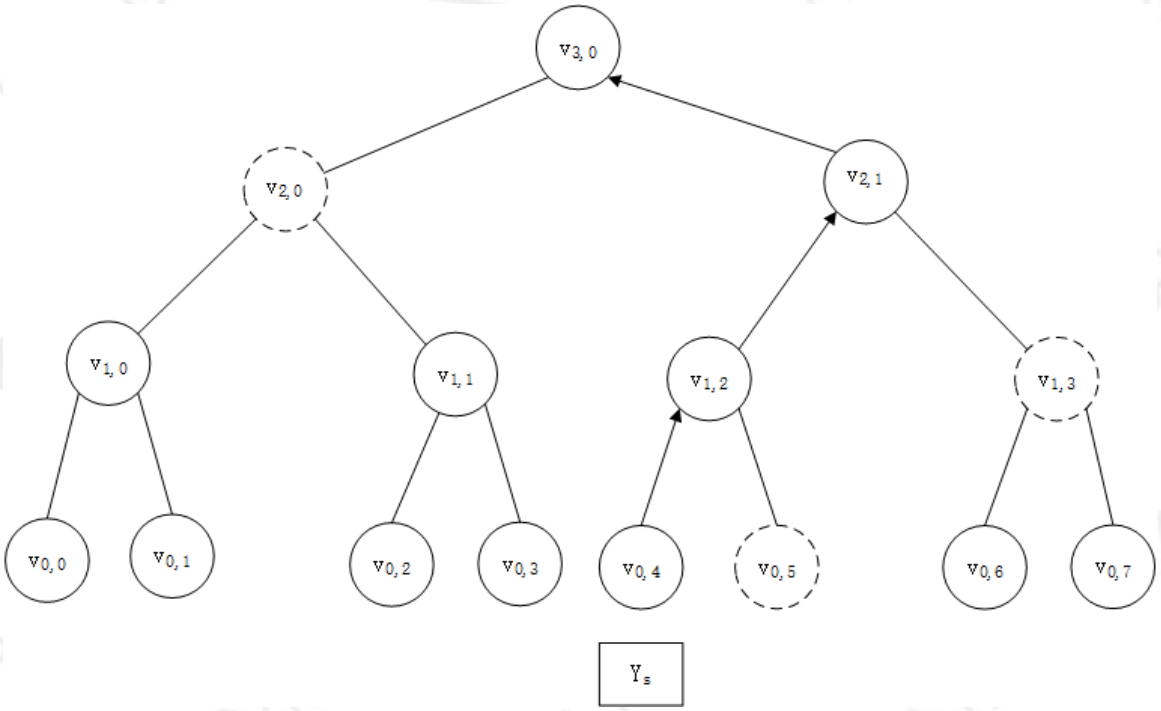
The verification method implementation includes the following steps:

Step 1: Process the message to be signed through the message digest generation module to generate a message digest;

Step 2: Determine the validity of the one-time signature part of the message digest by the one-time signature verification module;

Step 3: Determine the validity of the verification key through the Merkel tree root node verification module;

$T_0=\text{hash}(Y_s)$, if $\lfloor s/2^h \rfloor = 0 \bmod 2$, then $T_h= \text{hash}(T_{h-1} || p_{h-1})$, if $\lfloor s/2^h \rfloor = 1 \bmod 2$, then $T_h= \text{hash}(p_{h-1} || T_{h-1})$, here $1 \le h \le H$



Determine the validity of the key through the Merkel Tree Root Node

Step 4: Determine the overall validity of this signature through the comprehensive judgment module.

	MANX (lattice)	MANX (Hash)	InterValue	Hcash
Principle	ETRU system signing and encrypting system	Chain Merkle signature Scheme (CMSS)	NTRU signature algorithm	LWE signature alorithm
Speed	Fastest	Fast	Fast	Medium
Secret-key length	Small	Smallest	Medium	Medium
Signature length	Smallest	Small	Small	Medium
Encryption function and P2P directional sharing	Y	N	N	N
Homomorphic calculation	Y	N	N	N
	Suitable for scenarios which need high speed	Suitable for scenarios which need to control secret key length		

MANX Judgement Modules