Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.046816

ARTICLE

A Post-Quantum Cross-Domain Authentication Scheme Based on Multi-Chain Architecture

Yi-Bo Cao[1,*], Xiu-Bo Chen[1], Yun-Feng He[2], Lu-Xi Liu[2], Yin-Mei Che[2], Xiao Wang[2], Ke Xiao[3], Gang Xu[3] and Si-Yi Chen[1]

[1]Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China

[2]Information Center of China North Industries Group Corporation, Beijing, 100089, China

[3]School of Information Science and Technology, North China University of Technology, Beijing, 100144, China

*Corresponding Author: Yi-Bo Cao. Email: caoyibo@bupt.edu.cn

Received: 16 October 2023 Accepted: 28 December 2023 Published: 27 February 2024

ABSTRACT

Due to the rapid advancements in network technology, blockchain is being employed for distributed data storage. In the Internet of Things (IoT) scenario, different participants manage multiple blockchains located in different trust domains, which has resulted in the extensive development of cross-domain authentication techniques. However, the emergence of many attackers equipped with quantum computers has the potential to launch quantum computing attacks against cross-domain authentication schemes based on traditional cryptography, posing a significant security threat. In response to the aforementioned challenges, our paper demonstrates a post-quantum cross-domain identity authentication scheme to negotiate the session key used in the cross-chain asset exchange process. Firstly, our paper designs the hiding and recovery process of user identity index based on lattice cryptography and introduces the identity-based signature from lattice to construct a post-quantum cross-domain authentication scheme. Secondly, our paper utilizes the hashed time-locked contract to achieves the cross-chain asset exchange of blockchain nodes in different trust domains. Furthermore, the security analysis reduces the security of the identity index and signature to Learning With Errors (LWE) and Short Integer Solution (SIS) assumption, respectively, indicating that our scheme has post-quantum security. Last but not least, through comparison analysis, we display that our scheme is efficient compared with the cross-domain authentication scheme based on traditional cryptography.

KEYWORDS

Cross-domain identity authentication; lattice-based cryptography; blockchain; hashed time-locked contract

1 Introduction

With the acceleration of informatization, the volume of data on the network is increasing exponentially, and how to securely and efficiently share data has become an urgent issue. Blockchain technology offers an excellent solution to this problem. Due to its decentralized, tamper-proof, and traceable characteristics, it has gained favor among many researchers in data sharing [1–5] and data protection [6–8]. In IoT scenarios, the introduction of blockchain enables many entities from different industries to jointly participate in data management, which improve the data reliability and shareability. Since different participants may maintain multiple blockchains, there is a requirement to enable the exchange of asset and value data among different blockchains within multi-chain environments.

Cross-chain technology plays a vital role in achieving interoperability among different blockchains, which primarily encompasses notary technology, side chain/relay technology, distributed private key control, and hashed time-locked contract (HTLC). However, notary technology exhibits a strong centralized feature, rendering the entire system non-distributed. Side chain/relay technology necessitates the introduction of a blockchain cross-chain network, which can be challenging to implement. Distributed private key control technology can result in transaction delays, significantly increasing communication consumption. On the other hand, HTLC, originally derived from the lightning network [9], offers a straightforward implementation, quick response, and the ability to facilitate asset exchanges between different blockchains without the involvement of an additional party. This characteristic has garnered substantial attention from researchers. Mohanty et al. [10] introduced a secure payment channel protocol, named New Hashed Time-Locked Contract (n-HTLC), which does not require the sender to send messages to each intermediate user along the payment route. In 2022, Shamili et al. [11] proposed an off-chain hash time lock commitment called the Federation Payment Tree (FPT), which employed a payment channel to provide a zero-knowledge hash lock commitment and allowed interaction between parties without a consensus protocol. Monika et al. [12] proposed a swap scheme between blockchains through HTLC and calculated the time-lock equations based on the confirmation time of the probabilistic blockchain. To address the inefficiencies associated with multiple participants exchanging tokens between blockchains simultaneously, Barbàra et al. [13] introduced MP-HTLC, demonstrating that the number of transactions remains independent of the number of participants on the UTXO blockchain. Subsequently, Wadhwa et al. [14] proposed a lightweight HTLC scheme called He-HTLC, which is inert to stimulus manipulation attacks and has excellent security.

In real-world scenarios, asset exchanges may involve entities located in different trust domains. Blockchain nodes from a foreign domain can access entities only after passing identity authentication by the authentication server in the local domain. This setup prevents blockchain nodes from different domains from interacting directly. To address these challenges, cross-domain authentication has emerged, enabling identity authentication of entities in distinct trust domains through various cryptographic primitives and facilitating session key negotiation to ensure entity identity credibility and communication confidentiality. Existing cross-domain authentication schemes primarily fall into three categories: based on symmetric cryptography, public key infrastructure (PKI), and identity cryptography. Numerous researchers have developed cross-domain authentication schemes using these cryptographic primitives. For instance, Sirbu et al. [15] proposed a cross-domain authentication scheme using public key cryptography to encrypt identity information. Liu et al. [16] integrated the ElGamal algorithm into a cross-domain authentication protocol, enabling key negotiation between participants. Zhang et al. [17] established a cross-domain authentication protocol based on PKI architecture by introducing an elliptic curve digital signature algorithm. Furthermore, identity-based cross-domain authentication schemes have gained prominence due to their ability to effectively reduce certificate management overhead, and several identity-based cross-domain authentication protocols have been developed. Peng [18] introduced an identity-based multi-trust domain authentication model, analyzing the security and anonymity of the identity authentication process. Luo et al. [19] implemented an identity-based cross-domain authentication scheme incorporating an elliptic curve signature, thereby achieving user identity anonymity. More recently, Wei et al. [20] applied blockchain certificate authority (BCCA) in each domain as nodes in consortium blockchain to realize cross-domain authentication. Zhou et al. [21] proposed an authentication scheme employing identity-based encryption and secret sharing, suitable for deployment on public channels within virtual enterprises. In the Industrial Internet of Things (IIoT), Cui et al. [22] introduced an anonymous cross-domain authentication scheme, which improves authentication efficiency while meeting traceability, scalability, forward privacy, and identity anonymity requirements.

In the aforementioned scenario, cross-domain identity authentication of blockchain nodes is an indispensable component before performing cross-chain asset exchange based on HTLC between blockchains located in different trusted domains. As is widely recognized, the reliability of cross-domain authentication schemes primarily depends on the security of cryptographic algorithms. However, the advent of quantum computers has introduced a significant threat to traditional cryptography, as the Shor algorithm [23] can solve the discrete logarithm problem in probabilistic polynomial time (PPT). This poses a grave challenge to the security of traditional cryptographic methods, and the trustworthiness of cross-domain authentication schemes is no longer assured. Researchers have delved into the post-quantum cryptography as a response to this threat. Among these endeavors, lattice-based cryptography has emerged as the leading post-quantum cryptographic algorithm due to its rapid operational efficiency. Various researchers have devised lattice-based cryptosystems to withstand quantum computing attacks. For instance, Rückert [24] created the first identity-based signature using lattice techniques, which exhibited strong unforgeability in the standard model. In 2014, Tian et al. [25] developed an innovative identity-based signature scheme over lattice, with security grounded in the SIS hardness assumption. In this scheme, we apply lattice-based cryptography to construct a cross-domain identity authentication scheme with post-quantum security, realize the cross-domain identity authentication of access nodes in the multi-chain architecture, and utilize the hashed time-locked contract to complete the cross-chain asset exchange between domains.

To sum up, the contribution of our paper is described as follows:

(1) This paper constructs a post-quantum secure cross-domain identity authentication scheme based on the multi-chain architecture, improves the traditional cross-domain authentication and applies the cross-chain technology based on HTLC, to achieve the identity authentication of cross-domain access nodes in the multi-chain architecture and the cross-chain asset exchange of nodes in different trust domains.

(2) This paper designs the hiding and recovery of the identity index based on lattice cryptography and introduces the identity-based signature on lattice in [25], which is used for the authentication server to check the identity of nodes, ensures the security and reliability of the cross-domain authentication process, and can resist quantum computing attacks.

(3) In security analysis, the IND-CPA of the identity index and the unforgeability of signature can be reduced to Learning With Errors (LWE) and Short Integer Solution (SIS) assumption, respectively. This scheme is efficient in terms of operation number and time consumption of the user and authentication server compared with other cross-domain authentication schemes through the comparison analysis.

2 Preliminary

2.1 Lattice

Definition 1 (Lattice): Given $\mathbf{A} = (\mathbf{a}_1|\mathbf{a}_2|\ldots|\mathbf{a}_m) \in \mathbb{Z}^{n\times m}$ is a $n \times m$-dimension matrix containing n linearly independent vectors $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m \in \mathbb{Z}^n$. The n-dimension lattice Λ is generated by A, expressed as:

$$\Lambda(\mathbf{A}) = \left\{\mathbf{y} \in \mathbb{Z}^n | \, \mathbf{y} = \mathbf{Ac} = \sum_{i=1}^{m} c_i \mathrm{a}_i, \mathbf{c} \in \mathbb{Z}^m\right\}, \tag{1}$$

where A is called the basis of Λ.

Definition 2 (Full-rank integer lattice): Given a matrix $\mathrm{A} \in \mathbb{Z}^{n\times m}$, where q is a prime, m and n is a positive integer, define the full-rank lattice generated by A:

$$\Lambda_q^{\perp}(\mathrm{A}) = \{\mathbf{e} \in \mathbb{Z}^m | \, \mathbf{Ae} = \mathbf{0} \, (\mathrm{mod} q)\} \tag{2}$$

$$\Lambda_q(\mathrm{A}) = \left\{\mathbf{y} \in \mathbb{Z}^m | \, \exists \mathbf{s} \in \mathbb{Z}^n, \mathrm{A}^T\mathbf{s} = \mathbf{y} \, (\mathrm{mod} q)\right\} \tag{3}$$

2.2 Discrete Gaussian Distribution

Definition 3 (Discrete Gaussian distribution): For the Gaussian parameter $\sigma > 0$ and the center $\mathbf{c}$, the Gaussian distribution on $\Lambda \subset \mathbb{Z}^n$ is defined as: $\forall \mathbf{x} \in \Lambda, \rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp\left(-\pi \cdot \frac{\|\mathbf{x}-\mathbf{c}\|^2}{\sigma^2}\right)$. The discrete Gaussian distribution on Λ is defined as: $\forall \mathbf{y} \in \Lambda, D_{\Lambda,\sigma,\mathbf{c}}(\mathbf{y}) = \frac{\rho_{\sigma,\mathbf{c}}(\mathbf{y})}{\rho_{\sigma,\mathbf{c}}(\Lambda)}$, where $\rho_{\sigma,\mathbf{c}}(\Lambda) = \sum_{\mathbf{x}\in\Lambda} \rho_{\sigma,\mathbf{c}}(\mathbf{x})$.

2.3 Hardness Assumption on Lattice

Definition 4 (LWE assumption): Given a prime q, positive integer m and n, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a vector $\mathbf{v} \in \mathbb{Z}_q^n$, a noise vector $\mathbf{e} \leftarrow \chi$, and then search a vector $\mathbf{z} \in \mathbb{Z}_q^m$ such that $\mathbf{v} = \mathbf{Az} + \mathbf{e}$.

Definition 5 (SIS and ISIS assumption): Given a prime q, positive integer m and n, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a parameter β, and then search for a vector $\mathbf{z} \in \mathbb{Z}_q^m \backslash 0$ such that $\mathbf{Az} = \mathbf{0}$ and $\|\mathbf{z}\| \leq \beta$. The above assumption can be extended to inhomogeneous versions, given a prime q, positive integer m and n, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a parameter β, a vector $\mathbf{u} \in \mathbb{Z}_q^n$, and then search for a vector $\mathbf{z} \in \mathbb{Z}_q^m \backslash 0$ such that $\mathbf{Az} = \mathbf{u}$ and $\|\mathbf{z}\| \leq \beta$.

2.4 The Trapdoor and Sampling Lemma on Lattice

Lemma 1 (TrapGen) [26] Given an odd integer $q \geq 3$, and $m = \lceil 6n \log q \rceil$, there exists a PPT algorithm TrapGen (q, n) that calculates a matrix $\mathbf{A}$ statically closed the uniform distribution on $\mathbb{Z}_q^{n\times m}$, and a matrix $\mathbf{B} \in \mathbb{Z}^{m\times m}$ which is a basis of $\Lambda_q^{\perp}(\mathbf{A})$, such that $\|\mathbf{B}\| \leq O(n \log q)$ and $\left\|\tilde{\mathbf{B}}\right\| \leq O\left(\sqrt{n \log q}\right)$.

Lemma 2 (SamplePre) [27] Given an integer $q \geq 2$, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a matrix $\mathbf{B} \in \mathbb{Z}^{m\times m}$ which is a basis of $\Lambda_q^{\perp}(\mathbf{A})$, and a vector $\mathbf{v} \in \mathbb{Z}_q^n$. There exists a PPT algorithm SamplePre $(\mathbf{A}, \mathbf{B}, \mathbf{v}, \sigma)$ that calculates a vector $\mathbf{x} \in \mathbb{Z}^m$ statically closed $D^m_{\Lambda_q^{\mathbf{v}}(\mathbf{A}),\sigma}$ such that $\mathbf{Ax} = \mathbf{v} \mathrm{mod} q$.

Lemma 3 (SampleMat) [25] Given a prime $q \geq 2$, an integer $k \geq 2$, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a basis $\mathbf{B} \in \mathbb{Z}^{m\times m}$ of $\Lambda_q^{\perp}(\mathbf{A})$, and a matrix $\mathbf{V} = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k) \in \mathbb{Z}_q^{n\times k}$. There exists a PPT algorithm

$\text{SampleMat}\left(\mathbf{A}, \mathbf{B}, \mathbf{V}, \sigma\right)$ that calculates a matrix $\mathbf{S} \in \mathbb{Z}_q^{m \times k}$ statically closed $D^m_{\Lambda_q^{\mathbf{v}_1}(\mathbf{A}),\sigma} \times D^m_{\Lambda_q^{\mathbf{v}_2}(\mathbf{A}),\sigma} \times \cdots \times D^m_{\Lambda_q^{\mathbf{v}_k}(\mathbf{A}),\sigma}$ such that $\mathbf{AS} = \mathbf{V} \text{mod} q$.

2.5 *Rejection Sampling*

To output a signature independent of the secret key, we introduce the Rejection Sampling technique. Let **k** is the secret key of the signer, **y** is selected from a random distribution, **s** is the candidate signature computed by **y** adding to the function of **k**, f is the distribution of outputted signature, g is the distribution of candidate signature. For all **x** and $M > 0$, if $f\left(\mathbf{x}\right) \leq Mg\left(\mathbf{x}\right)$, the candidate signature is outputted with probability $\dfrac{f\left(\mathbf{s}\right)}{Mg\left(\mathbf{s}\right)}$. According to [28], the expected number of times to generate a valid signature is M.

3 System Model and Security Model

3.1 *System Model*

Fig. 1 shows the specific process of our scheme by taking the entity interaction between two domains as an example. In this example, we assume that domain A is the local domain and domain B is the external domain. The entities of each domain include an authentication server, private key generation center, and blockchain. The functions of each entity are as follows:

(1) **Authentication server (AS)**: AS is responsible for the identity registration and identity authentication of the blockchain nodes in the local domain, and maintains the identity list of the local domain. AS has its identity information that is exposed to each domain. The private key can be obtained from the private key generation center of the local domain. When an access request is made by a node in the foreign domain, the AS will send a request for assistance to the foreign AS. When the local AS receives the assistance authentication request from the foreign domain, it will authenticate the identity of the local node and return the authentication results to the foreign AS. In this scheme, the authentication server of domain A is referred to as AS_1, and the authentication server of domain B is referred to as AS_2.

(2) **Private key generation center (PKG)**: PKG is responsible for generating the private key of the local AS and blockchain node. After receiving the identity information of the AS or blockchain node, the private key corresponding to this identity information is calculated and returned. In this scheme, the private key generation center of domain A is called PKG_1 for short, and the private key generation center of domain B is called PKG_2.

(3) **Blockchain**: Blockchain is a decentralized network composed of many nodes, and this scheme adopts a consortium blockchain based on Hyperledger Fabric. The blockchain node has its identity information. It can obtain the private key from PKG of the local domain, complete the identity registration with the local AS, submit a cross-domain access request to the foreign AS, and exchange cross-chain assets based on HTLC with the foreign blockchain node after the identity authentication is successful. Smart contracts can automatically execute function codes and provide interfaces and function encapsulation for HTLC. In this scheme, the blockchain of domain A is referred to as blockchain A, and the blockchain of domain B is referred to as blockchain B.

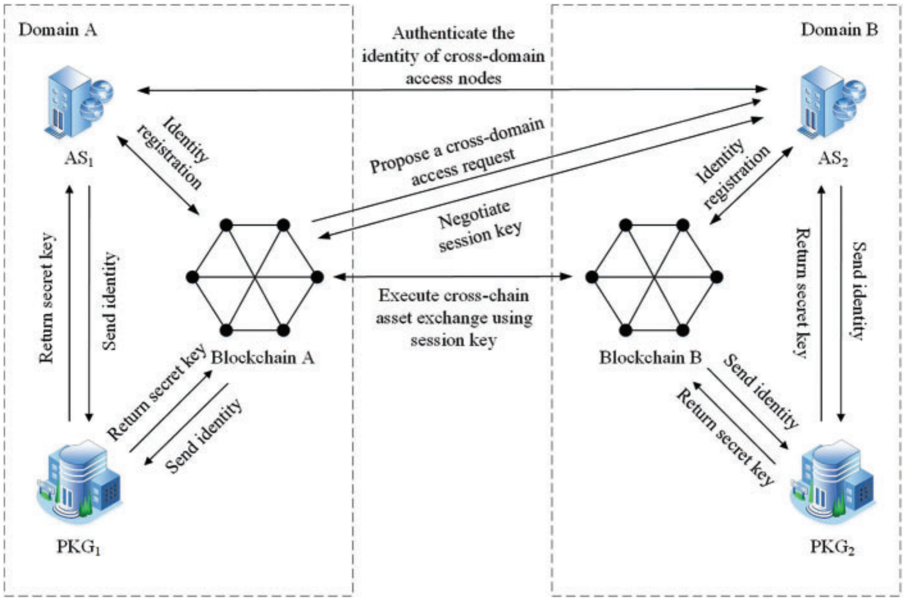

Figure 1: System architecture

3.2 Security Model

The IND-CPA secure of a post-quantum secure cross-domain identity authentication scheme is defined as a series of games between challenger C and adversary A as follows:

(1) **Setup**: Challenger C executes the System initialization algorithm and generates public parameters *pp* to send to adversary A.

(2) **Phase 1**: In this phase, adversary A can conduct H_2 and private key inquiries with challenger C, and C visits the H_2 **query** oracle **Private key query** oracle and returns the results to A.

H_2 **query**: Adversary A queries $H_2\left(\mathrm{ID}_i\right)$ corresponding to identity ID_i for i-th query, while challenger C maintains the query list L and calculates $H_2\left(\mathrm{ID}_i\right)$ to return to A.

Private key query: Adversary A queries $\mathbf{sk}_{\mathrm{ID}_i}$ corresponding to identity ID_i for i-th query, while challenger C maintains the query list L and calculates $\mathbf{sk}_{\mathrm{ID}_i}$ to return to A.

(3) **Challenge**: Adversary A selects $\mathbf{I}_{\mathrm{ID}_0}, \mathbf{I}_{\mathrm{ID}_1} \in \{0, 1\}^m$ and sends it to challenger C. Then, C selects $\xi \in \{0, 1\}$ and calculates $(\mathbf{R}_0{}^*, \mathbf{R}_1{}^*)$ corresponding to $\mathbf{I}_{\mathrm{ID}_\xi}$. Finally, C sends $(\mathbf{R}_0{}^*, \mathbf{R}_1{}^*)$ to A.

(4) **Phase 2**: Adversary A acquires the private key except Q^* through calling the Private key query oracle.

(5) **Guess**: After receiving $(\mathbf{R}_0{}^*, \mathbf{R}_1{}^*)$, adversary A selects a bit $\xi^* \in \{0, 1\}$, and wins this game if $\xi^* = \xi$.

Moreover, the advantage of adversary A breaking our scheme is defined as:

$$\mathrm{Adv}_A^{\text{IND-CPA}}(pp) = \left|\Pr\left[\xi^* = \xi\right] - \frac{1}{2}\right|. \tag{4}$$

Definition 6 (The IND-CPA security of a post-quantum secure cross-domain identity authentication scheme): Assuming that a post-quantum secure cross-domain identity authentication scheme is IND-CPA secure, if and only if the advantage $\mathrm{Adv}_{A}^{\text{IND-CPA}}(pp)$ is negligible for any PPT adversary A.

4 Our Proposed Scheme

Assume that domain A is the local domain and domain B is the external domain. Node AN_1 of blockchain A makes a cross-domain access request to domain B and wants to exchange cross-chain assets with node BN_1 of blockchain B. Moreover, AS_1 and AS_2 are honest and credible, and there is a secure and confidential channel between them. The specific process of our scheme is described as follows.

4.1 System Initialization

This section is responsible for creating the functions required for cross-chain in the blockchain smart contract, and setting the public parameters in the cross-domain process.

(1) **Blockchain initialization**: Blockchain in each domain deploys smart contracts and creates corresponding functions for cross-chain asset exchange of nodes. Smart contracts can automatically execute the created functions without human intervention.

(2) **Parameter initialization**: Set parameters m, n satisfying $m > 5n \log q$, where q is a prime and $q \geq 3$. Then, the TrapGen algorithm is called to generate the matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and the basis $\mathbf{B} \in \mathbb{Z}_q^{m\times m}$ of lattice $\Lambda(\mathbf{A})$ such that $\left\|\tilde{\mathbf{B}}\right\| \leq O\left(\sqrt{n \log q}\right)$, which $\mathbf{B}$ will be saved by PKG of each domain as the master key. Finally, four security hash functions H_1: $\mathbb{Z}_q^n \times \{0,1\}^* \to \{-1,0,1\}^m$, H_2: $\{0,1\}^* \to \mathbb{Z}_q^{n\times m}$, H_3: $\{0,1\}^* \times \mathbb{Z}^{m\times m} \to \{0,1\}^m$, and H_4: $\{0,1\}^m \to \{0,1\}^\kappa$ are selected, which κ is the length of the session key. Then, the public parameter is set to $pp = \{\mathbf{A}, H_1, H_2, H_3, H_4\}$.

4.2 Private Key Generation

In this section, PKG generates private keys for authentication servers and blockchain nodes.

(1) **The private key generation of AS**: AS_1 in domain A generates its own identity $\mathrm{ID}_{\mathrm{AS}_1} \in \{0,1\}^*$, exposes it to the AS entities in all domains, and sends it to PKG_1. PKG_1 runs the $\mathrm{SampleMat}\left(\mathbf{A}, \mathbf{B}, H_2\left(\mathrm{ID}_{\mathrm{AS}_1}\right), \sigma\right)$ algorithm to obtain the private key $\mathbf{sk}_{\mathrm{AS}_1} \in \mathbb{Z}^{m\times m}$ such that $\mathbf{A}\cdot\mathbf{sk}_{\mathrm{AS}_1} = H_2\left(\mathrm{ID}_{\mathrm{AS}_1}\right)$ and $\left\|\mathbf{sk}_{\mathrm{AS}_1}\right\| \leq \sigma\sqrt{m}$. Then, PKG_1 returns $\mathbf{sk}_{\mathrm{AS}_1}$ to AS_1. AS_1 can verify the correctness after receiving it through $\mathbf{A}\cdot\mathbf{sk}_{\mathrm{AS}_1} \overset{?}{=} H_2\left(\mathrm{ID}_{\mathrm{AS}_1}\right)$. Similarly, AS_2 in domain B can also interact with PKG_2 to generate its private key.

(2) **The private key generation of blockchain nodes**: AN_1 of domain A blockchain generates its own identity $\mathrm{ID}_{\mathrm{AN}_1} \in \{0,1\}^*$ and sends it to PKG_1. PKG_1 runs the $\mathrm{SampleMat}\left(\mathbf{A}, \mathbf{B}, H_2\left(\mathrm{ID}_{\mathrm{AN}_1}\right), \sigma\right)$ algorithm to obtain the private key $\mathbf{sk}_{\mathrm{AN}_1} \in \mathbb{Z}^{m\times m}$ such that $\mathbf{A}\cdot\mathbf{sk}_{\mathrm{AN}_1} = H_2\left(\mathrm{ID}_{\mathrm{AN}_1}\right)$ and $\left\|\mathbf{sk}_{\mathrm{AN}_1}\right\| \leq \sigma\sqrt{m}$. Then, PKG_1 returns $\mathbf{sk}_{\mathrm{AN}_1}$ to AN_1. AN_1 can verify the correctness after receiving it through $\mathbf{A}\cdot\mathbf{sk}_{\mathrm{AN}_1} \overset{?}{=} H_2\left(\mathrm{ID}_{\mathrm{AN}_1}\right)$. Similarly, BN_1 of domain B blockchain can also interact with PKG_2 to generate its private key.

4.3 Registration

In this section, the blockchain nodes in each domain interact with AS in the local domain to generate the identity index and add it to the identity list.

(1) **Calculating identity index**: AS_1 maintains an identity list $L_{\mathrm{A}} = [\,]$ in domain A. AN_1 calculates the identity index $\mathbf{I}_{\mathrm{AN}_1} = H_3\left(\mathrm{ID}_{\mathrm{AN}_1}, \mathbf{sk}_{\mathrm{AN}_1}\right)$, and sends the registration request to AS_1.

(2) **Adding the identity list**: AS_1 adds the identity $\mathrm{ID}_{\mathrm{AN}_1}$ and index $\mathbf{I}_{\mathrm{AN}_1}$ to the identity list $L_{\mathrm{A}} = \left[\left\{\mathrm{ID}_{\mathrm{AN}_1}, \mathbf{I}\ _{\mathrm{AN}_1}\right\}\right]$, and then returns the successful registration message of node AN_1.

Similarly, domain B blockchain node BN_1 can also interact with AS_2 and register identity.

4.4 Identity Authentication

In this section, the blockchain node in the local domain makes a cross-domain request and sends it to the foreign domain AS. The foreign domain AS requests the local domain AS to assist in authenticating the node's identity and negotiating the session key.

(1) AN_1 randomly selects vector $\mathbf{s} \in \mathbb{Z}_q^n$ and noise vector $\mathbf{x} \in \chi^m$, and calculates $\mathbf{R}_0 = \mathbf{A}^T\mathbf{s} + \mathbf{x}$, $\mathbf{R}_1 = H_2\left(\mathrm{ID}_{\mathrm{AS}_1}\right)^T\mathbf{s} + \mathbf{x} + \mathbf{I}_{\mathrm{AN}_1} \cdot \left\lfloor \frac{q}{2} \right\rfloor$. Then, AN_1 selects the current time T_1 and sends a cross-domain request message $m_{\mathrm{AN}_1 \to \mathrm{AS}_2} = \left\{\mathrm{ID}_{\mathrm{AS}_1}, \mathbf{R}_0, \mathbf{R}_1, \mathrm{ID}_{\mathrm{BN}_1}, \text{Cross-chain Asset Exchange, SHA256}, T_1\right\}$ to AS_2 in domain B. Among them, Cross-chain Asset Exchange means that the purpose of AN_1 accessing BN_1 is to exchange assets in the cross-chain scenarios, and SHA256 means that the hash function used in HTLC during the cross-chain asset exchange process is the SHA-256 algorithm.

(2) After AS_2 in domain B receives the cross-domain request from AN_1 in domain A, if T_1 is timely, AS_2 selects the current time T_2 and generates the assistance request message $m_{\mathrm{AS}_2 \to \mathrm{AS}_1} = \left\{\mathrm{ID}_{\mathrm{AS}_1}, \mathbf{R}_0, \mathbf{R}_1, T_1, \mathrm{ID}_{\mathrm{AS}_2}, T_2\right\}$. Then, AS_2 randomly selects the vector $\mathbf{r}_1 \leftarrow D_\sigma^m$, calculates $\mathbf{h}_{\mathrm{AS}_2} = H_1\left(\mathbf{Ar}_1, m_{\mathrm{AS}_2 \to \mathrm{AS}_1}\right)$, $\mathbf{z}_{\mathrm{AS}_2} = \mathbf{sk}_{\mathrm{AS}_2}\mathbf{h}_{\mathrm{AS}_2} + \mathbf{r}_1$, and generates the signature $\mathrm{sig}_{\mathrm{AS2}} = (\mathrm{h}_{\mathrm{AS2}}, \mathrm{z}_{\mathrm{AS2}})$ of the message $\mathrm{m}_{\mathrm{AS2\text{->}AS1}}$ with probability min (1,...). After that, $\left\{m_{\mathrm{AS}_2 \to \mathrm{AS}_1}, sig_{\mathrm{AS}_2}\right\}$ is sent to AS_1, indicating that AS_1 needs to assist in authenticating the identity of AN_1.

(3) After AS_1 receives the message $\left\{m_{\mathrm{AS}_2 \to \mathrm{AS}_1}, sig_{\mathrm{AS}_2}\right\}$, if T_2 is timely, executes the signature verification algorithm. If $\mathbf{h}_{\mathrm{AS}_2} = H_1\left(\mathbf{Az}_{\mathrm{AS}_2} - H_2\left(\mathrm{ID}_{\mathrm{AS}_2}\right)\mathbf{h}_{\mathrm{AS}_2}, m_{\mathrm{AS}_2 \to \mathrm{AS}_1}\right)$ and $\left\|\mathbf{z}_{\mathrm{AS}_2}\right\| \le 2\sigma\sqrt{m}$, AS_1 has successfully authenticated AS_2's identity. Secondly, AS_1 extracts $\mathbf{R}_0$ and $\mathbf{R}_1$ from $m_{\mathrm{AS}_2 \to \mathrm{AS}_1}$, calculates the vector $\mathbf{R}_1 - \mathbf{sk}_{\mathrm{AS}_1}{}^T\mathbf{R}_0$, and compares the absolute value of each component minus $\left\lfloor \frac{q}{2} \right\rfloor$ with $\frac{q}{4}$ to recover the identity index $\mathbf{I}_{\mathrm{AN}_1}{}'$. At this time, AS_1 traverses the elements in the identity list L_{A}. If $\mathbf{I}_{\mathrm{AN}_1} = \mathbf{I}_{\mathrm{AN}_1}{}'$, AS_1 will complete the identity authentication of AN_1. Then, AS_1 calculates the session key $\mathbf{k}_{\mathrm{AN}_1} = H_4\left(\mathbf{I}_{\mathrm{AN}_1}\right)$, selects the current time T_3, generates the assistance authentication message $m_{\mathrm{AS}_1 \to \mathrm{AS}_2} = \left\{\mathrm{ID}_{\mathrm{AS}_1}, \mathrm{ID}_{\mathrm{AS}_2}, T_2, \mathbf{k}_{\mathrm{AN}_1}, T_3\right\}$, randomly selects the vector $\mathbf{r}_2 \leftarrow D_\sigma^m$, calculates $\mathbf{h}_{\mathrm{AS}_1} = H_1\left(\mathbf{Ar}_2, m_{\mathrm{AS}_1 \to \mathrm{AS}_2}\right)$, $\mathbf{z}_{\mathrm{AS}_1} = \mathbf{sk}_{\mathrm{AS}_1}\mathbf{h}_{\mathrm{AS}_1} + \mathbf{r}_2$, and generates the signature $\mathrm{sig}_{\mathrm{AS1}} = (\mathrm{h}_{\mathrm{AS1}}, \mathrm{z}_{\mathrm{AS1}})$ of the message $\mathrm{m}_{\mathrm{AS1\text{->}AS2}}$ with probability min (1,...). Finally, AS_1 sends $\left\{m_{\mathrm{AS}_1 \to \mathrm{AS}_2}, sig_{\mathrm{AS}_1}\right\}$ to AS_2 in domain B through a secure and confidential channel, indicating that AS_1 has assisted AS_2 in completing the identity authentication of AN_1.

(4) AS_2 in domain B receives the message $\left\{m_{\mathrm{AS}_1 \to \mathrm{AS}_2}, sig_{\mathrm{AS}_1}\right\}$ from AS_1. If T_3 is timely, the signature verification algorithm will be executed. If $\mathbf{h}_{\mathrm{AS}_1} = H_1\left(\mathbf{Az}_{\mathrm{AS}_1} - H_2\left(\mathrm{ID}_{\mathrm{AS}_1}\right)\mathbf{h}_{\mathrm{AS}_1}, m_{\mathrm{AS}_1 \to \mathrm{AS}_2}\right)$ and $\left\|\mathbf{z}_{\mathrm{AS}_1}\right\| \le 2\sigma\sqrt{m}$, the signature verification is passed, indicating that AS_2 has successfully authenticated the identities of AS_1 and AN_1. Then, AS_2 adds $\left\{\mathrm{ID}_{\mathrm{AN}_1}, \cdot\right\}$ to the identity list L_{B} in domain B, which allows AN_1 to access nodes in domain B. At the same time, AS_2 sends the session key $\mathbf{k}_{\mathrm{AN}_1}$ and cross-chain information $\{\mathrm{ID}_{\mathrm{BN1}}, \text{Cross-chain Asset Exchange, SHA256}\}$ to blockchain B, selects the current time T_4, uses the session key $\mathbf{k}_{\mathrm{AN}_1}$ to encrypt the authentication success message, and sends it to AN_1 in domain A.

4.5 Cross-Chain Asset Exchange

After the cross-domain access request is allowed, the blockchain nodes in the local domain and the foreign domain conduct cross-chain asset exchange between domains based on HTLC.

(1) **Cross-chain preparation**: After receiving the message $m_{\mathrm{AS}_2 \to \mathrm{AN}_1}$ from AS_2, AN_1 calculates the session key $\mathbf{k}_{\mathrm{AN}_1} = H_4\left(\mathbf{I}_{\mathrm{AN}_1}\right)$ and decrypts $m_{\mathrm{AS}_2 \to \mathrm{AN}_1}$. If T_4 is timely, AN_1 knows that the identity authentication is successful and can exchange cross-chain assets with BN_1. At the same time, after receiving the message $\{\mathrm{ID}_{\mathrm{BN1}}$, Cross-chain Asset Exchange, SHA256$\}$ from AS_2, BN_1 is ready for asset exchange.

(2) **Cross-chain asset exchange between domains**: As shown in Fig. 2, firstly, AN_1 generates h randomly, calculates its hash value $H = \mathrm{SHA256}(h)$, and sends it to BN_1 through the cross-domain channel. Secondly, AN_1 selects the time t_1 and uses the hash value H and time t_1 to lock the asset a to be exchanged, and BN_1 selects the time t_2 such that $t_2 < t_1$, uses the hash value H and time t_2 to lock the asset b to be exchanged. Then, AN_1 calls the smart contract interface of blockchain B across domains and uses random values h to unlock asset b. At this time, BN_1 obtains the h from the contract of blockchain B and calls the smart contract interface of blockchain A across domains to unlock the asset a. If AN_1 and BN_1 unlock the assets within the specified time, the cross-chain asset exchange is successful, and the smart contracts of blockchain A and B send the asset a and b to BN_1 and AN_1 respectively through the cross-domain channel.

(3) **Timeout asset return**: As shown in Fig. 2, if one of the two nodes fails to unlock the assets within the specified time, the smart contract will return the assets to the nodes in the respective domain.

5 Security Analysis

5.1 Correctness

In this paper, the correctness of the cross-domain identity authentication scheme depends on the correctness of signature verification and identity index recovery described in Eqs. (5) and (6), respectively.

The correctness of signature verification:

$$\begin{aligned} &\mathbf{A}\mathbf{z}_{\mathrm{AS}} - H_2\left(\mathrm{ID}_{\mathrm{AS}}\right)\mathbf{h}_{\mathrm{AS}} = \mathbf{A}\left(\mathbf{sk}_{\mathrm{AS}}\mathbf{h}_{\mathrm{AS}} + \mathbf{r}\right) - H_2\left(\mathrm{ID}_{\mathrm{AS}}\right)\mathbf{h}_{\mathrm{AS}} \\ &= H_2\left(\mathrm{ID}_{\mathrm{AS}}\right)\mathbf{h}_{\mathrm{AS}} + \mathbf{A}\mathbf{r} - H_2\left(\mathrm{ID}_{\mathrm{AS}}\right)\mathbf{h}_{\mathrm{AS}} = \mathbf{A}\mathbf{r} \end{aligned} \tag{5}$$

For example, AS_1 receives the message $m_{\mathrm{AS}_2 \to \mathrm{AS}_1}$ and the signature $sig_{\mathrm{AS}_2} = \left(\mathbf{h}_{\mathrm{AS}_2}, \mathbf{z}_{\mathrm{AS}_2}\right)$ sent by AS_2, calculates $H_1\left(\mathbf{A}\mathbf{z}_{\mathrm{AS}_2} - H_2\left(\mathrm{ID}_{\mathrm{AS}_2}\right)\mathbf{h}_{\mathrm{AS}_2}, m_{\mathrm{AS}_2 \to \mathrm{AS}_1}\right) = H_1\left(\mathbf{A}\mathbf{r}, m_{\mathrm{AS}_2 \to \mathrm{AS}_1}\right)$, and compares it with $\mathbf{h}_{\mathrm{AS}_2}$ to verify the correctness of the signature.

The correctness of identity index recovery:

$$\begin{aligned} &\mathbf{R}_1 - \mathbf{sk}_{\mathrm{AS}}{}^T\mathbf{R}_0 = H_2\left(\mathrm{ID}_{\mathrm{AS}}\right)^T\mathbf{s} + \mathbf{x} + \mathbf{I}_{\mathrm{AN}}\left\lfloor \frac{q}{2} \right\rfloor - \mathbf{sk}_{\mathrm{AS}}{}^T\left(\mathbf{A}^T\mathbf{s} + \mathbf{x}\right) \\ &= H_2\left(\mathrm{ID}_{\mathrm{AS}}\right)^T\mathbf{s} + \mathbf{x} + \mathbf{I}_{\mathrm{AN}}\left\lfloor \frac{q}{2} \right\rfloor - H_2\left(\mathrm{ID}_{\mathrm{AS}}\right)^T\mathbf{s} - \mathbf{sk}_{\mathrm{AS}}{}^T\mathbf{x} = \mathbf{I}_{\mathrm{AN}}\left\lfloor \frac{q}{2} \right\rfloor + \underbrace{\mathbf{x} - \mathbf{sk}_{\mathrm{AS}}{}^T\mathbf{x}}_{\text{noise}} \end{aligned} \tag{6}$$

As described in [27], each component of the vector $\mathbf{x} - \mathbf{sk}_{\mathrm{AS}}{}^T\mathbf{x}$ is less than $\frac{q}{5}$. Consequently, each bit of the identity index $\mathbf{I}_{\mathrm{AN}}$ can be recovered correctly.

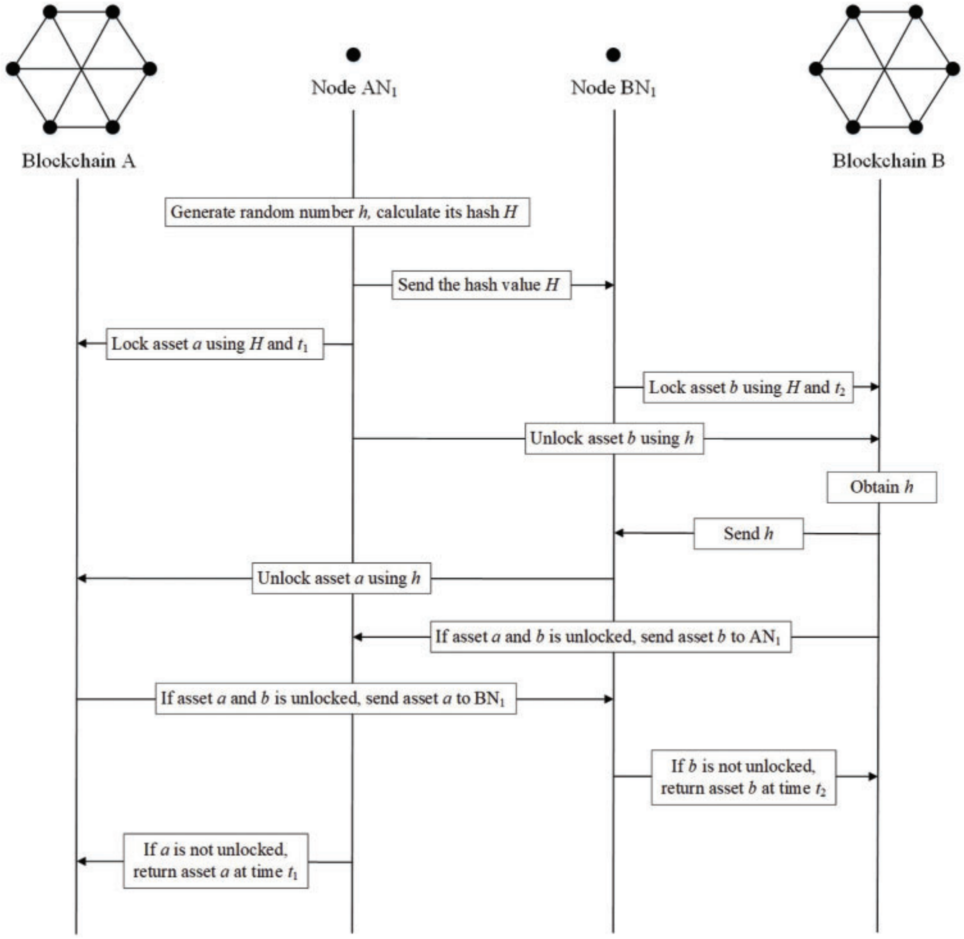
Blockchain A
Node AN_1
Node BN_1
Blockchain B
Generate random number *h*, calculate its hash *H*
Send the hash value *H*
Lock asset *a* using *H* and t_1
Lock asset *b* using *H* and t_2
Unlock asset *b* using *h*
Obtain *h*
Send *h*
Unlock asset *a* using *h*
If asset *a* and *b* is unlocked, send asset *b* to AN_1
If asset *a* and *b* is unlocked, send asset *a* to BN_1
If *b* is not unlocked, return asset *b* at time t_2
If *a* is not unlocked, return asset *a* at time t_1

Figure 2: The cross-chain asset exchange process of our scheme

5.2 The Unforgeability of the Signature Process

Theorem 1 Assuming that an adversary A can break the unforgeability of the signature process in polynomial time, a challenger C is executing a PPT algorithm that can break the SIS assumption.

Analysis: To sign the cross-domain message in our scheme, we introduce the identity-based signature algorithm from lattice in [25]. The detailed proof of **Theorem 4** in [25] has demonstrated that this algorithm can achieve the unforgeability under adaptive chosen message and identity attacks in the random oracle model, which can be reduced to SIS assumption.

Consequently, the signature process in our scheme is unforgeable and post-quantum secure to ensure the authenticity and credibility of identity in quantum computing circumstances.

5.3 The IND-CPA of the Hiding and Recovery of Identity Index

Theorem 2 Assuming that adversary A can break the IND-CPA security of the hiding and recovery of identity index in polynomial time, challenger C is executing a PPT algorithm that can break the LWE assumption.

Proof: Let adversary A have a non-negligible advantage ε to break the IND-CPA security of the hiding and recovery of identity index. For $i = 0, 1, \ldots, m$, $\mathbf{u}_i \in \mathbb{Z}_q^n$ and $x \leftarrow \chi$, challenger C maintains a series of LWE instances, named $\left(\mathbf{u}_i, R_{0,i}\right)$ such that $R_{0,i} = \mathbf{u}_i{}^T\mathbf{s} + x$. After that, challenger C and adversary A interact according to the IND-CPA game described in Section 3.2.

(1) **Setup**: Challenger C executes TrapGen algorithm in **System initialization** to obtain the matrix $\mathbf{A} = (\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m)$ and basis $\mathbf{B} \in \mathbb{Z}_q^{m\times m}$ of $\Lambda\left(\mathbf{A}\right)$, and defines $H_1\colon \mathbb{Z}_q^n \times \{0, 1\}^* \to \{-1, 0, 1\}^m$, $H_2\colon \{0, 1\}^* \to \mathbb{Z}_q^{n\times m}$, $H_3\colon \{0, 1\}^* \times \mathbb{Z}^{m\times m} \to \{0, 1\}^m$, and $H_4\colon \{0, 1\}^m \to \{0, 1\}^\kappa$. Then, C sends the public parameters $pp = \{\mathbf{A}, H_1, H_2, H_3, H_4\}$ to adversary A.

(2) **Phase 1**: In this phase, adversary A can conduct H_2 and private key inquiries with challenger C, and C visits the H_2 **query** oracle **Private key query** oracle and returns the results to A.

H_2 **query**: Let Q_{H_2} be the maximum number of adversary A queries to H_2, and challenger C maintains a query list L. The steps for adversary A to query the H_2 query oracle are as follows. Firstly, C selects $Q^* \in \left\{1, 2, \ldots, Q_{H_2}\right\}$ and computes a tuple $\left\{Q_i, \mathrm{ID}_i, H_2\left(\mathrm{ID}_i\right), \mathbf{sk}_{\mathrm{ID}_i}\right\}$ for i-th query Q_i. If $\left\{Q_i, \mathrm{ID}_i, H_2\left(\mathrm{ID}_i\right), \mathbf{sk}_{\mathrm{ID}_i}\right\}$ is in the query list L, C returns $H_2\left(\mathrm{ID}_i\right)$ to A. If $\left\{Q_i, \mathrm{ID}_i, H_2\left(\mathrm{ID}_i\right), \mathbf{sk}_{\mathrm{ID}_i}\right\}$ is not in L and $Q^* \neq Q_i$, C executes the $\mathrm{SampleMat}\left(\mathbf{A}, \mathbf{B}, H_2\left(\mathrm{ID}_i\right), \sigma\right)$ algorithm to obtain the private key $\mathbf{sk}_{\mathrm{ID}_i} \in \mathbb{Z}^{m\times m}$ such that $\mathbf{A} \cdot \mathbf{sk}_{\mathrm{ID}_i} = H_2\left(\mathrm{ID}_i\right)$ and $\left\|\mathbf{sk}_{\mathrm{ID}_i}\right\| \leq \sigma\sqrt{m}$, returns $H_2\left(\mathrm{ID}_i\right)$ to A, and then supplements $\left\{Q_i, \mathrm{ID}_i, H_2\left(\mathrm{ID}_i\right), \mathbf{sk}_{\mathrm{ID}_i}\right\}$ to L. If $\left\{Q_i, \mathrm{ID}_i, H_2\left(\mathrm{ID}_i\right), \mathbf{sk}_{\mathrm{ID}_i}\right\}$ is not in L and $Q^* = Q_i$, C defines $H_2\left(\mathrm{ID}_i\right) = (\mathbf{u}_0, \mathbf{u}_0, \ldots, \mathbf{u}_0)$ to return to A, selects $\mathbf{sk}_{\mathrm{ID}_i}$ at random, and supplements $\left\{Q_i, \mathrm{ID}_i, H_2\left(\mathrm{ID}_i\right), \mathbf{sk}_{\mathrm{ID}_i}\right\}$ to L.

Private key query: Adversary A selects ID_i to query the corresponding private key. After that, challenger C retrieves ID_i in the query list L. If ID_i is not found, C calls H_2 **query** to add $\left\{Q_i, \mathrm{ID}_i, H_2\left(\mathrm{ID}_i\right), \mathbf{sk}_{\mathrm{ID}_i}\right\}$ to L. Otherwise, if $Q^* \neq Q_i$, C returns $\mathbf{sk}_{\mathrm{ID}_i}$ to A. If $Q^* = Q_i$, C aborts this process.

(3) **Challenge**: Adversary A constructs $\mathbf{I}_{\mathrm{ID}_0}, \mathbf{I}_{\mathrm{ID}_1} \in \{0, 1\}^m$ corresponding to $\mathrm{ID}_0, \mathrm{ID}_1$ which cannot be queried in Phase 1 and sends them to challenger C. Then, C selects $\xi \in \{0, 1\}$, and calculates: $\mathbf{R}_0{}^* = \left(R_{0,1}, R_{0,2}, \ldots, R_{0,m}\right)^T$ and $\mathbf{R}_1{}^* = \left(R_{0,0}, R_{0,0}, \ldots, R_{0,0}\right)^T + \mathbf{I}_{\mathrm{ID}_\xi} \cdot \left\lfloor \frac{q}{2} \right\rfloor$. On the other hand, C samples $(\mathbf{R}_0{}^*, \mathbf{R}_1{}^*)$ from $\mathbb{Z}_q^n \times \mathbb{Z}_q$ randomly. Finally, C sends $(\mathbf{R}_0{}^*, \mathbf{R}_1{}^*)$ to A.

(4) **Phase 2**: Adversary A acquires the private key through calling the **Private key query**, and cannot query about the private keys corresponding to ID_0 and ID_1.

(5) **Guess**: After receiving $(\mathbf{R}_0{}^*, \mathbf{R}_1{}^*)$, adversary A selects a bit $\xi^* \in \{0, 1\}$. If $\xi^* = \xi$, A wins this game.

Analysis: If $\left(\mathbf{u}_i, R_{0,i}\right)$ is a solution of LWE assumption, $(\mathbf{R}_0{}^*, \mathbf{R}_1{}^*)$ is calculated as follows:

$$\mathbf{R}_0{}^* = \left(R_{0,1}, R_{0,2}, \ldots, R_{0,m}\right)^T = \left(\mathbf{u}_1{}^T\mathbf{s} + x, \mathbf{u}_2{}^T\mathbf{s} + x, \ldots, \mathbf{u}_m{}^T\mathbf{s} + x\right)^T = \mathbf{A}^T\mathbf{s} + \mathbf{x} \tag{7}$$

$$\begin{aligned}\mathbf{R}_1{}^* &= \left(R_{0,0}, R_{0,0}, \ldots, R_{0,0}\right)^T + \mathbf{I}_{\mathrm{ID}_\xi} \cdot \left\lfloor \frac{q}{2} \right\rfloor = \left(\mathbf{u}_0{}^T\mathbf{s} + x, \mathbf{u}_0{}^T\mathbf{s} + x, \ldots, \mathbf{u}_0{}^T\mathbf{s} + x\right)^T + \mathbf{I}_{\mathrm{ID}_\xi} \cdot \left\lfloor \frac{q}{2} \right\rfloor \\ &= \left(\mathbf{u}_0, \mathbf{u}_0, \ldots, \mathbf{u}_0\right)^T\mathbf{s} + \mathbf{x} + \mathbf{I}_{\mathrm{ID}_\xi} \cdot \left\lfloor \frac{q}{2} \right\rfloor\end{aligned} \tag{8}$$

Obviously, $(\mathbf{R}_0{}^*, \mathbf{R}_1{}^*)$ is valid, and for adversary A, the probability that adversary A outputs $\xi^* = \xi$ is $\Pr\left[\xi^* = \xi\right] = \frac{1}{2} + \varepsilon$. If $(\mathbf{R}_0{}^*, \mathbf{R}_1{}^*)$ is selected randomly, the probability that A outputs $\xi^* = \xi$ is

$\Pr\left[\xi^* = \xi\right] = \frac{1}{2}$. Consequently, the advantage that adversary A makes correct judgment is:

$$\mathrm{Adv}_A^{\text{IND-CPA}}(pp) = \left|\Pr\left[\xi^* = \xi\right] - \frac{1}{2}\right| = \left|\frac{1}{2}\cdot\left(\frac{1}{2}+\varepsilon\right) + \frac{1}{2}\cdot\frac{1}{2} - \frac{1}{2}\right| = \frac{\varepsilon}{2}. \tag{9}$$

Considering the successful execution of the IND-CPA game, the advantage of solving the LWE assumption is $\left(1 - \frac{1}{Q_{H_2}}\right)\cdot \mathrm{Adv}_A^{\text{IND-CPA}}(pp) = \frac{Q_{H_2}-1}{2Q_{H_2}}\cdot\varepsilon$, which is negligible for adversary A.

To sum up, the hiding and recovery of the identity index in our scheme has IND-CPA security, making the cross-domain identity authentication process secure and reliable in quantum scenarios.

6 Comparison Analysis

Table 1 compares the security features of references [19,20,29,30] and our scheme. Resistance to counterfeit attacks means that the authentication server in each domain can verify the identity of the node and the authentication server in the foreign domain to avoid the attack of the fake user on the system. Resistance to replay attacks means that the message is verified to be timely by introducing a timestamp in the message to avoid the replay attack of the attacker. Post-quantum computing attacks refer to a cross-domain authentication scheme based on post-quantum cryptography to avoid quantum computing attacks launched by attackers equipped with quantum computers. To sum up, the lattice-based cross-domain authentication scheme proposed in our paper meets the above three security characteristics, and the unforgeability of signature and the IND-CPA security of identity index is reduced to SIS and LWE assumptions, respectively.

Table 1: Feature comparison with other cross-domain authentication schemes

Scheme	Resistance to counterfeit attack	Resistance to replay attack	Resistance to quantum computing attack	Assumption
Luo et al. [19]	√	√	×	DL
Wei et al. [20]	√	√	×	DL
Chen et al. [29]	√	√	×	ECDH
Li et al. [30]	√	√	×	DL, CDH, BDH
Our scheme	√	√	√	SIS, LWE

In Table 2, many notations in our scheme are defined. Table 3 defines the symbol and meaning of the operation, and compares the operation number of the key generation, signature process, and verification process of our scheme with [19,20,29]. It is evident that our scheme has fewer operation number than [19,20] and [29] in the aforementioned three areas. After that, Table 4 compares this scheme with [20] and [30] in terms of the user and authentication server time consumption. Our scheme realizes cross-domain identity authentication through the interaction of authentication servers in the local domain and the foreign domain. Therefore, the time consumption of the authentication server is divided into the local domain authentication server (AS_1) and the foreign domain authentication server (AS_2). Obviously, the operation designed in our scheme is mainly the multiplication of matrices, and its efficiency is much higher than the pairing operation on groups in [20] and [30].

Table 2: Symbol definition

Notations	Descriptions	Notations	Descriptions
H	Hash operation	T_H	The time consumption of hash operation
SampleMat	Calling SampleMat	T_{Mul_M}	The time consumption of matrix multiplication
Mul_M	Matrix multiplication	T_{Pair}	The time consumption of bilinear pairing
Mul_G	Multiplication of point in group	T_{Mul_G}	The time consumption of element multiplication in group
$Pairing$	Bilinear pairing		

Table 3: The comparison of operation number

Scheme	Key generation	Signature process	Verification process
Luo et al. [19]	$H + Mul\_G$	$H + Mul\_G$	$2H + 3Mul\_G$
Wei et al. [20]	$H + 2Mul\_G$	$H + 5Mul\_G + 5Pairing$	$H + Mul\_G + 2Pairing$
Chen et al. [29]	$H + 2Mul\_G$	$2H+4Mul\_G+Pairing+2Xor$	$2H + 3Mul\_G + 2Pairing + 2Xor$
Our scheme	$H+$SampleMat	$H + 2Mul\_M$	$2H + 2Mul\_M$

Table 4: The comparison of time consumption of the user and authentication server

Scheme	The time consumption of user	The time consumption of authentication server
Wei et al. [20]	$T_H + 3T_{Mul\_G} + 3T_{Pair}$	$T_H + T_{Mul\_G} + 2T_{Pair}$
Li et al. [30]	$2T_H + 6T_{Mul\_G} + 2T_{Pair}$	–
Our scheme	$T_H + 2T_{Mul\_M}$	AS$_1$: $4T_H + 5T_{Mul\_M}$ AS$_2$: $3T_H + 4T_{Mul\_M}$

7 Conclusion

To solve the problem of entity authentication between domains, we propose a post-quantum cross-domain authentication scheme by designing the transmission and recovery process of the identity index based on lattice cryptography and introducing the identity-based signature from lattice in our scheme. In addition, we apply HTLC to realize the cross-chain asset exchange between blockchain nodes in different trust domains. Moreover, security analysis shows that our scheme meets the correctness, unforgeability of signatures, and IND-CPA security for identity index under quantum computing. Finally, comparison analysis shows that our scheme can resist counterfeit attacks and replay attacks, and is more efficient in terms of operation number and time consumption of the user and authentication server compared to many schemes based on traditional cryptography.

Acknowledgement: All authors would like to thank the anonymous reviewers for their constructive suggestions, which improve the quality of this work.

Funding Statement: This work was supported by the Defense Industrial Technology Development Program (Grant No. JCKY2021208B036).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Yi-Bo Cao, Xiu-Bo Chen; security proofs: Yi-Bo Cao, Gang Xu; analysis and interpretation of results: Yi-Bo Cao, Si-Yi Chen; draft manuscript preparation: Yun-Feng He, Lu-Xi Liu, Yin-Mei Che, Xiao Wang, Ke Xiao. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin and K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G enabled internet of drones," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, 2021.

[2] Z. Zhou, Y. Tian, J. Xiong, J. Ma, and C. Peng, "Blockchain-enabled secure and trusted federated data sharing in IIoT," *IEEE Trans. Industr. Inform.*, vol. 19, no. 5, pp. 6669–6681, 2023.

[3] T. Wu *et al.*, "Blockchain-based anonymous data sharing with accountability for Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 6, pp. 5461–5475, 2022.

[4] Y. Xie, X. Chen, and Y. Yang, "A new lattice-based blind ring signature for completely anonymous blockchain transaction systems," *Secur. Commun. Netw.*, vol. 2022, pp. 4052029, 2022.

[5] X. Chen, S. Xu, T. Qin, Y. Cui, S. Gao and W. Kong, "AQ-ABS: Anti-quantum attribute-based signature for EMRs sharing with blockchain," in *Proc. 2022 IEEE Wireless Commun. and Netw. Conf. (WCNC)*, 2022, pp. 1176–1181.

[6] W. Liang *et al.*, "PDPChain: A consortium blockchain-based privacy protection scheme for personal data," *IEEE Trans. Reliab.*, vol. 72, no. 2, pp. 586–598, 2023.

[7] S. Xu, X. Chen, and Y. He, "EVchain: An anonymous blockchain-based system for charging-connected electric vehicles," *Tsinghua Sci. Technol.*, vol. 26, no. 6, pp. 845–856, 2021.

[8] Y. Cheng, S. Xu, M. Zang, S. Jiang, and Y. Zhang, "Secure authentication scheme for VANET based on blockchain," in *Proc. 2021 7th Int. Conf. Comput. Commun. (ICCC)*, 2021, pp. 1526–1531.

[9] J. Poon and T. Dryja, *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*, Canada: 1Bitcoin Inc., 2016.

[10] S. K. Mohanty and S. Tripathy, "*n*-HTLC: Neo hashed time-lock commitment to defend against wormhole attack in payment channel networks," *Comput. Secur.*, vol. 106, pp. 102291, 2021.

[11] P. Shamili and B. Muruganantham, "Federation payment tree: An improved payment channel for scaling and efficient zk-hash time lock commitment framework in blockchain technology," *Concurr. Eng.*, vol. 30, no. 4, pp. 317–324, 2022.

[12] Monika, R. Bhatia, A. Jain, and B. Singh, "Hash time locked contract based asset exchange solution for probabilistic public blockchains," *Cluster Comput.*, vol. 25, no. 6, pp. 4189–4201, 2022.

[13] F. Barbàra and C. Schifanella, "MP-HTLC: Enabling blockchain interoperability through a multiparty implementation of the hash time-lock contract," *Concurr. Computa.: Pract. Exp.*, vol. 35, no. 9, pp. e7656, 2023.

[14] S. Wadhwa, J. Stöter, F. Zhang, and K. Nayak, "He-HTLC: Revisiting incentives in HTLC," *Cryptol. ePrint Arch.*, 2022.

[15] M. A. Sirbu and J. Chuang, "Distributed authentication in kerberos using public key cryptography," in *Proc. SNDSS'97*, 1997, pp. 134–141.

[16] K. Liu, S. Qing, and Y. Meng, "An improved way on kerberos protocol based on public-key algorithms," *J. Softw.*, vol. 12, no. 6, pp. 872–877, 2001.

[17] W. Zhang, X. Wang, and M. K. Khan, "A virtual bridge certificate authority-based cross-domain authentication mechanism for distributed collaborative manufacturing systems," *Secur. Commun. Netw.*, vol. 8, no. 6, pp. 937–951, 2015.

[18] H. Peng, "An identity-based authentication model for multi-domain," *Chinese J. Comput.*, vol. 29, no. 8, pp. 1271, 2006 (In Chinese).

[19] C. Luo, S. Huo and H. Xing, "Identity-based cross-domain authentication scheme in pervasive computing environments," *J. China Ins. Commun.*, vol. 32, no. 9, pp. 111–115+122, 2011 (In Chinese).

[20] S. Wei, S. Li and J. Wang, "A cross-domain authentication protocol by identity-based cryptography on consortium blockchain," *Chinese J. Comput.*, vol. 44, no. 5, pp. 908–920, 2021 (In Chinese).

[21] X. Zhou, F. Miao and Y. Xiong, "A certificate authority domain-based cross-domain authentication scheme for virtual enterprise using identity based encryption," in *Proc. 2021 7th Int. Conf. Big Data Comput. Commun. (BigCom)*, 2021, pp. 144–149.

[22] J. Cui, N. Liu, Q. Zhang, D. He, C. Gu and H. Zhong, "Efficient and anonymous cross-domain authentication for IIoT based on blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 2, pp. 899–910, 2022.

[23] P. W. Shor, "Polynomial time algorithms for discrete logarithms and factoring on a quantum computer," in *Proc. Algorithmic Number Theory: First Int. Symp.*, NY, USA, 1994, pp. 289–289.

[24] M. Rückert, "Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles," in *Proc. Post-Quantum Cryptogr.: Third Int. Workshop, PQCrypto 2010*, Darmstadt, Germany, 2010, pp. 182–200.

[25] M. Tian and L. Huang, "Efficient identity-based signature from lattices," in *Proc. ICT Syst. Secur. Privacy Protection: 29th IFIPTC 11 Int. Conf., SEC 2014*, Marrakech, Morocco, 2014, pp. 321–329.

[26] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," *Theor. Comput. Syst.*, vol. 48, pp. 535–553, 2011.

[27] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. the Fortieth Annual ACM Symp. Theory Comput.*, 2008, pp. 197–206.

[28] J. Von Neumann, "Various techniques used in connection with random digits," *J. Research Nat. Bur. Stand. Appl. Math. Series*, vol. 12, pp. 36–38, 1951.

[29] Y. Chen, C. Zhong, C. Zhou, L. Xue and H. Huang, "Design of cross-domain authentication scheme based on medical consortium chain," *Comput. Sci.*, vol. 49, no. 6, pp. 537–543, 2022.

[30] Y. Li, W. Chen, Z. Cai, and Y. Fang, "CAKA: A novel certificateless-based cross-domain authenticated key agreement protocol for wireless mesh nsetworks," *Wirel. Netw.*, vol. 22, pp. 2523–2535, 2016.