Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Anti-quantum cross-chain identity authentication approach using dynamic group signature*

Huifang YU†‡1,2, Mengjie HUANG1
1*School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an 710121, China*
2*Ministry of Education Key Laboratory of Cyberspace Security, Information Engineering University, Zhengzhou 450001, China*
†E-mail: yuhuifang@xupt.edu.cn

Received May 27, 2024; Revision accepted Oct. 10, 2024; Crosschecked Apr. 22, 2025

Abstract: To solve the privacy leakage and identity island problems in cross-chain interaction, we propose an anti-quantum cross-chain identity authentication approach based on dynamic group signature (DGS-AQCCIDAA) for smart education. The relay-based cross-chain model promotes interconnection in heterogeneous consortium blockchains. DGS is used as the endorsement strategy for cross-chain identity authentication. Our approach can ensure quantum security under the learning with error (LWE) and inhomogeneous small integer solution (ISIS) assumptions, and it uses non-interactive zero-knowledge proof (NIZKP) to protect user identity privacy. Our scheme has low calculation overhead and provides anonymous cross-chain identity authentication in the smart education system.

Key words: Cross-chain; Identity authentication; Dynamic group signature (DGS); Anti-quantum security; Zero-knowledge proof
https://doi.org/10.1631/FITEE.2400443 **CLC number:** TP309

1 Introduction

Blockchain is a combination of cryptography, peer-to-peer communication, consensus mechanisms, smart contracts, and other technologies. Blockchain is used to construct a trusted system (Ma et al., 2020) because of its decentralization and anti-tampering. There are three types of blockchain: the public blockchain is completely open and transparent with no identity authorization, the consortium blockchain includes the identity authorization access mechanism, and the private blockchain is maintained by a single node in the network.

Public key infrastructure (PKI) based identity management in the consortium chain uses a certificate to authenticate the user identity. The certificate-based authentication scheme cannot provide anonymous authentication services and will result in leakage of private information. In addition, because each consortium blockchain is independent with no unified identity management system, the identity island problem (Yang et al., 2019) exists. Providing a unified identity for different blockchains and protecting user information are vital problems of blockchain.

Cross-chain technology (Yu and Mu, 2024) is an important method for consortium blockchain to achieve interoperability and improve scalability. Cross-chain identity authentication technology can achieve unified identity management and authentication between blockchains, and solve the problem of identity islands. There have been several cross-

---

‡ Corresponding author

* Project supported by the Horizontal Project (No. HX2024-002), the Open Foundation of Key Laboratory of Cyberspace Security of the Ministry of Education of China (No. KLCS20240102), and the Natural Science Basis Research Program of Shaanxi Province (Nos. 2025JC-YBMS-652 and 2025JC-YBMS-676)

ORCID: Huifang YU, https://orcid.org/0000-0003-4711-3128; Mengjie HUANG, https://orcid.org/0009-0006-6059-7154

chain authentication schemes. An identity authentication model for cross-chain (Wang et al., 2022b) solves the identity authentication problem in heterogeneous application chains and eliminates duplicate authentication when the application chain accesses the cross-chain system, but identity information leakage still occurs in cross-chain transactions. The cross-chain identity authentication mechanism in the Internet of Things (IoT) using identity-based encryption (Shao et al., 2021) causes a performance bottleneck. Lightweight identity authentication (Wang et al., 2022a) in a cross-chain framework cannot protect the identity of users in cross-chain interaction. The cross-chain authentication scheme based on certificate-less signcryption (Liu et al., 2024) has a high degree of decentralization and scalability, but it is unable to solve the problem of user identity information leakage in the identity authentication process. Currently, cross-chain identity authentication is focused mainly on decentralized identity management and authentication, and no research has been reported on anonymous identity authentication.

The group signature is anonymous and traceable, so it can be used to construct anonymous authentication protocols. However, traditional group signature schemes are not resistant to quantum computing attacks. The lattice-based cryptosystem (Yu et al., 2023; Yu and Bai, 2024) has attracted extensive attention due to its anti-quantum security. Gordon et al. (2010) combined the preimage sampling function and zero-knowledge proof technique to achieve a lattice-based group signature. This scheme has a long key and signature and the identity of group members cannot be changed in the initial phase, so it cannot be applied in scenarios that have dynamic features. An anonymous authentication system using lattice-based group signatures (Libert et al., 2016) adds a group member access mechanism to allow new users to join the group, but the joining process is complex and there is no group member revocation mechanism. A fully dynamic group signature (DGS) (including access and revocation mechanisms) scheme in a lattice based on Merkle hash trees (Ling et al., 2017) has high calculation overhead and cannot easily revoke members. The verifier-local revocation (VLR) model (Boneh and Shacham, 2004) is simple to implement and the calculation cost in the revocation phase is very low in practical applications. Verifier requires only to download the VLR list to determine if the identity is valid. Langlois et al. (2014) succeeded in using the VLR revocation mechanism in lattice-based group signature.

In this article, we present an anti-quantum cross-chain identity authentication approach based on DGS (DGS-AQCCIDAA) for smart education. The main contributions are as follows: (1) DGS-AQCCIDAA uses the group signature and relay architecture to realize anonymous identity authentication, which protects the identity privacy of the users in the authentication process. (2) DGS-AQCCIDAA allows the relay chain administrator nodes to open the signature to trace the signer and ensures that the anonymity is not abused. (3) DGS-AQCCIDAA adds access and revocation functions to realize dynamic management of cross-chain users. (4) DGS-AQCCIDAA security is based on the hardness of learning with error (LWE) and the inhomogeneous small integer solution (ISIS) problems in the lattice, so it can resist quantum computing attacks in the smart education field.

2 Preliminaries

Notations used in this paper are listed in Table 1.

Table 1 Notations used in this paper

Notation	Description
$\mathbb{Z}$	Set of integers
$\mathbb{R}$	Set of real numbers
$\boldsymbol{a}, \boldsymbol{b}$	Vectors
$\boldsymbol{A}, \boldsymbol{B}$	Matrices
H	A hash function
$\leftarrow_R$	Sampling at random
$\lVert\cdot\rVert$	2-parameter of a vector
$\lVert\cdot\rVert_\infty$	∞-parameter of a vector
ω, O	Standard asymptotic notations
Cert_i	Certificate for group member i
DID	Digital identifier of the user
D	Gaussian distribution

2.1 Lattice theory

Let $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_m$ be m linearly independent vectors in the n-dimensional Euclidean space $\mathbb{R}^n$. Lattice $\boldsymbol{\Lambda}$ is defined as the set of all linear combinations of integer coefficients on $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_m$, where $\boldsymbol{\Lambda} = L(\boldsymbol{B}) = L(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_m) = \{\sum_{i=1}^{n} c_i \boldsymbol{b}_i | c_i \in \mathbb{Z}\}$, $\boldsymbol{B}$ is the basis of $\boldsymbol{\Lambda}$, m is the order of $\boldsymbol{\Lambda}$, and n

is the dimension of $\boldsymbol{\Lambda}$. $\boldsymbol{\Lambda}$ is called a full-rank lattice when $m=n$.

Definition 1 Given $q,m,n \in \mathbb{Z}$, a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, and a vector $\boldsymbol{u} \in \mathbb{Z}_q^n$, the special integer lattices are as follows:

$$\begin{cases}\boldsymbol{\Lambda}^{\perp}(\boldsymbol{A}) = \{\boldsymbol{e} \in \mathbb{Z}_q^m : \boldsymbol{Ae} = \boldsymbol{0} \ (\mathrm{mod}\ q)\}, \\ \boldsymbol{\Lambda}_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}) = \{\boldsymbol{e} \in \mathbb{Z}_q^m : \boldsymbol{Ae} = \boldsymbol{u} \ (\mathrm{mod}\ q)\}.\end{cases} \tag{1}$$

Definition 2 Given a lattice $\boldsymbol{\Lambda}$, a center vector $\boldsymbol{c} \in \mathbb{R}^n$, and $s \in \mathbb{R}^+$, $\forall \boldsymbol{x} \in \boldsymbol{\Lambda}$, $\rho_{s,\boldsymbol{c}}(\boldsymbol{x}) = \exp(-\pi\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2})$, and $\rho_{s,\boldsymbol{c}}(\boldsymbol{\Lambda}) = \sum_{\boldsymbol{x}\in\boldsymbol{\Lambda}} \rho_{s,c}(\boldsymbol{x})$, the Gaussian distribution in $\boldsymbol{\Lambda}$ is as follows:

$$D_{\boldsymbol{\Lambda},s,\boldsymbol{c}}(\boldsymbol{x}) = \frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{s,\boldsymbol{c}}(\boldsymbol{\Lambda})}, \quad \forall \boldsymbol{x} \in \boldsymbol{\Lambda}. \tag{2}$$

2.2 Hard assumptions in the lattice

Hard assumptions of DGS-AQCCIDAA are introduced in this subsection:

1. Small integer solution (SIS) problem: Given an integer q, a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, and a real number β, the SIS problem is to find a non-zero vector $\boldsymbol{e} \in \mathbb{Z}^m$ such that $\boldsymbol{Ae} = \boldsymbol{0}$ (mod q) and $\|\boldsymbol{e}\| \le \beta$.

2. ISIS problem: Given an integer q, a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, a real number β, and a vector $\boldsymbol{u} \in \mathbb{Z}_q^n$, the ISIS problem is to find a non-zero vector $\boldsymbol{e} \in \mathbb{Z}^m$ such that $\boldsymbol{Ae} = \boldsymbol{u}$ (mod q), and $\|\boldsymbol{e}\| \le \beta$.

3. Split-SIS problem: Given $q, N \in \mathbb{Z}$, a matrix $\boldsymbol{A} = (\boldsymbol{A}_1 \parallel \boldsymbol{A}_2) \leftarrow_R \mathbb{Z}_q^{n\times(2m)}$, and $\beta \in \mathbb{R}$, the split-SIS problem is to find a tuple $\boldsymbol{x} = ((\boldsymbol{x}_1, \boldsymbol{x}_2), h) \in \mathbb{Z}^{2m} \times \mathbb{Z}$ such that $\boldsymbol{x}_1 \ne \boldsymbol{0}$ (or $h\boldsymbol{x}_2 \ne \boldsymbol{0}$), $\|\boldsymbol{x}\| \le \beta$, $h \in [1, N]$, and $\boldsymbol{A}_1\boldsymbol{x}_1 + h\boldsymbol{A}_2\boldsymbol{x}_2 = \boldsymbol{0}$.

4. LWE problem: Given q, $\alpha \in \mathbb{R}^+$, a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, and a vector $\boldsymbol{u} \in \mathbb{Z}_q^n$, where the modulus $q \ge 3$ and $\boldsymbol{e} \leftarrow_R \chi_\alpha^m$ is randomly extracted from the Gaussian noise distribution χ:

(1) Searchable LWE problem: The searchable LWE problem is to calculate the vector $\boldsymbol{s} \in \mathbb{Z}_q^n$ with non-negligible probability such that $\boldsymbol{u} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} + \boldsymbol{e}$.

(2) Decisional LWE problem: Given a random vector $\boldsymbol{s} \in \mathbb{Z}_q^n$, the decisional LWE problem is to distinguish whether $\boldsymbol{u} \in \mathbb{Z}_q^n$ is obtained from an example of the LWE problem ($\boldsymbol{u} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} + \boldsymbol{e}$) or randomly chosen from the uniform distribution $\mathbb{Z}_q^n$.

5. Extended-LWE (eLWE) problem: Given q, $\alpha \in \mathbb{R}^+$, a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, a vector $\boldsymbol{b} \in \mathbb{Z}_q^m$, and $\boldsymbol{e} \leftarrow_R \chi_\alpha^m$, the eLWE problem is to find the non-zero vectors $\boldsymbol{s}$ and $\boldsymbol{x}$ such that $\boldsymbol{b} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} + p\boldsymbol{e} + \boldsymbol{x}$, where $p \ge (\alpha q\sqrt{m} + \beta)m^2$ and $\|\boldsymbol{x}\| \le \beta$.

2.3 Polynomial time algorithm in lattice

1. Trapdoor generation algorithm: Given integers n, $q = \mathrm{poly}(n)$ and $m = O(n\log q)$, the trapdoor generation algorithm TrapGen(q,m,n) outputs a random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ and a full-rank lattice $\boldsymbol{T_A} \subset \boldsymbol{\Lambda}^{\perp}(\boldsymbol{A})$, where $\boldsymbol{A}$ is indistinguishable from the uniform distribution on $\mathbb{Z}_q^{n\times m}$ and $\|\boldsymbol{T_A}\| \le \sqrt{O(n\log q)}$.

2. Preimage sampling algorithm: Given a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, a full-rank lattice $\boldsymbol{T_A} \subset \boldsymbol{\Lambda}^{\perp}(\boldsymbol{A})$, a random vector $\boldsymbol{u} \in \mathbb{Z}_q^n$, and a Gaussian parameter $\sigma = O(\sqrt{n\log q})$, the preimage sampling algorithm SamplePre$(\boldsymbol{A}, \boldsymbol{T_A}, \boldsymbol{u}, \sigma)$ outputs a vector $\boldsymbol{e} \leftarrow D_{\boldsymbol{\Lambda}_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}),\sigma}$ such that $\|\boldsymbol{e}\| \le \sigma\sqrt{m}$ and $\boldsymbol{Ae} = \boldsymbol{u}$ (mod q).

3. Super sampling algorithm: Given the matrices $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ and $\boldsymbol{C} \in \mathbb{Z}_q^{n\times n}$, the super sampling algorithm SuperSamp$(\boldsymbol{A}, \boldsymbol{C})$ outputs a full-rank matrix $\boldsymbol{T_B} \subset \boldsymbol{\Lambda}^{\perp}(\boldsymbol{B})$ and a matrix $\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}$ such that $\boldsymbol{AB}^{\mathrm{T}} = \boldsymbol{C}$, where $\|\boldsymbol{T_B}\| \le m^{1.5}\omega(\sqrt{\log m})$.

4. Lattice basis delegation algorithm: Given a matrix $\boldsymbol{A}' \in Z_q^{n\times(2m)}$, a full-rank lattice $\boldsymbol{T_A} \subset \boldsymbol{\Lambda}^{\perp}(\boldsymbol{A})$, and a real $s = m\omega(\log m)$, the lattice basis delegation algorithm ExtBasis$(\boldsymbol{A}', \boldsymbol{T_A}, s)$ outputs a matrix $\boldsymbol{T_{A'}} \subset \boldsymbol{\Lambda}^{\perp}(\boldsymbol{A}')$ such that $\|\boldsymbol{T_{A'}}\| \le m^{1.5}\omega(\sqrt{\log m})$.

2.4 Non-interactive zero-knowledge proof

The non-interactive zero-knowledge proof (NIZKP) protocol is a two-party protocol and an important tool in cryptographic protocols. The prover can prove to the verifier that he/she owns the knowledge but does not reveal any information about the knowledge. NIZKP reduces the number of interactions to a single one and enables offline proof and public verification. Non-interactive zero-knowledge proof of knowledge (NIZKPoK) used in this study is as follows:

1. NIZKPoK for ISIS relations (Laguillaumie et al., 2013) is

$$\begin{aligned}R_{\mathrm{ISIS}} =\big\{ &(\boldsymbol{A}, \boldsymbol{y}, \beta; \boldsymbol{x}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n \times \mathbb{R} \times \mathbb{Z}_q^m : \\ &\boldsymbol{Ax} = \boldsymbol{y}, \|\boldsymbol{x}\| \le \beta\big\}.\end{aligned} \tag{3}$$

2. Given a matrix $\boldsymbol{A} = (\boldsymbol{A}_1 \parallel \boldsymbol{A}_2)$ and a vector $\boldsymbol{y} = (\boldsymbol{y}_1, \boldsymbol{y}_2) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^m$, where $0 < \|\boldsymbol{y}_2\| \le \beta\sqrt{m}$, the prover can provide a proof about $\boldsymbol{x} = (\boldsymbol{x}_1, \boldsymbol{x}_2, h) \in \mathbb{Z}^{2m+1}$ such that $f_{\boldsymbol{A}}(\boldsymbol{x}_1, \boldsymbol{x}_2, h) =$

$(\boldsymbol{A}_1\boldsymbol{x}_1 + h\boldsymbol{A}_2\boldsymbol{x}_2, \boldsymbol{x}_2) = \boldsymbol{y}$ $(\|\boldsymbol{x}_1\| \le \beta\sqrt{m}, h \in [1, N])$ when $\boldsymbol{x}_2 = \boldsymbol{y}_2$.

NIZKPoK for split-SIS relations (Laguillaumie et al., 2013) is

$$\begin{aligned} R_{\text{Split-SIS}} = \{ & (\boldsymbol{A}, \boldsymbol{y}, \beta, N; \boldsymbol{x}_1, h) \in \mathbb{Z}_q^{n\times(2m)} \times (\mathbb{Z}_q^n \\ & \times \mathbb{Z}_q^m) \times \mathbb{R} \times \mathbb{Z} \times \mathbb{Z}_q^m \times \mathbb{Z} : \boldsymbol{A}_1\boldsymbol{x}_1 \\ & + h\boldsymbol{A}_2\boldsymbol{y}_2 = \boldsymbol{y}_1, \|\boldsymbol{x}_1\| \le \beta\sqrt{m}, h \in [1, N] \}. \end{aligned} \tag{4}$$

3. NIZKPoK for LWE relations (Nguyen et al., 2015) is

$$\begin{aligned} R_{\text{LWE}} = \{ & (\boldsymbol{A}, \boldsymbol{b}, \alpha; \boldsymbol{t}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m \times \mathbb{R} \times \mathbb{Z}_q^n : \\ & \|\boldsymbol{b} - \boldsymbol{A}^{\mathrm{T}}\boldsymbol{t}\| \le \alpha q\sqrt{m} \}. \end{aligned} \tag{5}$$

4. NIZKPoK for eLWE relations (Laguillaumie et al., 2013) is

$$\begin{aligned} R_{\text{eLWE}} = \{ & (\boldsymbol{A}, \boldsymbol{b}, \gamma; \boldsymbol{t}, \boldsymbol{e}, \boldsymbol{x}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m \times \mathbb{R} \\ & \times \mathbb{Z}_q^n \times \mathbb{Z}^m \times \mathbb{Z}^m : \boldsymbol{b} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{t} + p\boldsymbol{e} + \boldsymbol{x}, \\ & \gamma = \max\left(\alpha q\sqrt{m}, \beta\right), \|\boldsymbol{x}\| \le \gamma, \|\boldsymbol{e}\| \le \gamma \}. \end{aligned} \tag{6}$$

3 Model description

3.1 Cross-chain system model

Currently, cross-chain architecture solutions have a notary mechanism, side chain/relay, distributed private key control, and hash time locking. The risk of centralization exists in a notary architecture; there are application limitations in hash time locking and distributed private key control. The side chain increases the network complexity and includes a security risk. The relay chain architecture has wider application prospects. DGS-AQCCIDAA relies on the relay chain architecture (He et al., 2023) and the model of the cross-chain system as shown in Fig. 1. The cross-chain system model consists of three parts: relay chain, application chain, and cross-chain gateway. The model details are as follows:

1. The relay chain is responsible for cross-chain identity registration, identity authentication, identity management, and forwarding of cross-chain transactions. All entities involved in the cross-chain network maintain the relay chain via the consensus mechanism. Cross-chain information is stored in the relay chain ledger.

2. The application chain is the connection of the consortium chains via the cross-chain system. It can join the cross-chain system with a unique identity and interact with other application chains in the cross-chain network. A cross-chain contract is deployed on the application chain to execute the cross-chain events.

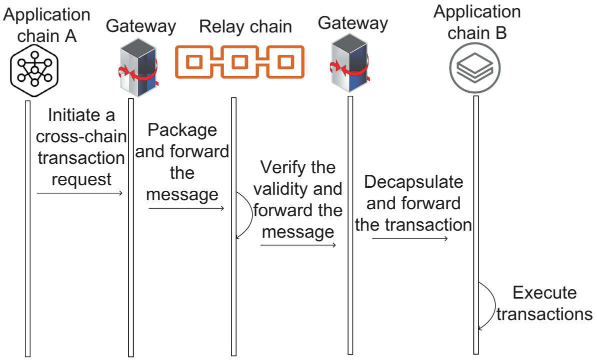

Fig. 1 Architecture of the cross-chain system model

3. The cross-chain gateway is responsible for monitoring, routing, proxy forwarding, and so on. The gateway submits the cross-chain transactions to the relay chain.

3.2 Identity registration process

To secure cross-chain transactions, each application chain obtains the digital identifier (DID) through the execution of an identity registration contract. The registration process of a cross-chain DID is shown in Fig. 2.

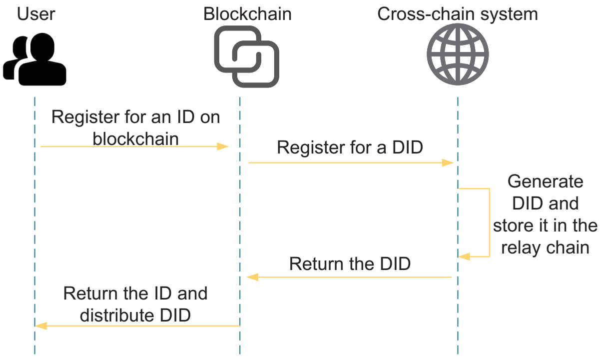

Fig. 2 Registration process of a cross-chain digital identifier (DID)

DID (Zhong et al., 2021) is a type of decentralized identifier. Blockchain makes identity management decentralized, tamper-resistant, cost-effective, and controllable for users. Current architectures and applications of DID are based mainly on blockchain. The application chain sends the data (public key and transaction address) to the relay chain for cross-chain identity registration. The registration proposal is valid after it passes the voting of relay chain nodes. The application chain can participate in the cross-chain system after obtaining the DID.

3.3 Authentication model

In the field of smart education, blockchain can be applied in the identity management of academics, teachers, and graduates to ensure the validity of education data due to the features of distributed data storage, peer-to-peer transmission, tamper-proofing, and consensus confirmation. Usually, each user needs to register his/her identity once in a different educational institution, but a user may have multiple accounts in multiple blockchain systems. Leakage of unified and trusted digital identities in education will greatly increase the service cost of the application chain. A cross-chain mechanism can exchange and circulate the information and value between originally different blockchains using technical means, and can manage the trust and authentication between different blockchain systems in multi-chain scenarios.

The DGS-AQCCIDAA-based cross-chain identity authentication for smart education is shown in Fig. 3. This interactive process contains three entities: user set, application chain, and relay chain. The model details in Fig. 3 are as follows:

1. The user set is a collection of users involved in the smart education system, including graduates, teachers, learners, and other staff.

2. The application chain is applied in the identity management of the user set. Application chain nodes (group members) apply to the group manager to join the group and authenticate with nodes on the other application chain.

3. The relay chain nodes (group managers) complete the creation of the group, generate the group public key and group private key, and publish the group public key to all group members. Group managers manage groups through revocation and access mechanisms. Entities in the cross-chain system need to request a group certificate from the relay chain for anonymous authentication.

4 DGS-AQCCIDAA

Relay chain nodes act as the group managers to create the group, and each application chain node acts as a group member. The DGS-AQCCIDAA algorithm is described in the following subsections.

4.1 Setup

The group manager inputs $(1^n, 1^N)$ and outputs the system parameters, where n is the security parameter and N is the maximum number of group members. The parameters of DGS-AQCCIDAA are listed in Table 2.

The group manager selects a positive integer m, two primes $p, q \in \mathbb{Z}$, $s, \alpha, \beta, \eta, \delta \in \mathbb{R}$, $\boldsymbol{A}_0, \boldsymbol{A}_1 \leftarrow_R \mathbb{Z}_q^{n\times m}$, and a secure hash function H.

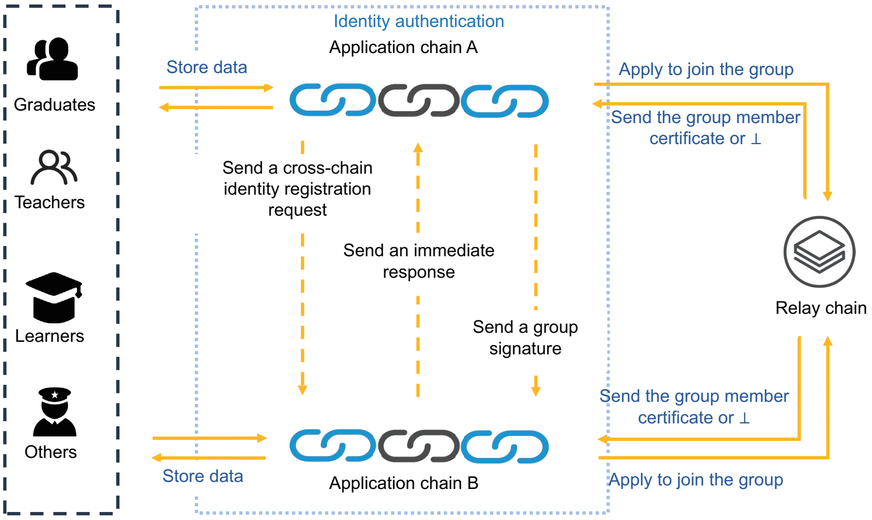

Fig. 3 DGS-AQCCIDAA-based cross-chain identity authentication model in smart education

Table 2 Parameters of DGS-AQCCIDAA

Parameter	Value or asymptotic bound
m	$m = 6n^{1+\delta}$
p	$p = m^4 \cdot \omega\big((\log m)^{1.5}\big)$
q	$q = m^{2.5} \cdot \max\big(m^6 \cdot \omega\big((\log m)^{2.5}\big), 4N\big)$
α	$\alpha = 2\frac{\sqrt{m}}{q}$
β	$\beta = m^{1.5} \cdot \omega\big((\log m)^{1.5}\big)$
s	$s = m \cdot \omega(\log m)$
η	$\eta = m^2 \cdot \omega\big((\log m)^{1.5}\big)$
δ	$n^{1+\delta} > \lceil (n+1)\log q + n \rceil$
t	$t = \omega(\log m)$
H	$H: \{0,1\}^* \rightarrow \{0,1\}^t$

The group manager publishes the global system parameter set as follows: $\phi = \{n, N, m, q, s, p, \alpha, \beta, \eta, \boldsymbol{A}_0, \boldsymbol{A}_1, H\}$.

4.2 KeyGen

The algorithm details concerning the key generation are as follows:

1. $\text{KeyGen}_{\text{GM}}(\phi)$: The group manager generates $(\boldsymbol{A}, \boldsymbol{T}_{\boldsymbol{A}}) \leftarrow \text{TrapGen}(q, m, n)$ and $(\boldsymbol{B}, \boldsymbol{T}_{\boldsymbol{B}}) \leftarrow \text{SuperSamp}(\boldsymbol{A}, \boldsymbol{0})$. The master private key of the group manager is $\mathbf{msk} = \boldsymbol{T}_{\boldsymbol{A}}$, the master public key is $\mathbf{mpk} = \boldsymbol{A}$, the trace private key is $\mathbf{tsk} = \boldsymbol{T}_{\boldsymbol{B}}$, and the trace public key is $\mathbf{tpk} = \boldsymbol{B}$.

2. $\text{KeyGen}_{\text{Gm}}(\phi)$: The group member samples a short vector $\boldsymbol{r}_i \leftarrow D_\sigma^n$ on the lattice, selects $\boldsymbol{F} \leftarrow_R \mathbb{Z}_q^{m\times n}$, and calculates $\boldsymbol{u}_i = \boldsymbol{F}\boldsymbol{r}_i \pmod q$. The signature private key of the group member is $\mathbf{usk} = \boldsymbol{s}_i$, and the public key is $\mathbf{upk} = \boldsymbol{u}_i$.

Note that the group public key is $\mathbf{gpk} = (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{F}, \boldsymbol{u}_i)$.

4.3 Group member joining

The application chain sends $(\text{DID}, \boldsymbol{u}_i, \text{sig}(\boldsymbol{u}_i))$ to the group manager. The group manager verifies the validity of the signature using the public key information submitted by the application chain node during the identity registration, to judge whether the node is a legitimate user in the cross-chain system and whether the node can join the group. If the identity of the node is invalid or the DID is a group member, the joining process is terminated; otherwise, the group manager carries out the following:

1. For the DID, the group manager selects $i \in [1, N]$ to calculate $\bar{\boldsymbol{A}}_i = [\boldsymbol{A} \parallel \boldsymbol{A}_0 + i\boldsymbol{A}_1] \in \mathbb{Z}_q^{n\times(2m)}$. The group manager generates $\boldsymbol{T}_{\bar{\boldsymbol{A}}_i} \leftarrow \text{ExtBasis}(\bar{\boldsymbol{A}}_i, \boldsymbol{T}_{\boldsymbol{A}}, s)$, where $\boldsymbol{T}_{\bar{\boldsymbol{A}}_i} \in \mathbb{Z}_q^{m\times m}$ and $\|\boldsymbol{T}_{\bar{\boldsymbol{A}}_i}\| \leq s\sqrt{m}$.

2. The group manager sets $\boldsymbol{w}_i = \boldsymbol{A}\boldsymbol{u}_i \pmod q$ and generates $(\boldsymbol{x}_0, \boldsymbol{x}_1) \leftarrow \text{SamplePre}(\bar{\boldsymbol{A}}_i, \boldsymbol{T}_{\bar{\boldsymbol{A}}_i}, \beta, \boldsymbol{w}_i)$, where $(\boldsymbol{x}_0, \boldsymbol{x}_1) \in D_{\mathbb{Z}^{2m},\beta}$. $\mathbf{Tag}_i = \boldsymbol{A}_0\boldsymbol{u}_i \pmod q \in \mathbb{Z}_q^n$ is the revocation tag of the group member.

3. The group manager sends $\text{Cert}_i = (i, \boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{w}_i, \mathbf{Tag}_i)$ to the application chain node via a secure channel. The group manager updates $\mathbf{gpk} = (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{F}, \boldsymbol{u}_i, \boldsymbol{w}_i)$.

4.4 Group member revocation algorithm

The algorithm details for group member revocation are as follows:

1. $\text{Revoke}_{\text{GM}}$: The group manager adds $\mathbf{Tag}_i$ to the revocation list RL. This algorithm returns 1 if the revocation is successful and 0 otherwise.

2. $\text{Revoke}_{\text{Gm}}$: The group member sends $(\mathbf{Tag}_i, \boldsymbol{u}_i, \text{sig}(\boldsymbol{u}_i))$ to the group manager. If the identity of the group member is valid, the group administrator adds $\mathbf{Tag}_i$ to the revocation list RL. This algorithm returns 1 if the revocation is successful and 0 otherwise.

4.5 Group signature

Inputting $(\mathbf{gpk}, \mathbf{usk}, \text{Cert}_i, m)$, this group algorithm carries out the following:

1. The group member selects $\boldsymbol{s} \leftarrow_R \mathbb{Z}_q^n$, $\boldsymbol{e}_0 \leftarrow_R \chi_\alpha$, and calculates $\boldsymbol{c}_0 = \boldsymbol{B}^{\text{T}}\boldsymbol{s} + p\boldsymbol{e}_0 + \boldsymbol{x}_0$ to generate a proof π_0 about $(\boldsymbol{s}, \boldsymbol{e}_0, \boldsymbol{x}_0)$ such that $(\boldsymbol{B}, \boldsymbol{c}_0, \eta; \boldsymbol{s}, \boldsymbol{e}_0, \boldsymbol{x}_0) \in R_{\text{eLWE}}$.

2. The group member selects $\boldsymbol{e}_i \leftarrow_R \chi_\alpha$ and calculates $\boldsymbol{c}_1 = \boldsymbol{B}^{\text{T}}\mathbf{Tag}_i + \boldsymbol{e}_i$ to produce a proof π_1 about $(\mathbf{Tag}_i, \boldsymbol{e}_i)$ such that $(\boldsymbol{B}, \boldsymbol{c}_1, \alpha; \mathbf{Tag}_i, \boldsymbol{e}_i) \in R_{\text{LWE}}$.

3. The group member produces a proof π_2 about $\boldsymbol{r}_i$, such that $(\boldsymbol{F}, \boldsymbol{u}_i, \beta; \boldsymbol{r}_i) \in R_{\text{ISIS}}$.

4. Let $\bar{\beta} = \lfloor \beta \rfloor$, $l = \lceil \log_{\bar{\beta}} \rceil N$, $\boldsymbol{b} = \boldsymbol{A}_1\boldsymbol{x}_1$, $\boldsymbol{y}_0 = \boldsymbol{e}_i$ $(i = 1, 2, \cdots, N])$, $\boldsymbol{y}_1 = \boldsymbol{x}_0$, $\boldsymbol{y}_2 = (v_0, v_1, \cdots, v_{l-1}) \in \mathbb{Z}_{\bar{\beta}}^l$, and $\boldsymbol{D} = \big(\boldsymbol{b}, \bar{\beta}\boldsymbol{b}, \cdots, \bar{\beta}^{l-1}\boldsymbol{b}\big) \in \mathbb{Z}_q^{n\times l}$. The group member generates a proof π_3 about $(\boldsymbol{y}_0, \boldsymbol{y}_1, \boldsymbol{y}_2)$ such that

$$\begin{aligned} R_{\text{Com}} = \big\{ & (\boldsymbol{A}, \boldsymbol{D}, \boldsymbol{u}_0, \boldsymbol{u}_1, \eta; \boldsymbol{y}_0, \boldsymbol{y}_1, \boldsymbol{y}_2) \in \mathbb{Z}_q^{n\times m}, \\ & \mathbb{Z}_q^{n\times l}, \mathbb{Z}_q^n, \mathbb{Z}_q^n, \mathbb{R}, \mathbb{Z}_q^m, \mathbb{Z}_q^m, \mathbb{Z}_{\beta}^l : \\ & \boldsymbol{t}_0 = p\boldsymbol{A}\boldsymbol{y}_0 - \boldsymbol{D}\boldsymbol{y}_2, \\ & \boldsymbol{t}_1 = p\boldsymbol{A}\boldsymbol{y}_0 + \boldsymbol{A}\boldsymbol{y}_1, \|\boldsymbol{y}_j\| < \eta, j = 0, 1, 2 \big\}, \end{aligned} \tag{7}$$

where Com is a promise message, and $H(\boldsymbol{x}_1, \pi_0, \pi_1, \pi_2, m, \text{Com})$ is the challenge of

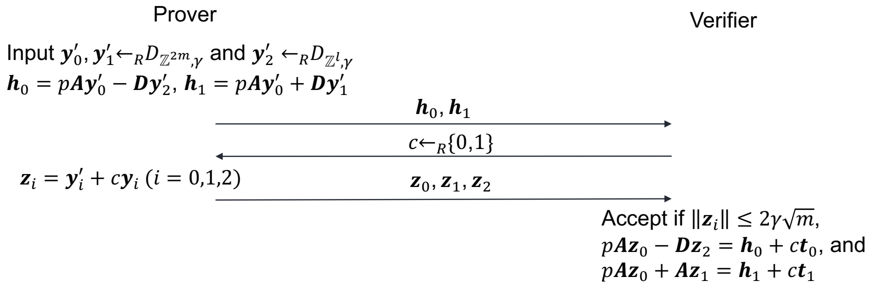

Fig. 4 Protocol π_3 with a single-bit challenge

π_3. Protocol π_3 with a single-bit challenge is as shown in Fig. 4.

The group member finally outputs the signature $\Sigma = (\boldsymbol{c}_0, \boldsymbol{c}_1, \boldsymbol{x}_1, \pi_0, \pi_1, \pi_2, \pi_3)$ to the verifier.

4.6 Verify

GVerify$(\mathbf{gpk}, m, \Sigma, \mathrm{RL}) \to 0/1$: The verifier first checks the validity of RL. For $\mathbf{Tag}_i \in \mathrm{RL}$, the verifier calculates $\boldsymbol{e}_i' = \boldsymbol{c}_1 - \boldsymbol{B}^{\mathrm{T}}\mathbf{Tag}_i$. If $\|\boldsymbol{e}_i'\| \le \alpha q\sqrt{m}$, user identity i has been revoked and the signature is rejected. Otherwise, the verifier checks the validity of π_0–π_3, $\|\boldsymbol{x}_1\| \le \beta\sqrt{m}$, and $\boldsymbol{A}_1\boldsymbol{x}_1 \ne \boldsymbol{0}$. The verifier outputs 1 if the signature is legal and 0 otherwise.

4.7 Open signature

Gopen$(\mathbf{gpk}, \mathbf{gtsk}, \Sigma) \to i$: The group manager obtains $\boldsymbol{c}_0$ using $\boldsymbol{T}_{\boldsymbol{B}}$ and calculates $\boldsymbol{z}_1 = \boldsymbol{A}_1\boldsymbol{x}_1$, $\boldsymbol{z}_2 = A\boldsymbol{x}_0 + \boldsymbol{A}_0\boldsymbol{x}_1$. If $\boldsymbol{z}_1 \ne \boldsymbol{0}$ and $\exists i \in [1, N]$ satisfying $\boldsymbol{z}_2 + i\boldsymbol{z}_1 = \boldsymbol{w}_i$, the group manager outputs i and $\perp$ otherwise.

5 Correctness analysis

The correctness analysis for DGS-AQCCIDAA is as follows.

5.1 Correctness of the group signature algorithm

According to $\beta = s\sqrt{2m} \cdot \omega\left(\sqrt{\log(2m)}\right) \ge \|\tilde{\boldsymbol{T}}_{\bar{\boldsymbol{A}}_i}\| \cdot \omega\left(\sqrt{\log(2m)}\right)$, $\boldsymbol{x}_0, \boldsymbol{x}_1 \in D_{\mathbb{Z}^m,\beta}$, $\|\boldsymbol{x}_j\| \le \beta\sqrt{m}$ $(j \in \{0,1\})$, $\|\boldsymbol{e}_k\| \le \alpha q\sqrt{m}$ $(k \in \{0, 1, \cdots, N\})$, and $\eta = \max(\beta, \alpha q\sqrt{m})$, the signature algorithms can generate $\boldsymbol{c}_0, \boldsymbol{c}_1$ and NIZKP π_0–π_3. Because $\boldsymbol{x}_1 \in D_{\mathbb{Z}^m,\beta}$, $\Pr[\boldsymbol{A}_1\boldsymbol{x}_1 = \boldsymbol{0}] \le O(q^{-n})$ and π_0–π_3 are complete (Laguillaumie et al., 2013), $\Sigma = (\boldsymbol{c}_0, \boldsymbol{c}_1, \boldsymbol{x}_1, \pi_0, \pi_1, \pi_2, \pi_3)$ is shown to be correct.

5.2 Correctness of the open signature algorithm

For DGS-AQCCIDAA, we know that $\boldsymbol{T}_{\boldsymbol{B}}^{\mathrm{T}}\boldsymbol{c}_0 = \boldsymbol{T}_{\boldsymbol{B}}^{\mathrm{T}}(p\boldsymbol{e}_0 + \boldsymbol{x}_0) \pmod q$, $\boldsymbol{T}_{\boldsymbol{B}} \in \mathbb{Z}^{m\times m}$ is a full-rank matrix, and $\boldsymbol{T}_{\boldsymbol{B}}^{\mathrm{T}}(p\boldsymbol{e}_0 + \boldsymbol{x}_0)_\infty \le 3m^8\omega\big((\log m)^{3.5}\big) \le q/2$. Therefore, we have $\boldsymbol{x}_0' = p\boldsymbol{e}_0 + \boldsymbol{x}_0$ for Gaussian elimination.

Because $\beta = m^{1.5}\omega\big((\log m)^{1.5}\big)$, $p = m^{2.5}\beta$, $\|\boldsymbol{x}_0\|_\infty \le \|\boldsymbol{x}_0\| \le p$, the group manager can obtain $\boldsymbol{x}_0 = \boldsymbol{x}_0' \pmod p$. The group manager can calculate $\boldsymbol{w}_i = \bar{\boldsymbol{A}}_i(\boldsymbol{x}_0, \boldsymbol{x}_1) = \boldsymbol{A}\boldsymbol{x}_0 + (\boldsymbol{A}_0 + i\boldsymbol{A}_1)\boldsymbol{x}_1 = \boldsymbol{z}_2 + i\boldsymbol{z}_1$, thus successfully determining user i.

6 Security analysis

DGS-AQCCIDAA also meets the chosen plaintext attack (CPA)-anonymity and traceability requirements (Nguyen et al., 2015). The process of proving its security is as follows.

6.1 Anonymity

Theorem 1 If an adversary A can attack CPA-anonymity under chosen-plaintext attacks of DGS-AQCCIDAA with non-negligible advantage ε, there must exist a challenge algorithm Γ to solve the LWE problem.

Proof CPA-anonymity proof relies on two games G_0 and G_1. Game G_0 is as follows:

1. Γ obtains $\mathbf{gpk} = (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{F}, \boldsymbol{u}_i, \boldsymbol{w}_i)$, $\mathbf{usk} = \boldsymbol{r}_i, i \in [1, N]$, $\mathbf{tsk} = \boldsymbol{T}_{\boldsymbol{B}}$, and group member certificate Cert_i. Γ initializes the revocation list RL and the set of corrupted users U. Γ sends $\mathbf{gpk}$ to adversary A.

2. A may issue an adaptive query about the signature of an arbitrary message m to any group member, and $\mathit{\Gamma}$ runs the group signature algorithm to answer it. A also issues a corruption query to group member i. $\mathit{\Gamma}$ updates $U=U\cup\{i\}$ and returns Cert_i to A. For each revocation query to group member i, $\mathit{\Gamma}$ updates the revocation list $\mathrm{RL}=\mathrm{RL}\cup\{i\}$ and returns $\mathbf{Tag}_i$ to A.

3. A selects a message m^* and two identity identifiers $i_0,i_1\in[1,N]$, where $i_b\notin U$ and $\mathbf{Tag}_{i_b}\notin\mathrm{RL}$ ($b\in\{0,1\}$).

4. $\mathit{\Gamma}$ selects $b\leftarrow_R\{0,1\}$, generates a legal signature $\mathit{\Sigma}=(\boldsymbol{c}_0,\boldsymbol{c}_1,\boldsymbol{x}_1,\pi_0,\pi_1,\pi_2,\pi_3)$, and then sends $\mathit{\Sigma}$ to A.

Subsequently, A can do the same query as before, but A cannot query Cert_{i_b} or $\mathbf{Tag}_i$, where $b\in\{0,1\}$. $\mathit{\Gamma}$ finally returns a guess b' about b to A.

Game G_1 is essentially the same as G_0, but with the following revision in step 4: a simulated signature is used instead of a legal signature. The simulated signature for message m^* is $\mathit{\Sigma}^*=(\boldsymbol{c}_0^*,\boldsymbol{c}_1^*,\boldsymbol{x}_1^*,\pi_0^*,\pi_1^*,\pi_2^*,\pi_3^*)$, where:

1. $(\pi_0^*,\pi_1^*,\pi_2^*,\pi_3^*)$ are generated by the NIZKP simulator ($(\pi_0,\pi_1,\pi_2,\pi_3)$ are generated by random oracles in G_0). Based on NIZKP, $(\pi_0^*,\pi_1^*,\pi_2^*,\pi_3^*)$ and $(\pi_0,\pi_1,\pi_2,\pi_3)$ are statistically close to each other.

2. $\mathit{\Gamma}$ chooses $\boldsymbol{x}_1^*\leftarrow_R D_{\mathbb{Z}^m,\beta}$. Based on $\mathrm{SamplePre}(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{u},\sigma)$, $\boldsymbol{x}_1^*$ and $\boldsymbol{x}_1$ chosen in G_1 and G_0 are statistically close.

3. $\boldsymbol{g}_i\leftarrow_R\mathbb{Z}_q^n$. $\mathit{\Gamma}$ computes $\boldsymbol{c}_1^*=\boldsymbol{B}^{\mathrm{T}}\boldsymbol{g}_i+\boldsymbol{e}_i$. Based on the LWE assumption, $\boldsymbol{c}_1^*$ and $\boldsymbol{c}_1$ chosen in G_1 and G_0 are statistically indistinguishable.

4. $\boldsymbol{d}\leftarrow_R\mathbb{Z}_q^m$. $\mathit{\Gamma}$ computes $\boldsymbol{c}_0^*=\boldsymbol{d}+\boldsymbol{x}_0^*$. Based on the LWE assumption, $\boldsymbol{c}_0^*$ and $\boldsymbol{c}_0$ chosen in G_1 and G_0 are statistically indistinguishable.

In summary, because G_1 is statistically indistinguishable from G_0 and $\mathit{\Sigma}^*$ is independent of b, the probability that $b'=b$ is close to 1/2 (Nguyen et al., 2015). The advantage that adversary A wins in game G_1 is negligible. Therefore, DGS-AQCCIDAA has CPA-anonymity under the LWE assumption.

6.2 Full traceability

Theorem 2 If an adversary A can attack the traceability of DGS-AQCCIDAA with non-negligible advantage ε, there must exist a challenge algorithm C to solve the ISIS problem.

Proof Given a matrix $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ and a vector $\boldsymbol{u}\in\mathbb{Z}_q^n$, a non-zero vector $\boldsymbol{x}\in\mathbb{Z}_q^m$ can be found to satisfy $\|\boldsymbol{x}\|\le\mathrm{poly}(m)$ and $\boldsymbol{Ax}=\boldsymbol{u}\pmod q$. C is required to perform the following: C selects $R\leftarrow_R\{-1,1\}^m$ and an integer $i^*\leftarrow_R\left[-4m^{2.5}N+1,4m^{2.5}N-1\right]$, and obtains $(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}})\leftarrow\mathrm{TrapGen}(n,m,q)$, and $(\boldsymbol{B},\boldsymbol{T}_{\boldsymbol{B}})\leftarrow\mathrm{SuperSamp}(n,m,q,\boldsymbol{A},\pm 0)$. Then, C chooses $\boldsymbol{F}\leftarrow_R\mathbb{Z}_q^{n\times m}$, samples $\boldsymbol{r}_i\leftarrow D_\sigma^n$, and computes $\boldsymbol{u}_i=\boldsymbol{Fr}_i(\mathrm{mod}\ q)$ and $\boldsymbol{w}_i=\boldsymbol{Ax}_0+\boldsymbol{A}_0\boldsymbol{x}_1+i^*\boldsymbol{A}_1\boldsymbol{x}_1$. C sets $\mathrm{RL}=\varnothing$ and $U=\varnothing$.

C calculates the following answers for all $i\in[1,N]$ and $i\neq i^*$:

1. C calculates $\bar{\boldsymbol{A}}_i=[\boldsymbol{A}\parallel\boldsymbol{A}_0+i\boldsymbol{A}_1]=\left[\boldsymbol{A}\parallel\boldsymbol{AR}+\left(i-i^*\right)\boldsymbol{A}_1\right]$ and obtains $\boldsymbol{T}_{\bar{\boldsymbol{A}}_i}\leftarrow\mathrm{ExtBasis}(\bar{\boldsymbol{A}}_i,\boldsymbol{T}_{\boldsymbol{A}},s)$.

2. C calculates $\mathbf{Tag}_i=\boldsymbol{A}_0\boldsymbol{u}_i\pmod q$ and sends it to A. Here, $\mathbf{gpk}\leftarrow(\boldsymbol{A},\boldsymbol{B},\boldsymbol{F},\boldsymbol{u}_i,\boldsymbol{w}_i)$ and $\mathbf{Tag}_i$ are statistically close to the real scenario. A cannot know i^*. C sends $(\mathbf{gpk},\mathbf{Tag}_i)$ to A.

Queries: After C receives a corruption query about i from A, C stops and aborts if $i=i^*$ or $i\notin[1,N]$. Otherwise, C sets $U=U\cup\{i\}$ and sends $\boldsymbol{z}_i$ to A.

A issues a signature query about group member i and message m to a random oracle. Then, A sends the signature to C. If $i\notin[1,N]$, C rejects the signature; if $i=i^*$, C uses the NIZKP simulator to generate π_0^*–π_3^* and sends a new signature to A. Otherwise, C sends $\mathit{\Sigma}=(\boldsymbol{c}_0,\boldsymbol{c}_1,\boldsymbol{x}_1,\pi_0,\pi_1,\pi_2,\pi_3)$ to A as a signature of i.

Forgery phase: A returns a message m^*, a set of revocation lists RL^*, and a forged signature $\mathit{\Sigma}^*=(\boldsymbol{c}_0^*,\boldsymbol{c}_1^*,\boldsymbol{x}_1^*,\pi_0^*,\pi_1^*,\pi_2^*,\pi_3^*)$ with probability ε. Running the tracing algorithm will cause a tracing failure or output an identity index $i\in U\backslash\mathrm{RL}^*$. $i\in U\backslash\mathrm{RL}^*$ indicates the set of users in the corruption list but not in the forged revocation list RL^*.

C extracts $\boldsymbol{x}_0^*,\boldsymbol{x}_1^*$ and the success probability of extraction is at least $\varepsilon\left(\varepsilon/q_h-2^{-t}\right)$ (Bellare and Neven, 2006), where q_h is the maximum number of times that A accesses the hash function. Consider two cases:

1. If $i\neq i^*$, C aborts and fails. The probability of $i\neq i^*$ is at most $\left(8m^{2.5}-1\right)/(8m^{2.5}N)$.

2. $\left[\boldsymbol{A}\parallel\boldsymbol{AR}+\left(i-i^*\right)\boldsymbol{A}_1\right]\left(\boldsymbol{x}_0^*,\boldsymbol{x}_1^*\right)=\boldsymbol{Ax}_0^*+\boldsymbol{ARx}_1^*=\boldsymbol{w}_i=\boldsymbol{Au}_i$ while $i=i^*$, where $i\le 4\eta m^2$. Then, $\boldsymbol{x}=\boldsymbol{x}_0^*+\boldsymbol{Rx}_1^*$ is the solution to the ISIS problem. Because $i^*\leftarrow_R\left[-4m^{2.5}N+1,4m^{2.5}N-1\right]$, the probability of $i=i^*$ is at least $1/(8m^{2.5}N)$, and then the probability that C can solve the ISIS problem is at least $\varepsilon\left(\varepsilon/q_h-2^{-t}\right)/(8m^{2.5}N)$.

Based on the above description, DGS-AQCCIDAA satisfies full traceability under the ISIS assumption.

7 Performance analysis

In this section, we analyze the performance of DGS-AQCCIDAA and existing group signatures (Libert et al., 2016; Ling et al., 2017; Li et al., 2019). The processor is Intel® Core™ i5-1135G7@2.40 GHz; the operating system is 64-bit Windows 10.

Table 3 lists the average running time for cryptographic operations. The pairing-based cryptography (PBC) library is called to calculate the average time cost of each cryptographic operation. In the simulations, the lattice dimension m is set to 1000 for sufficient security of cryptographic schemes, and n is selected such that $m \geq 5n\log q$. Because the generation of large prime numbers is random, we obtain an average result by multiple simulations.

A performance comparison among several schemes is shown in Table 4, where n is the security parameter, N is the number of group members, $q \in \mathbb{Z}$ is the modulus, and $t = \omega\left(\log m\right)$ $\left(m = 6n^{1+\delta}\right)$ is the number of interactions between the prover and verifier in the zero-knowledge proof π_3. According to Table 4, the public and private key sizes are small and independent of N in DGS-AQCCIDAA. Compared with Libert et al. (2016), the revocation function is achieved in DGS-AQCCIDAA and the implementation of the VLR mechanism is simple. Compared with Li et al. (2019), the process of group member access and revocation requires interaction with a Turing machine in Li et al. (2019), which complicates the process of identity authentication. In addition, Libert et al. (2016), Ling et al. (2017), and Li et al. (2019) used the Stern-type protocol for the authentication. The soundness error of single-bit schemes in Libert et al. (2016), Ling et al. (2017), and Li et al. (2019) is 2/3, but the soundness error of DGS-AQCCIDAA is just 1/2, where the soundness error is the probability of a malicious prover convincing an honest verifier that a false statement is true.

Table 3 Average time of cryptographic operations

Operation type	Time (ms)
Hash function, T_{H}	11.69
Gaussian sampling, T_{G}	23.03
Matrix or vector multiplication, T_{M}	8.32
Polynomial modular multiplication, T_{PM}	3.94
Matrix or vector addition, T_{A}	1.32

Table 5 shows a comparison of the characteristics of DGS-AQCCIDAA and other cross-chain authentication schemes proposed by Shao et al. (2021) and Wang et al. (2022a, 2022b). Compared to other schemes, DGS-AQCCIDAA does not have a single point of failure and can realize anonymous authentication to protect the privacy of users, so our scheme is more flexible in user identity management.

Table 4 Performance comparison among several schemes

Scheme	Public key size	Private key size	Signature size
Libert et al. (2016)'s	$O\left(mn\log N\log q\right)$	$O\left(m\right)$	$O\left(tm\log q\right)$
Ling et al. (2017)'s	$O\left(mn\log N\log q\right)$	$O\left(mn\log N\log q\right)$	$O\left(tm\log N\log q\log \beta\right)$
Li et al. (2019)'s	$O\left(mn\log q\right)$	$O\left(m\right)$	$O\left(tm\log q\right)$
DGS-AQCCIDAA	$O\left(mn\log q\right)$	$O\left(m\right)$	$O\left(tm\log q\right)$

Scheme	Total time cost	Revocation model
Libert et al. (2016)'s	$(9t+9)\,T_{\mathrm{M}} + (11t+8)\,T_{\mathrm{A}} + 2tT_{\mathrm{G}} + 2T_{\mathrm{H}}$	–
Ling et al. (2017)'s	$(9t+3)\,T_{\mathrm{M}} + (8t+1)\,T_{\mathrm{A}} + 2tT_{\mathrm{G}} + T_{\mathrm{H}}$	Merkle tree
Li et al. (2019)'s	$(9t+10)\,T_{\mathrm{M}} + (11t+10)\,T_{\mathrm{A}} + (2t+7)T_{\mathrm{G}} + 6T_{\mathrm{H}}$	VLR
DGS-AQCCIDAA	$(6t+6)\,T_{\mathrm{M}} + (7t+5)\,T_{\mathrm{A}} + 2tT_{\mathrm{G}} + T_{\mathrm{H}}$	VLR

Table 5 Characteristic comparison among several schemes

Scheme	Cross-chain mechanism	Single point of failure	Protection of identity privacy	Anonymous authentication	Anti-quantum attack	Revocation of identity
Wang et al. (2022b)'s	Relay	×	×	×	×	×
Shao et al. (2021)'s	Notary	✓	×	×	×	×
Wang et al. (2022a)'s	Relay	×	×	×	×	×
DGS-AQCCIDAA	Relay	×	✓	✓	✓	✓

MATLAB software is used to manage the simulations, where t is the number of interactions between the prover and verifier in NIZKP π_3. Fig. 5 shows that, with the increase of t, the total time increases linearly. However, the increase of t in DGS-AQCCIDAA is the slowest. To sum up, DGS-AQCCIDAA has lower calculation overhead than the schemes of Libert et al. (2016), Ling et al. (2017), and Li et al. (2019).

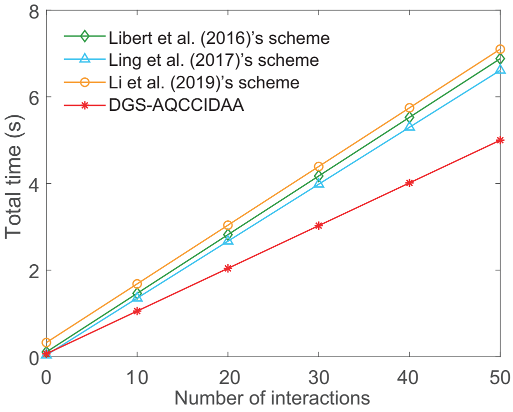

Fig. 5 Total time comparison among several schemes

8 Conclusions

We propose a security model based on DGS that is well adapted to cross-chain services and identity authentication. The scheme meets the identity authentication requirement of the application chain in a cross-chain system. In addition, DGS-AQCCIDAA has no frame attack because the private key of user i is a short vector $\boldsymbol{r}_i$ generated by a Gaussian sampling algorithm and the public key is $\boldsymbol{u}_i = \boldsymbol{F}\boldsymbol{r}_i \pmod q$ $(\boldsymbol{F}\leftarrow_R \mathbb{Z}_q^{m\times n})$. If the group manager or colluded group member wants to forge a signature for i, the group manager or colluded group member must generate a NIZKP π_2. Because of the reliability of π_2, the group manager or colluded group member does not know $\boldsymbol{r}_i$ and therefore cannot generate a π_2.

Contributors

Huifang YU designed the research. Huifang YU and Mengjie HUANG drafted and revised the paper.

Conflict of interest

Both authors declare that they have no conflict of interest.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

Bellare M, Neven G, 2006. Multi-signatures in the plain public-key model and a general forking lemma. Proc 13th ACM Conf on Computer and Communications Security, p.390-399. https://doi.org/10.1145/1180405.1180453

Boneh D, Shacham H, 2004. Group signatures with verifier-local revocation. Proc 11th ACM Conf on Computer and Communications Security, p.168-177. https://doi.org/10.1145/1030083.103010

Gordon DS, Katz J, Vaikuntanathan V, 2010. A group signature scheme from lattice assumptions. 16th Int Conf on the Theory and Application of Cryptology and Information Security on Advances in Cryptology, p.395-412. https://doi.org/10.1007/978-3-642-17373-8_23

He QW, Lin QX, Lin H, et al., 2023. Cross-chain-based medical data security sharing scheme. *Comput Syst Appl*, 32(5):97-104 (in Chinese). https://doi.org/10.15888/j.cnki.csa.009087

Laguillaumie F, Langlois A, Libert B, et al., 2013. Lattice-based group signatures with logarithmic signature size. 19th Int Conf on the Theory and Application of Cryptology and Information Security on Advances in Cryptology, p.41-61. https://doi.org/10.1007/978-3-642-42045-0_3

Langlois A, Ling S, Nguyen K, et al., 2014. Lattice-based group signature scheme with verifier-local revocation. Proc 17th Int Conf on Public Key Cryptography, p.345-361. https://doi.org/10.1007/978-3-642-54631-0_20

Li XL, Lv XL, Guo LJ, et al., 2019. A dynamic group signature scheme based on lattice for large groups. *J Univ Electron Sci Technol China*, 48(1):80-87 (in Chinese). https://doi.org/10.3969/j.issn.1001-0548.2019.01.014

Libert B, Ling S, Mouhartem F, et al., 2016. Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. 22nd Int Conf on the Theory and Application of Cryptology and Information Security on Advances in Cryptology, p.373-403. https://doi.org/10.1007/978-3-662-53890-6_13

Ling S, Nguyen K, Wang HX, et al., 2017. Lattice-based group signatures: achieving full dynamicity with ease. Proc 15th Int Conf on Applied Cryptography and Network Security, p.293-312. https://doi.org/10.1007/978-3-319-61204-1_15

Liu DY, Zhang JQ, Zhang X, et al., 2024. Cross-chain identity authentication scheme based on certificate-less signcryption. *J Comput Appl*, 44(12):3731-3740 (in Chinese). https://doi.org/10.11772/j.issn.1001-9081.2023121824

Ma ZF, Wang XC, Jain DK, et al., 2020. A blockchain-based trusted data management scheme in edge computing. *IEEE Trans Ind Inform*, 16(3):2013-2021. https://doi.org/10.1109/TII.2019.2933482

Nguyen PQ, Zhang J, Zhang ZF, 2015. Simpler efficient group signatures from lattices. 18th IACR Int Conf

on Practice and Theory in Public-Key Cryptography, p.401-426.
https://doi.org/10.1007/978-3-662-46447-2_18

Shao SS, Chen F, Xiao XY, et al., 2021. IBE-BCIOT: an IBE based cross-chain communication mechanism of blockchain in IoT. *World Wide Web*, 24(5):1665-1690.
https://doi.org/10.1007/s11280-021-00864-9

Wang SS, Ma ZF, Liu JW, et al., 2022a. Research and implementation of cross-chain security access and identity authentication scheme of blockchain. *Netinfo Secur*, 22(6):61-72 (in Chinese).
https://doi.org/10.3969/j.issn.1671-1122.2022.06.007

Wang SS, Dai BR, Zhu ML, et al., 2022b. User identity authentication model for cross-chain system. *Comput Eng Appl*, 58(19):135-141 (in Chinese).
https://doi.org/10.3778/j.issn.1002-8331.2107-0251

Yang C, Li JW, Li HW, et al., 2019. A research on heterogeneous identity alliance unified identity model. *Inform Secur Commun Secur*, (6):27-35 (in Chinese).
https://doi.org/10.3969/j.issn.1009-8054.2019.06.006

Yu HF, Bai XP, 2024. Identity-based searchable attribute signcryption in lattice for a blockchain-based medical system. *Front Inform Technol Electron Eng*, 25(3):461-471. https://doi.org/10.1631/FITEE.2300248

Yu HF, Mu WZ, 2024. ABE-based postquantum cross-blockchain data exchange approach for smart agriculture. *IEEE Trans Ind Inform*, 20(10):12083-12091.
https://doi.org/10.1109/TII.2024.3413684

Yu HF, Zhang Q, Li L, 2023. Certificateless anti-quantum blind signcryption for e-cash. *J Ind Inform Integr*, 40:100632. https://doi.org/10.1016/j.jii.2024.100632

Zhong T, Shi PC, Chang JS, 2021. JointCloud cross-chain verification model of decentralized identifiers. IEEE Int Performance, Computing, and Communications Conf, p.1-8.
https://doi.org/10.1109/IPCCC51483.2021.9679363