Huifang YU, Mengjie HUANG, 2025. Anti-quantum cross-chain identity authentication approach using dynamic group signature. *Frontiers of Information Technology & Electronic Engineering*, 26(5):742-752. https://doi.org/10.1631/FITEE.2400443

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

Key words: Cross-chain; Identity authentication; Dynamic group signature (DGS); Anti-quantum security; Zero-knowledge proof

Corresponding author: Huifang YU
E-mail: yuhuifang@xupt.edu.cn
ORCID: https://orcid.org/0000-0003-4711-3128

Motivation

1. Blockchain technology is used to construct a trusted system because of its decentralization and anti-tampering. Each blockchain is independent with no unified identity management system, so there exists the identity island problem. It is a vital problem to provide a unified identity for different blockchains and protecting user information.

2. Lattice-based group signature can be used to construct anonymous authentication protocols because of its anonymity, traceability, and anti-quantum security. Lattice-based group signature can not only protect the identity privacy of users but also resist quantum computing in the smart education filed.

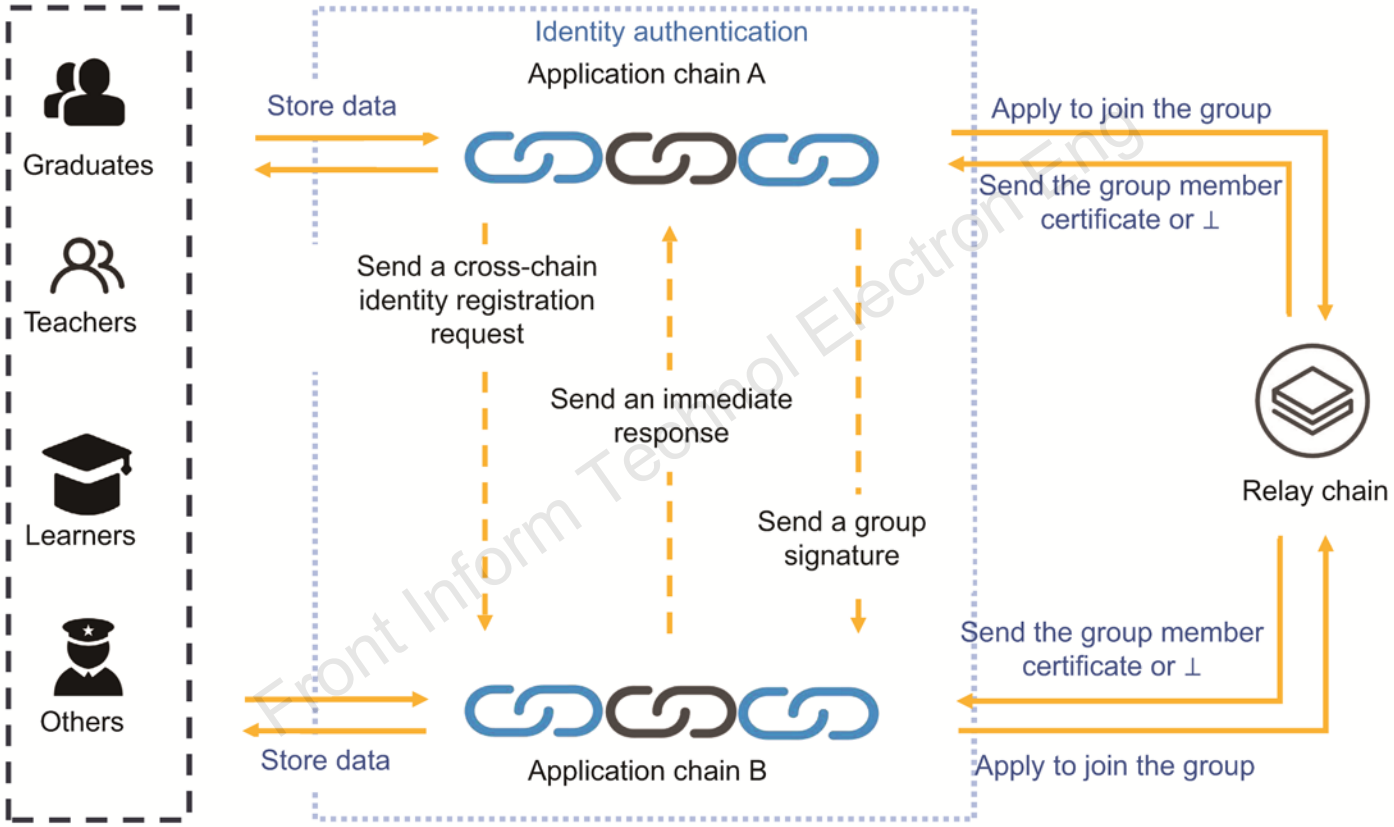
Main idea

1. To protect the identity privacy of users and resist quantum computing in the smart education field, we propose an anti-quantum cross-chain identity authentication approach based on dynamic group signature (DGS-AQCCIDAA).

2. Group signature and relay architecture are used to realize anonymous identity authentication and protect the identity privacy of users in a cross-chain authentication process.

3. DGS-AQCCIDAA allows the relay chain administrator nodes to open the signature to trace the signer and ensures that the anonymity is not abused.

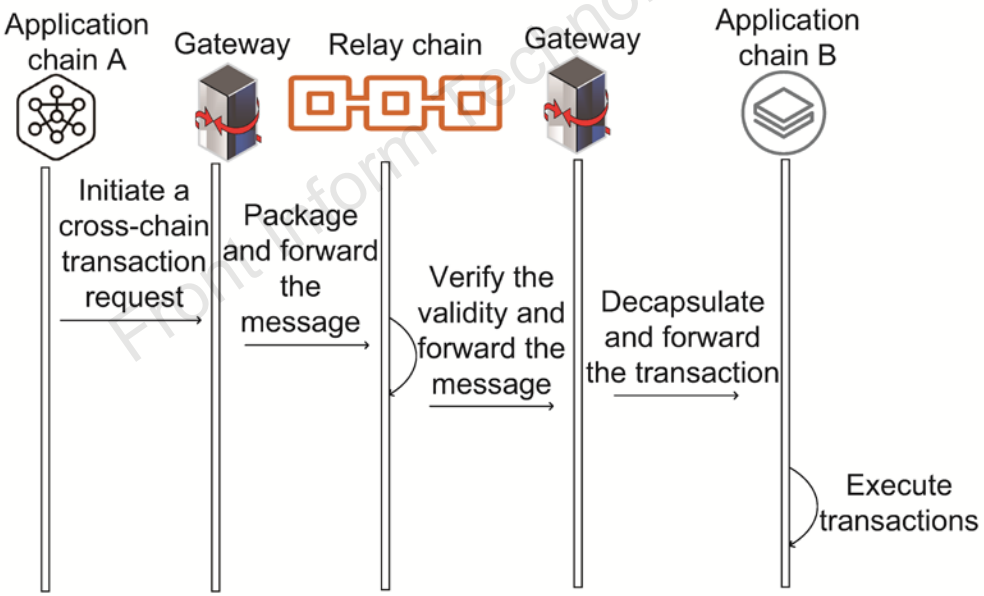
Framework



Cross-chain identity authentication framework in smart education

Method

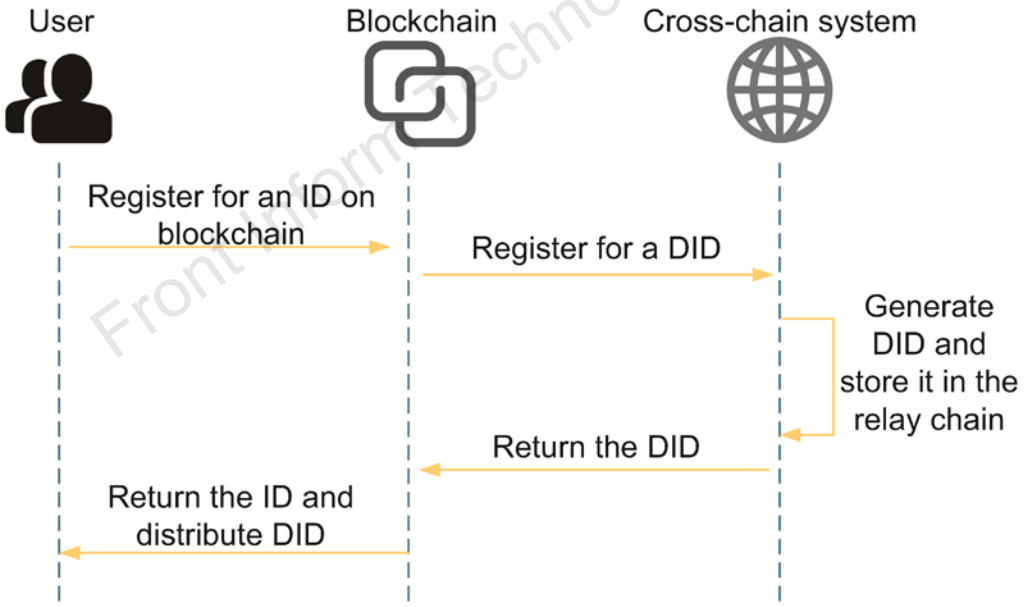
1. To improve the decentralization of a cross-chain system, we use the relay architecture to implement cross-chain interactions. The cross-chain system model consists of a relay chain, an application chain, and a cross-chain gateway.



Architecture of the cross-chain system model

Method

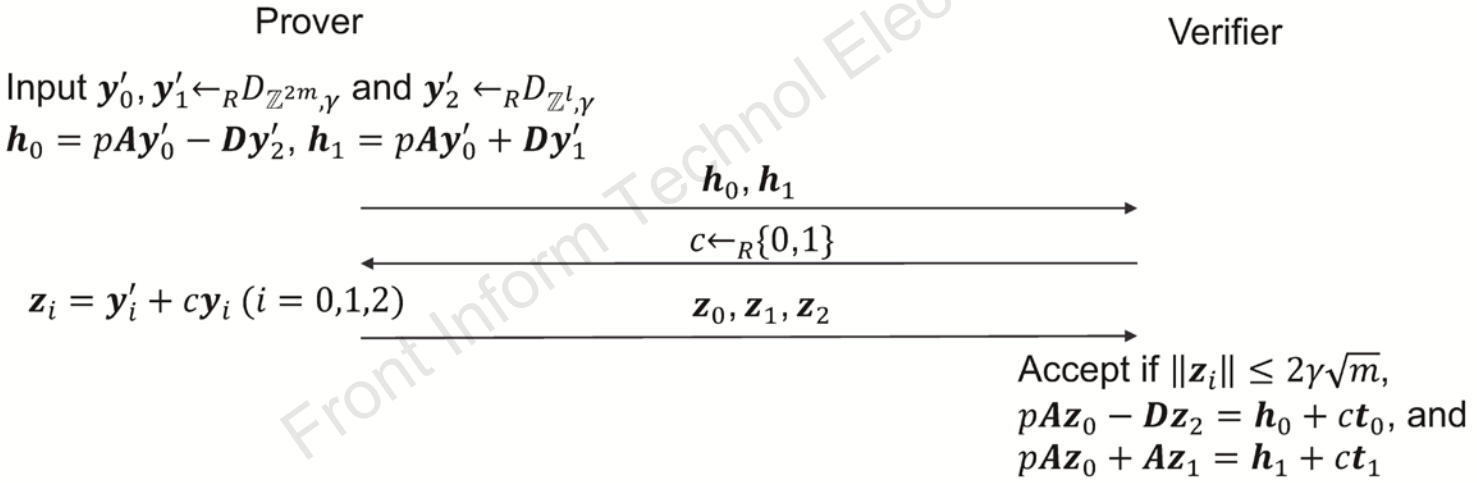
2. To achieve a unified management of users' identities in the cross-chain process, a cross-chain identity registration model is provided as follows. The application chain can participate in the cross-chain process after obtaining the digital identifier (DID).



Registration process of a cross-chain DID

Method

3. To protect the privacy of users' identities, lattice-based group signature is constructed to realize the identity authentication, which is based mainly on non-interactive zero-knowledge proof.



Zero-knowledge proof with a single-bit challenge

Major results

Table 4 Performance comparison among several schemes

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

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	×	✓	✓	✓	✓

Conclusions

1. The anti-quantum cross-chain identity authentication approach from dynamic group signature can protect the identity privacy of users and resist quantum computing in smart education.

2. The relay-based cross-chain model can promote interconnection between heterogeneous consortium blockchains. Because the relay architecture is easily scalable and the signature size of group signature is independent of the number of groups, our scheme can realize cross-chain identity authentication between different blockchains.