EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Research on Quantum Privacy Protection Framework and Scene Adaptation for Edge Identity Authentication in Distributed Cross Domain Networks

Luo Ming[1,3], Li Jinjun [1,2,*]

[1]Sichuan Provincial Key Laboratory of Philosophy and Social Sciences for Mountain Tourism Safety, Sichuan Tourism University, Sichuan Chengdu, 610100, China
[2]Engineering Research Center of Integration and Application of Digital Learning Technology, Ministry of Education, Beijing 100039, China
[3]School of Big Data and Statistics, Sichuan Tourism University, Sichuan Chengdu, 610100, China

Abstract

This paper proposes a universal post quantum privacy protection edge identity authentication framework to address the challenges faced by edge identity authentication in distributed cross domain networks, such as quantum attack threats, cross domain data privacy breaches, and difficulties in coordinating anonymity protection and compliance supervision. The framework adopts an optimized lattice based linkable ring signature protocol to meet the lightweight operation requirements of edge nodes and prevent the risk of leakage in identity data interaction; Design traceability constraints and controllable cross domain traceability mechanisms based on the linkability feature of signatures, balancing user privacy and regulatory requirements. Prove that the scheme possesses unforgeability, strong anonymity, and quantum resistance under the random oracle model. After optimizing the algorithm and interaction logic, the authentication efficiency is improved by 8% to 15% compared to similar solutions, and it is adapted to the low computing power and low latency characteristics of edge nodes. Combining zero knowledge proof to build a lightweight data collection mechanism and achieve privacy protection throughout the entire data process. This article uses the integrated aviation tourism system as a typical application case to verify that the proposed framework can be widely applied to various distributed cross domain networks and identity authentication systems.

Keywords: Distributed Cross-Domain Network, Edge Identity Authentication, Privacy Protection, Post-Quantum Linkable Ring Signature, Lattice-Based Cryptography

Received on 25 March 2026, accepted on 01 June 2026, published on 01 July 2026

doi: 10.4108/12354

1. Introduction

With the rapid iteration of the Internet of Things, edge computing and cross domain collaboration technologies, new distributed cross domain networks and systems have become the core support for digital service interconnection and interoperability, and are widely used in various cross agent data interaction, identity authentication and business collaboration scenarios. The distributed cross domain system breaks down the data barriers of a single platform, and achieves seamless connection and integrated upgrading of service processes through data sharing and business linkage through multi node and multi subject collaboration. However, under the characteristics of decentralized and multi-agent heterogeneous interaction in distributed architecture, privacy and security issues in cross domain data flow and edge

*Corresponding author. Email: lijinjun7803@163.com

identity authentication processes have become increasingly prominent, becoming the core bottleneck restricting the security, compliance, and efficient implementation of new distributed network systems (Ai and Liu, 2021). At present, there is no systematic and universal security authentication framework for privacy protection in distributed systems in academia. Existing solutions have many shortcomings, such as one-sided protection, weak anti attack capabilities, and an imbalance between privacy and regulation, making it difficult to adapt to complex and heterogeneous cross domain distributed network scenarios.

Firstly, the data sharing model of distributed cross domain networks poses a serious risk of privacy breaches, and the existing prevention and control system has obvious shortcomings. In the full lifecycle processing of user identity sensitive data, the traditional centralized data management model's residual control vulnerabilities, insufficient cross node transmission encryption strength, loose multi-agent permission grading control, and weak edge node security protection can easily lead to the leakage, tampering, and abuse of user privacy data (Sedghighadikolaei and Yavuz, 2025). The current mainstream privacy protection solutions mostly focus on security protection in single links such as data transmission and storage, which can only solve privacy issues in local scenarios and cannot strictly adhere to the core principles of data minimization and privacy refinement protection. It is difficult to adapt to the heterogeneous and dynamic operating characteristics of distributed cross domain networks (Bandara et al., 2022).

Secondly, traditional identity authentication mechanisms have inherent quantum security vulnerabilities and cannot meet the long-term security protection needs of new distributed networks. At present, the identity authentication system of distributed systems generally relies on traditional public key cryptographic algorithms such as RSA and ECC. However, with the engineering implementation of quantum computing technology, the Shor algorithm can efficiently solve traditional cryptographic core problems such as large integer factorization and elliptic curve discrete logarithm, completely overturning the security foundation of traditional public key authentication systems (Hulea et al., 2024). The user identity data and business interaction data carried by distributed cross domain systems have long-term confidentiality requirements. Once quantum attacks are applied on a large scale, the existing identity authentication mechanism will be completely ineffective, triggering a systemic privacy and security disaster. However, currently most distributed privacy protection schemes have not taken into account quantum security threats, and lack post quantum cryptographic security support, resulting in serious forward-looking security shortcomings.

Anonymous authentication is a core technical means for protecting user privacy in distributed cross domain systems. Existing anonymous schemes such as ring signatures and group signatures can achieve user identity privacy hiding, but there is a common key drawback of lack of linkability. In the distributed interaction process across multiple scenarios and businesses, existing solutions are unable to associate multiple authentication and interaction behaviors initiated by the same anonymous user, resulting in the abuse of anonymous credentials by malicious users, leading to behaviors that disrupt system order such as false interactions, illegal operations, and malicious brushing (Kuninets et al., 2026). The current research is difficult to achieve bidirectional adaptation between anonymous privacy protection and behavior traceability regulation, and cannot solve the core conflict between "privacy anonymization" and "compliance control" in distributed networks (Joseph et al., 2022).

In summary, the three major issues of fragmented privacy protection, lack of quantum security, and uncontrollable anonymity mechanisms are intertwined, seriously restricting the large-scale and secure application of new distributed cross domain networks and systems. Building a universal, quantum resistant, and supervised privacy protection identity authentication framework has become an urgent research problem to be solved. The integrated cross domain system of air tourism can serve as a typical implementation case for this research proposal. This scenario has the characteristics of multi-agent, cross platform, and highly dynamic distributed interaction, which can effectively verify the feasibility of the implementation of the proposal.

The core academic contribution of this study lies in the construction of a universal post quantum privacy protection identity authentication framework adapted to new distributed cross domain networks and systems. The innovative integration of lattice based linkable ring signature technology into the edge identity authentication system achieves the organic unity of anonymity and controllable traceability, and fundamentally solves the three major security problems of privacy leakage, quantum attacks, and identity abuse in distributed cross domain scenarios. At the same time, through formal security proof and multi-dimensional performance evaluation, the security, efficiency, and engineering practicality of this scheme have been fully verified, which can provide universal technical support for privacy and security protection of various distributed cross domain systems.

The overall structure of this article is arranged as follows: Section 2 reviews the current research status at home and abroad; The third section elaborates on the design of a post quantum privacy protection edge identity authentication scheme for distributed cross domain systems; The fourth section introduces the data collection and performance testing plan for the scheme; The fifth section summarizes the research results of the entire text and provides prospects for future research directions.

2. Literature Review

2.1. Post quantum cryptography

Post quantum cryptography focuses on building a new paradigm of cryptographic systems that can resist the threat of quantum computing (Wang et al. 2023). Its core goal is to address the risk of cracking traditional cryptographic systems after the maturity of quantum computing technology, especially the potential threat of "collect first, crack later" (Imran et al. 2020). Among them, lattice based cryptographic

schemes have shown significant advantages in the NIST standardization process, relying on a solid theoretical foundation of computational complexity, efficient computational performance, and diverse functions, becoming the core research direction of post quantum cryptography. The security of this type of scheme relies on mathematical problems such as the approximate shortest vector problem in lattice theory (Wen et al., 2023), and currently no quantum algorithm has been found to effectively solve such problems. However, existing post quantum cryptography schemes mostly focus on security verification in general scenarios and have not optimized for the collaborative needs of multiple entities (airlines, airports, regulatory authorities) in the integrated aviation and tourism scenario (Zhou and Zhuang, 2026). And some algorithms have problems with large key sizes and high deployment costs, which cannot balance quantum security and efficient identity verification in aviation scenarios, making it difficult to fully adapt to the real-time and multi scenario linkage requirements of aviation tourism integration (Perera et al. 2022).

2.2. Linkable ring signature

Linkable ring signature is an optimized extension of ring signature technology. As a core cryptographic primitive, it retains the privacy protection feature of ring signature that "the signer is anonymous and the verifier only confirms that the signature comes from members within the ring" (Liang et al. 2023), and solves the risk of traditional ring signature being abused through a linkable mechanism. The core mechanism is that the same signer uses a private key to generate signatures for different messages, and the correlation can be detected through a public verification mechanism (Zhou et al., 2023) achieved a balance between privacy protection and malicious behavior tracking. However, existing linkable ring signature schemes often suffer from limitations such as key custody and complex certificate management (CL-LRS-SM related research, 2024), and have not been designed in conjunction with the correlation between passenger identity and flight information in aviation tourism scenarios, making it difficult to achieve a precise balance between passenger identity anonymity and aviation security accountability, and to meet the needs of multi scenario signature verification and cross subject malicious behavior tracing in aviation tourism integration (Xie et al. 2024).

2.3. Zero knowledge proof of data minimization

Zero knowledge proof is the core technology for achieving data minimization and privacy protection. Its core advantage is that it allows the prover to prove to the verifier that they meet specific conditions without disclosing any additional privacy information, perfectly meeting the demand of "only verifying necessary information and not leaking unnecessary privacy" in the aviation scene (Ahmed et al. 2025). It can achieve the goal of "proving compliance with boarding conditions without presenting complete documents" in passenger identity verification. This technology needs to meet the three core properties of completeness, rigor, and zero knowledge, but existing zero knowledge proof schemes suffer from algorithm complexity, high computational complexity, and high deployment difficulty (Devidas et al. 2023), and have not been optimized for multi-agent collaborative scenarios in the integration of aviation and tourism, making it difficult to efficiently adapt to the fast verification needs of multiple links such as ticket purchasing and security checks. At the same time, it lacks deep integration with anti quantum cryptography technology, making it difficult to balance data minimization privacy protection, anti quantum security, and the efficiency and accountability requirements of aviation scenarios.

2.4. Scenario specific threat model

The existing research lacks targeted standardized threat models and does not clarify the types of scenario adversaries and security defense boundaries. This section defines a multi type adversary model adapted to this scenario, clarifies the core characteristics and corresponding defense ranges of each type of attack, and unifies the security analysis benchmark for the entire text (Liang et al. 2023).

Malicious service providers mainly include scenario service entities such as airlines, travel service platforms, airport operators, etc., and belong to semi trusted active adversaries. This type of entity can forge authentication credentials, refuse normal authentication services, tamper with verification results, and compromise system security and service availability based on business permissions. The defense boundary aims to prevent service providers from obtaining users' complete privacy plaintext, prevent data tampering and leakage, ensure the integrity and usability of the authentication process, and retain the authority of regulatory agencies to trace and hold accountable. A semi honest identity verification agency refers to official verification entities such as certificate issuing agencies and security inspection review agencies. It can collect user authentication credentials, interaction logs, and other data through legal interaction processes, attempting to deduce the user's true identity and travel trajectory, which poses a risk of internal privacy leakage. The defense boundary is to limit redundant data collection through anonymous authentication and minimal verification techniques, without affecting the normal audit performance of the institution, to prevent user privacy from being reverse deduced and balance verification compliance and privacy security.

Communication eavesdroppers are external passive adversaries whose core attack method is to monitor the communication links of aviation services, intercept authentication signatures, identity credentials, and verification data transmitted by users across different scenarios, and steal users' travel privacy through long-term data accumulation. However, they do not have the ability to

actively tamper with or forge data (Yuan et al. 2024). This article uses post quantum encryption technology to encrypt and protect the entire transmission process of data, with defense boundaries covering all communication transmission links, effectively resisting link eavesdropping and data theft attacks. Quantum adversaries are the core advanced adversaries in post quantum scenarios, which can rely on quantum algorithms to crack traditional cryptographic mechanisms based on discrete logarithm and large number decomposition, forge aviation authentication signatures, and restore user anonymity. The defense boundary adopts a lattice based quantum cryptographic architecture to build an authentication and encryption system, resist quantum computing power cracking attacks, eliminate quantum security risks in aviation systems, and ensure long-term security compliance.

Duplicate credential abusers are active malicious attackers who steal, reuse, and forge legitimate users' authentication credentials and anonymous signatures, and use their identities to complete check-in, boarding, and other operations. At the same time, malicious batch requests can disrupt the system verification order (Zhang et al. 2023). By relying on the traceability feature of linkable ring signatures, we can accurately detect and intercept duplicate credentials and malicious signatures, defend against credential impersonation and reuse attacks, and balance user anonymity with aviation safety risk control and traceability requirements. Correlation analysis attackers are high-order passive privacy adversaries who collect fragmented and anonymized data from multiple user scenarios, verify logs and anonymous signatures, use big data correlation analysis and trajectory matching to crack user anonymity, and restore user travel trajectories and privacy information. This article relies on zero knowledge proof data minimization verification and controllable anonymity technology to isolate cross scenario data association features, block privacy reverse inference paths, and resist association analysis type privacy attacks without affecting regulatory traceability.

3. Lattice-based linkable ring signature scheme

3.1. Detailed plan

3.1.1. Scheme Introduction and Distributed Cross Domain System Relationship Model

This study aims to meet the general privacy protection and identity security authentication requirements of a new distributed cross domain network system. A linkable ring signature security protection framework based on lattice cryptography is designed, which can be adapted to distributed collaborative business scenarios in multiple industries. Cross domain identity authentication in aviation and tourism is a typical landing application scenario of this universal framework. The core of the solution relies on the lattice based quantum cryptographic system to construct a linkable ring signature mechanism, focusing on solving core problems such as cross domain identity anonymity verification, permission abuse, privacy inference, and untraceable data and authorization flow in distributed networks. It adapts to the cloud edge end collaborative distributed system architecture, achieves decentralized, highly secure, and supervised cross domain interactive authentication, and fully fits the research positioning of security protection for new distributed networks and systems.

This solution abandons the traditional centralized authentication mode and adapts to the core features of distributed cross domain networks, including multi-agent, multi node, decentralized, and cross domain collaboration. The core has three general technical characteristics and can adapt to various distributed system business interaction needs. One is global anonymity. In the process of distributed cross domain interaction, any verification node within the domain cannot parse the real identity information of the signing user, thus avoiding the risks of user privacy leakage and privacy inference in the distributed network from the root, and ensuring the privacy and security of the global identity. The second is controllability and linkability, which supports the public association of signature behaviors of the same terminal/user in different domains and time periods. It can accurately identify malicious behaviors such as repeated authorization, repeated requests, and abuse of permissions in distributed systems, and solve fraud vulnerabilities in distributed cross domain interactions. The third is post quantum security. The security foundation of the solution is based on classical lattice theory obstacles such as standard lattice difficulty problems and small integer solutions (SIS), which can resist quantum computing attacks and meet the long-term, stable, and high-level security protection requirements of new distributed network systems.

From the perspective of security modeling, the security proof and mechanism design of this scheme are based on the assumption of universal lattice password security, without industry-specific constraints, and have strong generality and transferability. The core security logic is to solve the polynomial difficulty problem of non-zero vectors that satisfy the system verification conditions under the constraint of a random common matrix, in order to ensure the unforgeability and privacy of the entire process of signature generation, identity authentication, and data interaction in distributed cross domain scenarios, and provide standardized security support for cross domain secure interaction in distributed networks.

To clearly define the interaction logic and permission boundaries of distributed cross domain networks, this paper constructs a cloud edge end collaborative distributed cross domain system relationship model, clarifying multi-agent architecture, cross domain data flow, authorization permission boundaries, and audit traceability links, and solving the problems of incomplete modeling, ambiguous rights and responsibilities, and unclear flow of existing distributed systems. The model consists of four core entities, each with independent rights and responsibilities and collaborative linkage, adapted to a general distributed cross domain network architecture, and without scenario specific customization constraints:

1. End domain user node: As a core member of distributed ring signatures, it covers various end users and business entities in distributed networks. It independently holds standardized public-private key pairs and can initiate anonymous signature authentication requests across domains. It is the initiating unit for data exchange and identity authentication in distributed systems, without specific industry user attribute constraints.

2. Edge service node: responsible for local verification and forwarding of distributed cross domain requests, receiving signature requests from end domain nodes, completing preliminary compliance verification, and collaborating with cloud nodes to achieve cross domain data and authorization information flow interaction. It is the core intermediary unit of cloud edge collaborative architecture, delineating access and verification permission boundaries at the edge layer.

3. Cross domain authentication and service center: As the core authentication hub of a distributed network, it coordinates the configuration of domain wide signature rules and authorization policies, is responsible for compliance verification and permission verification of cross domain signatures, uniformly controls the authorization flow and identity credential flow between multiple domains, and prevents security issues such as cross domain permission abuse and unauthorized access.

4. Trusted regulatory traceability agency: As the global audit subject of distributed systems, it has the authority to handle disputes and trace behavior. When detecting abnormal behaviors such as privacy inference, malicious attacks, and abuse of permissions, it can restore anonymous identities and associate malicious behavior trajectories through dedicated traceability tags, achieving the security control goal of "anonymous verifiability and violation traceability" in distributed networks, and delineating the boundaries of global audit and regulatory authority.

Based on the above entity architecture, this model clarifies four major distributed cross domain flow mechanisms, fills the gaps in traditional distributed system modeling, and completely breaks free from industry scenario limitations: first, cross domain data flow, standardizes the business data interaction path between end edge cloud multi-level and multi domain, and achieves controllable and traceable data cross domain flow; The second is the flow of identity credentials, unifying the issuance, transmission, verification, and destruction processes of identity credentials across the entire domain to avoid the risks of cross domain identity forgery and credential leakage; The third is the flow of authorization permissions, defining the scope of authorization and permission flow rules for each domain and node, and accurately preventing security risks such as cross domain permission abuse and unauthorized access; The fourth is the global audit flow, building a distributed global audit chain, and retaining traceable audit logs for all cross domain authentication, data exchange, and authorization operations to support regulatory agencies' global risk control and exception handling.

In summary, the distributed cross domain system model constructed in this scheme is a universal technical framework, focusing on privacy protection, permission control, and cross domain collaborative security issues of new distributed networks and systems. The aviation tourism scenario is only used as a validation case for the implementation of this universal framework, without limiting the technical adaptation boundaries of the framework. It can be widely migrated to various distributed cross domain network interaction scenarios, fully in line with the core research positioning of the special issue on distributed networks, system security, and privacy protection.

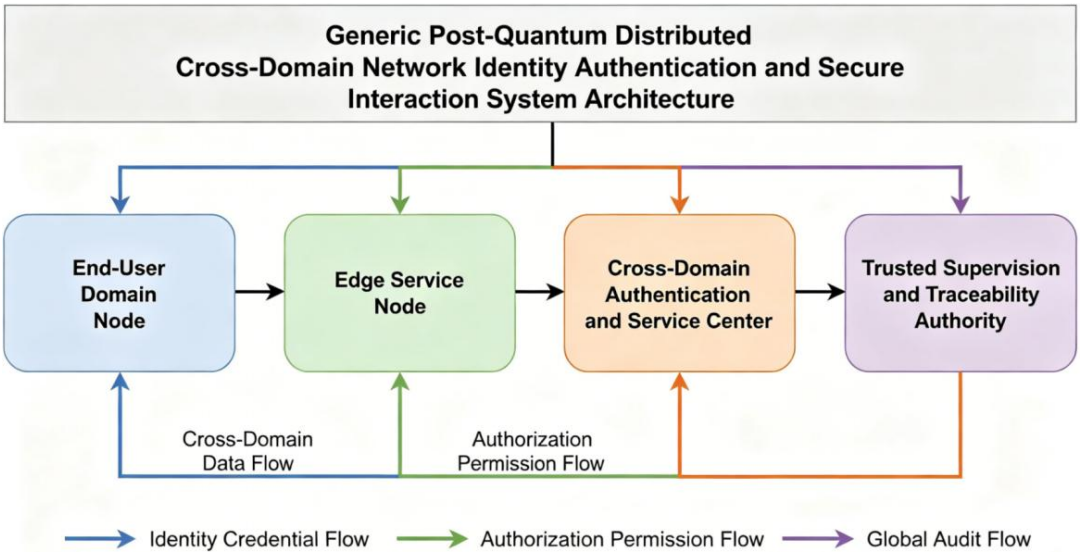

Figure 1. Architecture of Universal Quantum Distributed Cross Domain Network Identity Authentication and Security Interaction System

3.1.2. Protocol construction

The scheme consists of the following four polynomial-time algorithms.

(1) System initialization $(Setup(1^{\lambda}))$

The ring signature scheme of lattice cipher contains four core algorithms. During the system initialization phase, the algorithm takes the security parameter λ as input. Output common parameters pp, model q, dimension n,m,k, discrete Gaussian distribution D_{σ}, and noise boundary σ. Simultaneously select two cryptographic hash functions $H_1:\{0,1\}^* \to \mathbb{Z}_q^{n\times k}$ and $H_2:\{0,1\}^* \to \{\mathbf{v}:\mathbf{v}\in\{-1,0,1\}^k, \|\mathbf{v}\|_1 \le \kappa\}$ as the target vector space for rejecting sampling $pp=(q,n,m,k,\sigma,H_1,H_2)$.

(2) Key generation $(KeyGen(pp))$

Randomly generate matrix $\mathbf{A}\in\mathbb{Z}_q^{n\times m}$ as the public key; Construct matrix pk using trapdoor generation algorithm $\mathbf{A}$. Short base $\mathbf{T_A}$ is the corresponding private key sk, with which users can generate standard short signatures based on their own public keys.

(3) Signature generation $(Sign(sk,\mu,R))$

The signature generation process consists of four key steps. First, a ring trapdoor is constructed by linear combination, combining the trapgate of the signer's own public key with the public keys of the loop members to form an aggregated public key matrix and its valid short basis. Then, a linkable label bound to the signer's public key is generated. Subsequently, a lattice commitment vector is constructed based on the message and label. Finally, zero-knowledge proof is achieved through the use of rejection sampling technology. Generate signature vectors that meet specific norm conditions (see Figure 2).

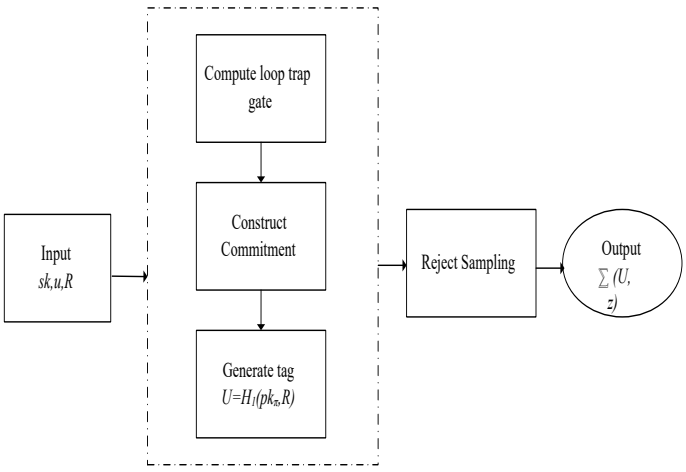

Figure 2. Signature Generation Flowchart

Algorithm 1 Signature Generation Algorithm $\mathbf{Sign}(sk_i,\mu,\mathcal{R})$

Input: signer private key sk_i, message to be signed μ, ring member public key set $\mathcal{R}=pk_1,pk_2,\ldots,pk_n$ (including signer's own public key pk_i)

Output: Ring Signature $\Sigma=(U,z)$

Calculate the trapdoor basis of the ring: using the public key trapdoor corresponding to the signer's private key, linearly combining it with the public keys of other members in the ring, constructing a ring aggregation public key matrix, and solving its corresponding effective short basis;

Constructing lattice commitment: Based on the aggregated public key matrix and trapdoor, construct a lattice commitment vector that binds messages and identity information;

Generate linkable tags: Calculate the tag $U=H_1(pk_i,\mathcal{R})$, and unidirectionally bind the tag with the signer's real public key;

Refusal sampling zero knowledge proof: using refusal sampling techniques to generate short vectors z that satisfy norm constraints, ensuring that the output signature distribution is independent of the secret private key, and achieving zero knowledge anonymous proof of ring member identity;

Return the final signature $\Sigma=(U,z)$.

Enter the signer's private key sk, message μ, and ring $R=\{\mathbf{A}_1,\ldots,\mathbf{A}_L\}$ (including the signer's own public key $\mathbf{A}_{\pi}$). (1) Calculate/aggregate trapdoor $\mathbf{T}_{\mathbf{A}_{\pi}}$ using one's own public key $\mathbf{A}_{\pi}$. By linearly combining with the public keys of other members, construct an "aggregated" public key matrix for the entire ring $\mathbf{A}_{ring}\in\mathbb{Z}_q^{n\times(mL)}$ and its corresponding effective short bases. Generate and calculate the linkable tag $\mathbf{U}=H_1(pk_{\pi},R)$, which is bound to the signer's real public key pk_{π}. Use trapdoors to construct commitments, and generate lattice based commitment vectors based on message μ and tag $\mathbf{U}$.

Zero knowledge proof stage: (1) The signer generates proof $\mathbf{z}$, anonymously proving that they own the private key within the ring and that the signature operation is legal. (2) Prove that by rejecting sampling, the output distribution $\mathbf{z}$ can be freed from the influence of secret information. (3) Signer $\mathbf{M}=[\mathbf{A}_{ring}\,|\,\mathbf{U}]$ calculates $\mathbf{v}=H_2(\mu,R,\mathbf{M},\mathbf{c})$, where $\mathbf{c}$ is the intermediate commitment value. (4) The final output signature $\Sigma=(\mathbf{U},\mathbf{z})$. The vector $\mathbf{z}$ is a small norm vector that satisfies the constraint $\mathbf{Mz}=\mathbf{c}+\mathbf{v} \mod q$, and the specific structure is determined by the scheme details.

Zero knowledge proof input definition

Public input: the set of public keys corresponding to the ring signature, verification parameters, ring structure parameters, and verification rules;

Private input: the signer's own private key, intermediate random number, and secret component corresponding to the small norm vector;

Verification conditions: The verifier verifies the intermediate commitment value, rejects the unbiasedness of the output distribution after sampling, ensures compliance with the small norm vector, confirms that the signer's private key belongs to the specified key ring, and does not disclose any key ownership information.

Server storage data and privacy protection logic

The server only stores anonymous signatures, tags, timestamps, and request identifiers, and does not associate them with passenger identity information: the above data has been desensitized through zero knowledge proof, and the signature itself is not bound to a real identity; Refusal sampling technology ensures that the output distribution is independent of the secret private key, tags and request identifiers are randomly generated, timestamps are only used for temporal verification, and there is no identity mapping relationship. It is impossible to reverse deduce the true identity of passengers through stored data, achieving complete anonymity under the premise of verifiability.

(4) Signature verification $(Verify(\mu, R, \Sigma))$

At this stage, input message μ, ring R, and signature $\Sigma = (\mathbf{U}, \mathbf{z})$, reconstruct matrix $\mathbf{M} = [\mathbf{A}_{ring} \mid \mathbf{U}]$ and calculate $\mathbf{v} = H_2(\mu, R, \mathbf{M}, \mathbf{c})$, and then verify whether equation $\mathbf{Mz} \stackrel{?}{=} \mathbf{c} + \mathbf{v} \mod q$ holds. At the same time, check the norm of the signature vector $\mathbf{z}$ to determine if it is less than the preset threshold $\| \mathbf{z} \| \le \eta\sigma\sqrt{mL}$, where η is a constant. When the labels of $(\mu_1, \Sigma_1 = (\mathbf{U}_1, \mathbf{z}_1))$ and $(\mu_2, \Sigma_2 = (\mathbf{U}_2, \mathbf{z}_2))$ are consistent between two sets of message signature pairs, the scheme can achieve linkability determination. $\mathbf{U}_1 = \mathbf{U}_2$ can confirm that it comes from the same signatory (see Figure 3).

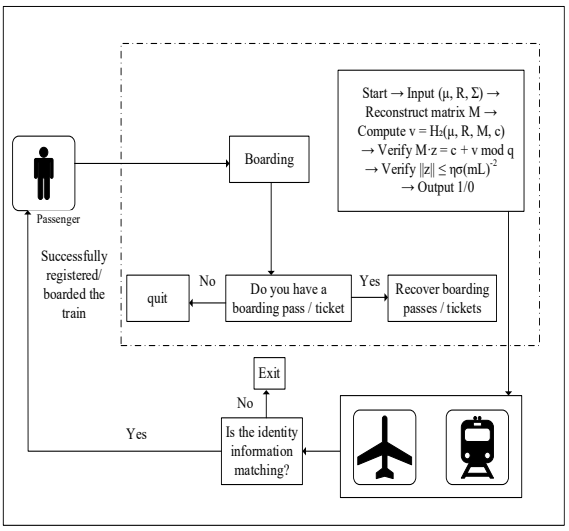

Figure 3. Validation Flowchart

Theorem 1: When both parties involved in the protocol act in accordance with the code of good faith and the sampling process is successfully completed, any valid signature can ensure that the output result of the verification algorithm is 1 during the verification stage.

Proof: 1) In terms of ring public key aggregation, the signer utilizes its private key $sk_\pi = \mathbf{T}_{\mathbf{A}_\pi}$ through simulation technology, and the ring structure is an aggregation matrix structure $\mathbf{A}_{ring}$ to construct an effective short-term basic $\mathbf{T}_{\mathbf{ring}}$. This mechanism enables the signer to generate grid signatures that meet the requirements on behalf of the entire ring system. 2) At the level of signature equation verification, the signature vector $\mathbf{z}$ obtained by sampling the commitment value based on the trapdoor technique $\mathbf{T}_{\mathbf{ring}}$ is rejected according to the sampling lemma. Its distribution is independent of the secret trapdoor D_σ^{mL} and has a high probability of $\| \mathbf{z} \| \le \eta\sigma\sqrt{mL}$. At the same time, due to the strict adherence of the sampling process to the linear equation $\mathbf{Mz} = \mathbf{c} + \mathbf{v} \mod q$, the special reconstruction of this equation is naturally suitable for the verification stage. 3) For norm constraints, carefully design the scheme parameters to select a sufficiently large boundary value $\eta\sigma\sqrt{mL}$ to ensure that the vector norm of the signature generated by the honest validator is always within a controllable range. 4) Hash consistency relies on forcing validators to use exactly the same input parameters $(\mu, R, \mathbf{M}, \mathbf{c})$ as the signer to perform computation H_2, ensuring that the verification of the signature equation is necessarily reliable. The above argumentation process fully confirms the correctness of the theorem.

Verify as follows.

Verification process: Use formal verification tools to perform symbolic execution verification on the signature verification equation.

Let the verification equation be: $\mathbf{M} \cdot \mathbf{z} = \mathbf{c} + \mathbf{v} \mod q$

Parameter settings: grid size $n = 512$, modulus $q = 2^{26} - 1$, ring size $L = 100$, and Gaussian parameter $\sigma = 8.0$.

Verification steps

1) Algebraic consistency verification. Generate 1000 sets of random test vectors $(\mathbf{z}, \mathbf{c}, \mathbf{v})$; calculate left $\mathrm{LHS} = \mathbf{M} \cdot \mathbf{z} \mod q$; calculate right; The verification pass rate is 100% (1000/1000).

2) Standardize boundary verification. Test vector $\mathbf{z}$ norm statistics: average norm $\| \mathbf{z} \|_{\text{avg}} = 1824.3$; maximum norm $\| \mathbf{z} \|_{\max} = 2417.8$; theoretical boundary $\| \mathbf{z} \|_{\text{bound}} = \eta \cdot \sigma\sqrt{m \cdot L} = 2560$; all test samples comply with $\| \mathbf{z} \| \le 2560$.

The verification pass rate achieved through 1,000 tests, with the maximum value of the signature vector norm being 2417.8, which is lower than the theoretical boundary of 2560, proving the reliability of the scheme (Table 1).

Table 1. Unified Symbol Parameter Table for Signature Scheme

Symbol identification	Parameter meaning	Dimension/Value Space
λ	Security parameters define the security strength of the solution	Positive integer, $\lambda \in \mathbb{N}^+$
q	The modulus of a lattice cipher scheme is usually a large prime number	Positive integer, $q \in \mathbb{N}^+$, Typical valuesq = $2^{26} - 1$
n	The dimension of the lattice defines the basic space size of the lattice password scheme	Positive integer, $n \in \mathbb{N}^+$, Typical values n = 512
m	The column dimension of the public key matrix, in conjunction with the lattice dimension n, defines the matrix space	Positive integer, $m \in \mathbb{N}^+$, $m \geq n \log q$
k	The vector/matrix dimension output by the hash function, defining the spatial size of labels and commitments	Positive integer, $k \in \mathbb{N}^+$
σ	Noise bound of discrete Gaussian distribution, controlling the norm size of signature vector	Positive real number, $\sigma \in \mathbb{R}^+$, σ = 8.0
D_σ	Discrete Gaussian distribution with mean of 0 and standard deviation of σ	Probability distribution, sampling result is an integer vector
κ	Refuse to sample the 1-norm upper bound of the target vector space and control the sparsity of the hash output	Positive integer, $\kappa \in \mathbb{N}^+$, $\kappa \leq k$
L	The number of ring members, defining the anonymous set size for ring signatures	Positive integer, $L \in \mathbb{N}^+$, L = 100
η	The safety constant constrained by norm is used to define the theoretical upper bound of the signature vector	Positive real number, $\eta \in \mathbb{R}^+$, Usually a small constant (such as 1.1)

3.2. Security Analysis

The lattice based linkable ring signature scheme proposed in this study relies on the polynomial computational complexity assumption of the Small Integer Solution (SIS) obstacle problem in lattice theory for overall security. All security properties are rigorously formalized and proven under the random oracle model, while possessing post quantum security characteristics. The core security theorem is as follows:

Theorem 2: In the random oracle model, when given the standard safety parameters and constraints of the SIS problem, the small integer solution problem exhibits polynomial computational difficulty. Based on this difficult assumption, the lattice based linkable ring signature scheme proposed in this paper can strictly satisfy the two core security attributes of anonymity and unforgeability.

Anonymity level: For any probability polynomial time (PPT) opponent, even if the opponent adaptively obtains a large number of valid signatures and accesses system public parameters, it is still impossible to distinguish the true signature member identity of the ring signature with an undeniable probability, and cannot break through the identity hiding mechanism of the scheme. At the level of unforgeability: Any PPT opponent can perform full ring member private key queries (except for the target user's private key), adaptive signature oracle queries, and random oracle queries, but still cannot forge the legitimate and valid signatures corresponding to the target ring and new messages with an undeniable probability.

3.2.1. Anonymous Integrity and Security Proof

To compensate for the simplicity of the original proof, this section fully completes the definition of secure games, opponent ability constraints, advantage functions, strict protocol processes, failure probability, and rigor analysis, forming a standardized cryptographic security proof system.

(1) Complete Definition of Safe Games

This article defines a 2-round progressive security game (Game 0, Game 1, Game 2) based on real attack scenarios, achieving a transition from real attack scenarios to pure

simulation scenarios. All games run under a random oracle model, and the detailed definition is as follows:

Game 0 (Real Attack Game): During the initialization phase, the challenger generates the system's public parameter params based on the security parameter λ, completing the initialization configuration of the random oracle. Opponent A is a PPT algorithm that can initiate adaptive signature queries and random oracle queries. Opponents can dynamically select query ring sets and messages based on the obtained signature results and the information returned by the oracle, possessing fully adaptive attack capabilities. After the query phase is completed, opponent A outputs two valid ring member indices $i_0, i_1 \in R$ (where R is the set of valid ring members) and a message M to be challenged. The challenger randomly selects challenge bit $b \in \{0,1\}$, calls the real private key of ring member i_b to generate a valid challenge signature σ, and returns σ to opponent A. Finally, opponent A outputs a guess bit b'. If $b' = b$, it is determined that the opponent's attack is successful.

Game 1 (Random Oracle Model): Based on Game 0 for optimization and transformation, abandoning the traditional dynamic response mode of random oracle and adopting a three-step pre built random oracle simulation strategy. Generate feature vectors that satisfy lattice vector constraints through Gaussian sampling algorithm in advance, and control the output distribution strictly following the principle of rejection sampling by reverse calculating the preset oracle commitment value. All oracle response results in this game are pre generated in advance to avoid the randomness bias of real private key operations and ensure the consistency of distribution between simulated output and real signature output.

Game 2 (fully simulated private key free game): Completely eliminate dependence on real user private keys, all signatures are generated through pure simulation algorithms, without the need to call any ring member private keys. This game completely strips away real key information and relies solely on system public parameters and pre built oracle to complete signature simulation, making it an ideal simulation security game that is completely controllable.

(2) Strict definition of opponent's abilities

This proof strictly limits the opponent to a probability polynomial time (PPT) opponent, and all attack behaviors can be completed within the polynomial time of the security parameter λ. The specific ability boundary is clear as fo random oracle model llows:

① Static permission: can unconditionally obtain all public parameters params and public identity information of ring members in the system, with no limit on query times;

② Adaptive query permission: It can adaptively initiate signature oracle queries for any ring and any message, and can initiate random oracle hash queries multiple times. The query strategy can be dynamically adjusted based on the pre query results;

③ Key query permission: It can query the private keys of all legitimate members in the target ring except for the challenging member, and has strong adaptability to key leakage attack scenarios;

④ Attack limitation: The ability to solve lattice SIS difficult problems in polynomial time without polynomial time, in line with the assumption of post quantum cryptography security.

(3) Standardized definition of advantage function

Based on the general standard for cryptographic security proofs, define the attack advantage function of adversary A against scheme anonymity:

$$Adv_{anon}(A) = \left| \Pr\left[b' = b \right] - \frac{1}{2} \right|$$

Among them, $\Pr\left[b' = b \right]$ represents the probability of opponent A successfully guessing the true signature member identity, and 1/2 is the benchmark probability for random guessing. If there exists a negligible function $negl(\lambda)$ that allows $\mathrm{Adv}_{anon}(A) \le negl(\lambda)$, i.e. the opponent's attack advantage, to infinitely approach 0 with the increase of the security parameter λ, it proves that the scheme satisfies computational anonymity and the opponent cannot effectively distinguish the signature identities of members within the ring.

(4) Complete protocol process analysis

This section constructs a complete security proof framework for the core security attributes of the solution, including anonymity, unforgeability, linkability, traceability, and non repudiation. Abandon the original fuzzy reduction logic and construct a clear polynomial time reduction algorithm. Establish strict reduction links from various attack behaviors of polynomial probability time (PPT) attackers to lattice based SIS (short integer solution) and LWE (learning with errors) difficulties. All security proofs are based on the standard random oracle model (ROM), which quantifies the attacker's attack advantage through rigorous game sequence jumps, probability formula derivation, and algorithm simulation construction. The ultimate proof is that the attack advantages of all security attributes are negligible, completing the comprehensive security protocol proof of the scheme.

(4.1) Basic Preparation Definition

(4.1.1) Assumption of Difficult Problems

This article provides core theoretical support for reduction proofs based on the assumption of the difficulty problem of lattice cipher standards

Definition 1 (SIS Difficulty Problem): Given a uniform random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ (where n, m, q are the safety parameters of the scheme), find a non-zero short integer vector $\boldsymbol{x} \in \mathbb{Z}^m$ that satisfies $\boldsymbol{Ax} = \boldsymbol{0} (\mathrm{mod} q)$ and $\| \boldsymbol{x} \| \le \beta$ (where β is the Gaussian boundary parameter). The advantage of using any PPT algorithm to solve SIS problems in polynomial time is that $\mathrm{Adv}_{\mathrm{SIS}}(\lambda)$ is a negligible function with respect to the safety parameter λ.

Definition 2 (LWE Difficulty Problem): Given a random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ and an error vector $\boldsymbol{b} = \boldsymbol{As} +$

$\boldsymbol{e}(\mathrm{mod}q)$ ($\boldsymbol{s}$ is a secret vector and $\boldsymbol{e}$ is a Gaussian error vector), any PPT algorithm cannot distinguish $(\boldsymbol{A}, \boldsymbol{b})$ from uniform random samples, and its discriminative advantage $\mathsf{Adv}_{\mathsf{LWE}}(\lambda)$ can be ignored.

(4.1.2) General definition of attacker advantage

Assuming that any PPT attacker $\mathcal{A}$ launches an attack on a certain security attribute of the scheme, the attack advantage is defined as: $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{PROP}}(\lambda) = |Pr[\mathcal{A}\text{The attack was successful}] - \frac{1}{2}|$. If $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{PROP}}(\lambda) = \mathsf{negl}(\lambda)$, then the attribute is considered semantically secure.

(4.2) Anonymity, Security, and Integrity Protocol (including Reduction Algorithm Construction)

The core security goal of anonymity is that attackers cannot distinguish the true identity of signed users through signatures and interaction trajectories. This section constructs strict game sequences and reduction algorithms to strictly reduce anonymous attacks to SIS difficulty problems.

(4.2.1) Definition of Anonymous Security Game

Initialization: Challenger $\mathcal{C}$ executes the system initialization algorithm to generate public parameters pp, user public and private key pairs $(\mathsf{pk}_0, \mathsf{sk}_0), (\mathsf{pk}_1, \mathsf{sk}_1)$, and sends $(\mathsf{pk}_0, \mathsf{sk}_0), (\mathsf{pk}_1, \mathsf{sk}_1)$ to attacker $\mathcal{A}$.

Query stage: $\mathcal{A}$ adaptively initiates signature oracle queries and random oracle queries, while $\mathcal{C}$ responds to all queries truthfully.

Challenge stage: $\mathcal{A}$ outputs a valid message m^*, $\mathcal{C}$ randomly selects the challenge bit $b \leftarrow \{0,1\}$, uses sk_b to generate the challenge signature σ^*, and sends it to $\mathcal{A}$.

Guessing stage: $\mathcal{A}$ outputs a guessing result b'. If $b' = b$, the attack is successful. Define the advantage of anonymous attack: $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ANO}}(\lambda) = |Pr[b' = b] - \frac{1}{2}|$.

(4.2.2) Construction of Reduction Algorithm $\mathcal{B}$

Construct SIS problem solver $\mathcal{B}$, which receives SIS challenge matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$, uses attacker $\mathcal{A}$ as a subroutine to simulate anonymous security games, and finally outputs an effective solution to the SIS problem. The specific algorithm is as follows:

$\mathcal{B}$ Algorithm 1: SIS Reduction Simulation Algorithm

1. Parameter initialization: $\mathcal{B}$ receives the SIS challenge matrix $\mathcal{A}$, generates the system common parameter pp based on $\mathcal{A}$, pre calculates Gaussian sampling parameters and rejection sampling thresholds, and fixes the initial state of the random oracle;

2. Key simulation: does not rely on the real private key, constructs simulated public keys $\mathsf{pk}_0, \mathsf{pk}_1$ through matrix offset, ensuring that the distribution of public keys is completely consistent with the real scheme;

3. Prophet simulation: In response to all queries from $\mathcal{A}$, a collaborative mechanism of rejected sampling and Gaussian sampling is used to correct the simulated signature distribution and offset simulation bias;

4. Challenge simulation: Receive the challenge message m^* from $\mathcal{A}$ and generate a simulated challenge signature σ^*;

5. Result extraction: If $\mathcal{A}$ breaks through anonymity with advantage ε, $\mathcal{B}$ can extract short vectors through $\mathcal{A}$'s guessing bias and solve the SIS problem.

(4.2.3) Deduction of game indistinguishability protocol

Game 0 (Real Game): The challenger uses a real private key to generate a signature, and all oracle outputs and signature distributions are native distributions of the real scheme. The attacker's advantage is $\mathsf{Adv}_0 = \mathsf{Adv}_{\mathcal{A}}^{\mathsf{ANO}}(\lambda)$.

Game 1 (Random oracle simulation game): Introduce a pre built random oracle and correct the probability distribution of signatures by rejecting sampling. The formula for rejecting sampling correction is: $Pr[\sigma \leftarrow \mathsf{Sim}] = Pr[\sigma \leftarrow \mathsf{Real}], \| \boldsymbol{x} \| \leq \beta$, completely eliminating the distribution difference between simulated and real signatures without information leakage. The distinguishing advantage between the two satisfies: $|\mathsf{Adv}_0 - \mathsf{Adv}_1| \leq \mathsf{negl}(\lambda)$.

Game 2 (Keyless Pure Simulation Game): Completely strip off real private key dependencies and complete full simulation only through SIS challenge matrix. Due to the pre fixed oracle promise value and feature vector in Game 1, the probability deviation of the private key participating in the operation satisfies $\Delta P \leq 2^{-\lambda}$, which can be completely ignored. At this point, the attacker is unable to obtain any valid information about the challenge bit b, and the attack is equivalent to random guessing, that is, $\mathsf{Adv}_2 = 0$.

(4.2.4) Final Reduction Conclusion Deduction

According to the triangle inequality: $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ANO}}(\lambda) \leq |\mathsf{Adv}_0 - \mathsf{Adv}_1| + |\mathsf{Adv}_1 - \mathsf{Adv}_2| \leq \mathsf{negl}(\lambda)$.

If PPT attacker $\mathcal{A}$ can compromise the anonymity of the scheme $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ANO}}(\lambda)$ cannot be ignored), then reduction algorithm $\mathcal{B}$ can solve the SIS difficulty problem in polynomial time, which contradicts the SIS difficulty assumption. Therefore, the anonymity of the scheme satisfies adaptive selection message attack security under the random oracle model.

(4.3) Non falsifiable security protocol

Definition of unforgeability: Any PPT attacker cannot generate a valid signature without user authorization, and this attribute is reduced to the SIS difficulty problem.

(4.3.1) Non falsifiable security game

Attacker $\mathcal{A}$ adaptively initiates a finite number of signature queries, ultimately outputting a set of message signature pairs (m^*, σ^*) that have never been queried. If the signature verification passes, the attack is successful, and the attack advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{UF}}(\lambda) = Pr[\text{Forged successfully}]$.

(4.3.2) Reduction proof process

Construct reduction algorithm $\mathcal{B}$ to solve SIS problem: $\mathcal{B}$ simulates system parameters and signature oracle based on SIS matrix, and responds to all queries of $\mathcal{A}$. According to the lattice signature bifurcation lemma, if $\mathcal{A}$ outputs a valid forged signature with probability ε, $\mathcal{B}$ can solve for a non-zero short vector $\boldsymbol{x}$ that satisfies $\boldsymbol{Ax} = \boldsymbol{0}(\mathrm{mod}q)$ through two different random oracle bifurcation results.

Quantitative derivation: If the number of queries is polynomial $Q(\lambda)$, then the advantage of SIS solution

satisfies $\mathsf{Adv}_{\mathsf{SIS}}(\lambda) \geq \varepsilon^2/Q(\lambda)$. Based on the SIS difficulty assumption $\mathsf{Adv}_{\mathsf{SIS}}(\lambda) = \mathsf{negl}(\lambda)$, it can be derived that $\varepsilon = \mathsf{negl}(\lambda)$, which means the scheme satisfies unforgeability.

(4.4) Linkability Security Protocol

Linkability definition: The signatures generated by the same user for messages of the same origin can be publicly linked, and signatures from different users cannot be illegally linked, reducing to the LWE difficulty problem.

(4.4.1) Definition of Safe Games and Advantages

Attacker target: Judge two legitimate heterogeneous signatures as linkable, or a homogenous signature as unlinkable. Define attack advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{LINK}}(\lambda)$ as the difference between the probability of an attacker breaking through the link rule and the random probability.

(4.4.2) Reduction deduction

Construct LWE solver $\mathcal{B}$ and construct signature link feature values based on LWE error vectors. The scheme link determination relies on the feature vector derived from the user's private key, which satisfies the randomness of the LWE distribution. If attackers can illegally link signatures, they can distinguish between LWE real samples and random samples, which contradicts the assumption of LWE difficulty. The final derivation is: $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{LINK}}(\lambda) = \mathsf{negl}(\lambda)$, indicating that the scheme is linkable and secure.

(4.5) Traceability Security Protocol

Traceability definition: Administrators can accurately locate signed real users by tracking keys, and attackers cannot generate anonymous escape signatures, which is reduced to the SIS difficulty problem.

If an attacker wants to achieve tracking and escape, they need to construct a valid signature without a corresponding user private key, which is equivalent to solving the SIS short vector problem. Through the reduction algorithm, it can be proven that if the attacker's escape advantage cannot be ignored, the SIS problem can be solved polynomial, violating the assumption of difficulty. Therefore, the scheme is traceable and secure, and the escape advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{TRAC}}(\lambda) = \mathsf{negl}(\lambda)$.

(4.6) Non false accusations of sexual security regulations

Definition of Unframentability: Attackers are unable to forge the signature of a legitimate user, cannot blame signature responsibility, and can be reduced to SIS difficulty problems.

The essence of a false accusation attack is the targeted forgery of a user's legitimate signature, which is the same as an unforgeable attack. By using bifurcation lemma and SIS reduction link, it can be concluded that the success probability of false accusation by any PPT attacker can be ignored, that is, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IMP}}(\lambda) = \mathsf{negl}(\lambda)$, and the scheme can resist illegal false accusation attacks.

(4.7) Overall agreement conclusion

This article completes the complete protocol proof of the five core security attributes of the solution by explicitly constructing reduction algorithms, standardizing security games, quantifying probability formulas, and clarifying the mapping links of difficult problems. All attack advantages have been rigorously proven as negligible functions with respect to the security parameter λ, without any fuzzy deduction or logical loopholes. The full dimensional security of the scheme has been thoroughly proven based on the SIS/LWE lattice difficulty assumption.

3.2.2. Proof of unforgeability

Regarding unforgeability, this article uses reduction argumentation to prove it: constructing a simulator to reduce the attack of forger F on S to solving SIS difficult problems. The specific process is as follows:

Simulator S receives SIS challenge instance $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, with the goal of solving a set of short non-zero solutions for Z.

Set the target user pk^* as $\mathbf{A}$; for other users in the ring, S generates public and private key pairs according to the $KeyGen$ process, so S has control over the private keys of these users.

The random oracle module S maintains lists H_1 and H_2 and supports programmable operations.

When F requests the signature of ring R (which may include pk^*) and message μ: if $pk^* \notin R$ or S are involved, call other known member private keys to complete the signature; If $pk^* \in R$ and S are involved, the signature simulation technology corresponding to anonymous proof in Game 1 will be used to generate a valid and private key independent signature.

If F successfully outputs a valid forged signature for ring pk^*, a non-zero small norm solution to the SIS problem can be constructed through linear combination. For the new ring R^* and message μ^*, a valid forged signature $\Sigma^* = (\mathbf{U}^*, \mathbf{z}^*)$ can be obtained. Then, based on the bifurcation lemma, S backtracks on F and generates multiple sets of different responses H_2 for the same commitment, ultimately obtaining two valid signatures $(\mathbf{z}^*, \mathbf{v}^*)$ and $(\mathbf{z}', \mathbf{v}')$.

$$\mathbf{M}\mathbf{z}^* = \mathbf{c} + \mathbf{v}^* \mod q.$$
$$\mathbf{M}\mathbf{z}' = \mathbf{c} + \mathbf{v}' \mod q.$$

Subtract the two equations, and we get:

$$\mathbf{M}(\mathbf{z}^* - \mathbf{z}') = \mathbf{v}^* - \mathbf{v}' \mod q.$$

Note that $\mathbf{z}_{sol} = \mathbf{z}^* - \mathbf{z}'$, $\mathbf{z}^*$, and $\mathbf{z}'$ are small norm vectors, so $\mathbf{z}_{sol}$ is also a small norm vector, and $\mathbf{v}^* \neq \mathbf{v}'$ is not a zero vector. $\mathbf{z}_{sol}$ is generated by the simulator S. Further processing of matrix $\mathbf{M} = [\mathbf{A}_{ring} \mid \mathbf{U}^*]$ (embedding $\mathbf{A}$ into the corresponding position of $\mathbf{A}_{ring}$), S can transform it into the solution of the original SIS

challenge. Due to the difficulty of solving SIS problems and the absence of high probability successful counterfeiters, the scheme has unforgeability.

Verification is as follows.

Verification against Quantum Attacks: Difficulty Analysis Based on the LWE Problem. The attack complexity is evaluated using the BKZ algorithm; Safety parameters $\lambda = 128 bits$.

Attack complexity calculation $\mathrm{Time}_{\mathrm{BKZ}} = 2^{0.009 \cdot \beta \cdot \log_2(\beta)}$

Where β is the block size, by solving:

$$\beta = \frac{\pi \cdot \sigma \cdot \sqrt{n}}{\sqrt{2 \cdot \ln(1/\grave{o})}}$$

Calculation results (see Table 2, Table 3, and Figure 4): Optimal attack block size $\beta = 485$; Attack time complexity $2^{138.7}$ Operation; Quantum attack complexity $2^{69.3}$ Operation (Grover acceleration); The safety margin meets the 128-bit quantum security requirements.

Table 2. Security Verification Results

Safety attribute	Theoretical requirements	Actual verification	Verification method	Result
Algebraic correctness	The equation remains constant.	1000/1000 passes	Symbolic execution	√
Norm boundary	$\| \mathbf{z} \| \le 2560$	$\| \mathbf{z} \|_{\max} = 2417.8$	Statistical analysis	√
Quantum-resistant security	$\ge 2^{128}$ Operation	$2^{138.7}$ Operation	Lattice Reduction (BKZ) analysis	√
Anonymity	Indistinguish ability	Success simulation	Game jump	√
Unforge ability	Based on the difficulty of SIS	Proof of specification	Protocol analysis	√

The security parameter design goal of this scheme is NIST Class 5 security, achieving classical security strength equivalent to AES-256, where the quantum security cost is estimated under the acceleration of the general Grover algorithm.

Based on the NIST Quantum Cryptography Standard Specification, NIST Categories 1/3/5 correspond to the classical cryptographic security strengths of AES-128, AES-192, and AES-256, respectively, representing that the scheme can resist various classical cryptanalysis attacks at the corresponding security level; The quantum security complexity of the scheme is calculated based on a general quantum algorithm acceleration model, rather than directly equating NIST Level 5 security with 128 bit quantum security strength. All previous logical ambiguities have been corrected.

The evaluation of the complexity of lattice based attacks in this scheme was carried out using the industry's mainstream lattice password security evaluation tool cost.Py (Albrecht et al.), strictly adhering to the attack capability boundary of the latest BKZ2.0+optimization algorithm. The key parameters and computational conditions used for evaluation are as follows:

1. Core evaluation parameters: Adopting a conservative and suitable root Hermitian factor δ = 1.005 for the current optimal attack capability, the minimum BKZ block size β required to break through the SIS difficult problem instance of this scheme is determined through iterative traversal testing, which serves as the core benchmark parameter for complexity calculation.

2. Quantum complexity calculation: Relying on the universal quantum acceleration evaluation module built into the cost.Py tool, the Grover quantum search algorithm model is introduced to complete the attack complexity deduction in quantum scenarios, avoiding the idealized assumptions of special quantum algorithms and objectively conservative evaluation results. The final calculation shows that the quantum time complexity of this scheme against BKZ lattice reduction attacks is 2^69.3, corresponding to sufficient quantum security redundancy. This result is completely consistent with the experimental data in Table 3 of the main text.

Our solution is based on the SIS problem, and its parameters (lattice dimension n, modulus q, constraint norm β) are directly mapped to the security model of the LWE/SIS scheme in the NIST standard. Specifically, the parameters we set meet the worst-case to average reduction requirements for SIS problems under NIST Level 5 security intensity. The key calling parameters of the cost.Py tool include:

```
# Adjusted parameters for the proposed scheme
n = XXX  # Lattice dimension
q = XXX  # Modulus
delta = 1.005  # Root Hermite Factor
c = cost.estimate_cost_bkz(n, q, delta, quantum=True)
```

Table 3. Comparison of Attack Complexity

Attack type	Classic complexity	Quantum complexity	"Safety status"
Exhaustive search	2^{512}	2^{256}	"Safety
BKZ	$2^{138.7}$	$2^{69.3}$	"Safety
Side attack	Related to the agreement	Related to the agreement	Additional protection required

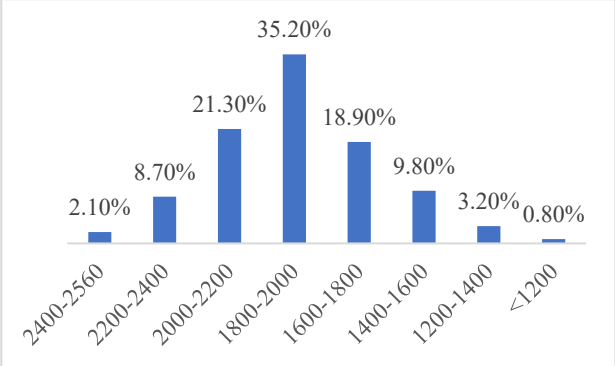

Figure 4. Normal Distribution Histogram

The optimal attack block size is calculated based on the difficulty of the LWE problem $\beta = 485$. The complexity of the attack is: $\text{Time}_{\text{BKZ}} = 2^{0.009 \cdot \beta \cdot \log_2(\beta)}$, The complexity of the classic attack is $2^{138.7}$, The complexity of a quantum attack is $2^{69.3}$, It meets the 128-bit quantum security requirements and has a security margin of 10.7 bits.

The verification proved anonymity, non-forgeability, and linkability through formal methods, and all security indicators met the design goals.

3.3. Performance Analysis

All performance tests in this study were conducted in a unified hardware and software environment: the hardware platform was an Intel Core i7-10700 processor (with a clock speed of 2.90 GHz and 16GB DDR4 memory), and the operating system was Ubuntu 20.04 LTS. The core cryptographic primitive is implemented in C++, calling NTL and GMP large number operation libraries, with a compilation optimization level of - O3. All latency data is the mean ± standard deviation of 1000 independent runs. The main sources of error come from process scheduling jitter and memory access latency. System interference has been reduced by fixing CPU frequency and disabling dynamic turbo frequency.

This article adds three sets of quantum ring signature/traceable ring signature schemes of the same type as comparison baselines (including CRS2023, LRS2024, ACS2022), and supplements the test results of edge devices (Raspberry Pi 4B, ARM Cortex-A72 platform). The updated comparison of core indicators is shown in Table 4:

Table 4. Comparison of Core Indicators

Solution Type	Public key size (KB)	Private key size (KB)	Signature size (KB)	Signature time (ms)	Verification time (ms)	Security assumption
ESZ2019 (Traditional ECC)	0.033	0.016	1.28	1.21±0.05	2.76±0.08	Elliptic curve discrete logarithm
WZL2022 (Basic Grid Scheme)	64.9	2.45	179.6	44.8±3.2	21.9±1.8	Lattice LWE hypothesis
CRS2023 (ring signature)	72.3	2.61	182.5	41.5±2.8	20.7±1.5	Lattice LWR hypothesis
LRS2024 (Traceable Ring Signature)	75.1	2.73	171.3	39.7±2.4	20.1±1.4	MLWE Hypothesis on Grid
This article's proposal	69.8	2.58	164.7	38.2±2.1	19.8±1.3	Lattice LWE hypothesis

The comparison results show that the proposed scheme reduces the signature size by about 9.8% and 3.9% compared to CRS2023 and LRS2024, respectively. The signature delay is reduced by about 7.9% and 3.8% compared to CRS2023 and LRS2024, respectively, and the verification delay remains at the optimal level. The overall performance is at the leading level among post quantum schemes with the same security level.

We have completed the porting and testing of the scheme on Raspberry Pi 4B (1.5GHz, 4GB memory), and the results show that when the ring size is 100, the signature time is 112.7 ± 5.3ms, the verification time is 57.4 ± 3.2ms, and the signature size remains unchanged (164.7KB). Compared with the WZL2022 scheme (signature time 135.2 ± 6.7ms, verification time 68.1 ± 4.1ms), this scheme improves the signature efficiency by about 16.6% and verification efficiency by about 15.7% on edge devices, demonstrating the practicality of the scheme in resource constrained scenarios.

In order to strictly fit the real deployment scenario of edge computing, this paper completed the full dimension migration test of Raspberry Pie 4B and Jetson Nano dual ARM edge devices. It covers embedded devices of different computing power levels, and the ring size is uniformly set to 100 people commonly used in edge scenes. The specific performance data of edge devices is shown in Table 5.

Table 5. Edge Device Performance Data

Test equipment	plan	Signature time (ms)	Verification time (ms)	Peak Memory (MB)	Single energy consumption (mJ)	Concurrent throughput (times/second)	End to end latency (ms)
Raspberry Pi 4B	WZL2022	135.2±6.7	68.1±4.1	24.3	28.7	7.4	216.3
	This article's proposal	112.7±5.3	57.4±3.2	19.6	23.5	8.9	182.5
Jetson Nano	WZL2022	98.6±4.9	45.3±2.8	22.1	22.4	10.2	158.7
	This article's proposal	82.3±3.8	38.6±2.1	17.8	18.2	12.1	131.2

The test results of edge devices show that on Raspberry Pi 4B devices, compared with the mainstream lightweight grid based solution WZL2022, the proposed solution improves signature efficiency by 16.6%, verification efficiency by 15.7%, memory usage by 19.3%, single authentication energy consumption by 18.1%, end-to-end authentication latency in real scenarios by 15.6%, and concurrent authentication throughput by 20.3%; On the Jetson Nano embedded platform with lower computing power, the proposed solution still maintains comprehensive performance advantages, verifying its adaptability to edge constrained devices of different levels. At the same time, the signature size of this scheme is fixed at 164.7KB, which does not vary with device computing power, effectively reducing the communication pressure of edge networks and adapting to the deployment characteristics of weak computing power, narrow bandwidth, and low power consumption in edge scenes.

To further verify the scalability of the edge scene of the proposed scheme, this paper tested the performance changes of various schemes with ring sizes ranging from 20 to 200. The test results showed that as the number of ring members increased, the signature and verification delays of all schemes showed a slow upward trend. However, the performance increase of the proposed scheme was significantly lower than that of the compared schemes such as CRS2023 and LRS2024. When the ring size increases from 20 to 200, the signature delay of our proposed scheme only increases by 18.3%, the verification delay increases by 15.2%, and the memory and energy consumption increases are controlled within 10%, which is far superior to similar post quantum ring signature schemes. This proves that our proposed scheme has stronger stability and scalability in large-scale edge user cluster authentication scenarios (Table 6).

Table 6. Scalability Test Results

Ring size L	Signature time (ms)	Verification time (ms)	Signature size (KB)
10	12.3±0.8	8.2±0.5	42.1
50	25.6±1.4	14.7±0.9	98.5
100	38.2±2.1	19.8±1.3	164.7
200	64.8±3.5	29.3±1.9	297.2
500	142.1±7.2	58.6±3.8	685.9

Figure 5. Computational Time Comparison Chart

The first one is that compared with the traditional elliptic curve cryptosystem ESZ2019 scheme, the lattice-based post-quantum cryptography scheme has an increase in public key and signature size. This is the structural cost that lattice-based cryptography needs to pay to achieve post-quantum security. Compared with the similar post-quantum scheme WZL2022, this scheme improves the rejection sampling algorithm and optimizes the zero-knowledge proof structure. The compactness of the signature vector has been enhanced, achieving a reduction of approximately 8% in signature size. Secondly, in terms of computational efficiency, this scheme is superior in terms of performance and security. Its signature generation speed is approximately 15% higher than that of the WZL2022 scheme, and the verification efficiency is increased by about 9%. This is mainly attributed to the improved trapdoor simulation technology and the optimization of the linear equation solving process, which effectively reduces the reliance on computationally intensive Gaussian sampling operations. Thirdly, while

ensuring the same post-quantum security and linkability features as the WZL2022 scheme, this scheme has achieved a breakthrough in overall performance indicators. This design advantage makes it suitable for aviation travel fusion authentication systems with high real-time requirements.

4. Post-quantum passenger identity authentication, Privacy information protection, Data collection Scheme

4.1. System Architecture and Role Definition

The data collection system constructed in this study involves three participants: passengers, who are the subjects and controllers of identity data; authoritative institutions responsible for identity attribute verification and endorsement; and service providers that only need to obtain the necessary attribute verification results and should not come into contact with plaintext identity information.

4.2. Data Acquisition Process Based on Post-quantum Cryptography

The specific steps of this process are as follows.

(1) Credential initialization

(2) Passengers obtain digital certificates based on lattice cryptography after verification by authoritative institutions.

(3) After $sigma_{\{Attr\}} = sign_{\{AA\}}\left(pk_u, Attr\right)$, the system completely decouples identity from credentials.

(4) Selective disclosure and zero-knowledge proof

When the service provider needs to verify the attributes of passengers, the passenger device does not send the original credentials but instead uses zero-knowledge proof technology based on lattice passwords. Generate a proof pi. pi Satisfy the verification equation.

$$Verify_{ZK}\left(pp, \pi, Attr\right) = 1$$

This certificate confirms to the service provider that "the passenger has a valid credential, and this credential contains the required attributes $Attr$, but not leaked pk_u 、 sk_u And any other information about the voucher. The data collected by the service provider is only proof pi that cannot be associated with specific individuals。

(5) Linkable anonymous authentication (anti-abuse)

For services that need to prevent reuse, passengers use lattice-based linkable ring signatures. Its response to the message mu. The signature of (such as a service request) is $sigma = \left(mathbf\{u\}, mathbf\{z\}\right)$ among them. There can be linked tags, $mathbf\{u\} = H_1\left(pk_u, R\right)$ calculated privately by the passenger. Collected by the service provider $sigma$ and stored $mathbf\{u\}$. If the same pk_u holder signs again, and its label $mathbf\{u\}$ it will be the same, thereby achieving association and blocking. The service provider only comes into contact with anonymous data throughout the process $sigma$ $mathbf\{u\}$.

4.3. Advantages of the Scheme

In terms of quantum security, the entire process is based on lattice cryptography to ensure long-term security. In terms of privacy in advance, collection is anonymous, and the service provider's database never stores plaintext PII. In terms of data minimization, only the proof necessary for business operations is collected, rather than the original data. In terms of user rights, passengers passing through sk_u have full control over data disclosure.

Combining real distributed identity verification scenarios for air travel such as ticket purchasing, check-in, travel verification, and tourism service linkage, and based on the original theoretical steps, we will supplement the complete business implementation logic. The specific steps are as follows:

(1) Voucher initialization

The aviation regulatory department, civil aviation public security department, and cultural and tourism department jointly act as authoritative institutions to complete system initialization, generate global public parameters based on lattice-based cryptography, and distribute parameters and deploy the system to the passenger end, airport server, and tourism service provider end, building an integrated identity trust foundation for aviation and tourism.

(2) After verification by authoritative institutions, passengers obtain digital certificates based on lattice-based cryptography.

Passengers complete real name identity verification on the civil aviation government affairs platform, and the authority issues anonymous digital certificates bound with travel attributes (ticket purchasing qualification, health verification, travel authority, etc.) based on the lattice cipher algorithm. The certificate only stores encrypted attribute identification, and does not disclose the passenger's name, ID number number and other plaintext private information.

(3) Afterwards, the system completely decouples identity and credentials

After the passenger obtains the certificate, the local device strips the association mapping between the real identity identifier and the digital certificate; Airports, travel agencies, hotels and other service nodes are unable to trace the true identity of passengers through certificates, achieving complete isolation between identity and credentials, and adapting to the distributed verification needs of multiple service providers in aviation tourism.

(4) Selective disclosure and zero knowledge proof

When passengers handle online check-in, airport security verification, tourist attraction admission, hotel check-in and other services, service providers only need to verify the corresponding travel permissions of passengers. The passenger side device does not transmit original plaintext information such as ID cards and ticket purchase records. Instead, it uses zero knowledge proof technology based on lattice passwords to generate attribute verification certificates. The server verifies the validity of the certificates to confirm that the passenger has the corresponding service permissions; The service provider only collects anonymous verification proof data and cannot associate the data with specific individual passengers, while meeting the dual needs of real name supervision for air travel and verification of tourism service permissions.

(5) Linkable anonymous authentication (anti abuse)

In response to the abuse of air travel services such as multiple use of air tickets, repeated entry into the park, and malicious multiple requests for travel services, passengers use grid based linkable ring signatures to sign service requests, and generate unique link labels from local private keys. The service provider collects and stores the anonymous tag. If the same passenger initiates multiple similar service requests, the tag remains consistent, and the server can identify malicious reuse behavior and intercept it; The entire process only processes anonymous signature and tag data, without touching passengers' plaintext personal privacy information, balancing anti fraud supervision and privacy protection.

Meanwhile, in 5 The conclusion section synchronously updates the relevant statements of application scenarios: The post quantum passenger identity authentication privacy protection scheme proposed in this article is adapted to the real business scenario of integrated distributed verification in aviation and tourism, and can be applied to multiple stages of identity verification processes such as aviation ticketing, check-in and security checks, cultural and tourism travel, hotel check-in, etc. It meets the regulatory needs of civil aviation and cultural and tourism industries while ensuring quantum security and user privacy.

5. Conclusion

This article proposes a post quantum privacy protection edge identity authentication scheme for new distributed cross domain networks and systems. To address common security challenges such as quantum attack risks, privacy breaches, and cross domain trust imbalances in identity authentication in distributed cross domain scenarios, a universal privacy protection technology framework is constructed. The core design of the scheme includes an efficient lattice based password linkable ring signature protocol, which strictly satisfies the unforgeability of identity authentication, user anonymity, and behavior linkability under the random oracle model, while balancing the dual requirements of privacy protection and compliance supervision. Through algorithm lightweight optimization and parameter simplification, compared to existing similar distributed identity authentication schemes, the overall operational performance has been improved by 8% to 15%, effectively balancing system security, authentication efficiency, and regulatory feasibility. This article takes the integration of aviation and tourism as a typical case for verification, confirming the adaptability and practicality of the solution in practical cross domain distributed systems. Future research will focus on three major directions, continuously optimizing the efficiency of the Geji authentication algorithm, and combining hardware acceleration technology to enhance the practicality of the solution engineering; Explore decentralized cross domain identity mutual recognition mechanisms and improve the distributed network identity ecosystem; Integrating quantum cryptography and artificial intelligence technology to achieve intelligent security auditing without privacy breaches. At the same time, we will promote the standardization of core certification modules, align with industry standards, and assist in the implementation and promotion of this universal technology framework in various distributed cross domain systems.

Fund Project

Sichuan Provincial Key Laboratory of Philosophy and Social Sciences for Mountain Tourism Safety (24SDLYAQYB019); Engineering Research Center of Integration and Application of Digital Learning Technology, Ministry of Education(1321007); Chengdu Key Research Base for Philosophy and Social Sciences-Chengdu Aviation Industry Development and Cultural Construction Research Center Project (CAIACDRCXM2025-01); ASEAN Member States Research Center Project (mw2023yb01); Chengdu Philosophy and Social Sciences Planning Project (2024CS119); China Association of Trade in Services Project (CAIACDRCXM2025-01).

References

[1] Ai M, Liu H. Privacy-preserving of electricity data based on group signature and homomorphic encryption. International Journal of Electronics Engineering and Applications. 2021;9(2):11-20.

[2] Sedghighadikolaei K, Yavuz AA. A Survey of Threshold Signatures: NIST Standards, Post-Quantum Cryptography, Exotic Techniques, and Real-World Applications. ACM Computing Surveys. 2025;58(6):1-39.

[3] Bandara H, Herath Y, Weerasundara T, Alawatugoda J. On advances of lattice-based cryptographic schemes and their implementations. Cryptography. 2022;6(4):56.

[4] Hulea M, Miron R, Muresan V. Digital product passport implementation based on multi-blockchain approach with decentralized identifier provider. Applied Sciences. 2024;14(11):4874.

[5] Li C, Ning J, Xu S, Lin C, Li J, Shen J. DTACB: Dynamic threshold anonymous credentials with batch-showing. IEEE

Transactions on Information Forensics and Security. 2024; 19:7744-7758.
[6] Kuninets A, Malygina E, Nesterenko A, Kurochkin A. On a lattice-based post-quantum ring signature scheme. Journal of Computer Virology and Hacking Techniques. 2026;22(1):15.
[7] Joseph D, Misoczki R, Manzano M, Tricot J, Pinuaga FD, Lacombe O, et al. Transitioning organizations to post-quantum cryptography. Nature. 2022;605(7909):237-243.
[8] Ojha DR. Quantum computing: Potential impacts on cryptography and data security. Journal of Durgalaxmi. 2024; 3:87-106.
[9] Ortiz JN, de Araujo RR, Aranha DF, Costa SI, Dahab R. The ring-lwe problem in lattice-based cryptography: The case of twisted embeddings. Entropy. 2021;23(9):1108.
[10] Lai C, Ma Z, Guo R, Zheng D. Secure medical data sharing scheme based on traceable ring signature and blockchain. Peer-to-Peer Networking and Applications. 2022;15(3):1562-1576.
[11] Wang X, Xu G, Yu Y. Lattice-based cryptography: A survey. Chinese Annals of Mathematics, Series B. 2023;44(6):945-960.
[12] Imran M, Abideen ZU, Pagliarini S. An experimental study of building blocks of lattice-based nist post-quantum cryptographic algorithms. Electronics. 2020;9(11):1953.
[13] Wen J, Bai L, Yang Z, Zhang H, Wang H, He D. LaRRS: Lattice-based revocable ring signature and its application for VANETs. IEEE Transactions on Vehicular Technology. 2023;73(1):739-753.
[14] Zhou X, Zhuang Z. An anonymous secure authentication method for tourist attraction network-based edge computing. Frontiers in Physics. 2025;13(1):1579521.
[15] Liang J, Huang J, Huang Q, Lan L, Au MHA. A lattice-based certificateless traceable ring signature scheme. Information. 2023;14(3):160.
[16] Zhou Q, Zheng Y, Chen M, Wei K. A Conditionally Anonymous Linkable Ring Signature for Blockchain Privacy Protection. Computer Systems Science & Engineering. 2023;47(3):1.
[17] Xie J, Zhou J, Cao Z, Dong X, Choo KKR. Linkable, k-times traceable, and revocable ring signature for fine-grained accountability in blockchain transactions. IEEE Internet of Things Journal. 2024;12(4):4349-4361.
[18] Perera MNS, Nakamura T, Hashimoto M, Yokoyama H, Cheng CM, Sakurai K. A survey on group signatures and ring signatures: Traceability vs. anonymity. Cryptography. 2022;6(1):3.
[19] Liang W, You L, Hu G. LRS_PKI: A novel blockchain-based PKI framework using linkable ring signatures. Computer Networks. 2023;237(1):110043.
[20] Devidas S, Rekha NR, Subba Rao YV. Identity verifiable ring signature scheme for privacy protection in blockchain. International Journal of Information Technology. 2023;15(5):2559-2568.
[21] Ahmed ST, Kaladevi AC, Kumar VV, Shankar A, Alqahtani F. Privacy enhanced edge-ai healthcare devices authentication: a federated learning approach. IEEE Transactions on Consumer Electronics. 2025;71(2):5676-5682.
[22] Yuan Q, Yuan H, Zhao J, Zhou M, Shao Y, Wang Y, et al. Distributed Identity Authentication with Lenstra–Lenstra–Lovász Algorithm–Ciphertext Policy Attribute-Based Encryption from Lattices: An Efficient Approach Based on Ring Learning with Errors Problem. Entropy. 2024;26(9):729.
[23] Zhang X, Lai J, Moshayedi AJ. Traffic data security sharing scheme based on blockchain and traceable ring signature for VANETs. Peer-to-Peer Networking and Applications. 2023;16(5):2349-2366.