IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 29 February 2024, accepted 8 March 2024, date of publication 18 March 2024, date of current version 22 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3376385

RESEARCH ARTICLE

Enhancing Copyright Protection Through Blockchain and Ring Signature Algorithm From Lattice

JIAN JIANG*, YULONG GAO*, AND YILE LI
State Key Laboratory of Media Convergence and Communication, Communication University of China, Beijing 100024, China

Corresponding author: Yulong Gao (ylgao@cuc.edu.cn)

This work was supported in part by the Research and Development of Digital System and Application Platform for Art Archives under Grant HG22031; in part by the National Natural Science Foundation of China (NSFC) under Grant 62272040; in part by Beijing Natural Science Foundation under Grant 4222038; in part by the National Key Research and Development Program of China under Grant 2021ZD0111404 and Grant 2022YFC3302103-01; in part by the Fundamental Research Funds for Central Universities under Grant CUC22GZ012, Grant CUC230A013, and Grant CUC230D016; in part by Beijing Municipal Natural Science Foundation under Grant M22002 and Grant 4212019; in part by the National Natural Science Foundation of China under Grant 62172005; in part by the Fundamental Research Funds of the Communication University of China under Grant CUC22GP006; and in part by the Strategic Research Program of Science and Technology Commission of the Ministry of Education of China under Grant JYB2022-01.

*Jian Jiang and Yulong Gao contributed equally to this work.

ABSTRACT Applying blockchain to copyright protection is currently a popular research trend. However, the characteristics of blockchain open data also lead to the threat of copyright privacy leakage. Targeting at this issue, we design a secure digital copyright protection scheme based on blockchain and ring signature algorithm, which can achieve privacy protection of copyright information and improve the efficiency of data authentication. In this paper, we design a new ring signature scheme based on lattice. In this scheme, by using the lattice basis delegation algorithm, user's public-private key pair is generated without expanding the dimension of lattice. Subsequently, according to the rejection sampling, message is signed by signer's secret keys and other ring participants' public keys. It can reduce scheme's computational complexity. Finally, by combining ring signatures with blockchain technology, a new copyright protection scheme is proposed. More importantly, this scheme is proven to be secure with its correctness and anonymity. Meanwhile, it has less communication costs and shorter key sizes than those in other similar schemes. The results show that the proposed new scheme has good performance and efficiency.

INDEX TERMS Blockchain, copyright protection, information security, cryptography, ring signature.

I. INTRODUCTION

With the advent of the digital age, the issue of digital copyright protection is becoming increasingly prominent. The effectiveness of traditional digital copyright protection technologies is limited in various aspects, such as copyright confirmation, efficiency of copyright authentication, and reliability of copyright information [1]. At the same time, the lack of effective regulation and legal protection also provides opportunities for infringement of digital copyright, leading to endless copyright disputes and causing considerable difficulties for creators, publishers, and consumers of digital content.

Blockchain technology is a decentralized database technology based on cryptographic algorithms and distributed network technology. It has the characteristics of immutability, decentralization, and transparency, providing a new solution for digital copyright protection [2]. In recent years, the general public has gradually realized the enormous advantages of blockchain technology in various fields, providing a theoretical basis for the combination of blockchain and digital copyright protection. Digital copyright protection based on blockchain technology can achieve advantages such as the immutability of copyright information, the efficiency of copyright recognition, the rapid dissemination of copyright information, and the fairness and transparency of copyright [3].

The associate editor coordinating the review of this manuscript and approving it for publication was S. K. Hafizul Islam.

There are significant differences between the blockchain transaction and traditional trading. Firstly, it is reflected in the aspect of recording and confirming the specific content of transactions. Traditional trading systems rely more on their center, where all recording and confirmation are completed. Once the center is damaged and there is no backup, it is easy to cause the loss of transaction data. However, in blockchain systems, the confirmation and recording of transactions do not rely on a certain center, and there is even no so-called center at all. The confirmation of transactions is carried out by nodes on the network. Secondly, in terms of storing transaction data, traditional trading systems store transaction data through a center and do not disclose it. In blockchain trading systems, instead of using a center to store transaction data, the entire network nodes are used to jointly store transaction data. The transaction data is completely public and can be accessed by people at any time.

Unfortunately, the open and transparent nature of blockchain has also caused some security issues. When potential attackers learn that multiple transaction records are the same input address through data cleaning, filtering, analysis, etc., they can infer the financial status, investment preferences, and privacy information of node users, as well as transaction partners [4].

Although blockchain is externally displayed as a public address list composed of a random combination of numbers and letters, these addresses will be associated with several Bitcoins stored at that address. Although traders complete transactions anonymously, the blockchain address is public and can still be traced back to the transaction process associated with that address [5].

Ring signature is one of the important cryptographic methods for privacy protection. Due to its excellent anonymity, it has been widely used in fields such as email, data exchange, electronic transactions, and electronic currency. However, ring signature scheme is faced with two problems which cannot be ignored. On the one hand, in the traditional public-key cryptosystem, digital certificate is used to bind user's identity and public key for verifying identity himself. Unfortunately, with the increasing number of users, the management and verification of certificates need to occupy a large number of system resources, which reduces its efficiency. Especially in ring signature scheme, the verifier not only needs to verify signer's public-key certificate, but also verifies the public-key certificates of other users in the ring. Furthermore, before signing, the signer also needs to verify the certificates of other users in the ring to ensure its anonymity. Obviously, if the number of users is much large, both efficiency and verification of scheme will be seriously affected.

On the other hand, many identity-based ring signature schemes are presented whose security mainly depends on hard number theory problems, such as discrete logarithm, integer factorization, especially bilinear pairings [6], [7], [8]. Nonetheless, quantum computing attack has a powerful parallel computing ability which threatens the security of conventional cryptographic algorithms. As is known to all, Shor's quantum algorithms can efficiently solve the discrete logarithms problem and factoring integers problem [9]. It has been proved that these quantum algorithms can be used for breaking some conventional cryptographic algorithms, such as RSA [10], DSA [11] and ECDSA [12], [13] algorithms.

Due to the need for blockchain technology to share some data and transaction information in order to achieve consensus among nodes in the blockchain and maintain data synchronization between distributed nodes. If third-party malicious users participate in node verification when sharing information in blockchain, there is a risk of privacy information leakage in transactions. Therefore, blockchain technology has the characteristics of openness and transparency, which not only ensures the secure sharing of data, but also poses hidden dangers to privacy security for copyright protection.

Therefore, in order to avoid the leakage of privacy information of copyright registrants during data transmission and transactions, and to improve the quantum security of cryptographic algorithms, a new ring signature algorithm for lattice ciphers is designed in this paper. Based on this algorithm and blockchain technology, an A new secure digital copyright protection scheme is designed. In this scheme, the data information of copyright privacy between users is encrypted, and the copyright information of digital works is traded and confirmed through blockchain. Thus, it can better ensure the security of copyright information registration and transaction processes.

II. RELATED WORK

A. BLOCKCHAIN

Blockchain technology is an advanced distributed shared ledger system that enables efficient data sharing and reliable management. Unlike traditional centralized ledgers, blockchain is decentralized and does not have a single control mechanism. All participants can jointly maintain and manage the entire network. Due to the use of advanced encryption technology and consensus mechanisms, blockchain data is tamperproof, and all transactions are traced and traceable throughout the entire process, ensuring data integrity and security. Meanwhile, due to the openness and transparency of blockchain, anyone can view the information and transaction records within it, ensuring the fairness and transparency of data. It is precisely these characteristics that give blockchain its advantages, especially its immutable and transparent characteristics that provide a trust foundation for blockchain applications. Traceability makes verifying the authenticity of information more reliable. Meanwhile, due to the characteristics of collective maintenance, the attack difficulty of attackers has also been improved.

Privacy information is very important in blockchain technology, which can be mainly divided into two aspects. The first aspect is the transaction content, which includes important information such as the payer, receiver, transaction amount, etc. The information is the basic elements of the transaction, which can help us understand the actual situation

of the transaction and the involved users. At the same time, the information is also part of the privacy information, which needs to be properly protected to avoid being used by illegal elements for malicious attacks or infringing on the privacy of users [14]. Another aspect is the user address. The user address in the blockchain is associated with the public key. A user can have multiple addresses, and each address corresponds to a series of transaction records. Because the address is public, anyone can view the transaction records, so it is necessary to protect the privacy information of the address. The transaction information in the blockchain is correlated, which is beneficial for information tracing. However, attackers can also leverage the correlation between information and analyze it. With continuous analysis, the user information in the blockchain is further mined, and attackers can link the user's identity information with the blockchain address, resulting in privacy leakage [15]. In response to the leakage of transaction privacy in blockchain, scholars at home and abroad have proposed information-hiding mechanisms based on cryptography theory, hash algorithms, etc., to encrypt and hide transaction information such as transaction funds, transaction participants, transaction correlation, etc., to achieve non-traceability of user privacy information, thereby ensuring the privacy security of users in blockchain [16]. At present, the research on information-hiding protection methods for blockchain mainly focuses on three cryptographic techniques: homomorphic encryption, zero-knowledge proof, and ring signature.

B. PRIVACY PROTECTION

For protecting user's privacy in signature scheme, in 2001, ring signature was first proposed [17]. The design of ring signature is very useful and valuable. Generally speaking, in a ring signature scheme, at first, a message signer needs to generate a ring of arbitrary members including himself. Then, he uses his secret key and other ring participants' public keys to generate a valid ring signature. In this way, arbitrary verifier can be convinced that this ring signature is generated by one of these ring members, but cannot know this signer's identity exactly. Therefore, due to its anonymity and unforgeability, ring signature is used in many practical applications, for instance, e-voting, whistle blowing [18], anonymous membership authentication [19], especially Monero based on blockchain [20].

Shamir presented an identity-based cryptosystem for the first time. User's public key is regarded as the identity, which reduces system overhead and improves its efficiency. In addition, for the second problem, in order to resist quantum computing attack, lattice-based cryptography was proposed [21], [22], [23]. Gentry et al. presented some special constructions with trapdoor function [24]. They first proposed trapdoor functions which can be used to construct lattice-based signature scheme and identity-based encryption. Afterwards, Cash et al. proposed the bonsai trees algorithm [25]. Meanwhile, by adopting rapped trapdoor one-way function, Rückert proposed the lattice-based blind signature scheme (LBSS) [26] and the lattice-based identity-based signature scheme (LIBSS) [27]. Afterwards, Cash et al. designed a novel cryptographic definition of bonsai trees from lattice [28]. Agrawal et al. proposed a new algorithm which can delegate a short lattice basis [29]. In 2012, the rejection sampling lemma is proposed [30]. This new method is quite simple and efficient. And this signature scheme is provably secure based on the worst-case hardness of the shortest independent vector problem (SIVP). Wang et al. constructed a lattice-based ring signature scheme by using lattice basis delegation technique [31]. He also extended it to the identity-based ring signature scheme. Unfortunately, he does not provide security proof in his paper, and his scheme is rather inefficient. Then, Jia et al. proposed an identity-based ring signature from lattice with higher computation performance [32]. Wang et al. presented a ring signature scheme from lattice [33]. Nevertheless, the unforgeabilities of schemes in [32]and [33] are proven in the random oracle model. In 2020, Cai proposed a practical byzantine fault tolerance (IPBFT) algorithm. And a digital music copyright protection system is designed based on the blockchain [34]. Then in 2021, Liu et al. proposed a post-quantum secure ring signature to enhance security and privacy in Cybertwin-driven 6G. Recently, in 2023, Liu et al. improves the ring signature technology to ensure the privacy and anonymity of blockchain data [35].

The proof length of the Borromean ring signature used in Monroe is relatively large, and the proof length is linearly related to the upper bound of the interval to be proven. The transaction size is affected by the length of the range proof, resulting in lower efficiency. At present, the latest Monroe coin scheme uses Bulletproofs technology to replace Borromean ring signatures and optimize the performance of the range proof algorithm. Related improved algorithms have also been proposed, such as Aurora [34], Libra [35], Ligero++ [36], Wolverine [37]. The introduction of methods such as zero knowledge proof and ring signature can technically achieve anonymization of blockchain nodes. However, correspondingly, there are also hidden dangers of ''double spending attack'' and difficult supervision in the recorded data of blockchain nodes. Therefore, how to implement privacy protected blockchain anonymity solutions has become a key issue that the blockchain industry needs to address.

III. RING SIGNATURE SCHEME BASED ON LATTICE

A. LATTICE AND LEMMAS

$\mathbb{R}, \mathbb{Z}$ denote the set of all reals and the set of positive integers, respectively. Let $\mathbb{R}^m$ be the m-dimensional Euclidean vector space with its usual topology. $m \in \mathbb{Z}, n \in \mathbb{Z}, m \geq n$.and L denote Λ lattice, the orthogonal lattice corresponding to Λ is represented by $\Lambda^{\perp}$, vector $\mathbf{x} = (x_1, x_2, \cdots, x_{n-1}, x_n)^T$ in the space $\mathbb{R}^m$, and its Euclidean norm $\|\mathbf{x}\| = \sqrt{x_1^2 + x_2^2 + \cdots x_{n-1}^2 + x_n^2}$.

Definition 1: Lattice. Given n-linearly independent vectors, lattice L generated by them is the set of vectors.

$$\mathbf{L}(\mathbf{v_1}, \mathbf{v_2}, \cdots, \mathbf{v_n}) = \left\{ \sum_{i=1}^{n} a_i \mathbf{v_i} \,|a_i \in \mathbb{Z}, i = 1, \cdots, n \right\} \quad (1)$$

$V = [\mathbf{v_1}, \mathbf{v_2}, \cdots, \mathbf{v_n}]$ is known as a basis of the lattice L. The same lattice can be represented by different lattice bases. Given a prime number q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, define:

$$\Lambda_q(\mathbf{A}) = \left\{ y \in \mathbb{Z}^m \,\middle|\, y = \mathbf{A}^T \mathbf{x} \bmod q, \mathbf{x} \in \mathbb{Z}^n \right\}, \quad (2)$$

$$\Lambda_q^{\perp}(\mathbf{A}) = \left\{ y \in \mathbb{Z}^m \,|\mathbf{A}y = 0 \bmod q \right\}. \quad (3)$$

Definition 2: Lattice SIS problem. Given an integer q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and a real constant $v > 0$, find a nonzero vector $\mathbf{x} \in \mathbb{Z}^m$ such that $\mathbf{Ax} \equiv 0 \bmod q$ and $\|\mathbf{x}\| \le v$.

Based on the hardness of SIS problem, for any polynomial-bounded m, v and any prime $q \ge v \cdot \omega\sqrt{n \log n}$, solving SIS on the average is as hard as approximating the shortest independent vector problem (SIVP) in the worst case.

Lemma 1: For a lattice L with dimensional m and rank $n, \mathbf{c} \in \mathbb{R}^m$, positive real $\varepsilon < \exp(-4\pi)$ and $s \ge \eta_\varepsilon(L)$, for random $\mathbf{x} \in L$ such that $D_{L,s,\mathbf{c}}(\mathbf{x}) \le \frac{1+\varepsilon}{1-\varepsilon} 2^{-n}$.

Lemma 2: Let $q > 2$, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{B}$ is a basis of $\Lambda_q^{\perp}(\mathbf{A})$, and Gaussian parameter $s \ge \|\tilde{\mathbf{B}}\|\omega(logm)$. Then any vector $\mathbf{y} \in \mathbb{Z}_q^n$, algorithm *SamplePre*($\mathbf{A}$, $\mathbf{B}$, $\mathbf{y}$, s) outputs a vector $\mathbf{e} \in Z_q^m$ from a distribution that is statistically close to $\mathbf{e} \in Z_q^m$.

Lemma 3: For any prime $q = poly(n)$ and any $m \ge 5n \lg q$, there is a probabilistic polynomial-time algorithm *TrapGen*(1^n) that outputs a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a full-rank set $\mathbf{S} \subset \Lambda^{\perp}(\mathbf{A}, q)$. The distribution of A is statistically close to uniform over $\mathbb{Z}_q^{n\times m}$ and the length $\|\mathbf{S}\| \le L = m^{1+\varepsilon} \wedge \varepsilon > 0$.

Lemma 4: Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and an m-dimensional lattice $\Lambda_q^{\perp}(\mathbf{A})$, then input a basis T of the lattice $\Lambda_q^{\perp}(\mathbf{A})$ which has a nonsingular matrix $\mathbf{R} = \mathbf{T}^{-1}$ and $\mathbf{R} \in \mathbb{Z}^{m\times m}$, input a Gaussian parameter $s \ge \left\|\tilde{\mathbf{T}}\right\| m^d \omega(\lg^{d+1}(m))$, *BasisDel*($\mathbf{A}$, $\mathbf{R}$, $\mathbf{T}$, s) can output a basis $\mathbf{B}$ of $\Lambda^{\perp}(\mathbf{AR}^{-1})$ with overwhelming probability $\left\|\tilde{\mathbf{B}}\right\| \le s\sqrt{m}$.

Lemma 5: Rejection sampling. Suppose that V is a subset $\mathbb{Z}^m$ and each element v has norm less than t, $\sigma = \omega(t\sqrt{\log m})$, and $h : V \to \mathbb{R}$ is a probability distribution. Then there exists a constant $M = O(1)$ such that the distribution of the following two algorithms less $x \leftarrow D_{v,\sigma}^m$ than $2^{-\omega(\log m)}/M$.

Algorithms A: $v \leftarrow h, x \leftarrow D_{v,\sigma}^m$, output (x, v) with the probability $\min(D_\sigma^m(x)/MD_{v,\sigma}^m(x), 1)$.

Algorithms B: $v \leftarrow h, x \leftarrow D_\sigma^m$, output (x,v) with the probability $1/M$.

The probability that Algorithms A outputs something is at least $(1 - 2^{-\omega(\log m)})/M$.

B. RING SIGNATURE SCHEME

Suppose that the number q is a prime and $q \ge 2, m \ge 5\, n \lg q$, the security parameter n is a positive integer, and $H_1 : \{0,1\}^* \to \mathbb{Z}_q^{m\times m}$ is a collision-resistant hash function. $H_2 : Z_q^m \times \{0,1\}^{*q} \to \left\{v = \{-d, \cdots, d\}^k : \|v\| \le t, d \in N^+, t \in R\right\}$. There are k users in the ring, so the ring is represented as $U = \{ID_1, I\,D_2, \cdots, I\,D_k\}$.

Setup (1^n). Based on the lattice SIS problem and lemma 1, inputs security parameters (n, q), outputs a uniformly random matrix $A_0 \in Z_q^{n\times m}$ with a corresponding short basis $\mathbf{S}_0 \in \Lambda^{\perp}(\mathbf{A}_0, q)$

For each user $U = \{ID_1, I\,D_2, \cdots, I\,D_k\}$. The hash function that takes as input ID, outputs $R = H(ID)$ and message $M \in \{0,1\}^d, d$ is the length of message M. Signer selects d independent matrices $\mathbf{C}_1, \mathbf{C}_2, \cdots, \mathbf{C}_d \in \mathbb{Z}_q^n$. In this way, the signer obtains the public parameter $PP = \langle \mathbf{A}_0, \mathbf{C}_1, \mathbf{C}_2, \cdots, \mathbf{C}_d \rangle$.

KeyGen ($PP, m\ s, M\ K$)**.** Select a matrix set $A = \left\{A_i \in Z_q^{n\times m} \mid i = 1, \cdots, n\right\}$. And compute $pk_i = A_0 \mid A_i, p\ k_i \in Z_q^{n\times m}$. By running the ExtBasis algorithm and RandBasis algorithm. The corresponding private key can be generated $sk_i \leftarrow RandBasis\,(ExtBasis\,(S_0, p\ k_i, s)\,, s)$.

RingSign. For a user ring $U = \{ID_1, I\,D_2, \cdots, I\,D_k\}$, Set $j = \{1, 2, \cdots, k\}$, Uniform random select $t \in D_\sigma^m = \left\{t \in R \mid \|t\|^{-1} \le s\right\}$, then select vectors $\mathbf{u}_j \leftarrow D_\sigma^m$. By running the SamplePre algorithm to output the sample $s_i \leftarrow SamplePre\,(pk_i, s\ k_i, s, u)$, and set $x_i = s_i + \mathbf{u}_i$, $v = H_2\left(\sum_{j=1}^{k} A_{ID_j}\mathbf{u}_j, M\right)$

Let $j = \{1, 2, \cdots, k\}$, if $j \ne i, x_j = \mathbf{u}_j$. If $j = i, x_j = x_i$. At last, generate the ring signature $e = (x_1, x_2, \cdots, x_k, v)$.

Verify (PP, U, M, e). For this signature e, through the following two steps, each user can verify its correctness.

For each $x_j, j \in \{1, 2, \cdots, k\}$, verify $\left\|x_j\right\| \le 2\sigma\sqrt{m}$.

$$\text{Verify } v = H_2\left(\sum_{j=1}^{\kappa} A_{ID_j} x_j - A_{ID_i} S_i, M\right).$$

In this scheme, by using the lattice basis delegation algorithm without expanding the dimension of lattice and the rejection sampling lemma, a message is signed with signer's secret key and other ring participants' public keys. Thus, these methods we used can reduce the computational complexity and communication cost, and the proposed ring signature scheme becomes more efficient.

IV. COPYRIGHT PROTECTION SCHEME

In this paper, we design a new blockchain-based secure copyright protection scheme using the ring signature algorithm. In this scheme, users in the copyright system are divided into three categories, including copyright owners, system administrators, and copyright buyers.

A. COPYRIGHT OWNER

Copyright owners can register, upload, and trade ownership of digital works in this copyright protection scheme. When a new buyer purchases the corresponding digital work, they become the new copyright owner of the digital work

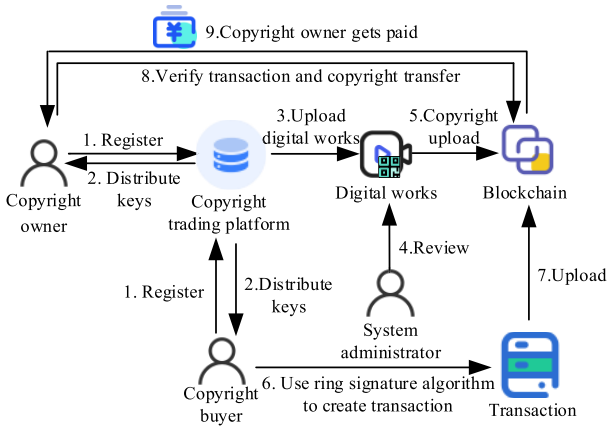

FIGURE 1. Digital copyright protection scheme based on blockchain.

B. SYSTEM ADMINISTRATOR

The System administrator mainly maintains and upgrades the digital copyright protection system based on this solution, ensuring the normal operation of the system, reviewing the content of digital works, managing the digital works and other related data stored in the system, and ensuring the security and reliability of the system data.

C. COPYRIGHT BUYER

Firstly, the copyright buyer cannot be the copyright owner themselves. The buyer can view the digital image work and detailed information of the image, such as copyright owner and price information, through the system, and then trade and purchase the copyright of the digital work. After successful payment and completion of the transaction, the buyer can obtain the corresponding copyright of the purchased digital work, complete the conversion of the copyright owner, become the new owner of the current image copyright, and can resell the purchased image work.

Based on this ring signature algorithm proposed in this paper, a blockchain-based secure digital copyright protection scheme has been designed, as shown in the following Figure 1. The specific process of the scheme is as follows.

Step 1: The copyright owner and copyright buyer register as users of the system.

Step 2: The copyright trading platform distributes their respective keys, including public and private keys, to system users, namely copyright owners and copyright buyers.

Step 3: Copyright owners upload their digital works through copyright trading platforms;

Step 4: The System administrator reviews the content of the digital work to ensure that the tradable digital works on the copyright trading platform comply with relevant legal regulations;

Step 5: Through review, if the digital work complies with relevant laws and regulations, the copyright of the work will be registered through the system to determine its ownership. Finally, authorize the copyright owner of the digital work to price and sell it.

Step 6: After the copyright buyer selects the digital work to purchase, they use the ring signature algorithm to generate a new transaction order, complete the payment of the copyright of the digital work, and protect the privacy of the trader's identity information to achieve privacy trading.

Step 7: The transaction order is published on the blockchain network, and the miner receives multiple transaction orders and then packages a new block. Mining new blocks through consensus mechanism to confirm and add the new transaction to the blockchain;

Step 8: The copyright owner confirms the transaction and transfers the copyright of the corresponding digital work to the copyright buyer;

Step 9: The blockchain trading platform completes the authentication of the final transaction and the transfer of copyright, confirms the completion of the transaction, and the system transfers the payment amount of the copyright buyer to the wallet address of the copyright owner. The copyright transaction ends. Copyright buyer become the new copyright owners of digital works through blockchain technology and can perform operations such as pricing, selling and other operations on the digital works.

Among them, the trading party inputs the password and decrypts it to obtain a private key. The private key is generated by the ring signature scheme's key generation algorithm, and then it will be used to ring sign the transaction data based on the proposed ring signature algorithm mentioned above. During verification, it will only verify whether the signature comes from a specific member in the ring, but cannot verify whether it is a specific member in the ring, which achieves the purpose of protecting blockchain identity and privacy transactions.

Compared to traditional copyright protection mechanisms, applying blockchain to our copyright protection scheme has the following advantages.

(1) Decentralized rapid property rights confirmation

The copyright confirmation method based on blockchain relies on its decentralized characteristics to store digital image information on the chain, including name, copyright author identity, timestamp, and other information. At the same time as the work is uploaded, the copyright can be determined without the need for complex processes such as central registration agency review and certificate production. Therefore, this solution can shorten the authentication cycle, reduce the cost of copyright registration, and achieve decentralized and fast authentication.

(2) Automated copyright trading

Blockchain introduces smart contracts, allowing transactions to take place without a third party. Once completed, the transactions are traceable and cannot be changed. Smart contracts can simplify the copyright transaction process based on blockchain, and efficient consensus mechanisms can improve the speed of block verification. Therefore, blockchain-based copyright trading is an automated, efficient and low-cost trading method.

(3) Convenient and reliable copyright certification

It is difficult to obtain evidence of infringement in the process of copyright protection, and judicial resources are limited during the litigation process, which often results in high costs and long time for rights protection. In this scheme, copyright owner can store various types of information as evidence on the chain, including identity identification and transaction information. In the process of rights protection, copyright verifiers can use blockchain to facilitate evidence collection and improve the efficiency of rights protection.

(4) The immutability of copyright data

In the process of this copyright protection scheme, storing copyright data on the blockchain as needed can ensure the immutability of copyright data. That is, copyright data can achieve authenticity and trustworthiness.

V. SECURITY AND PERFORMANCE ANALYSIS

A. CORRECTNESS

Theorem 1: This proposed scheme satisfies correctness.

Proof of Theorem 1: Suppose that there is a set l, and $j - l = \{i\}$. Such that

$$\begin{aligned}\sum_{j=1}^{k} A_{ID_j} x_j - A_{ID_i} s_i &= \sum_{l=1}^{k} A_{ID_l} u_l + A_{ID_i} x_i - A_{ID_i} s_i \\ &= \sum_{l=1}^{k} A_{ID_l} u_l + A_{ID_i} (s_i + u_i) - A_{ID_i} s_i \\ &= \sum_{l=1}^{k} A_{ID_l} u_l + A_{ID_i} s_i + A_{ID_i} u_i - A_{ID_i} s_i \\ &= \sum_{j=1}^{k} A_{ID_j} u_j \end{aligned} \tag{4}$$

Thus, we can have

$$v = H_2\left(\sum_{j=1}^{k} A_{ID_j} x_j - A_{ID_i} s_i, M\right) \tag{5}$$

With the proof of the equations (4) and (5), the proposed ring signature scheme satisfies the correctness.

B. ANONYMITY

Theorem 2: The proposed ring signature scheme satisfies anonymity.

Proof: Suppose that there exists adversary $\mathcal{A}$ attacking this ring signature scheme based on the definition of anonymity.

KeyGen. Challenger C selects a ring $U = \{ID_1, ID_2, \ldots, ID_k\}$ and runs *KeyGen* algorithm to obtain a secret key pair set $\{(pk_1, sk_1), (pk_2, sk_2), \ldots, (pk_k, sk_k)\}$.

Queries. Challenger C answers the hash queries and signing queries from adversary $\mathcal{A}$. Suppose $\mathcal{A}$ selects a participant with his *ID*. Challenger C returns this *ID*'s public and private key pair (pk_i, sk_i), and runs *Ringsign* algorithm to output a signature $e = (x_1, x_2, \cdots, x_k, v)$., Then C returns e' to adversary $\mathcal{A}$.

Challenge. adversary $\mathcal{A}$ submits message M', ring U' and two participants $\{ID_{a_0}, ID_{a_1}\} \in U$. Then, the challenger C chooses a bit $b \in \{0, 1\}$ and runs *Ringsign* algorithm to output signature, then return e' to adversary $\mathcal{A}$.

Guess. adversary $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ and verifies $b' = b$.

For this signature, if $j \neq a_b, x_j = \mathbf{u}_j$. If $j = a_b$, $x_j = x_i$.According to lemma 5, both $e = (x_1, x_2, \cdots, x_k, v)$ and $e' = (x'_1, x'_2, \cdots, x'_k, v')$ are indistinguishable from Gauss distribution $\left(\mathrm{D}_{\sigma}^{\mathrm{m}}\right)^{l+1}$. These two signatures are computationally indistinguishable.

C. UNFORGEABILITY

Theorem 3: Under the assumption of lattice SIS problem, this proposed ring signature scheme is existentially unforgeable in the random oracle model.

Proof: Suppose that there is a polynomial-time adversary $\mathcal{A}$. He can break this signature scheme and the probability of successfully forging a legitimate signature is ε. Then, the algorithm T does so by interacting with the adversary $\mathcal{A}$ as the Hash queries and Sign queries. The adversary $\mathcal{A}$ issues k queries on identity $U = \{ID_1, ID_2, \cdots, ID_k\}$.

Forgery. Adversary $\mathcal{A}$ submits a message M', a ring $U_2 \subseteq U$, a user $ID_a (1 \leq a \leq l)$, adversary $\mathcal{A}$ can forge a signature $e' = (x'_1, x'_2, \cdots, x'_l, v')$.

According to our signature scheme, if $e' = (x'_1, x'_2, \cdots, x'_l, v')$ is a legal signature of ring $U_2 \subseteq U$, so we can have

$$A_{ID_j} x'_j - A_{ID_i} s'_i = A_{ID_j} \mathbf{u}_j. \tag{6}$$

Because challenger C uses private key queries to obtain the private key $\mathbf{S}_a$ of ID_a, $e'' = (x''_1, x''_2, \cdots, x''_l, v'')$ is also a legal signature of ring $U_2 \subseteq U$, thus, we have

$$A_{ID_j} x'_j - A_{ID_i} s''_i = A_{ID_j} \mathbf{u}_j. \tag{7}$$

Through the analysis of Equations (6) and (7), we can have

$$A_{ID_j} x'_j - A_{ID_i} s'_i = A_{ID_j} \mathbf{u}_j = A_{ID_j} x'_j - A_{ID_i} s''_i. \tag{8}$$

So $A_{ID_i} s''_i - A_{ID_i} s'_i = 0$, thus, we have

$$A_{ID_i}(s''_i - s'_i) = 0 \tag{9}$$

Let $f = s''_i - s'_i$, so $A_{ID_i} f = 0 \bmod q$, and such that

$$\|f\| = \left\|s''_i - s'_i\right\| \leq \left\|s''_i\right\| + \left\|s'_i\right\| \leq \sigma\sqrt{m} + \sigma\sqrt{m} = 2\sigma\sqrt{m}. \tag{10}$$

Thus, for the lattice SIS problem with $(q, m, 2\sigma\sqrt{m})$, this solution is non-zero. Consequently, according to the preimage min-entropy property, this non-zero solution with probability no less than $SIS_{s\sqrt{m}}$. And this adversary A succeeded in forging a valid signature with the probability of ε, $pro(i = 1) = q_e^{-1}$. Therefore, the non-zero solution to this $SIS_{q,m,2\sigma\sqrt{m}}$ problem with a negligible probability $\left(1 - 2^{-\omega(\lg m)}\right) q_e^{-1} \varepsilon$. Thus, the probability that adversary A forges legal and valid signature is negligible. Under the lattice SIS problem assumption, the proposed linkable ring signature scheme satisfies unforgeability. This completes the proof.

TABLE 1. Comparison with other schemes based on lattice.

Scheme	Public key size	Signing key size	Signature size
Ref.[31]	$3nm\log q$	$5m^2\log q$	$2m\log q$
Ref.[32]	$3nm\log q$	$2m(m\text{-}n)\log q$	$3m\log q$
Ref.[33]	$(n+k)m\log q$	$m^2\log q$	$2m\log q$
Our work	$(n+k)m\log q$	$m^2\log q$	$m\log q$

TABLE 2. Comparison of time costs.

Scheme	Master key generation	User key generation	Signature generation
Ref.[31]	Ttg	$mTeb + Trb$	$(k+1)mTsp + kmnTmul$
Ref.[32]	Ttg	$Tmul+Tinv + Tbd\ kTsp$	$2mkTmul+Tgsp$
Ref.[33]	kT_{tg}	$gTsp$	$m(k+1)\ Tmul$
Our work	Ttg	$kTbd$	$T_{sp}+ mk\ Tmul$

D. COMPARISON

More importantly, in this subsection, we compare it with other lattice-based ring signature schemes. In our paper, we adopt rejection sampling lemma to sign message, which can reduce the computational complexity and improve the efficiency of signature scheme. More importantly, we prove the unforgeability of our proposed ring signature scheme in the standard model. In summary, comparing with other schemes, our identity-based ring signature scheme has better performance in security and efficiency.

Assume the parameters (n, m, q, k) are the same in this paper and the similar literatures, then Tab. 1 shows the details of the efficiency comparison results. As compared with other lattice-based ring signature schemes in [31], [32], and [33], the size of public key, private key and signature are all larger than the proposed scheme. In addition, our scheme can resist the quantum computing attacks.

Meanwhile, *Ttg*, *Tbd*, *Teb*, *Terb*, *Trb*, *Tsp*, *Tgsp*, *Tmul, Tinv* are set to represent the average consumption time of the following algorithms *Trapgen*, *Basisdel*, *Extbasis*, *Extrandbasis*, *Randbasis*, *Samplepre*, *Gensamplepre* and *Vector multiplication* and *Matrix inverse calculation* respectively. Then, the master key generation time, user key generation time and signature generation time in these above ring signature schemes are compared respectively, and the time cost comparison results are shown in Table 2. Among them, our ring signature scheme only uses the *Trapgen* algorithm once in the master key generation, and the user key generation adopts the *Basisdel* algorithm k times. Using the rejection sampling lemma, the main steps of generating ring signature adopt simple vector multiplication. Through this comprehensive comparison, it shows that in the transaction signature process, our scheme's time cost is less than that in other schemes.

VI. CONCLUSION

Blockchain technology is a decentralized database technology based on cryptographic algorithms and distributed network technology. It has the characteristics of immutability, decentralization, and transparency. Therefore, it can provide a new method for digital copyright protection. In this study, we design a secure digital copyright protection scheme based on blockchain technology and ring signature algorithm, which can achieve the immutability of copyright information and the efficiency of copyright authentication. Especially, due to the unconditional anonymity of ring signatures, the signer only uses their own private key and the public keys of all members in the ring when signing, thus fully protecting the identity privacy of transactions in the copyright system. In this ring signature scheme, by using the lattice basis delegation algorithm, user's public-private key pair is generated without expanding the dimension of lattice. Subsequently, according to the rejection sampling lemma, a message is signed by signer's secret keys and other ring participants' public keys. In this way, the scheme reduces the computational complexity. Finally, we analyze the security of the ring signature algorithm in the modified scheme and prove its correctness and anonymity. The results show that this scheme can effectively hide the identity of copyright trading users and ensure the security of digital copyright privacy information.

REFERENCES

[1] T. Nurhaeni, L. Nirmalasari, A. Faturahman, and S. Avionita, "Transformation framework design on digital copyright entities using blockchain technology," *Blockchain Frontier Technol.*, vol. 1, no. 1, pp. 35–43, Jul. 2021, doi: 10.34306/bfront.v1i01.5.

[2] W. Liang, D. Zhang, X. Lei, M. Tang, K.-C. Li, and A. Y. Zomaya, "Circuit copyright blockchain: Blockchain-based homomorphic encryption for IP circuit protection," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1410–1420, Jul. 2021, doi: 10.1109/TETC.2020.2993032.

[3] X. Zhang and Y. Yin, "Research on digital copyright management system based on blockchain technology," in *Proc. IEEE 3rd Inf. Technol., Netw., Electron. Autom. Control Conf. (ITNEC)*, Mar. 2019, pp. 2093–2097.

[4] K.-C. Li and R.-H. Shi, "A flexible and efficient privacy-preserving range query scheme for blockchain-enhanced IoT," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 720–733, Jan. 2023, doi: 10.1109/JIOT.2022.3203182.

[5] T. Jiang, A. Sui, W. Lin, and P. Han, "Research on the application of blockchain in copyright protection," in *Proc. Int. Conf. Culture-Oriented Sci. Technol. (ICCST)*, Oct. 2020, pp. 616–621.

[6] H. Mala, M. Dakhil-alian, and M. Brenjkoub, "A new identity-based proxy signature scheme from bilinear pairings," in *Proc. 2nd Int. Conf. Inf. Commun. Technol.*, 2004, pp. 3304–3308.

[7] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, "Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction," *Theor. Comput. Sci.*, vol. 469, pp. 1–14, Jan. 2013, doi: 10.1016/j.tcs.2012.10.031.

[8] S. S. M. Chow, S. M. Yiu, and L. C. K. Hui, "Efficient identity based ring signature," in *Proc. 3rd Int. Conf.*, New York, NY, USA, Jun. 2005, pp. 7–10.

[9] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 20–22.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[11] L. Harn, M. Mehta, and W.-J. Hsin, "Integrating Diffie–Hellman key exchange into the digital signature algorithm (DSA)," *IEEE Commun. Lett.*, vol. 8, no. 3, pp. 198–200, Mar. 2004, doi: 10.1109/LCOMM.2004.825705.
[12] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the Theory and Application of Cryptographic Techniques*. Cham, Switzerland: Springer, 1985.
[13] S. V. S. Vasundhara and D. K. V. D. Dr. K. V. Durgaprasad, "Elliptic curve cryptosystems," *Indian J. Appl. Res.*, vol. 4, no. 3, pp. 308–311, Oct. 2011.
[14] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019, doi: 10.1016/j.jnca.2018.10.020.
[15] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surveys*, vol. 52, no. 3, pp. 1–34, Jul. 2019, doi: 10.1145/3316481.
[16] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digit. Commun. Netw.*, vol. 7, no. 3, pp. 295–307, Aug. 2021, doi: 10.1016/j.dcan.2020.05.008.
[17] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. 7th Int. Conf. Theory Appl. Cryptol. Inf. Secur. Gold Coast*, 2001, pp. 9–13.
[18] J. K. Liu and D. S. Wong, "On the security models of (threshold) ring signature schemes," in *Proc. 7th Int. Conf.*, 2004, pp. 204–217.
[19] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in *Proc. Annual International Cryptology Conference*, Santa Barbara, CA, USA, 2002, pp. 18–22.
[20] S. F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, "Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero," in *Proc. 22nd Eur. Symp. Res. Comput. Secur.*, 2017, pp. 11–15.
[21] K. Lauter, "Postquantum opportunities: Lattices, homomorphic encryption, and supersingular isogeny graphs," *IEEE Secur. Privacy*, vol. 15, no. 4, pp. 22–27, Aug. 2017, doi: 10.1109/MSP.2017.3151338.
[22] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 22–24.
[23] M. Ajtai, "Generating hard instances of the short basis problem," in *Automata, Languages and Programming: 26th International Colloquium*. Cham, Switzerland: Springer, 1999, pp. 11–15.
[24] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 4th Annu. ACM Symp. Theory Comput.*, May 2008, pp. 17–20.
[25] C. Peikert, "Bonsai trees (or, arboriculture in lattice-based cryptography)," *J. Cryptol.*, vol. 25, pp. 601–639, 2012, doi: 10.1007/s00145-011-9105-2.
[26] M. Rückert, "Lattice-based blind signatures," in *Proc. International Conference Theory Application Cryptology Information Security*, Singapore, 2010, pp. 5–9.
[27] M. Rückert, "Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles," in *Proc. 3rd Int. Workshop*, 2010, pp. 25–28.
[28] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," *J. Cryptol.*, vol. 25, no. 4, pp. 601–639, Oct. 2012, doi: 10.1007/s00145-011-9105-2.
[29] S. Agrawal, D. Boneh, and X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in *Proc. 30th Annu. Cryptol. Conf.*, 2010, pp. 15–19.
[30] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Proc. Annual International Conference Theory Applications Cryptographic Techniques*. Cham, Switzerland: Springer, 2012, pp. 15–19.
[31] J. Wang and B. Sun, "Ring signature schemes from lattice basis delegation," in *Proc. 13th Int. Conf.*, 2011, pp. 23–26.
[32] X. Jia, D. He, Z. Xu, and Q. Liu, "An efficient identity-based ring signature scheme over a lattice," *J. Cryptologic Res.*, vol. 4, no. 4, pp. 392–404, 2017.
[33] R. Zhao, S. Wang, and Y. Zhang, "Lattice-based ring signature scheme under the random Oracle model," *Int. J. High Perform. Comput. Netw.*, vol. 11, no. 4, p. 332, 2018.
[34] Z. Cai, "Usage of deep learning and blockchain in compilation and copyright protection of digital music," *IEEE Access*, vol. 8, pp. 164144–164154, 2020.
[35] J. Liu, Y. Yu, K. Li, and L. Gao, "Post-quantum secure ring signatures for security and privacy in the cybertwin-driven 6G," *IEEE Internet Things J.*, vol. 8, no. 22, pp. 16290–16300, Nov. 2021.
[36] H. Ma and Y. Li, "Blockchain privacy protection scheme based on ring signature," in *Proc. 8th Int. Conf. Intell. Informat. Biomed. Sci. (ICIIBMS)*, Okinawa, Japan, Nov. 2023, pp. 394–397.
[37] E. Ben-Sasson, A. Chiesa, M. Riabzev, N. Spooner, M. Virza, and N. P. Ward, "Aurora: Transparent succinct arguments for R1CS," in *Proc. 38th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2019, pp. 19–23.
[38] T. Xie, J. Zhang, Y. Zhang, C. Papamanthou, and D. Song, "Libra: Succinct zero-knowledge proofs with optimal prover computation," in *Proc. 39th Annu. Int. Cryptol. Conf.*, 2019, pp. 18–22.
[39] R. Bhadauria, Z. Fang, C. Hazay, M. Venkitasubramaniam, T. Xie, and Y. Zhang, "Ligero++: A new optimized sublinear IOP," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, Nov. 2020, pp. 2025–2038.
[40] C. Weng, K. Yang, J. Katz, and X. Wang, "Wolverine: Fast, scalable, and communication-efficient zero-knowledge proofs for Boolean and arithmetic circuits," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Francisco, CA, USA, May 2021, pp. 1074–1091.

JIAN JIANG was born in Ningbo, Zhejiang, China, in 1990. He received the B.S. degree in digital media art and the M.S. degree in computer technology from the Communication University of China, in 2013 and 2017, respectively, where he is currently pursuing the Ph.D. degree. He is with the Big Data Center, China Digital Culture Group. His research interests include digital culture processing, creative production of digital cultural product content, digital publication and distribution, and blockchain.

YULONG GAO received the Ph.D. degree from Beijing University of Posts and Telecommunications, in 2021. He is currently a Lecturer with the School of Computer and Cyber Sciences, Communication University of China, Beijing, China. His research interests include information security, blockchain, cryptography, and quantum network coding.

YILE LI was born in Henan, China, in 2004. She is currently pursuing the bachelor's degree with the School of Computer and Cyber Sciences, Communication University of China, Beijing, China. Her research interests include information security, blockchain, and cryptography.