Hindawi
Security and Communication Networks
Volume 2022, Article ID 4052029, 12 pages
https://doi.org/10.1155/2022/4052029

Research Article

A New Lattice-Based Blind Ring Signature for Completely Anonymous Blockchain Transaction Systems

Yi-Yang Xie, Xiu-Bo Chen, and Yi-Xian Yang

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

Correspondence should be addressed to Xiu-Bo Chen; flyover100@163.com

Received 24 February 2022; Revised 19 July 2022; Accepted 27 July 2022; Published 1 September 2022

Academic Editor: Anmin Fu

Blockchain technology has been widely applied in numerous industries with its decentralization, verifiability, distributivity, and immutability. However, the identity privacy security of blockchain users is facing serious threats because of the openness of traditional blockchain transaction information. Moreover, numerous traditional cryptographic algorithms used by blockchain transaction networks are difficult to attack quantum computing. In this paper, we propose a new lattice-based blind ring signature scheme in allusion to completely anonymous blockchain transaction systems. There into, the blind ring signature can implement the complete anonymity of user identity privacy in blockchain transactions. Meanwhile, lattice cryptography can availably resist quantum computing attacks. Firstly, the proposed signature scheme has strong computational security based on the small integer solution (SIS) problem and a high sampling success rate by utilizing the techniques of rejection sampling from bimodal Gaussian distribution. Secondly, the proposed signature scheme can satisfy the correctness and security under the random oracle model, including anonymity, blindness, and one-more unforgeability. Thirdly, we construct a blockchain transaction system based on the proposed blind ring signature algorithm, which realizes the completely anonymous and antiquantum computing security of the blockchain users' identity privacy. Finally, the performance evaluation results show that our proposed blind ring signature scheme has lower latency, smaller key size, and signature size than other similar schemes.

1. Introduction

Blockchain has gained much attention that is widely used in digital currency, medical, government services, and other applications, however, the security problems of blockchain have become increasingly prominent in recent years. As the data information needs to be jointly maintained by each node in the blockchain distributed network, it requires that the transaction information must be public, which will lead to the disclosure of personal identity privacy data. In many classical blockchain systems represented by Bitcoin [1], users utilize a string of numbers unrelated to their real identity information as the transaction address, which preliminarily realizes the anonymity of identity privacy. Unfortunately, because transactions in the Bitcoin network can be linked, attackers can discover users' real identity information by their blockchain addresses [2, 3]. Therefore, to realize the veritable anonymity of the users' identity privacy, it is necessary to ensconce the relationship between users and their corresponding blockchain addresses.

The anonymity of identity information can be realized by ring signature and blind signature cryptography algorithms. Ring signature, developed from group signature [4], was first proposed by Rivest [5] in 2001. In the ring signature scheme, multiple users spontaneously constitute a ring and then randomly choose a member in the ring to sign the message. The signer uses his secret key and ring public keys of all members to generate a legal and valid ring signature. The ring signature prevents the exposure of the actual signer and invariably protects the signer's identity privacy. Another algorithm that can provide anonymity is the blind signature, which was first proposed by Chaum [6] in 1983. In the blind signature scheme, the signer can sign the message in case of unknowing the true content of the signature file. The sign

holder sends the blinded message to the signer for signature. The blind signature guarantees that signers hardly infer sign holders' real identity information through the blind message, which effectively protects sign holders' identity information privacy. In the blockchain transaction network, numerous anonymous transaction schemes are based on blind signature or ring signature [7–9]. However, the ring signature or blind signature can only guarantee the anonymity of a single user participating in the blockchain transaction, which cannot protect the identity privacy of both parties at the same time. To satisfy the complete anonymity of blockchain transaction users' identity privacy, it is significant to establish a blind ring signature scheme suitable for complete anonymous blockchain transactions. In 2005, Chan et al. [10] first proposed a blind ring signature algorithm, and since then, numerous blind ring signature schemes have been designed [11–13].

The security of traditional signature algorithms depends on integer decomposition, discrete logarithm and bilinear equivalent mathematical problems. Unfortunately, quantum computing can easily solve traditional difficult mathematical problems. Shor [14] proposed a quantum algorithm that lets RSA cryptography, elliptic curve cryptography, and cryptosystems based on bilinear pairings face serious security challenges. Grover [15] proposed a quantum search algorithm that could provide secondary acceleration for search problems, which seriously threatened the security of symmetric cryptography and the Hash function. Therefore, it is a key research work to find a cryptosystem that can resist quantum computing attacks.

Lattice cryptography is a kind of antiquantum computing cryptography with strong security and high computational efficiency, which is widely used in digital signature algorithm design and blockchain transaction networks. Gentry et al. [16] first designed a signature algorithm with lattice trapdoor sampling, whose security depends on solving the SIS problem. Lyubashevsky [17] proposed a signature scheme without trapdoor sampling, which uses rejection sampling to greatly improve the sampling efficiency. Ducas et al. [18] designed a new signature algorithm with lattice rejection sampling, which further improves the sampling success rate through random sampling on bimodal Gaussian distribution. In 2018, Gao et al. [19] first proposed a postquantum blockchain system, which integrated a lattice-based signature algorithm. In 2022, Zou et al. [20] proposed a lattice-based proxy signature scheme for anonymous blockchain-enabled electronic reporting systems, which not only realized the anonymity of user identity but also solved the problem of misbehaviors untraceability on the blockchain. Moreover, Rückert [21] proposed the first blind lattice-based signature algorithm. Li et al. [22] proposed a new blind signature algorithm applied in blockchain anonymous transaction authentication on the lattice. In addition, Melchor et al. [23] designed the first ring signature algorithm based on lattice cryptography. To further improve the sampling success rate, Wang et al. [24] designed a new ring signature algorithm using Lyubashevsky's rejection sampling signature [17]. In 2019, Le et al. [25] designed the first blind ring signature algorithm based on the SIS problem with rejection sampling. Moreover, numerous lattice-based blind signature and ring signature schemes have been proposed [26, 27].

In this paper, we design a new lattice-based blind ring signature algorithm in allusion to the completely anonymous blockchain transaction system. The constructed transaction system satisfies the requirements of the user's identity privacy protection and resistance to quantum attacks. There are three main contributions, which are as follows:

(1) We propose a new lattice-based blind ring signature algorithm using the rejection sampling technology. Sampling on the bimodal Gaussian distribution can greatly improve the success rate. In addition, we give proof of correctness and security under the random oracle model, including anonymity, blindness, and one-more unforgeability.

(2) We construct a completely anonymous blockchain transaction system based on the proposed blind ring signature and provide detailed processes of the anonymous transaction. The system satisfies the goal of blockchain users' identity privacy protection and antiquantum computing security.

(3) We evaluate the performance of the proposed signature algorithm with other similar literature schemes, including the sampling method, algorithm latency, the size of the signature, and secret and public keys. The evaluation results indicate that our proposed scheme has lower latency and smaller key and signature sizes than other similar schemes.

The organization of this paper is as follows: we present some lattice theories and the blind ring signature's definition and security model in Section 2. In Section 3, a new lattice-based blind ring signature is designed. In Section 4, we prove the security of our signature algorithm. We construct a completely anonymous blockchain transaction system based on the proposed blind ring signature in Section 5. The performance evaluation of signature algorithms is shown in Section 6. Finally, we provide a conclusion of the paper in Section 7.

2. Preliminaries

2.1. Some Related Theories of Lattice

Definition 1 (Lattice [28]). Given a matrix $\mathbf{B} \in \mathbb{R}^{m\times n}$ consists of a group of m-dimensional linearly independent vectors $\mathbf{b}_1,\ldots,\mathbf{b}_2,\ldots\mathbf{b}_n$. where $m \geq n$ Define lattice Λ generated by $\mathbf{B}$ as the set.

$$\Lambda(\mathbf{B}) = \{\mathbf{Bx} \mid \mathbf{x} \in \mathbb{Z}^n\}. \tag{1}$$

Given a prime number q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and $\mathbf{e} \in \mathbb{Z}_q^n$, define some q-ary lattices.

$$\Lambda_q(\mathbf{A}) = \left\{\mathbf{y} \in \mathbb{Z}^m \mid \mathbf{y} \in \mathbf{A}^T\mathbf{x} \bmod q, \mathbf{x} \in \mathbb{Z}^n\right\},$$
$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{y} = \mathbf{0} \bmod q\}, \quad (2)$$
$$\Lambda_q^{e}(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{y} = \mathbf{e} \bmod q\}.$$

Definition 2 (Discrete Gaussian Distribution [17]). Define $D_{\mathbf{v},\sigma}^m(\mathbf{z}) = \rho_{\mathbf{v},\sigma}^m(\mathbf{z})/\rho_{\mathbf{v},\sigma}^m(\mathbb{Z}^m)$ as a discrete Gaussian distribution, where $\rho_{\mathbf{v},\sigma}^m(\mathbf{z}) = (1/\sqrt{2\pi\sigma^2})^m e^{-\|\mathbf{z}-\mathbf{v}\|^2/(2\sigma^2)}$ and $\rho_{\mathbf{v},\sigma}^m(\mathbb{Z}^m) = \sum_{\mathbf{z}\in\mathbb{Z}^m}\rho_{\sigma}^m(\mathbf{z})$.

Definition 3 (SIS problem). Given a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and parameters m, n, q, β, the $\mathrm{SIS}_{q,n,m,\beta}$ problem is to find a nonzero integer vector $\mathbf{v} \in \mathbb{Z}_q^m$, such that $\mathbf{A}\mathbf{v} = \mathbf{0}(\bmod q)$ and $\|\mathbf{v}\| \le \beta$.

Lemma 1 (see [17]). For any $\mathbf{v} \in \mathbb{R}^m$, $\sigma > 0$, $k > 1$, it satisfies the following:

$$\Pr\{\|\mathbf{z}\| > k\sigma\sqrt{m}\,; z \leftarrow D_{\sigma}^m\} \le k^m e^{(m/2)(1-k^2)}. \quad (3)$$

Lemma 2 (see [17]). For any $\mathbf{v} \in \mathbb{Z}^m$, $\sigma = \alpha\|\mathbf{v}\|$, $\alpha > 0$, it satisfies the following:

$$\Pr\left\{\frac{D_{\sigma}^m(\mathbf{z})}{D_{\mathbf{v},\sigma}^m(\mathbf{z})} < e^{(12/\alpha)+(1/(2\alpha^2))} : \mathbf{z} \leftarrow D_{\sigma}^m\right\} > 1 - 2^{-100}. \quad (4)$$

More specially, if $\alpha = 12$, $\sigma = 12\|\mathbf{v}\|$, *then* $(D_{\sigma}^m(\mathbf{z})/D_{\mathbf{v},\sigma}^m(\mathbf{z})) < e^{1+(1/288)}$ *with a probability of at least* $1 - 2^{-100}$.

Lemma 3 (Rejection Sampling [17]). *Select a random vector* $\mathbf{v} \in \mathbb{Z}^m$ *and a real number* $\sigma = \omega(t\sqrt{\log m})$, *given a subset* $V = \{\mathbf{v} \in \mathbb{Z}^m : \|\mathbf{v}\| < t\}$, *and define on* V *a probability distribution* h: $V \longrightarrow \mathbb{R}$. *Then, there exists a constant* $M = O(1)$ *such that the outputs of the following two algorithms* A *and* $\mathbf{B}$ *have a negligible statistical distance of* $\Delta(\mathbf{A}, \mathbf{B}) = 2^{-\omega(\log m)}/M$:

Algorithm $\mathbf{A}$: $\mathbf{v} \leftarrow h$, $\mathbf{z} \leftarrow D_{\mathbf{v},\sigma}^m$, *output* $(\mathbf{z}, \mathbf{v})$ *with probability* $\min(D_{\sigma}^m(\mathbf{z})/(MD_{\mathbf{v},\sigma}^m(\mathbf{z})), 1)$.

Algorithm $\mathbf{B}$: $\mathbf{v} \leftarrow h$, $\mathbf{z} \leftarrow D_{\sigma}^m$, *output* $(\mathbf{z}, \mathbf{v})$ *with probability* $1/M$.

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

More specially, if $\sigma = \alpha t$ for any $\alpha > 0$, then $M = e^{(12/\alpha)+(1/(2\alpha^2))}$. The two algorithms A and $\mathbf{B}$ have a negligible statistical distance off $\Delta(\mathbf{A}, \mathbf{B}) = 2^{-100}/M$, and the probability that A outputs something is at least $(1 - 2^{-100})/M$.

2.2. Blind Ring Signature Model

2.2.1. System Model. The blind ring signature system model is composed of four parts called setup, key generation, signature, and verification [25]. The detailed steps are as follows:

Setup. Input a security parameter n and output public parameters PP.

Key generation. Generate public key pk and secret key sk for each member of the ring $R = \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_l\}$ according to the input set of public parameters PP.

Signature. The user Υ submits a message m and blinds it to μ before sending the message to the signer. Then, the ring R chooses a signer Σj, who takes the secret key sk_j. The signer Σj signs the message μ and generates a blinded signature Σ'. The user Υ unblinds Σ' and gets the real signature Σ.

Verification. Output 1 or 0 according to the public parameters PP, message m, signature Σ, and ring public keys $PK = \{pk_i\}_{i\in[l]}$. The output of 1 means that the verification is passed, and 0 indicates that it is otherwise.

2.2.2. Security Model. The security model of the blind ring signature includes anonymity, blindness, and one-more unforgeability.

Anonymity: the anonymity property ensures that the user cannot know which member of the ring was the real signer participating in the blind ring signature protocol. For any polynomial-time adversary, the blind ring signature scheme satisfies the anonymity under full key exposure if his advantage in winning the following game with the challenger is negligible.

(1) Setup: assume n to be the system security parameter. The challenger calls the setup algorithm in the blind ring signature scheme to generate the set of common parameters PP. Then, according to the common parameters PP, the challenger calls the key generation algorithm to generate a set of public and secret keys (PK, SK) for the ring $R = \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_l\}$. The challenger sends the set of common parameters PP and public key PK to the adversary .

(2) Query: the adversary submits a message m, a ring R, an index I, and the corresponding public key pk_{i} to the challenger . The challenger queries the corresponding secret key sk_i according to the index I and then calls the signature algorithm to generate a blinded signature Σ_i' on m for the adversary .

(3) Challenge: the adversary submits a message m, a ring R, and two public keys $pk_{i_b} \in R$ to the challenger for the signature query, where $b \in \{0, 1\}$. The challenger chooses a random bit $b \in \{0, 1\}$. Then, it uses the secret key sk_{i_b} and calls the signature algorithm to generate a blinded signature Σ_i' on m and returns Σ_i' to the adversary .

(4) Guess: the adversary outputs a bit b' as a guess of the random bit b. He wins the game if $b' = b$.

The advantage of the adversary in the above game is defined as follows:

$$\mathrm{Adv}_{\mathrm{BRS}}^{\mathrm{anonymity}}(A) = \left|\Pr\{b' = b\} - \frac{1}{2}\right|. \quad (5)$$

Blindness: it is a basic attribute of the blind ring signature, i.e., all members in the ring cannot know any information about the message to be signed. In other words, the attacker cannot distinguish the original signature of which message a blind ring signature comes from. For any polynomial-time adversary , the blind ring signature scheme satisfies the statistical blindness if his advantage in winning the following game with the challenger is negligible.

(1) Setup: assume n to be the system security parameter. The challenger calls the setup algorithm in the blind ring signature scheme to generate the set of common parameters PP. Then, according to the common parameters PP, the challenger calls the key generation algorithm to generate a set of public and secret keys (PK, SK) for the ring $R = \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_l\}$. The challenger sends the set of common parameters PP and public key PK to the adversary .

(2) Challenge: the adversary α chooses two different blinded messages μ_0 and μ_1, a subring $R' \in R$, and its corresponding public keys PK to send it to the challenger . The challenger chooses a random bit $b \in \{0, 1\}$, then sets up a blind ring signature protocol taking μ_b and the ring R' as input. The adversary chooses a signer Σj in the ring R' to sign the hidden blinded message μ_b. Finally, the adversary obtains the unblinded signature $\Sigma_b \neq \perp$, otherwise, it restarts this game.

(3) Guess: the adversary outputs a bit b' as a guess of the random bit b. He wins the game if $b' = b$.

The advantage of the adversary in the above game is defined as follows:

$$\mathrm{Adv}_{\mathrm{BRS}}^{\mathrm{blindness}}(A) = \left|\Pr\{b' = b\} - \frac{1}{2}\right|. \tag{6}$$

One-more unforgeability: the one-more unforgeability property ensures that the attacker cannot successfully forge a new correct signature through multiple signature inquiries. For any polynomial-time adversary , the blind ring signature scheme satisfies the one-more unforgeability if his probability of winning the following game with the challenger is negligible.

(1) Setup: assume n to be the system security parameter. The challenger calls the setup algorithm in the blind ring signature scheme to generate the set of common parameters PP. Then, according to the common parameters PP, the challenger calls the Key generation algorithm to generate a set of public and secret keys (PK, SK) for the ring $R = \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_l\}$. The challenger sends the set of common parameters PP and public key PK to the adversary . The secret key SK cannot be disclosed.

(2) Query: the adversary submits a message m, a ring R, and its corresponding public keys PK. Then, adaptively, it makes multiple hash queries and blind ring signature queries to the challenger . The challenger must return the hash value $H(m)$ and signature value Σ of the corresponding message m to the adversary .

(3) Forge: the adversary uses the result of multiple queries to forge Σ^* of the target message m^*. One-more unforgeability requires that the pair (m^*, Σ^*) has never passed the signature verification algorithm.

3. Proposed Blind Ring Signature Algorithm

Our proposed blind ring signature algorithm includes five parts: key generation, message blinded, signature, unblind, and verification.

Key generation. Assume n is a system security parameter. We generate the common parameter PP, which has been selected by the same methodology of Li's scheme [22]. The independent public and secret key pairs $(\mathbf{A}_i, \mathbf{S}_i)$ for each signer $\mathcal{S}_i, i \in [l]$ of the ring $R = \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_l\}$ are generated using the method described in Ducas's scheme [18], where $\mathbf{A}_i \in \mathbb{Z}_{2q}^{n\times m}$, $\mathbf{S}_i \in \mathbb{Z}_{2q}^{m\times n}$, and satisfying $\mathbf{A}_i\mathbf{S}_i = q\mathbf{I}_n \pmod{2q}$.

Message blinded: the signer of the ring R first computes a commitment to the user Υ. Then, the user Υ hides the original message m by running the message blinded algorithm and outputting the blinded messageμ. The detail is shown in algorithm 1.

Signature: the ring R chooses a signer Σj. Σj calls the signature algorithm after receiving the blinded message μ and then outputs the blinded signature Σ'. The detail is shown in algorithm 2.

Unblind: the user Υ runs the unblind algorithm after receiving the blinded signature Σ' and then outputs the real blind ring signature Σ. The detail is shown in algorithm 3.

Verification: the verifier runs the verification algorithm after receiving the original message m and bling ring signature Σ. Then, he outputs 1 if the verification is passed. It is 0, otherwise. The detail is shown in algorithm 4.

4. Correctness and Security Proof

4.1. Correctness. For the generated blind ring signature $\Sigma = (\{\mathbf{e}_i\}_{i\in[l]}, \mathbf{c})$, $\{\mathbf{e}_i\}_{i\in[l]}$ are sampled from the distribution $D_{\sigma_3}^m$, and according to Lemma 1, $\|\mathbf{e}_i\| \le \eta\sigma_3\sqrt{m}$ is established with an overwhelming probability for all $i \in [l]$. Therefore, the correctness is to prove $\sum_{i\in[l]}\mathbf{A}_i\mathbf{e}_i + q\mathbf{c} = \mathbf{x} + \mathbf{w} \pmod{2q}$. The proof of the equation is as follows:

$$\begin{aligned}
\sum_{i\in[l]}\mathbf{A}_i\mathbf{e}_i + q\mathbf{c} &= \sum_{i\in[l]}\mathbf{A}_i\mathbf{y}_i + \sum_{i\in[l]}\mathbf{A}_i\mathbf{z}_i + q\mathbf{c} \\
&= \sum_{i\in[l]\setminus\{j\}}\mathbf{A}_i\mathbf{z}_i + \mathbf{A}_j\mathbf{z}_j + \sum_{i\in[l]}\mathbf{A}_i\mathbf{y}_i + q\mathbf{c} \\
&= \sum_{i\in[l]\setminus\{j\}}\mathbf{A}_i\mathbf{r}_i + \mathbf{A}_j\left(\mathbf{r}_j + \mathbf{S}_j\mu\right) + \sum_{i\in[l]}\mathbf{A}_i\mathbf{y}_i + q\mathbf{c} \\
&= \sum_{i\in[l]}\mathbf{A}_i\mathbf{r}_i + \mathbf{A}_j\mathbf{S}_j\mu + \sum_{i\in[l]}\mathbf{A}_i\mathbf{y}_i + q\mathbf{c} \\
&= \mathbf{x} + \mathbf{w} + q(-1)^t\mathbf{I}_n\mathbf{c} + q\mathbf{c} = \mathbf{x} + \mathbf{w} \pmod{2q}.
\end{aligned} \tag{7}$$

Input: system public parameters PP, original message m, public keys $\{\mathbf{A}_i\}_{i\in[l]}$ of the ring R.
Output: blinded message μ.
Step 1: choose a set of random vectors $\{\mathbf{r}_i\}_{i\in[l]}$ from the bimodal Gaussian distribution $D^m_{\sigma_2}$.
Step 2: compute the commitment $\mathbf{x} = \sum_{i\in[l]}\mathbf{A}_i\mathbf{r}_i \pmod{2q}$.
Step 3: choose a set of blind factors $\{\mathbf{y}_i\}_{i\in[l]}$ from the bimodal Gaussian distribution $D^m_{\sigma_3}$.
Step 4: compute $\mathbf{w} = \sum_{i\in[l]}\mathbf{A}_i\mathbf{y}_i \pmod{2q}$.
Step 5: compute $\mathbf{c} = H(\mathbf{x} + \mathbf{w} \pmod{2q}, m)$.
Step 6: choose a random bit $t \leftarrow \{0,1\}^n$.
Step 7: compute $\mu = (-1)^t\mathbf{c}$.
Step 8: output the blinded message μ with probability $\min(D^m_{\sigma_1}(\mu)/(M_1 D^m_{\mathbf{c},\sigma_1}(\mu)), 1)$.

Algorithm 1: Message blinded algorithm.

Input: system public parameters PP, blinded message μ, the secret key $\mathbf{S}_j$ of the signer Σj.
Output: blinded signature $\Sigma' = \{\mathbf{z}_i\}_{i\in[l]}$.
Step 1: for all $i \in [l]/\{j\}$: compute $\mathbf{z}_i = \mathbf{r}_i$; for j: compute $\mathbf{z}_j = \mathbf{r}_j + \mathbf{S}_j\mu$.
Step 2: output $\mathbf{z}_j$ with probability $\min(D^m_{\sigma_2}(\mathbf{z}_j)/(M_2 D^m_{\mathbf{S}_j\mu,\sigma_2}(\mathbf{z}_j)), 1)$.
Step 3: output the blinded signature $\Sigma' = \{\mathbf{z}_i\}_{i\in[l]}$.

Algorithm 2: Signature algorithm.

Input: system public parameters PP, blinded signature $\Sigma' = \{\mathbf{z}_i\}_{i\in[l]}$.
Output: blind ring signature $\Sigma = (\{\mathbf{e}_i\}_{i\in[l]}, \mathbf{c})$.
Step 1: for all $i \in [l]$: compute $\mathbf{e}_i = \mathbf{y}_i + \mathbf{z}_i$.
Step 2: output $\mathbf{e}_i$ with probability $\min(D^m_{\sigma_3}(\mathbf{e}_i)/(M_3 D^m_{\mathbf{y}_i,\sigma_3}(\mathbf{e}_i)), 1)$.
Step 3: output the real blind ring signature $\Sigma = (\{\mathbf{e}_i\}_{i\in[l]}, \mathbf{c})$.

Algorithm 3: Unblind algorithm.

Input: system public parameters PP, original message m, public keys $\{\mathbf{A}_i\}_{i\in[l]}$ of the ring R, blind ring signature $\Sigma = (\{\mathbf{e}_i\}_{i\in[l]}, \mathbf{c})$.
Output: 1 or 0.
Step 1: verify that $\|\mathbf{e}_i\| \le \eta\sigma_3\sqrt{m}$ for all $i \in [l]$.
Step 2: verify that $\mathbf{c} = H(\sum_{i\in[l]}\mathbf{A}_i\mathbf{e}_i + q\mathbf{c} \pmod{2q}, m)$.
Step 3: output 1 if the verification in steps 1 and 2 passed and 0 otherwise.

Algorithm 4: Verification algorithm.

4.2. Security Proof

4.2.1. Anonymity. The adversary submits a message m and two users $\mathcal{U}_{i_0}, \mathcal{U}_{i_1} \in R$ to the challenger for a signature query. The challenger randomly chooses a bit $b \in \{0,1\}$ and calls the message blinded algorithm and signature algorithm to generate a blinded signature $\Sigma_{i_b}{}' = \{z_1, \ldots, z_{i_b}, \ldots, z_l\}$ on m, where $\mathbf{z}_{i_b} = \mathbf{r}_{i_b} + \mathbf{S}_{i_b}\mu$, output probability $\min(D^m_{\sigma_2}(\mathbf{z}_{i_b})/M_2 D^m_{\mathbf{S}_{i_b}\mu,\sigma_2}(\mathbf{z}_{i_b}), 1)$, and $\mathbf{z}_i = \mathbf{r}_i \leftarrow D^m_{\sigma_2}$ for all $i \in [l]/\{i_b\}$. Then, the challenger returns Σ_i' to the adversary . Let two random variables X_0 and X_1 represent the blinded signatures generated by the user $\mathcal{U}_{i_0}$ and $\mathcal{U}_{i_1}$.

Suppose that the adversary obtains the blinded signature $\Sigma_{i_b}{}' = \{\mathbf{z}_1, \ldots, \mathbf{z}_{i_b}, \ldots, \mathbf{z}_l\}$ by sampling each $\mathbf{z}_i$ from $D^m_{\sigma_2}$ with probability $1/M_2$, let the random variable Y represent the blinded signature generated by this way. The statistical distance [28] between X_0 and Y satisfies $\Delta(X_0, Y) \le 2^{-\omega(\log m)}/M_2$, and the statistical distance between X_1 and Y satisfies $\Delta(X_1, Y) \le 2^{-\omega(\log m)}/M_2$. Therefore, we have the following:

$$\Delta(X_0, X_1) \le \Delta(X_0, Y) + \Delta(X_1, Y) \le \frac{2^{1-\omega(\log m)}}{M_2}. \quad (8)$$

The statistical distance between X_1 and X_1 is negligible. Therefore, the distribution of blinded signatures Σ_{i_0}' and Σ_{i_1}' is indistinguishable. The proposed scheme satisfies anonymity.

4.2.2. Blindness. The adversary submits two different blinded messages, μ_0 and μ_1, and interacts with two different users $\mathcal{U}_{i_0}$ and $\mathcal{U}_{i_1}$. The adversary and the challenger only choose one of the two users for establishing an interactive blind ring signature protocol. It should be noted that the adversary does not know the user's information who is interacting with him, i.e., we can only prove that the outputs, i.e., the two blind messages μ_0 and μ_1, are indistinguishable, and the corresponding blind ring signature Σ_{i_0} and Σ_{i_1} are also indistinguishable, where $b \in \{0, 1\}$ and $\Sigma_{i_b} = \{\mathbf{e}_1, \ldots \mathbf{e}_{i_b}, \ldots, \mathbf{e}_l\}$.

For two blinded messages, μ_0 and μ_1, because of the construction $\mu = (-1)^t \mathbf{c}$ and the output probability $\min(D^m_{\sigma_1}(\mu)/(M_1 D^m_{\mathbf{c},\sigma_1}(\mu)), 1)$, we can get that μ_0 and μ_1 are sampled from the same distribution $D^m_{\sigma_1}$. Therefore, the statistical distance between μ_0 and μ_1 satisfies $\Delta(\mu_0, \mu_1) = 0$ and they are indistinguishable. For two blind ring signatures Σ_{i_0} and Σ_{i_1}, because $\mathbf{e}_i = \mathbf{y}_i + \mathbf{z}_i$ for all $i \in [l]$ and the output probability $\min(D^m_{\sigma_3}(\mathbf{e}_i)/(M_3 D^m_{\mathbf{y}_i,\sigma_3}(\mathbf{e}_i)), 1)$, we can get Σ_{i_0} and Σ_{i_1} are sampled from the same distribution $D^m_{\sigma_3}$. Therefore, the statistical distance between Σ_{i_0} and Σ_{i_1} satisfies $\Delta(\Sigma_{i_0}, \Sigma_{i_1}) = 0$, and they are indistinguishable. The proposed scheme satisfies blindness.

4.2.3. One-More Unforgeability

Theorem 1. *If an adversary α can successfully give the effective forgery, there will be existing a polynomial-time algorithm Φ that can solve the* $\mathrm{SIS}_{q,n,lm,\beta}$ *problem with non-negligible probability.*

Proof. We will prove the one-more unforgeability of the scheme by the simulation game between challenger and adversary . The simulation game controlled by challenger is executed as follows:

Setup: challenger builds two initial empty lists, List 1 and List 2, respectively, to store the hash value $H(m)$ and signature value $\Sigma = (\{\mathbf{e}_i\}_{i\in[l]}, \mathbf{c})$ of message m. Then, adversary will make hash queries and signature queries to challenger.

Hash queries: *The adversary* sends a hash query for message m to challenger . Challenger checks List 1, where List 1 consists of the pair $(m, H(m))$. If the queried message m is in List 1, challenger sends the corresponding $H(m)$ to *adversary*. If not, challenger will compute a new $H(m)$, restore $(m, H(m))$ into List 1, and send it to *adversary*.

Signature queries: *The adversary* sends a signature query for message m to challenger. hThe challenger checks List 2, where List 2 consists of the pair $(m, \Sigma = (\{\mathbf{e}_i\}_{i\in[l]}, \mathbf{c}))$. If the queried message m is in List 2, challenger sends the corresponding signature value $\Sigma = (\{\mathbf{e}_i\}_{i\in[l]}, \mathbf{c})$ to adversary . If not, challenger will generate a new signature, restore the new pair $(m, \Sigma = (\{\mathbf{e}_i\}_{i\in[l]}, \mathbf{c}))$ into List 2, and send it to adversary .

Forge: suppose $\mathbf{c}_j$ is a result of a hash query made by the adversary . Then, we can get the following:

$$H\left(\sum_{i\in[l]} \mathbf{A}_i \mathbf{e}_i^* + q\mathbf{c}_j \,(\mathrm{mod}\, 2q), m^*\right) = H\left(\sum_{i\in[l]} \mathbf{A}_i \mathbf{e}_i' + q\mathbf{c}_j \,(\mathrm{mod}\, 2q), m'\right). \tag{9}$$

For two different blind ring signature pairs, $(m^*, \Sigma^* = (\{\mathbf{e}_i^*\}_{i\in[l]}, \mathbf{c}_j))$ and $(m', \Sigma' = (\{\mathbf{e}_i'\}_{i\in[l]}, \mathbf{c}_j))$. We can find a hash collision if there exists inequality in the input of the hash function H on both sides of the equal sign of equation (10). Therefore, we can derive that $\sum_{i\in[l]} \mathbf{A}_i \mathbf{e}_i^* + q\mathbf{c}_j = \sum_{i\in[l]} \mathbf{A}_i \mathbf{e}_i' + q\mathbf{c}_j \,(\mathrm{mod}\, 2q)$, $m^* = m'$ with an overwhelming probability. Further simplification can be obtained as $\sum_{i\in[l]} \mathbf{A}_i (\mathbf{e}_i^* - \mathbf{e}_i') = 0 \,(\mathrm{mod}\, 2q)$. Let $\mathbf{e}_i = \mathbf{e}_i^* - \mathbf{e}_i'$, and we have the following:

$$\sum_{i\in[l]} \mathbf{A}_i \mathbf{e}_i = [\mathbf{A}_1 \mid \mathbf{A}_2 \mid \ldots \mid \mathbf{A}_l]\left(\mathbf{e}_1^T, \mathbf{e}_2^T, \ldots, \mathbf{e}_l^T\right)^T. \tag{10}$$

Let $\mathbf{A} = [\mathbf{A}_1 \mid \mathbf{A}_2 \mid \cdots \mid \mathbf{A}_l] \in \mathbb{Z}^{n\times lm}$ and $\mathbf{e} = (\mathbf{e}_1^T, \mathbf{e}_2^T, \ldots, \mathbf{e}_l^T)^T \in \mathbb{Z}^{lm}$. Then, we have $\mathbf{Ae} = \mathbf{0} \,(\mathrm{mod}\, 2q)$.As the forgery of the adversary is valid, there exists at least a bit i such that $\mathbf{e}_i^* \neq \mathbf{e}_i'$ and $\mathbf{e}_i^* - \mathbf{e}_i' \neq 0 \,(\mathrm{mod}\, q)$ with an overwhelming probability, i.e., we can get $\mathbf{e} \neq \mathbf{0} \,(\mathrm{mod}\, q)$ with great probability. Finally, we say that we can successfully solve the SIS problem. The detailed proving process is as follows:

Suppose that $\mathbf{c}_j$ is a result of a hash query made by the adversary , and we can get a new valid forgery $\Sigma' = (\{\mathbf{e}_i'\}_{i\in[l]}, \mathbf{c}_j')$ for message m^* and ring R^*. We have $\mathbf{c}_j' \neq \mathbf{c}_j$ and $\sum_{i\in[l]} \mathbf{A}_i \mathbf{e}_i^* + q\mathbf{c}_j = \sum_{i\in[l]} \mathbf{A}_i \mathbf{e}_i' + q\mathbf{c}_j'$ with a non-negligible probability according to the Forking lemma [29]. Let $\mathbf{e}_i = \mathbf{e}_i^* - \mathbf{e}_i'$, $\mathbf{A} = [\mathbf{A}_1 | \mathbf{A}_2 | \cdots | \mathbf{A}_l]$ and $\mathbf{e} = (\mathbf{e}_1^T, \mathbf{e}_2^T, \ldots, \mathbf{e}_l^T)^T$. We have $\mathbf{Ae} = q(\mathbf{c}_j' - \mathbf{c}_j) \,(\mathrm{mod}\, 2q)$. Because $\mathbf{c}_j' \neq \mathbf{c}_j$ and $q(\mathbf{c}_j' - \mathbf{c}_j) = 0 \,(\mathrm{mod}\, q)$, we can derive $\mathbf{e} \neq \mathbf{0} \,(\mathrm{mod}\, 2q)$ and $\mathbf{Ae} = \mathbf{0} \,(\mathrm{mod}\, q)$. In addition, as $\|\mathbf{e}_i^*\| = \|\mathbf{e}_i'\| \leq \eta\sigma_3\sqrt{m}$ for all $i \in [l]$, according to algorithm 4, we have $\|\mathbf{e}_i\| = \|\mathbf{e}_i^* - \mathbf{e}_j'\| \leq \|\mathbf{e}_i'\| + \|\mathbf{e}_i'\| = 2\eta\sigma_3\sqrt{m}$. Then, it satisfies $\|\mathbf{e}\| = \sum_{i\in[l]} \|\mathbf{e}_i\| \leq 2l\eta\sigma_3\sqrt{m}$. Therefore, $\mathbf{e}$ is a solution to the $\mathrm{SIS}_{q,n,lm,\beta}$ problem with $\beta = 2l\eta\sigma_3\sqrt{m}$, where $\mathbf{Ae} = \mathbf{0} \,(\mathrm{mod}\, q)$ and $\mathbf{e} \neq \mathbf{0} \,(\mathrm{mod}\, q)$. The proposed scheme satisfies the one-more unforgeability. □

5. The Completely Anonymous Blockchain Transaction System

In this section, we construct a completely anonymous blockchain transaction system based on the proposed lattice-based blind ring signature algorithm. Assume a blockchain transaction is required between Alice and Bob, and stipulate

that Alice transfers accounts to Bob. The transaction between Alice and Bob is recorded in a ledger and packaged into the blockchain. The overall schematic diagram of the anonymous blockchain transaction system is shown in Figure 1. The detailed process mainly includes the following five steps:

Key generation: firstly, Alice constructs a ring R composed of multiple members and calls the key generation algorithm and then gets the public and secret key pair (pk_A, sk_A) of ring R, where $pk_A = (pk_1, \ldots, pk_a, \ldots pk_n)$ is a set of ring public keys.

Transaction generation: Bob initiates a transaction request with Alice and generates a piece of transaction information m. Bob and Alice run the blind ring signature algorithm in Section 3. Then, Bob selects the blind factor and utilizes the ring public keys pk_A of Alice to blind the transaction information m to μ. Alice uses the secret key sk_A to generate a signature Σ' for blinded transaction information μ. Bob obtains the real blind ring signature Σ of the transaction information m using the unblind algorithm. Finally, Bob generates a new transaction Tx utilizing the ring public keys pk_A and the blind ring signature Σ of the transaction information m.

Transaction authentication: Bob broadcasts the transaction Tx to the blockchain network, and the miner nodes in the blockchain use the ring public keys pk_A of Alice to verify whether the blind ring signature Σ is correct. It indicates that the transaction is correct if the verification passes, and then, it encapsulates the transaction Tx in a new block. Otherwise, the transaction will be discarded.

Network-wide consensus. The miners broadcast communication through the consensus mechanism and agree to add a new block containing the transaction to the blockchain. Meanwhile, miners who create the new block will be rewarded by the system.

Transaction completion: after blockchain miners have successfully reached the network-wide consensus on the transaction, Bob can consume the transfer received from Alice under the above steps.

The proposed transaction system has the characteristic of complete anonymity that can hide the identity privacy information of both parties participating in a blockchain transaction. For the internal attackers involved in the transaction, based on the blind signature feature, as the transaction initiator performs blind processing on the transaction information, the internal attacker cannot associate any veritable identity of the initiator through the transaction information. Therefore, for the input of each transaction, the internal attacker cannot trace whether it was initiated by the same user. For the external attackers not involved in the transaction, based on the ring signature feature, as the signature of the transaction is verified through ring public keys rather than a unique public key, it is impossible to determine the specific public key associated with the real signer. Therefore, for the output of any two transactions, the external attacker cannot link to the same transaction user. Moreover, the signature algorithm adopted in this system is based on the SIS problem, which cannot be availably solved by existing quantum computing algorithms. Therefore, the system satisfies antiquantum computing security.

6. Performance Evaluation

In this section, we make an evaluation on the performance of the proposed signature algorithm by comparing with other similar literature schemes, including signature and verification algorithm latency, sampling method, the size of the signature, and secret and public keys. Firstly, we give some parameter settings, and then, the comparison results will be presented through theoretical analysis and simulation experiments.

6.1. Parameters Setting. The relevant public parameters of our scheme are set as shown in Table 1, which are the same as in [17]. We select the security level $k = 128$ bits and corresponding challenge size $\kappa = 28$ as an example. Meanwhile, the computational complexity of the SIS problem is maintained by reasonably selecting the parameter n, m, q, which can guarantee the security of public key and secret key. Moreover, the correctness error of the reject sample will be at the most 2^{-100}, which requires that $\sigma_1 = 12\|\nu\| = 12\sqrt{\kappa}$ and $M_1 = e^{12\sqrt{\kappa}/\sigma_1 + \kappa/2\sigma_1^2} = e^{1+1/288} \approx 2.72$. Then, M_2 and M_3 will be derived by the same method.

6.2. Comparison with Other Similar Schemes. We carry out the simulation experiment of efficiency comparison by utilizing MATLAB R2021b in the environment of Windows 11 with Intel(R) Core(TM) i7-10510U CPU 1.80 GHz and 16 G RAM. Assume that the same parameters (n, m, q, l, k, κ), set according to Table 1, are utilized in each of these schemes, the detailed keys and signature size comparison results are shown in Table 2. We choose the parameters $l = 10$, $q = 2^{27}$, $k = 128$ and $\kappa = 28$ for the simulation experiment. Then, we compute the public key size, secret key size, and signature size for the different security parameter n, such as 80, 112, 128, 192, 256, 512. The comparison results of the public key size, secret key size, and signature size are separately shown in Figures 2–4. It can be seen from the experimental results that the size of the signature, secret, and public keys of our proposed scheme are all smaller than others [25, 30]. Moreover, we generate the public and secret keys without trapdoor sampling, which improves sampling efficiency and saves more time for performance.

Next, the results of the signature and verification algorithm latency comparison are shown in Table 3. The signature algorithm latency of the blind ring signature scheme includes message blinded, signature, and unblind algorithm latency. Here, some notations,

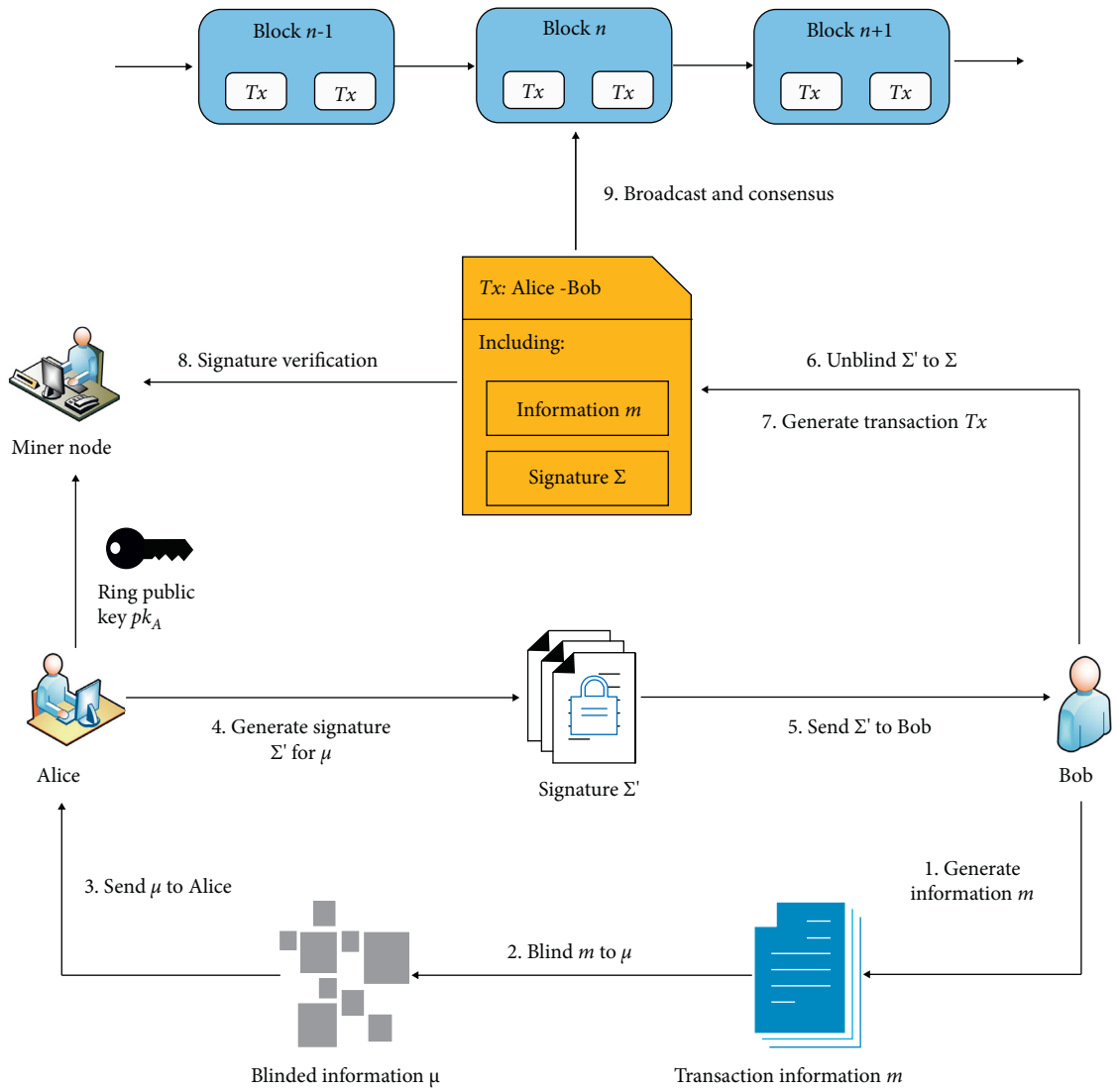

Figure 1: The completely anonymous blockchain transaction system.

Table 1: Public parameters setting.

Parameter PP	Definition	Example
N	Security parameter	512
l	Number of ring members	10
Q	poly (n), prime	2^{27}
m	$m = n \log q$	13824
H	Hash function H: $\{0,1\}^* \longrightarrow \{\mathbf{c} \in \{-1,0,1\}^k : \|\mathbf{c}\|_1 \leq \kappa\}$	-
k and κ	In the hash function H and $2^\kappa \cdot C_k^\kappa \geq 2^{100}$	$k = 128, \kappa = 28$
η	$[1.1, 1.3]$	1.1
σ_1	$12\sqrt{\kappa}$	63
σ_2	$12\eta\sigma_1\sqrt{mk}$	2^{20}
σ_3	$12\eta\sigma_2\sqrt{m}$	2^{30}
$M_1 = M_2 = M_3$	$\exp(12\sqrt{\kappa}/\sigma_1 + \kappa/2\sigma_1^2)$	2.72
Secret key size	$lmn \log 2q$	236 MB
Public key size	$lmn \log 2q$	236 MB
Signature size	$lm \log(12\sigma_3) + \kappa$	0.55 MB

Table 2: Keys and signature size comparison.

Scheme	Public key size	Secret key size	Signature size	Sampling method
Wang et al. [30]	$6lmn\log q$	$l(6m)^2\log q$	$6lm\log q + l$	Trapdoor sampling
Le et al. [25]	$6lmn\log q$	$6lmn\log q$	$6lm\log(12\sigma_3) + n + \kappa$	Trapdoor sampling
Our scheme	$lmn\log 2q$	$lmn\log 2q$	$lm\log(12\sigma_3) + \kappa$	Without trapdoor sampling

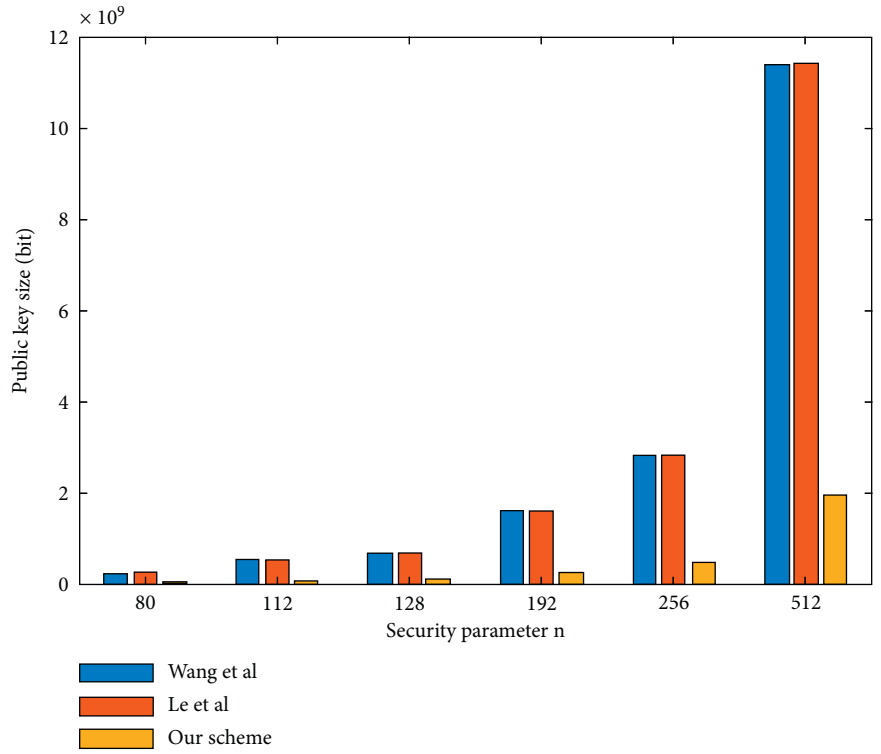

Figure 2: The comparison of public key size.

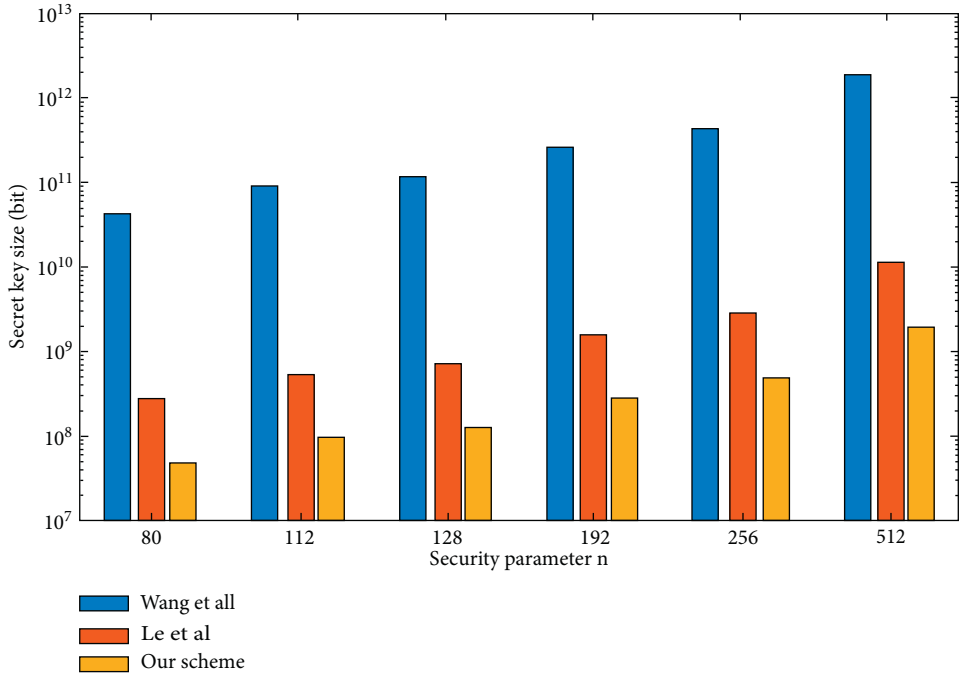

Figure 3: The comparison of secret key size.

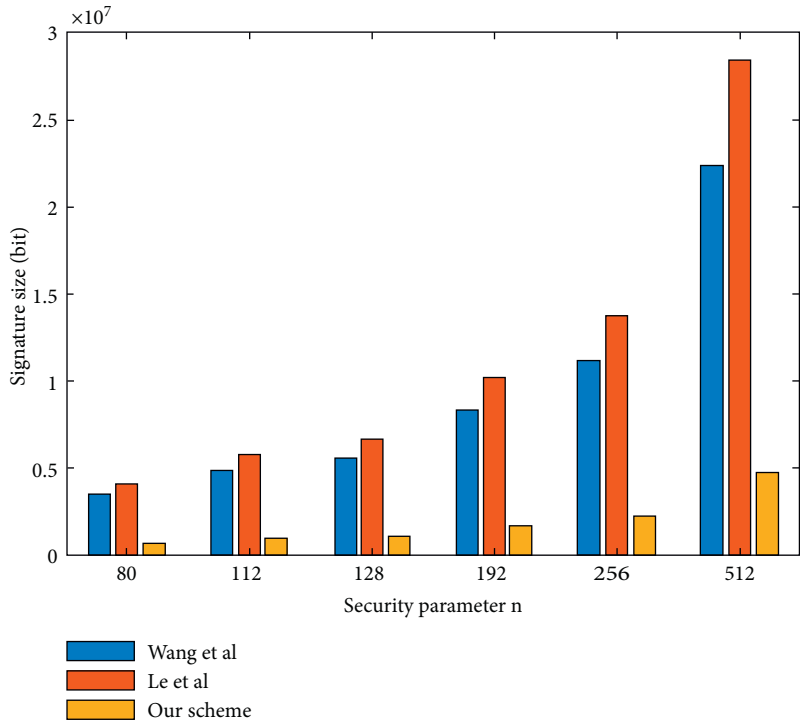

Figure 4: The comparison of signature size.

Table 3: Latency comparison.

Scheme	Signature algorithm latency	Verification algorithm latency
Le et al. [25]	$4(l+1)T_{\text{Mul}} + 2T_{\text{Hash}} + 3T_{RS} + T_{\text{Com}}$	$(l+1)T_{\text{Mul}} + T_{\text{Hash}} + T_{\text{Com}}$
Our scheme	$(2l+1)T_{\text{Mul}} + T_{\text{Hash}} + 2T_{\text{RS}}$	$(l+1)T_{\text{Mul}} + T_{\text{Hash}}$

such as T_{Mul}, T_{Hash}, T_{RS}, and T_{Com}, should be explained. The latency for multiplication is represented by T_{Mul}. The latency for the Hash operation is represented by T_{Hash}. The latency for rejection sampling operation is represented by T_{RS}. The latency for commitment function calculation is represented by T_{Com}. As can be seen from Table 3, our proposed blind ring signature scheme has lower signature and verification algorithm latency than the other similar scheme [25].

7. Conclusion

In this paper, we propose a new lattice-based blind ring signature scheme, which satisfies the correctness and security under the random oracle model, including anonymity, blindness, and one-more unforgeability. Meanwhile, the constructed blockchain transaction system based on our proposed blind ring signature satisfies the complete anonymity and antiquantum computing security of users' identity privacy. Moreover, the proposed signature scheme has lower latency, smaller key, and signature sizes than other similar schemes.

However, our proposed scheme has some limitations. On the one hand, the proposed blind ring signature scheme relies on the difficult problem on the standard lattice, which leads to some disadvantages, such as large storage space of the key matrix, low operation speed, and slow sampling rate, by comparing with structured lattice, such as ideal lattice. On the other hand, our constructed blockchain transaction system focuses on the implementation of user identity anonymity while ignoring the problem of double-spending attacks. In the future, firstly, we will study the linkable blind ring signature algorithm based on the ideal lattice to solve the limitations in the current work. Secondly, we will introduce the proposed blind ring signature algorithm into more specific blockchain application scenarios, such as medical blockchain and blockchain-enabled Internet of Things. Finally, we will study more cryptographic methods for blockchain data privacy protection, such as searchable encryption [32, 33], to improve blockchain privacy protection mechanisms.

Data Availability

The data and the code used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

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

Acknowledgments

This work was supported by the Fundamental Research Funds for Beijing Municipal Commission of Education, the Scientific Research Launch Funds of North China University of Technology, and Beijing Urban Governance Research Base of North China University of Technology.

References

[1] S. Nakamoto, "Bitcoin: A Peer-To-Peer Electronic Cash System," *Decentralized Business Review*, vol. 21260, 2008.

[2] M. Ober, S. Katzenbeisser, and K. Hamacher, "Structure and anonymity of the bitcoin transaction graph," *Future Internet*, vol. 5, no. 2, pp. 237–250, 2013.

[3] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Security and Privacy in Social Networks*, pp. 197–223, Springer, New York, NY, USA, 2013.

[4] D. Chaum and E. V. Heyst, "Group signatures," in *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 257–265, Springer, Heidelberg, Germany, 1991.

[5] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 552–565, Springer, Heidelberg, Germany, June 2001.

[6] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, pp. 199–203, Springer, Boston, MA, USA, 1983.

[7] X. Yi and K. Y. Lam, "A new blind ECDSA scheme for bitcoin transaction anonymity," in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pp. 613–620, Association for Computing Machinery, New York, NY, USA, June 2019.

[8] H. Yi, "A traceability method of biofuel production and utilization based on blockchain," *Fuel*, vol. 310, Article ID 122350, 2022.

[9] Z. Wang and J. Fan, "Flexible threshold ring signature in chronological order for privacy protection in edge computing," *IEEE Transactions on Cloud Computing*, vol. 10, no. 2, pp. 1253–1261, 2022.

[10] T. K. Chan, K. Fung, J. K. Liu, and V. K. Wei, "Blind spontaneous anonymous group signatures for ad hoc groups," in *Proceedings of the European Workshop on Security in Ad-Hoc and Sensor Networks*, pp. 82–94, Springer, Heidelberg, Germany, July 2004.

[11] Q. Wu, F. Zhang, W. Susilo, and Y. Mu, "An efficient static blind ring signature scheme," in *Proceedings of the International Conference on Information Security and Cryptology*, pp. 410–423, Springer, Heidelberg, Germany, May 2005.

[12] H. Sun and Y. Ge, "New certificateless blind ring signature scheme," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 12, no. 1, pp. 778–783, 2014.

[13] D. Hoang Duong, W. Susilo, and H. T. N. Tran, "A multivariate blind ring signature scheme," *The Computer Journal*, vol. 63, no. 8, pp. 1194–1202, 2020.

[14] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, IEEE, Santa Fe, NM, USA, November 1994.

[15] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pp. 212–219, Association for Computing Machinery, New York, NY, USA, July 1996.

[16] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, pp. 197–206, Association for Computing Machinery, New York, NY, USA, May 2008.

[17] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 738–755, Springer, Heidelberg, Germany, June 2012.

[18] L. Ducas, A. Durmus, T. Lepoint, and L. Vadim, "Lattice signatures and bimodal Gaussians," in *Proceedings of the Annual Cryptology Conference*, pp. 40–56, Springer, Heidelberg, Germany, July 2013.

[19] Y. L. Gao, X. B. Chen, Y. L. Chen, Y. Sun, X. X. Niu, and Y. X. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, Article ID 27205, 2018.

[20] H. Zou, X. Liu, W. Ren, and Z. Tianqing, "A decentralized electronic reporting scheme with privacy protection based on proxy signature and blockchain," *Security and Communication Networks*, vol. 2022, Article ID 5424395, 8 pages, 2022.

[21] M. Rückert, "Lattice-based blind signatures," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 413–430, Springer, Heidelberg, Germany, July 2010.

[22] C. Li, Y. Tian, X. Chen, and J. Li, "An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems," *Information Sciences*, vol. 546, pp. 253–264, 2021.

[23] C. A. Melchor, S. Bettaieb, and X. Boyen, "Adapting Lyubashevsky's signature schemes to the ring signature setting," in *Proceedings of the International Conference on Cryptology in Africa*, pp. 1–25, Springer, Heidelberg, Germany, June 2013.

[24] R. Zhao, S. Wang, and Y. Zhang, "Lattice-based ring signature scheme under the random oracle model," *International Journal of High Performance Computing and Networking*, vol. 11, no. 4, pp. 332–341, 2018.

[25] H. Q. Le, D. H. Duong, and W. Susilo, "A blind ring signature based on the short integer solution problem," in *Proceedings of the International Workshop on Information Security Applications*, pp. 92–111, Springer, Cham, New York, NY, USA, June 2019.

[26] G. Xu, Y. B. Cao, S. Y. Xu et al., "A novel post-quantum blind signature for log system in blockchain," *Computer Systems Science and Engineering*, vol. 41, no. 3, pp. 945–958, 2022.

[27] C. H. Jiao and X. Y. Xiang, "Anti-quantum lattice-based ring signature scheme and applications in VANETs," *Entropy*, vol. 23, no. 10, p. 1364, 2021.

[28] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, pp. 147–191, Springer, Heidelberg, Germany, 2009.

[29] M. Bellare and G. Neven, "Multi-signatures in the plain public-key model and a general forking lemma," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 390–399, Association for Computing Machinery, New York, NY, USA, October 2006.

[30] J. Wang and B. Sun, "Ring signature schemes from lattice basis delegation," in *Proceedings of the International Conference on Information and Communications Security*, pp. 15–28, Springer, Heidelberg, Germany, July 2011.

[31] D. Micciancio and S. Goldwasser, "Complexity of lattice problems: a cryptographic perspective," *Springer Science & Business Media*, vol. 671, 2012.

[32] G. Xu, S. Xu, Y. Cao, F. Yun, Y. Cui, Y. Yu et al., "PPSEB: a postquantum public-key searchable encryption scheme on blockchain for E-healthcare scenarios," *Security and Communication Networks*, vol. 2022, Article ID 3368819, 13 pages, 2022.

[33] G. Xu, Y. Cao, S. Xu, X. Liu, X. B. Chen, and Y. Yu, "A Searchable Encryption Scheme Based on Lattice for Log Systems in Blockchain," *CMC-Computers Materials & Continua*, vol. 72, no. 3, pp. 5429–5441, 2022.