Hindawi
Mathematical Problems in Engineering
Volume 2020, Article ID 7528571, 12 pages
https://doi.org/10.1155/2020/7528571

Research Article

An Identity-Based Blind Signature Scheme Using Lattice with Provable Security

Quanrun Li,[1,2] Chingfang Hsu,[2] Debiao He,[1,3] Kim-Kwang Raymond Choo,[4] and Peng Gong[5]

[1] *Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen 051800, China*
[2] *Information Security Lab, Computer School, Central China Normal University, Wuhan 430072, China*
[3] *School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China*
[4] *Department of Information Systems and Cyber Security and the Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249, USA*
[5] *School of Mechatronical Engineering, Beijing Institute of Technology, Beijing 100081, China*

Correspondence should be addressed to Peng Gong; penggong@bit.edu.cn

Received 24 January 2020; Accepted 17 April 2020; Published 11 May 2020

Academic Editor: Emilio Insfran Pelozo

With the rapid development of quantum computing and quantum information technology, the universal quantum computer will emerge in the near decades with a very high probability and it could break most of the current public key cryptosystems totally. Due to the ability of withstanding the universal quantum computer's attack, the lattice-based cryptosystems have received lots of attention from both industry and academia. In this paper, we propose an identity-based blind signature scheme using lattice. We also prove that the proposed scheme is provably secure in the random oracle model. The performance analysis shows that the proposed scheme has less mean value of sampling times and smaller signature size than previous schemes. Thus, the proposed scheme is more suitable for practical applications.

1. Introduction

Currently, the emergence of quantum computing causes a potential threat to the traditional cryptosystems. In 2011, the first commercial quantum computer "D-Wave One" was worked out, which provided the application of certain cracking algorithms to the traditional public key cryptography with feasible condition. Furthermore, it is because most of mathematical hard problems in the traditional cryptosystems are vulnerable to the strong computing power of quantum computers. Therefore, it is obvious that the influence quantum computers bring to the traditional cryptosystem will permeate into the information security and Internet security of all areas of a country, such as politics, economy, culture, and military.

Specifically, it can be explained from two main aspects: Firstly, for the integer factorization problem, the conjecture that an n-bit integer can be decomposed by the n-qubit quantum computer easily is proposed by Beauregard [1]. As for the discrete logarithm problem, Proos and Zalka [2] pointed out that n-bits elliptic curve discrete logarithmic problem [3, 4] can be solved by n-qubit quantum computer. Secondly, the valid length of the secret key in traditional cryptosystem will be half of the original length under the attack of quantum adversary.

Blind signature was first proposed by Chaum [5] to make electronic money in an electronic cash system. In general, the user can get a valid signature of any message through a blind signature scheme, where the signer knows nothing about the actual message. This special property makes the blind signature used widely. Therefore, a plenty of blind schemes were worked out after the work of Chaum, such as [6, 7]. However, those schemes had the significant problem on certificates, which is the core problem in public key infrastructure (PKI) cryptosystem. In 1984, the identity-based (ID-based) public key cryptosystem was worked out by Shamir [8], which is useful to eliminate the serious defect of the PKI cryptosystem. Since then, lots of ID-based blind signature schemes were proposed with efficient performance.

As is known to all, most of the above blind signature schemes cannot resist the attack of quantum algorithms. It is because the computational power of the quantum computers is so strong that the hard problems in those schemes are easy to be broken. In order to remove this threat, the postquantum cryptography appears in the vision of cryptographers, which is that the traditional cryptosystem still holds its security under the attack of the quantum adversary. In the postquantum cryptography systems, the lattice-based cryptography is the most promising. Currently, lots of cryptographic protocols have been devised on the lattice, such as [9–11].

There are several advantages of the lattice-based cryptography which are worth noting. Firstly, this cryptosystem has got widespread attention in the last decade. Then, this cryptography currently cannot be broken by any algorithms, including quantum algorithms. Moreover, lattice-based cryptography has the same level of security in the average case and the worst case. Finally, the designs of lattice-based schemes are very simple and efficient, including mainly matrix-vector multiplication, linear summation operation, and modulo operation.

Taking advantage of these benefits, some blind signature schemes were designed, but several problems included in these schemes make them inapplicable in the real environment. For example, some blind signature schemes lack the formal security proof or describe the ability of the adversary incorrectly. Besides, the efficiency shortcomings in other schemes are too serious to be neglected, such as the scheme proposed by Rückert [12] and the work of Zhang et al. [13]. The main reason for this is that complex algorithms are used in the process of signing or the efficient aborting technology is not involved in these blind signature schemes.

In order to improve the practicability of blind signature, a new ID-based scheme on lattice is proposed in this paper, which is more efficient and secure. Specifically, the main contributions of this paper are as follows:

(1) Firstly, our blind signature scheme can resist the attack of the malicious quantum adversaries, because it is based on lattice. Meanwhile, we prove that our scheme is secure based on SIS problem in the random oracle model. The lattice cryptosystem also makes it more efficient due to the simple operations involved in lattice-based algorithms.

(2) Secondly, we use the bimodal Gaussian rejection sampling in our scheme to prevent the leakage of critical information, such as the signer's secret key. Using this aborting technology, it makes the mean value of sampling times needed to generate a valid signature smaller. Additionally, we can get the blind signature with smaller size under this novel technology.

(3) Finally, because the framework of ID-based cryptosystem is used in our scheme, it means that the additional cost is not needed to manage lots of certificates in our scheme. Therefore, the proposed scheme under this cryptosystem is more practical in the real application.

2. Related Work

In this section, we will mainly talk about the related works on the blind signature schemes. Due to its excellent concealment, blind signature has been studied widely and put into the applications where important data needs to hold its privacy, such as electronic cash (e-cash) [14], electronic voting [15], and oblivious transfer [16].

In order to design electronic money used in the e-cash system, Chaum [5] proposed the first blind signature scheme. After the work of Chaum, lots of blind signature schemes were worked out based on PKI cryptosystem, the hardness of which is mostly based on the integer factorization problem or discrete logarithm problem [17–19]. However, as we all know, the issue of certificates' management is an apparent defect in this cryptosystem. Fortunately, the identity-based public key cryptography was proposed by Shamir [8] to eliminate this drawback.

Owing to the good advantages of ID-based cryptosystem, the first ID-based blind signature scheme was worked out by Zhang and Kim [20]. Later, Huang et al. [21] proposed another ID-based blind signature scheme in 2005. In 2008, a generalized ID-based blind signature with bilinear pairings was designed by Kalkan et al. [22]. Then, in 2010, Rao et al. [23] constructed a blind signature scheme on the basis of ID-based digital signature framework proposed by Hess [24]. Following the work of Rao et al, a provably secure randomized blind signature scheme was constructed by Fan et al. [25] using bilinear pairings. Furthermore, there were two other new ID-based blind signature schemes based on bilinear pairings designed by Zhang et al. [26] and Shakerian et al. [27], respectively, in the same year.

However, in 2011, He et al. [28] proposed a novel ID-based blind signature scheme using no bilinear pairings. Their work opened up a new direction in the design of the ID-based blind signature scheme, because the new blind signature scheme constructed by them guaranteed both high efficiency and anonymity. Later, a new provably secure and pairing-free ID-based partially blind signature scheme was worked out by Islam et al. [29] in 2016, which was used in an online e-cash system. Besides, this scheme was provably secure in the random oracle model. In 2017, an untraceable ID-based blind signature scheme without pairing for e-cash payment system was proposed by Kumar et al. [30]. Then, James et al. [31] proposed an efficient pairing-free ID-based blind signature scheme with message recovery in 2018.

Although ID-based cryptosystem can solve the efficiency drawback of schemes in PKI cryptosystem, it cannot resist the attack of quantum algorithms. In 2010, the first lattice-based blind signature scheme was proposed by Rückert [12], which was provably secure in the random oracle model. Later, in 2017, a novel round-optimal lattice-based blind signature scheme used in the cloud services was constructed by Zhu et al. [32]. Similarly, a new postquantum blind signature scheme on lattice was proposed by Zhang et al. [13] in 2018, in which the unimodal rejection sampling technology was used to improve the probability of generating a valid signature.

Unfortunately, the efficiency problem still existed in these schemes because they were designed under the PKI cryptosystem. So some ID-based blind signature schemes were worked out to deal with this disadvantage of previous schemes. In 2014, Zhang and Ma [33] proposed a lattice-based proxy blind signature scheme based on ID-based cryptosystem, whose security was held in the standard model. Then, another ID-based blind signature scheme on lattice was constructed by Gao et al. [34] in 2016, which was based on the standard model. Interestingly, a two-round ID-based blind signature scheme on lattice was still proposed by Gao et al. [35] on the random oracle model in 2017. In addition, this scheme was proved to have the power to resist the selective identity and chosen message attacks to remain unforgeable and unconditionally blind based on the SIS problem.

However, no aborting technology or only unimodal rejection sampling was used in these schemes. In 2013, Ducas et al. [36] proposed a modified aborting technology based on the original rejection sampling, called bimodal Gaussians rejection sampling, which reduces the rejecting field between the actual sampling distribution function and the expected sampling distribution function. This means that the signer can generate a valid signature with fewer samples. Additionally, this new aborting technology still keeps the basic ability to prevent the leakage of information of the signer's secret key. Therefore, using the bimodal Gaussian rejection sampling, a new ID-based blind signature scheme on lattice is constructed in this paper based on the work of Zhang et al. [13]. Our scheme has the excellent ability to resist quantum algorithm and high efficiency, combining the advantages of lattice-based cryptosystem with that of ID-based cryptosystem.

3. Preliminaries

In this section, the basic knowledge about lattices will be described firstly. Next, we introduce the Gaussian distribution in detail.

3.1. Lattices. A lattice L is defined as a discrete additive subgroup of n-dimensional Euclidean vector space $\mathbf{R}^n$. Namely, if $\mathbf{b}_1, \ldots, \mathbf{b}_n$ are n linearly independent vectors in $\mathbf{R}^n$, a lattice L is the set of all integer combinations of these vectors:

$$L(\mathbf{B}) = L(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathrm{Z} \right\}, \tag{1}$$

and the matrix $\mathbf{B}$ is one base of $L(\mathbf{B})$. Normally, n is described as its corresponding dimension.

In particular, the following two types of lattices should be paid more attention, called module lattice:

$$\begin{aligned} L_q^{\perp}(\mathbf{A}) &= \{\mathbf{x} \in \mathrm{Z}^m \colon \mathrm{A}\mathbf{x} = \mathbf{0} (\operatorname{mod} q)\}, \\ L_q^{\mathbf{u}}(\mathbf{A}) &= \{\mathbf{x} \in \mathrm{Z}^m \colon \mathrm{A}\mathbf{x} = \mathbf{u} (\operatorname{mod} q)\}. \end{aligned} \tag{2}$$

3.1.1. Small Integer Solution (SIS) Problem. Given a positive integer q, a matrix $\mathbf{A} \in \mathrm{Z}_q^{n*m}$, and a real number $\beta > 0$, the SIS problem is to find a nonzero vector $\mathbf{v} \in \mathrm{Z}^m$ such that $\mathbf{Av} = \mathbf{0} (\operatorname{mod} q)$, and $\|\mathbf{v}\| \leq \beta$. This kind of SIS problem is homogeneous. As for inhomogeneous SIS problem, it is to find a nonzero preimage $\mathbf{v} \in \mathrm{Z}^m$ satisfying $\mathbf{Av} = \mathbf{t} (\operatorname{mod} q)$, where $\|\mathbf{v}\| \leq \beta$.

Then, there are two important algorithms used in our protocol, which are applied to generate the secret keys of the trusted third party and the signer.

3.1.2. Trapdoor Generation Algorithm. An integer $q \geq 3$, $m > 5n \log q$; there is an effective algorithm $\mathrm{TrapGen}(q, m)$ that can generate a matrix $\mathbf{A} \in \mathrm{Z}_q^{n*m}$ and a basis $\mathbf{T}_A \in \mathrm{Z}^{m*m}$ of the lattice $L^{\perp}(\mathbf{A})$. Besides, the distribution of the matrix $\mathbf{A}$ is the uniform distribution in Z_q^{n*m} approximately and the orthogonal matrix $\widehat{\mathbf{T}_A} \leq O(\sqrt{n \log q})$.

3.1.3. General Preimage Sampling Algorithm. There are an integer $m \geq n$, a prime number q, and a positive integer k. The lattice $L^{\perp}(\mathbf{A})$ is defined by the matrix $\mathbf{A} \in \mathrm{Z}_q^{n*m}$. Additionally, the matrix $\mathbf{T}_A \in \mathrm{Z}^{m*m}$ is a base of the lattice $L^{\perp}(\mathbf{A})$. If the parameter of the Gaussian distribution $s \geq \|\widehat{\mathbf{T}_A}\| \omega(\sqrt{\log n})$, there is a polynomial-time algorithm $\mathrm{SampleMat}(\mathbf{A}, \mathbf{T}_A, s, \mathbf{U})$, where $\mathbf{U}$ is a random matrix defined in Z_q^{n*k}, sampling a matrix $\mathbf{V} \in \mathrm{Z}^{m*k}$ in a distribution closing to $G_{\mathbf{L}^{\mathrm{U}}(\mathbf{A}), s}$, such that $\mathbf{AV} = \mathbf{U} (\operatorname{mod} q)$.

3.2. Gaussian Distribution and Bimodal Gaussian Rejection Sampling

3.2.1. Gaussian Distribution. In statistics, the distribution function of continuous Gaussian distribution is $\rho_{c,\delta}(x) = e^{(-\|x-c\|^2/2\delta^2)}$, where c is the center and δ is the standard deviation. Furthermore, if $c = 0$, we usually make the equation simpler, writing it as $\rho_{\delta}(x)$. In the case of lattice L, the function is $\rho_{c,\delta}(L) = \sum_{\mathbf{x} \in L} \rho_{c,\delta}(\mathbf{x})$. So the discrete Gaussian distribution over Z is written as $G_{c,\delta}(x) = (\rho_{c,\delta}(x)/\rho_{c,\delta}(\mathrm{Z}))$. Meanwhile, the discrete Gaussian distribution defined over Z^m is normally described as $G_{c,\delta}^m(\mathbf{x}) = (\rho_{\mathbf{c},\delta}(\mathbf{x})/\rho_{c,\delta}(\mathrm{Z}^m))$. If the center $c = 0$, we usually write these two symbols as $G_{\delta}(x)$ and $G_{\delta}^m(\mathbf{x})$.

In the following, some theorems on the discrete Gaussian distribution are shown.

Theorem 1. *We assume that $k \geq 1$, so the following formula holds:*

$$\mathbf{Pr}\left[\|\mathbf{z}\| > k * \delta * \sqrt{m} \colon \mathbf{z} \longleftarrow G_{\delta}^{m}\right] < k^m e^{(m/2)\left(1-k^2\right)}. \tag{3}$$

Furthermore, if we have $\delta, r > 0$, and for any element $\mathbf{v} \in \mathbf{R}^m$, the following conclusion is made out:

$$\mathbf{Pr}\left[|\langle \mathbf{z}, \mathbf{v}\rangle| > r : \mathbf{z} \longleftarrow G_{\delta}^{m}\right] \leq 2e^{-\left(r^{2}/2\|\mathbf{v}\|^{2}\delta^{2}\right)}. \tag{4}$$

Theorem 2. *It is described that we have $\delta = \alpha\|\mathbf{v}\|$, where $\alpha > 0$, and $\mathbf{v}$ is an element in Z^{m}. We have*

$$\mathbf{Pr}\left[\frac{G_{\delta}^{m}(\mathbf{z})}{G_{\mathbf{v},\delta}^{m}(\mathbf{z})} < e^{12/\alpha+1/2\alpha^{2}} : \mathbf{z} \longleftarrow G_{\delta}^{m}\right] = 1 - 2^{-100}. \tag{5}$$

Theorem 3. *If the matrix $\mathbf{A} \in Z_{q}^{n*m}$ is chosen randomly and $\mathbf{e} \longleftarrow G_{Z^{m},\delta}$, we have that $\mathbf{t} = \mathbf{Ae}(mod\, q)$, whose distribution is uniform approximately in Z_{q}^{n}.*

3.2.2. Rejection Sampling. The rejection sampling is a useful aborting skill in lattice-based schemes. Speaking in formal terms, when the positive constant M and a special distribution f are given, we need to find another distribution g, which makes $f(x) \leq M * g(x)$. So we can say that the distribution $x \longleftarrow g$ is seen as another distribution f with the probability $f(x)/Mg(x)$. In general, M is the mean value of times to get an effective sample.

(1) Rejection Sampling Lemma. It is assumed that h is a distribution whose preimage is $\mathbf{V}$, where $\mathbf{V} \subseteq Z^{m}$, and $\mathbf{V}$ maps to $\mathbf{R}$. When $\delta = \omega(T\sqrt{\log m})$, we can have a constant $\mathbf{M}$ to give the distribution of the following output:

(1) $\mathbf{v} \longleftarrow h$.

(2) $\mathbf{z} \longleftarrow G_{\delta}^{m}$.

(3) The $(\mathbf{z}, \mathbf{v})$ is given out with the probability $1/\mathbf{M}$ is within the statistical distance $2^{-\omega(\log m)}/\mathbf{M}$ of another distribution:

(1) $\mathbf{v} \longleftarrow h$

(2) $\mathbf{z} \longleftarrow G_{\mathbf{v},\delta}^{m}$

(3) The output $(\mathbf{z}, \mathbf{v})$ is sent with the probability $\min(G_{\delta}^{m}(\mathbf{z})/\mathbf{M}G_{\mathbf{v},\delta}^{m}(\mathbf{z}), 1)$

(2) Bimodal Gaussian Rejection Sampling. In the original Gaussian rejection sampling, the mean value of repetitions of the sampling is $\mathbf{M} \approx e(1)$, when the standard deviation $\delta = \tau\|\mathbf{Sc}\|$, where the Gaussian "tail-cut" factor τ is proportional to the square root of the security parameter.

In this paper, we introduce the bimodal Gaussian rejection sampling in our scheme to get a smaller rejection area and signature size. As the paper in [13] mentioned, $\mathbf{z} = \mathbf{Sc} + \mathbf{y}$ is considered as signer's signature. But the form of the signature must be changed if we need to use the bimodal Gaussian rejection sampling in the scheme. Before the signer begins to sign the message, a random bit $b \in \{-1, 1\}$ is sampled. Then, the relevant signature is $\mathbf{z} = b\mathbf{Sc} + \mathbf{y}$. Thus, the probability distribution of $\mathbf{z}$ is $(1/2)G_{\mathbf{Sc},\delta}^{m} + (1/2)G_{-\mathbf{Sc},\delta}^{m}$. According to the requirement of rejection sampling, firstly, the inequality $f(x) \leq \mathbf{M} * g(x)$ must be held. Secondly, we need to make $\mathbf{M}$ as small as possible. For the sake of interpretation, we give out the following formula:

$$\begin{aligned}\frac{G_{\delta}^{m}(\mathbf{x})}{(1/2)G_{\mathbf{Sc},\delta}^{m}(\mathbf{x}) + (1/2)G_{-\mathbf{Sc},\delta}^{m}(\mathbf{x})} &= e^{\left(\left(\|\mathbf{Sc}\|^{2}/2\delta^{2}\right)/\cosh\left(\langle \mathbf{x},\mathbf{Sc}\rangle/\delta^{2}\right)\right)} \\ &\leq e^{\left(\|\mathbf{Sc}\|^{2}/2\delta^{2}\right)}.\end{aligned} \tag{6}$$

Because there is a fact in math that the inequality $\cosh(y) \geq 1$ is always true for any y, we can get the value $\mathbf{M} = e(1)$ by making δ get the value $\|\mathbf{Sc}\|/\sqrt{2}$ instead of the value $\tau\|\mathbf{Sc}\|$. It is easy to see that the mean value $\mathbf{M}$ in the bimodal Gaussian rejection sampling is smaller than that of original Gaussian rejection sampling. Besides, we know that the size of the final signature on lattice is roughly $\delta\sqrt{m}$ so that this size of the signature produced by using this rejection sampling is much shorter.

4. Security Model

In this section, the security model of the blind signature will be introduced in detail. Normally, in addition to all kinds of security attributes that a general signature scheme has, a blind signature should have two more security attributes:

(i) Blindness: the signer does not know the specific content of the actual message signed by itself.

(ii) Unforgeability: after a message is signed, the signer who gets the signature of this message cannot link this signature to the details of the corresponding process.

In fact, blindness means that a malicious signer can only get information independent of the actual message. In particular, there is a formal game used to describe the blindness.

4.1. Blindness Game. If any probabilistic polynomial-time algorithm cannot win the following game, we will consider the corresponding ID-based signature protocol as blind. In this game, there are two honest users $\mathbf{U}_0$ and $\mathbf{U}_1$. In addition, $\mathbf{A}$ is considered to be a malicious signer. The game of blindness is defined as follows:

(1) $\mathbf{A}$ gets the public parameters params by querying Setup.

(2) $\mathbf{A}$ performs $\text{Extract}(\text{params}, \text{ID}) \longrightarrow \mathbf{S}_{\text{ID}}$. Namely, $\mathbf{A}$ can get the secret key $\mathbf{S}_{\text{ID}}$ of the identity ID by using Key Extract algorithm.

(3) $\mathbf{A}$ chooses a random bit $\mathbf{b} \in \{0, 1\}$ secretly. Then it sends a pair of messages $(m_{\mathbf{b}}, m_{1-\mathbf{b}})$ to $\mathbf{U}_0$ and $\mathbf{U}_1$.

(4) $\mathbf{A}$ executes the signature scheme with $\mathbf{U}_0$ and $\mathbf{U}_1$, respectively. The messages input by $\mathbf{U}_0$ and $\mathbf{U}_1$ are $m_{\mathbf{b}}$ and $m_{1-\mathbf{b}}$.

(5) The outputs $(\delta_{\mathbf{b}}, m_{\mathbf{b}})$ and $(\delta_{1-\mathbf{b}}, m_{1-\mathbf{b}})$ received by $\mathbf{U}_0$ and $\mathbf{U}_1$ are sent to $\mathbf{A}$ in arbitrary order.

(6) $\mathbf{A}$ outputs a bit $\mathbf{b}' \in \{0, 1\}$.

It is worth noting that $\mathbf{A}$ wins the game of blindness if and only if $\mathbf{b}' = \mathbf{b}$. Moreover, we consider $\mathbf{A}\,\mathbf{dv}_{\mathrm{IDBS}}^{\mathrm{Blind}}$ as the advantage of $\mathbf{A}$ to win this game.

Next, another security game aimed at unforgeability will be defined as below. In this game, $\mathbf{S}$ acts as the challenger and $\mathbf{A}$ is an adversary playing as a user.

4.2. Unforgeability Game. We think that $\mathbf{A}$ can break the unforgeability of an ID-based blind signature scheme, if $\mathbf{A}$ makes q_E extract queries and q_S issue queries during the time t and the corresponding advantage $\mathbf{A}\,\mathbf{dv}_{\mathrm{IDPS}}^{\mathrm{UF}}$ of $\mathbf{A}$ is ε at least. Otherwise, this scheme is unforgeability. The game of unforgeability is defined as follows:

(1) Setup: after inputting the security parameter 1^{λ}, $\mathbf{S}$ runs the Setup algorithm to generate the systematic public parameter params and the master secret key $\mathbf{sk}$. Then, the public parameter params is sent to $\mathbf{A}$.

(2) Query: there are three kinds of queries that $\mathbf{A}$ can choose to send to $\mathbf{S}$.

   (a) Hash query: after getting this query, $\mathbf{S}$ would select a random value and return it to $\mathbf{A}$. It is worth noting that random oracle queries are responded by the challenger consistently.

   (b) Extract query: after receiving this query, $\mathbf{S}$ would run the Key Extract algorithm to get the relevant secret key $\mathbf{sk}_{\mathrm{ID}}$ and give it back to $\mathbf{A}$.

   (c) Issue query: after obtaining this query, $\mathbf{S}$ executes the sign algorithm with $\mathbf{A}$ cooperatively to get the signature $\mathbf{sig}$. But before this operation, $\mathbf{S}$ would get the ID's secret key $\mathbf{S}_{\mathrm{ID}}$ by performing the extract query. Finally, the signature $\mathbf{sig}$ is given back to $\mathbf{A}$.

(3) Forgery: after the above query phase, $\mathbf{A}$ will use the useful information to forge a signature $\mathbf{sig}^{\star}$ corresponding to the message $u^{\star}$ of the user, of which identity is $\mathrm{ID}^{\star}$. Additionally, $\mathbf{A}$ outputs n valid signature pairs $(u_1, \mathbf{sig}_1), \ldots, (u_n, \mathbf{sig}_n)$, where $(u^{\star}, \mathbf{sig}^{\star}) = (u_n, \mathbf{sig}_n)$. If the following conditions are satisfied by these signature pairs, we can conclude that $\mathbf{A}$ wins this game. Furthermore, $\mathbf{A}\,\mathbf{dv}_{\mathrm{IDBS}}^{\mathrm{UF}}$ is the advantage of $\mathbf{A}$ to get final success in this game.

   (a) For any i and j, we have that $u_i \neq u_j$, where $i \neq j$ and $i, j \in \{1, \ldots, n\}$.

   (b) $n > q_S$.

   (c) $\mathbf{A}$ never uses the extract query to get the secret key $\mathbf{s}_{\mathrm{ID}^{\star}}$ of the user whose identity is $\mathrm{ID}^{\star}$.

Generally, an ID-based blind signature is considered to have blindness and unforgeability, if $\mathbf{A}\,\mathbf{dv}_{\mathrm{IDBS}}^{\mathrm{Blind}}$ and $\mathbf{A}\,\mathbf{dv}_{\mathrm{IDBS}}^{\mathrm{UF}}$ of any polynomial time adversary are negligible.

5. Our Scheme

In this section, we will introduce our ID-based blind signature scheme in detail. Notably, there are two important algorithms used in our scheme, which are TrapGen and SampleMat[37, 38]. Meanwhile, public key generator (PKG) is the trusted third party.

5.1. System Setup. After getting the safety parameter 1^{λ} and n, PKG performs the following four steps:

(1) Choosing a prime number $q \geq 3$, $m > 5n \log q$, $s \geq L\omega(\sqrt{\log n})$, and $\delta = 12sm\lambda$, where $L = O(\sqrt{n \log q})$.

(2) Executing the algorithm $\mathrm{TrapGen}\,(q, m) \longrightarrow (\mathbf{A}, \mathbf{B})$, where $\|\widehat{\mathbf{B}}\| \leq L$. These matrices $\mathbf{A} \in Z_q^{n*m}$ and $\mathbf{B} \in Z_q^{m*m}$ are the public key and the secret key of PKG, respectively.

(3) Selecting two secure hash functions $H: \{0,1\}^* \longrightarrow \{\mathbf{v}: \mathbf{v} \in \{-1,0,1\}^n, \|\mathbf{v}\|_1 \leq n\}$ and $H_1: \{0,1\}^* \longrightarrow Z_q^{n*k}$. Actually, $k = m - n$.

(4) Making the parameters $\{\mathbf{A}, H, H_1\}$ public and keeping $sk = \mathbf{B}$ as a secret.

5.2. Key Extraction Phase. In our scheme, PKG uses the following method to generate the user's key pair. The key extract phase is shown in Figure 1.

(1) Computing $H_1\,(\mathrm{ID}) = \mathbf{A}' \in Z_q^{n*k}$ and performing the algorithm $\mathrm{SampleMat}\,(\mathbf{A}, \mathbf{B}, s, \mathbf{A}') \longrightarrow \mathbf{S}_{\mathrm{ID}}^{m*k}$. We can know that $\mathbf{A}\mathbf{S}_{\mathrm{ID}} = H_1\,(\mathrm{ID})$ and $\|\mathbf{S}_{\mathrm{ID}}\| \leq s\sqrt{m}$.

(2) Owing to $m > n$, getting $\mathbf{S}_{\mathrm{ID}} \longrightarrow \mathbf{S}_{\mathrm{ID}}'$, and choosing n rows of $\mathbf{S}_{\mathrm{ID}}$ randomly and then computing the relevant transposed matrix $\mathbf{S}'^{k*n} = \mathbf{S}_{\mathrm{ID}}'^{T}$ and finally calculating $A'' = \mathbf{A}'\mathbf{S}'\,(\mathrm{mod}\, q)$.

(3) Computing $\mathbf{A}_u^{n*m} = [2\mathbf{A}' \,|\, 2A'' + q\mathbf{I}]$ and $\mathbf{S}_u^{m*n} = [\mathbf{S}'/{-\mathbf{I}}]^T$, where $\mathbf{I}$ is the unit matrix, and then making the computation $\mathbf{T} = \mathbf{A}_u\mathbf{S}_u\,(\mathrm{mod}\, 2q) = q\mathbf{I}$. So, $\mathbf{T}$ and $\mathbf{A}_u$ are the user's public keys and $\mathbf{S}_u$ is the corresponding secret key.

5.3. Sign Phase. Essentially, this phase is an interactive three-move identification scheme over lattice based on SIS problem. It is assumed that u is the actual message needed to be signed. The specific interaction process is as follows:

(1) The signer selects a random vector $\mathbf{r} \longleftarrow G_{\delta_2}^m$ and calculates $\mathbf{x} = \mathbf{A}_u\mathbf{r}$. Then, $\mathbf{x}$ is transmitted to the user.

(2) Blind: the user chooses two blind factors $\mathbf{a} \longleftarrow G_{\delta_3}^m$ and $\mathbf{b} \longleftarrow G_{\delta_1}^n$ and computes $\mathbf{c} = H\,(\mathbf{x} + \mathbf{A}_u\mathbf{a} + \mathbf{T}\mathbf{b}\,(\mathrm{mod}\, 2q), \mathrm{com}\,(u, t))$. Noticeably, u is the message to be signed and t is a random value. Besides, the function *com* is a commitment. Then, $\mathbf{e} = p\mathbf{c} + \mathbf{b}$ is worked out, where $p \in \{-1, 1\}$. Finally, $\mathbf{e}$ is sent to the signer by using the bimodal Gaussian rejection sampling to stop $\mathbf{e}$ from leaking some information of $\mathbf{c}$.

(3) BSign: the signer selects $w \longleftarrow \{-1, 1\}$ randomly. Upon that, it can compute $\mathbf{y} = \mathbf{r} + w\mathbf{S}_u\mathbf{e}$. Similarly, $\mathbf{y}$ is sent to the user in the same way to hide relevant information of $\mathbf{S}_u$.

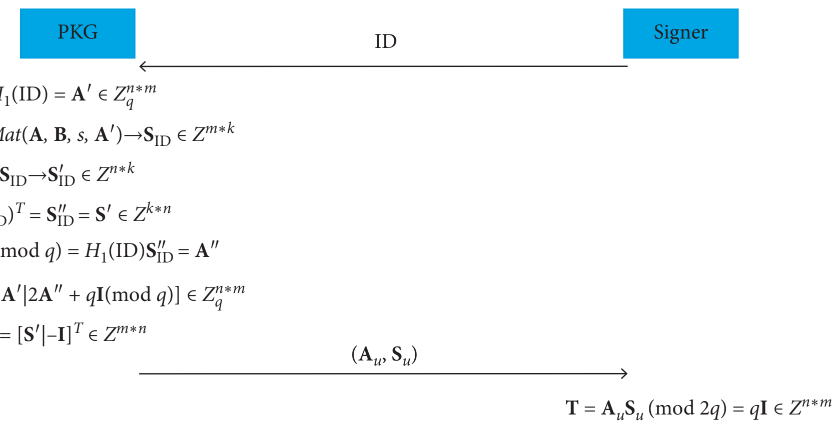
PKG
Signer
ID
$H_1(\mathrm{ID}) = \mathbf{A}' \in Z_q^{n*m}$
$SampleMat(\mathbf{A}, \mathbf{B}, s, \mathbf{A}') \rightarrow \mathbf{S}_{\mathrm{ID}} \in Z^{m*k}$
$\mathbf{S}_{\mathrm{ID}} \rightarrow \mathbf{S}'_{\mathrm{ID}} \in Z^{n*k}$
$(\mathbf{S}'_{\mathrm{ID}})^T = \mathbf{S}''_{\mathrm{ID}} = \mathbf{S}' \in Z^{k*n}$
$\mathbf{A}'\mathbf{S}' \,(\bmod q) = H_1(\mathrm{ID})\mathbf{S}''_{\mathrm{ID}} = \mathbf{A}''$
$\mathbf{A}_u = [2\mathbf{A}'|2\mathbf{A}'' + q\mathbf{I}(\bmod q)] \in Z_q^{n*m}$
$\mathbf{S}_u = [\mathbf{S}'|-\mathbf{I}]^T \in Z^{m*n}$
$(\mathbf{A}_u, \mathbf{S}_u)$
$\mathbf{T} = \mathbf{A}_u\mathbf{S}_u \,(\bmod 2q) = q\mathbf{I} \in Z^{n*m}$

Figure 1: Key extraction phase.

(4) Unblind: the user can get the value of $\mathbf{z} = \mathbf{y} + \mathbf{a}$. Then, $\mathbf{z}$ is output by the unimodal Gaussian rejection sampling. If $\mathbf{z} \in J$, we make result = $(\mathbf{a}, \mathbf{b}, \mathbf{c}, m, \mathrm{com}(u, t))$, where J is the rejection region of Gaussian sampling. Otherwise, we have result = accept. Finally, *result* is given to the signer.

(5) After holding *result*, the signer checks whether the value of result is accept or not. If it holds, the blind signature $(\mathbf{z}, \mathbf{c})$ is valid. On the contrary, if $\mathbf{e} - \mathbf{b} = m\mathbf{c} = mH(\mathbf{x} + \mathbf{A}_u\mathbf{a} + \mathbf{Tb}\,(\bmod 2q), \mathrm{com}(u, t))$, $\mathbf{c} = H(\mathbf{A}_u\mathbf{a} + \mathbf{A}_u\mathbf{y} - \mathbf{Tc}\,(\bmod 2q), \mathrm{com}(u, t))$, and $\mathbf{y} + \mathbf{a} \in J$, the signer restarts the sign phase with the user.

The sign phase is shown in Figure 2.

5.4. Verify Phase. In this phase, the verifier should check whether the following conditions are right or not:

(1) $\mathbf{c} = H(\mathbf{A}_u\mathbf{z} - q\mathbf{c}\,(\bmod 2q), \mathrm{com}(u, t))$

(2) $\|\mathbf{z}\| \leq 2\sqrt{m}\delta_3$

Actually, $(\mathbf{z}, \mathbf{c})$ is the final signature pair. If the two above conditions are satisfied, we have $\mathrm{Verify}(\mathbf{A}_u, \mathbf{T}, \mathbf{z}, \mathbf{c}, u) = 1$.

5.5. Correctness Analysis Phase. In this section, we mainly talk about the correctness and repetition of our blind signature. Firstly, we have

$$\begin{aligned}
\mathbf{A}_u\mathbf{z} - q\mathbf{c}\,(\bmod 2q) &= \mathbf{A}_u(\mathbf{y} + \mathbf{a}) - q\mathbf{c}\,(\bmod 2q) \\
&= \mathbf{A}_u(\mathbf{r} + k\mathbf{S}_u\mathbf{e}) + \mathbf{A}_u\mathbf{a} - q\mathbf{c}\,(\bmod 2q) \\
&= \mathbf{x} + k\mathbf{T}(m\mathbf{c} + \mathbf{b}) + \mathbf{A}_u\mathbf{a} - q\mathbf{c}\,(\bmod 2q) \\
&= \mathbf{x} + \mathbf{A}_u\mathbf{a} + kmq\mathbf{c} - q\mathbf{c} + k\mathbf{Tb}\,(\bmod 2q) \\
&= \mathbf{x} + \mathbf{A}_u\mathbf{a} + kq\mathbf{b}\,(\bmod 2q) \\
&= \mathbf{x} + \mathbf{A}_u\mathbf{a} + \mathbf{Tb}\,(\bmod 2q).
\end{aligned} \tag{7}$$

Thus, we have the fact that $\mathbf{c} = H(\mathbf{x} + \mathbf{A}_u\mathbf{a} + \mathbf{Tb}\,(\bmod 2q), \mathrm{com}(u, t)) = H(\mathbf{A}_u\mathbf{z} - q\mathbf{c}\,(\bmod 2q), \mathrm{com}(u, t))$. Additionally, on the basis of Theorem 1 and rejection sampling lemma, there is $\|\mathbf{z}\| \leq 2\delta_3\sqrt{m}$ with overwhelming probability.

Next, because the bimodal Gaussian rejection sampling is used in two places in our scheme, the mean value of repetitions is smaller than that of the original scheme. According to the introduction of Gaussian distribution, we have that

$$\begin{aligned}
&\frac{G^m_{\delta_3}(\mathbf{z})}{M_3 G^m_{\mathbf{y},\delta_3}(\mathbf{z})} \leq \frac{1}{M_3} e^{\left(24\|\mathbf{y}\|\delta_3 + \|\mathbf{y}\|^2/2\delta_3^2\right)} \leq 1, \\
&\frac{G^m_{\delta_2}(\mathbf{y})}{M_2\left((1/2)G^m_{\mathbf{S}_u\mathbf{e},\delta_2}(\mathbf{y}) + (1/2)G^m_{-\mathbf{S}_u\mathbf{e},\delta_2}(\mathbf{y})\right)} \\
&\quad \leq \frac{1}{M_2} e^{\left(\|\mathbf{S}_u\mathbf{e}\|^2/2\delta_2^2\right)} \leq 1, \\
&\frac{G^n_{\delta_1}(\mathbf{e})}{M_1\left((1/2)G^n_{\mathbf{c},\delta_1}(\mathbf{e}) + (1/2)G^n_{-\mathbf{c},\delta_1}(\mathbf{e})\right)} \\
&\quad \leq \frac{1}{M_1} e^{\left(\|\mathbf{c}\|^2/2\delta_1^2\right)} \leq 1.
\end{aligned} \tag{8}$$

In the rejection sampling lemma, we need to keep $M_i\,(i \in \{1, 2, 3\})$ as small as possible. Therefore, the value of M_i is worked out, where $M_1 = \mathbf{e}^{(\|\mathbf{c}\|^2/2\delta_1^2)}$, $M_2 = \mathbf{e}^{(\|\mathbf{S}_u\mathbf{e}\|^2/2\delta_2^2)}$, and $M_3 = \mathbf{e}^{(24\|\mathbf{y}\|\delta_3 + \|\mathbf{y}\|^2/2\delta_3^2)}$. Obviously, M_1 and M_2 are both less than the original values in the general rejection sampling, but not M_3. Therefore, it means that a valid blind signature can be generated successfully in lesser repetitions, whose specific number is $\prod_{i=1}^{3} M_i$.

6. Security Proof

In this section, we mainly prove that our scheme is blind and unforgeable by using the security model defined in Section 4. In fact, we need a malicious adversary to play games of security with a challenger.

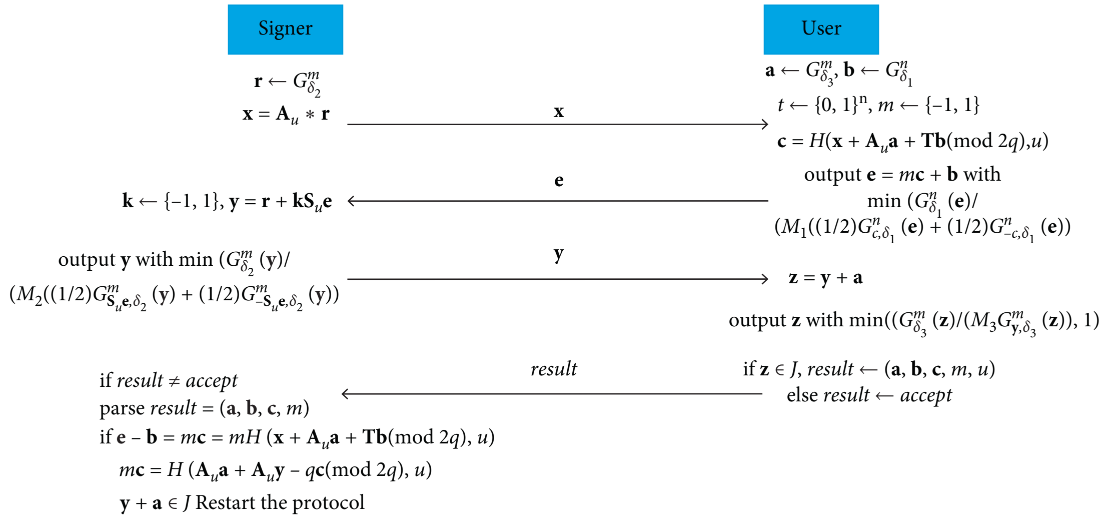
Signer
User
$\mathbf{r} \leftarrow G^m_{\delta_2}$
$\mathbf{x} = \mathbf{A}_u * \mathbf{r}$
$\mathbf{a} \leftarrow G^m_{\delta_3}, \mathbf{b} \leftarrow G^n_{\delta_1}$
$t \leftarrow \{0,1\}^n, m \leftarrow \{-1,1\}$
$\mathbf{x}$
$\mathbf{c} = H(\mathbf{x} + \mathbf{A}_u\mathbf{a} + \mathbf{Tb}(\text{mod } 2q), u)$
output $\mathbf{e} = m\mathbf{c} + \mathbf{b}$ with
$\min(G^n_{\delta_1}(\mathbf{e})/$
$(M_1((1/2)G^n_{c,\delta_1}(\mathbf{e}) + (1/2)G^n_{-c,\delta_1}(\mathbf{e}))$
$\mathbf{e}$
$\mathbf{k} \leftarrow \{-1,1\}, \mathbf{y} = \mathbf{r} + \mathbf{kS}_u\mathbf{e}$
output $\mathbf{y}$ with $\min(G^m_{\delta_2}(\mathbf{y})/$
$(M_2((1/2)G^m_{\mathbf{S}_u\mathbf{e},\delta_2}(\mathbf{y}) + (1/2)G^m_{-\mathbf{S}_u\mathbf{e},\delta_2}(\mathbf{y}))$
$\mathbf{y}$
$\mathbf{z} = \mathbf{y} + \mathbf{a}$
output $\mathbf{z}$ with $\min((G^m_{\delta_3}(\mathbf{z})/(M_3G^m_{\mathbf{y},\delta_3}(\mathbf{z})), 1)$
result
if $\mathbf{z} \in J$, *result* $\leftarrow (\mathbf{a}, \mathbf{b}, \mathbf{c}, m, u)$
else *result* $\leftarrow$ *accept*
if *result* $\neq$ *accept*
parse *result* $= (\mathbf{a}, \mathbf{b}, \mathbf{c}, m)$
if $\mathbf{e} - \mathbf{b} = m\mathbf{c} = mH(\mathbf{x} + \mathbf{A}_u\mathbf{a} + \mathbf{Tb}(\text{mod } 2q), u)$
$m\mathbf{c} = H(\mathbf{A}_u\mathbf{a} + \mathbf{A}_u\mathbf{y} - q\mathbf{c}(\text{mod } 2q), u)$
$\mathbf{y} + \mathbf{a} \in J$ Restart the protocol

FIGURE 2: Blind sign phase.

6.1. Blindness. We mainly prove the blindness of our scheme from the indistinguishability of views. Normally, views are the information conveyed between the signer and the users, as the following theorem shows.

Theorem 4. *The proposed ID-based blind signature scheme on lattice has blindness.*

Proof. As the game of blindness shows, a dishonest signer $\mathbf{A}^*(\mathbf{pk}, \mathbf{sk})$ selects two messages u_0 and u_1. Then these messages are sent to two honest users $\mathbf{U}_0(\mathbf{pk}, u_b)$ and $\mathbf{U}_1(\mathbf{pk}, u_{1-b})$, where $b \in \{0,1\}$. Then this malicious signer plays the game of blindness with $\mathbf{U}_0$ and $\mathbf{U}_1$ in the interactive way, respectively. Therefore, we can prove that our ID-based blind signature scheme is blind to $\mathbf{A}^*$ by showing all outputs of the users are independent of the relevant messages signed. We can see from the proposed scheme that the outputs are $\mathbf{e}$ and the final signature $(\mathbf{z}, \mathbf{c})$. Because we have that $\mathbf{c} \longleftarrow \{\mathbf{v} \in \{-1,0,1\}^n \colon \|\mathbf{v}\|_1 \leq n\}$, $\mathbf{c}$ is always a random number in the view of $\mathbf{A}^*$. Therefore, we can only consider two values $\mathbf{e}$ and $\mathbf{z}$.

Firstly, we consider about $\mathbf{e}$. We assume that $\mathbf{e}_b$ and $\mathbf{e}_{1-b}$ are generated in the game of blindness. $\mathbf{e}_b$ is held by $\mathbf{U}_0$. Similarly, $\mathbf{e}_{1-b}$ is corresponding to $\mathbf{U}_1$. In our scheme, we can know that $\mathbf{e} = m\mathbf{c} + \mathbf{b}$, where $\mathbf{c}$ can be seen as a random value. Besides, $\mathbf{e}$ is transmitted by using the bimodal Gaussian rejection sampling. Therefore, after getting $\mathbf{e}_b$ and $\mathbf{e}_{1-b}$, $\mathbf{A}^*$ cannot link $\mathbf{e}_b$ and $\mathbf{e}_{1-b}$ to their respective messages u_b or u_{1-b}. It is because the distribution of $\mathbf{e}_b$ and $\mathbf{e}_{1-b}$ is both $(1/2)G^n_{\mathbf{c},\delta_1} + (1/2)G^n_{-\mathbf{c},\delta_1}$, but the output distribution of them is the same as that of $\mathbf{b}$ under the bimodal Gaussian rejection sampling, which is $G^n_{\delta_1}$. In fact, the mean value of the distribution of $\mathbf{e}_b$ should be different from that of $\mathbf{e}_{1-b}$. However, we know these mean values can be considered as a random number. So we set the mean value as $\mathbf{c}$ uniformly for sake of simplicity. So we can say that the statistical distance between $\mathbf{e}_b$ and $\mathbf{e}_{1-b}$ is 0; namely, $\Delta(\mathbf{e}_b, \mathbf{e}_{1-b}) = 0$.

Next, we talk about $\mathbf{z}$. In the proposed scheme, we have that $\mathbf{z} = \mathbf{y} + \mathbf{a}$, where $\mathbf{a} \longleftarrow G^m_{\delta_3}$ is a blind factor. However, the output way of $\mathbf{z}$ is different from that of the above challenge $\mathbf{e}$, because the Gaussian rejection sampling used in this place is unimodal rather than bimodal. But this cannot make an influence on the blindness. Similarly, we assume that $\mathbf{z}_b$ is the final signature of $\mathbf{U}_0$ and $\mathbf{z}_{1-b}$ is related signature $\mathbf{U}_1$ received. Similarly, we set the mean value of distribution of $\mathbf{z}_b$ and $\mathbf{z}_{1-b}$ as $\mathbf{y}$. It is because the value $\mathbf{y}$ is computed by the signer that the distribution of $\mathbf{z}_b$ and $\mathbf{z}_{1-b}$ is both $G_{\mathbf{y},\delta_3}$. According to the Gaussian rejection sampling, the output distribution of $\mathbf{z}_b$ and $\mathbf{z}_{1-b}$ is the same as that of $\mathbf{a}$, which is $G^m_{\delta_3}$. Therefore, $\mathbf{A}^*$ cannot determine the corresponding messages of $\mathbf{z}_b$ and $\mathbf{z}_{1-b}$ from their output distribution. That is, the relevant statistical distance $\Delta(\mathbf{z}_b, \mathbf{z}_{1-b}) = 0$.

On the contrary, we assume that $\mathbf{A}^*$ gets the corresponding parameters ID and the secret key $\mathbf{S}_{\text{ID}}$ by playing the game of blindness with $\mathbf{U}_0$ and $\mathbf{U}_1$. Besides, $\delta(u_b)$ and $\delta(u_{1-b})$ are information $\mathbf{A}^*$ has after playing this game. It is worth noting that if $\mathbf{A}^*$ uses the method of guessing a random value of $\mathbf{b}'$ without any help to win the game of blindness, this probability is 1/2.

In addition, for $i \in \{0,1\}$, $\mathbf{x}_i, \mathbf{e}_i$, and $\mathbf{y}_i$ are the data exchanged between the signer and the user, when the issue query is performed by the user. Finally, $(\mathbf{z}_0, \mathbf{c}_0)$ and $(\mathbf{z}_1, \mathbf{c}_1)$ are returned to the dishonest signer $\mathbf{A}^*$. For each $i, j \in \{0,1\}$, there are two random blind factors $\mathbf{a}, \mathbf{b}$ that map $\mathbf{x}_i, \mathbf{e}_i, \mathbf{y}_i$ to $\mathbf{z}_j, \mathbf{c}_j$. Thus, $\mathbf{a} = \mathbf{z}_j - \mathbf{y}_i$ and $\mathbf{b} = -m\mathbf{c}_j + \mathbf{e}_i$. Since $\mathbf{T} = q\mathbf{I}$, where $\mathbf{I}$ is the unit matrix, we have

$$\begin{aligned}
\mathbf{c}_j &= H\left(\mathbf{A}_u\mathbf{z}_j - \mathbf{Tc}_j(\text{mod } 2q), \text{com}(u,t)\right)\\
&= H\left(\mathbf{A}_u(\mathbf{a} + \mathbf{y}_i) - \mathbf{T}[m(\mathbf{e}_i - \mathbf{b})](\text{mod } 2q), \text{com}(u,t)\right)\\
&= H\left(\mathbf{A}_u\mathbf{a} + \mathbf{A}_u\mathbf{y}_i + \mathbf{T}(\mathbf{e}_i - \mathbf{b})(\text{mod } 2q), \text{com}(u,t)\right)\\
&= H\left(\mathbf{A}_u\mathbf{y}_i + \mathbf{Te}_i + \mathbf{A}_u\mathbf{a} - \mathbf{Tb}(\text{mod } 2q), \text{com}(u,t)\right).
\end{aligned} \tag{9}$$

In the above equations, $\mathbf{y}_i, \mathbf{e}_i$ are two elements in one view and $\mathbf{z}_j, \mathbf{c}_j$ are two data in another view. Besides, two blind factors $\mathbf{a}$ and $\mathbf{b}$ are always included in the equation, which result in the indistinguishability to $\mathbf{A}^{\star}$. Therefore, the probabilistic polynomial time adversary $\mathbf{A}^{\star}$ makes out the right value of $\mathbf{b}$ successfully with probability 1/2.

In a word, our ID-based blind signature scheme on lattice has the security attribute of blindness. □

6.2. Unforgeability. In fact, unforgeability ensures that n valid signatures can be output by a malicious user at most. n is the maximum of queries that this adversary can make to the challenger. As the process of the game of unforgeability, we will give out the specific steps of this game on the basis of the proposed scheme.

Theorem 5. *If* $\mathbf{A}^{\star}$ *is a probabilistic polynomial time adversary, it can break our ID-based blind signature on lattice with the nonnegligible probability. So, we can construct a polynomial-time algorithm using* $\mathbf{A}^{\star}$ *as its subroutine to solve the SIS problem with overwhelming probability.*

Proof. We assume that h and l are the maximum of queries that $\mathbf{A}^{\star}$ can make to the random oracle H and the signer. Furthermore, the values of responses of the random oracle H are determined in advance. Thus, we have $H \longrightarrow \{\mathbf{c}_1, \ldots, \mathbf{c}_s\}$, where $s = l + h$, because the adversary would make a query to H before sending a signature query. As shown in the following content, $\mathbf{A}^{\star}$ plays the game of unforgeability with the challenger $\mathbf{S}$:

(i) Setup: after inputting the security parameter 1^{λ}, the challenger picks a random matrix $\mathbf{A} \in Z_q^{n*m}$ and a hash function $H_1\colon \{0,1\}^* \longrightarrow Z_q^{n*k}$. Additionally, the random oracle H is controlled by $\mathbf{S}$. Then, these systematic public parameters are opened to $\mathbf{A}^{\star}$.

(ii) Query: $\mathbf{A}^{\star}$ can make four types of queries to $\mathbf{S}$: $\mathbf{H}_1$ query, $\mathbf{H}$ query, extract query, and issue query. It is worth noting that $\mathbf{S}$ could maintain four empty lists before answering to those queries, namely, $\mathbf{H}_1^{\text{list}}$, $\mathbf{H}^{\text{list}}$, $\mathbf{SK}^{\text{list}}$, and $\mathbf{Sig}^{\text{list}}$. The specific processes of the answers to these queries will be displayed as follows:

   (1) $\mathbf{H}_1$ query: as mentioned above, $\mathbf{S}$ holds an empty list $\mathbf{H}_1^{\text{list}}$ in advance, whose form of item is $(\text{ID}, \mathbf{P}_{\text{ID}}, \mathbf{S}_{\text{ID}})$. After receiving an $\mathbf{H}_1$ query about the identity ID, $\mathbf{S}$ searches the corresponding item in $\mathbf{H}_1^{\text{list}}$ firstly. If there is an element $\text{ID}_i = \text{ID}$, $\mathbf{S}$ gives $\mathbf{P}_{\text{ID}_i}$ to $\mathbf{A}^{\star}$ as its response. Otherwise, $\mathbf{S}$ chooses a matrix $\mathbf{S}_{\text{ID}} \in Z^{m*k}$ at random, whose columns obey the distribution $G_{Z^m,\mathbf{s}}$. Then, $\mathbf{S}$ computes $\mathbf{P}_{\text{ID}} = \mathbf{A}\mathbf{S}_{\text{ID}}$. According to Theorems 1 and 3 in the Gaussian Distribution section, $\|\mathbf{S}_{\text{ID}}\| \leq \mathbf{s}\sqrt{\mathbf{m}}$ and a random matrix $\mathbf{P}_{\text{ID}} \in Z^{n*k}$ are held with nonnegligible probability. Finally, the new item $(\text{ID}, \mathbf{P}_{\text{ID}}, \mathbf{S}_{\text{ID}})$ is inserted into $\mathbf{H}_1^{\text{list}}$. Besides, $\mathbf{P}_{\text{ID}}$ is returned to $\mathbf{A}^{\star}$.

   (2) Extract query: after acquiring this query, $\mathbf{S}$ looks for the corresponding item $(\text{ID}, \mathbf{P}_{\text{ID}}, \mathbf{S}_{\text{ID}})$ in $\mathbf{H}_1^{\text{list}}$ firstly. Then $\mathbf{A}^{\star}$ gets a random matrix $\mathbf{S}'_{\text{ID}}$ from the matrix $\mathbf{S}_{\text{ID}}$, where $\mathbf{S}'_{\text{ID}} \in Z^{n*k}$. Moreover, $\mathbf{A}^{\star}$ can compute the transposed matrix $\mathbf{S}_{\text{ID}}''^{k*n}$ of the matrix $\mathbf{S}'_{\text{ID}}$ and we assign the value of $\mathbf{S}''_{\text{ID}}$ to $\mathbf{S}'$. In the end, $\mathbf{S}'$ is inserted in $\mathbf{SK}^{\text{list}}$ and $\mathbf{SK}_{\text{ID}} = [\mathbf{S}'\mathbf{I}]^T$ is given back to $\mathbf{A}^{\star}$. If a corresponding item does not exist, $\mathbf{S}$ picks a random matrix $\mathbf{S}' \in Z^{k*n}$ and makes an $\mathbf{H}_1$ query. Similarly, the new item $(\text{ID}, \mathbf{P}_{\text{ID}}, \mathbf{S}_{\text{ID}}, \mathbf{S}')$ is added in the list $\mathbf{SK}^{\text{list}}$ and the relevant matrix $\mathbf{SK}_{\text{ID}}$ is transmitted to $\mathbf{A}^{\star}$. Furthermore, $\mathbf{S}$ calculates $\mathbf{A}'' = \mathbf{P}_{\text{ID}}\mathbf{SK}_{\text{ID}} \pmod q$. Then, $\mathbf{S}$ can compute $\mathbf{A}_u = [2\mathbf{P}_{\text{ID}} | 2\mathbf{A}'' + q\mathbf{I}]$ and give $\mathbf{A}_u$ to the adversary as the public key of the user whose identity is ID.

   (3) $\mathbf{H}$ query: similarly, the challenger maintains an empty list $\mathbf{H}^{\text{list}}$, of which item is $(\mathbf{x}_i + \mathbf{A}\mathbf{a} + \mathbf{T}\mathbf{b}, u, \mathbf{h})$. When $\mathbf{A}^{\star}$ launches an $\mathbf{H}$ query, $\mathbf{S}$ searches the corresponding item in $\mathbf{H}^{\text{list}}$. If there is a related item in $\mathbf{H}^{\text{list}}$, the element $\mathbf{h}$ is given back to $\mathbf{A}^{\star}$. Otherwise, the answer $\mathbf{h}$ to the adversary is a random $\mathbf{c}_i$ that is not used yet, $i \in \{1, \ldots, s\}$. Besides, the new item $\mathbf{c}_i = \mathbf{h}$ is added in $\mathbf{H}^{\text{list}}$.

   (4) Issue query: after acquiring this query, $\mathbf{S}$ searches for the corresponding item $(\text{ID}, \mathbf{P}_{\text{ID}}, \mathbf{S}_{\text{ID}}, \mathbf{S}')$ on the basis of ID in $\mathbf{SK}^{\text{list}}$. Then, $\mathbf{S}$ uses $[\mathbf{S}' | -\mathbf{I}]^T$ as the secret key to execute the sign algorithm. Indeed, we can get the final signature $(\mathbf{z}, \mathbf{h})$. Finally, $\mathbf{S}$ sends $(\mathbf{z}, \mathbf{h})$ to $\mathbf{A}^{\star}$ as a response to this issue query.

(iii) Forgery: after completing l valid issue queries, $\mathbf{A}^{\star}$ gives out $l+1$ valid message-signature pairs $\{(\mathbf{z}_1, \mathbf{c}_1), u_1\}, \ldots, \{(\mathbf{z}_{l+1}, \mathbf{c}_{l+1}), u_{l+1}\}$ with nonnegligible probability ρ. It is worth noting that we always have $\|\mathbf{z}_i\| \leq 2\delta_3\sqrt{m}$.

If the response to an $\mathbf{H}$ query is predetermined, namely, $\mathbf{c} \notin \{\mathbf{c}_1, \ldots, \mathbf{c}_s\}$, $\mathbf{A}^{\star}$ can make $\mathbf{c}$ as the answer of the random oracle H with the probability $1/|H|$. Here, $|H|$ is the size of output set of the random oracle H. In other words, $\mathbf{c}$ is one element in $\{\mathbf{c}_1, \ldots, \mathbf{c}_s\}$ with probability $1 - (1/|H|)$. Therefore, $\mathbf{A}^{\star}$ can make a successful forgery $((\mathbf{z}_{l+1}, \mathbf{c}_{l+1}), u_{l+1})$ with the probability $\rho - (1/|H|)$, where $\mathbf{c}_{l+1}$ comes from $\{\mathbf{c}_1, \ldots, \mathbf{c}_s\}$. As mentioned previously, the $\mathbf{H}$ query can take place in two places, so we need to talk about the specific scheme in two different scenarios:

(1) Scenario 1: $\mathbf{c}$ is generated by $\mathbf{S}$ during responding to an issue query made by $\mathbf{A}^{\star}$. Because $\mathbf{c}$ is the response of a signature on $(\mathbf{A}_u\mathbf{z}' - \mathbf{T}\mathbf{c}, u')$, we can have $H(\mathbf{A}_u\mathbf{z} - \mathbf{T}\mathbf{c}, u) = H(\mathbf{A}_u\mathbf{z}' - \mathbf{T}\mathbf{c}, u')$. Thus, we must have that $u = u'$ and $\mathbf{A}_u\mathbf{z} - \mathbf{T}\mathbf{c} = \mathbf{A}_u\mathbf{z}' - \mathbf{T}\mathbf{c}$. If not, it means that we can find a collision of the hash function H. So, we can make a conclusion that $\mathbf{A}_u(\mathbf{z} - \mathbf{z}') = 0 \pmod{2q}$. Besides, we have $\|\mathbf{z} - \mathbf{z}'\| \leq 4\delta_3\sqrt{m}$, because $\|\mathbf{z}\|, \|\mathbf{z}\prime\| \leq 2\delta_3\sqrt{m}$.

(2) Scenario 2: $\mathbf{c}$ is an answer of the random oracle H. In order to solve the SIS problem, $\mathbf{S}$ replays the game of unforgeability with $\mathbf{A}^{\star}$. However, there is something different from the first process of this game. $\mathbf{S}$

changes the values of response of random oracle H, which is $(\mathbf{c}_1, \ldots, \mathbf{c}_{j-1}, \mathbf{c}_j', \ldots, \mathbf{c}_s')$. $\{\mathbf{c}_j', \ldots, \mathbf{c}_s'\}$ are different random values. According to the General Forking Lemma, $\mathbf{A}^\star$ can forge a new signature $(\mathbf{c}, \mathbf{z}^\star)$ of (ID, u_{l+1}) with the probability $\rho\prime$, such that $\mathbf{c} \neq \mathbf{c}_{l+1}$ and $\mathbf{A}_u \mathbf{z}_{l+1} - \mathbf{T}\mathbf{c}_{l+1} = \mathbf{A}_u \mathbf{z}^\star - \mathbf{T}\mathbf{c}$. Additionally, the probability of ρ' is

$$\rho' = \left(\rho - \frac{1}{|H|}\right)\left(\frac{\rho - (1/H)}{s} - \frac{1}{H}\right). \tag{10}$$

Because of $\mathbf{T} = \mathbf{A}_u \mathbf{SK}_{\mathrm{ID}}$, we can have

$$\mathbf{A}_u \left(\mathbf{z}_{l+1} - \mathbf{z}^\star + \mathbf{SK}_{\mathrm{ID}}\mathbf{c}_{l+1} - \mathbf{SK}_{\mathrm{ID}}\mathbf{c}\right) = 0. \tag{11}$$

In addition, $\|\mathbf{z}_{l+1}\|, \|\mathbf{z}^\star\| \leq 2\delta_3\sqrt{m}$ and $\|\mathbf{SK}_{\mathrm{ID}}\mathbf{c}_{l+1}\|, \|\mathbf{SK}_{\mathrm{ID}}\mathbf{c}\| \leq \mathbf{s}\lambda\sqrt{m}$ are held. Thus, with overwhelming probability, we have

$$\left\|\mathbf{z}_{l+1} - \mathbf{z}^\star + \mathbf{SK}_{\mathrm{ID}}\mathbf{c}_{l+1} - \mathbf{SK}_{\mathrm{ID}}\mathbf{c}\right\| \leq \left(4\delta_3 + 2\mathbf{s}\lambda\right)\sqrt{m}. \tag{12}$$

If $\mathbf{z}_{l+1} - \mathbf{z}^\star + \mathbf{SK}_{\mathrm{ID}}\mathbf{c}_{l+1} - \mathbf{SK}_{\mathrm{ID}}\mathbf{c} \neq 0$, then a valid solution of the SIS hard problem is found. Thus, we need to prove that the probability of $\mathbf{z}_{l+1} - \mathbf{z}^\star + \mathbf{SK}_{\mathrm{ID}}\mathbf{c}_{l+1} - \mathbf{SK}_{\mathrm{ID}}\mathbf{c} \neq 0$ is overwhelming. According to the property of minimum entropy of the preimage, we can know that there is another secret key $\mathbf{S}_{\mathrm{ID}}^\star$ such that $\mathbf{A}_u\mathbf{S}_{\mathrm{ID}}^\star = \mathbf{A}_u\mathbf{S}_{\mathrm{ID}}$, which is different from $\mathbf{S}_{\mathrm{ID}}$. Additionally, the adversary cannot distinguish the secret key $\mathbf{S}_{\mathrm{ID}}^\star$ from $\mathbf{S}_{\mathrm{ID}}$, after getting the view $(\mathbf{x}, \mathbf{e}, \mathbf{y})$. Currently, we assume the secret key used in this game is $\mathbf{S}_{\mathrm{ID}}^\star$. Furthermore, we calculate $\mathbf{r}'$ by the following way:

$$\begin{aligned}\mathbf{r}' &= \mathbf{y} - k\mathbf{S}_{\mathrm{ID}}^\star\mathbf{e} = \mathbf{r} + k\mathbf{S}_{\mathrm{ID}}\mathbf{e} - k\mathbf{S}_{\mathrm{ID}}^\star\mathbf{e} \\ &= \mathbf{r} + k\mathbf{e}\left(\mathbf{S}_{\mathrm{ID}} - \mathbf{S}_{\mathrm{ID}}^\star\right).\end{aligned} \tag{13}$$

As mentioned above, we have $\mathbf{A}_u\mathbf{S}_{\mathrm{ID}} = \mathbf{A}_u\mathbf{S}_{\mathrm{ID}}^\star$, so the equation $\mathbf{A}_u\mathbf{r}' = \mathbf{A}_u\mathbf{r}$ is set up. Then we can get $\mathbf{y}' = \mathbf{r}' + k\mathbf{S}_{\mathrm{ID}}^\star\mathbf{e} = \mathbf{y}$. Therefore, the event that $\mathbf{A}^\star$ wants to tell the relevant secret on the basis of $\mathbf{r}$ could not take place. Then, we have

$$\begin{aligned}&\mathbf{z}_{l+1} - \mathbf{z}^\star + \mathbf{S}_{\mathrm{ID}}\left(\mathbf{c}_{l+1} - \mathbf{c}\right) - \left(\mathbf{z}_{l+1} - \mathbf{z}^\star + \mathbf{S}_{\mathrm{ID}}^\star\left(\mathbf{c}_{l+1} - \mathbf{c}\right)\right) \\ &\quad = \left(\mathbf{S}_{\mathrm{ID}} - \mathbf{S}_{\mathrm{ID}}^\star\right)\left(\mathbf{c}_{l+1} - \mathbf{c}\right) \neq 0.\end{aligned} \tag{14}$$

So, if $\mathbf{z}_{l+1} - \mathbf{z}^\star + \mathbf{S}_{\mathrm{ID}}\left(\mathbf{c}_{l+1} - \mathbf{c}\right) = 0$, we can get the conclusion that $\mathbf{z}_{l+1} - \mathbf{z}^\star + \mathbf{S}_{\mathrm{ID}}^\star\left(\mathbf{c}_{l+1} - \mathbf{c}\right) \neq 0$ is satisfied. Simultaneously, the adversary cannot tell which secret key is used by the challenger $\mathbf{S}$ in the game. Thus, $\mathbf{z}_{l+1} - \mathbf{z}^\star + \mathbf{S}_{\mathrm{ID}}\left(\mathbf{c}_{l+1} - \mathbf{c}\right) \neq 0$ is set up with the probability 1/2 at least. □

7. Performance Evaluation

In this section, the performance analysis of our scheme is talked about in detail. Generally, we will give out the result of comparison between our scheme and two other representative articles in terms of communication complexity and computing complexity. Specifically, these data are mainly derived from the signature's size and computational cost of generating system parameters of the relevant scheme. Currently, most of the lattice-based blind signature schemes are proved secure in the random oracle model, where the scheme in [39] proposed by Rückert was the most authoritative in 2010. Besides, another blind scheme was proposed by Zhang et al. [13] in 2018, on which we design our new ID-based blind signature scheme. It is worth noting that we do not consider the computational cost of the key extraction phase of our scheme when we make a comparison of the performance between our scheme and Zhang et al.'s [13] signature scheme because their scheme is a PKI-based blind signature scheme on lattice.

Firstly, we show a detailed comparison between our scheme and the blind signature scheme proposed by Zhang et al. [13]. To keep the reasonability, we will use the same way in Zhang et al.'s scheme [13] to choose the public system parameters. Namely, the security level of our scheme is the same as that of the scheme [13] proposed by Zhang et al. owing to the Hermite factor $\delta = 1.007$ defined in [40], which can reach 80 bits. Table 1 shows some important system parameters in these two schemes, where n, q, and k are used to keep the hardness of SIS problem.

In Table 1, the parameters of the rejection sampling in our scheme are smaller than those of the scheme [13] proposed by Zhang et al. obviously. This is because the bimodal Gaussian rejection sampling is used in our scheme. Specifically, the size of a challenge is determined by the parameter κ. In general, κ should satisfy the condition $2^\kappa\binom{k}{\kappa} \geq 2^{100}$ to keep the correctness error at 2^{-100}. According to rejection sampling lemma, we need to keep the rejection area between the actual distribution and objective distribution as small as possible. In this way, the signature algorithm can generate a valid signature using as few repetitions as possible. On the basis of the property of bimodal Gaussian rejection sampling, we only need to require that $\delta = \|\mathbf{c}\|/\sqrt{2}$ instead of $12\|\mathbf{c}\|$. In this case, the bimodal Gaussian rejection sampling can work with the minimum mean value $M = e(1)$. Normally, because M_1 and M_2 are the mean values of the bimodal Gaussian rejection sampling, they are independent of δ_1, $\|\mathbf{c}\|$ and δ_2, $\|\mathbf{S}_u\mathbf{e}\|$. For M_1, we have that $M_1 = e^{(\kappa/(2\delta_1^2))}$ when $\delta_1 = \|\mathbf{c}\|/\sqrt{2} = \sqrt{\kappa}/\sqrt{2}$. This can hold because we have $\|\mathbf{c}\|_1 \leq \kappa$ and $\|\mathbf{c}\|_2 \leq \sqrt{\kappa}$. Similarly, we can get the optimal value of M_2 while we make that $\delta_2 = d\eta\,\delta_1\sqrt{mk}/\sqrt{2}$. However, because M_3 is the mean value of the unimodal rejection sampling, we need to only require that $\delta_3 = 12\eta\delta_2\sqrt{m}$. In addition, the distribution of the final signature $\mathbf{z}$ is $G_{\delta_3}^m$. By Theorem 1, we can determine that the size of $\mathbf{z}$'s every coefficient is $12\delta_3$ with the probability at least $1 - 2^{-100}$. Because the value of δ_3 in our scheme is far less than that in Zhang et al.'s scheme [13], we can get the smaller valid signature that is equal to $m\log(12\delta_3)$ bits approximately. Additionally, our M_1, M_2, and M_3 are smaller than those of the scheme proposed by Zhang et al. [13]. This means our blind signature scheme can use less time to generate a valid signature in the same security level. In the end, what we need to emphasize is that our blind signature scheme on lattice is based on the ID-based cryptosystem, which has already stronger efficiency than the PKI cryptosystem.

Table 1: The key parameters in blind signature scheme on lattice.

	Zhang et al.'s scheme	Value	Our scheme	Value
n	—	512	—	512
q	—	2^{27}	—	2^{27}
d	—	1	—	1
m	$64 + n\log q/\log(2d+1)$	8786	$64 + n\log q/\log(2d+1)$	8786
k	—	80	$m - n$	8274
κ	—	28	—	28
δ_1	$12\sqrt{\kappa}$	64	$\sqrt{\kappa}/\sqrt{2}$	2
M_1	$e^{((12(\sqrt{\kappa}/\delta_1))+(\kappa/2\delta_1^2))}$	2.72	$e^{(\kappa/(2\delta_1^2))}$	2.7
δ_2	$12\,d\eta\,\delta_1\sqrt{mk}$	2^{19}	$d\eta\,\delta_1\sqrt{mk}/\sqrt{2}$	30000
M_2	$e^{(1+1/288)}$	2.72	e	2.7
δ_3	$12\,d\eta\,\delta_2\sqrt{m}$	$2^{29.5}$	$12\eta\delta_2\sqrt{m}$	$3*10^7$
M_3	$e^{(1+1/288)}$	2.72	e	2.7
η	$[1.1, 1.3]$	1.1	$[1.1, 1.3]$	1.1

Table 2: The comparison of relevant blind signature scheme.

Schemes	Signature size	Security level (bits)	Cryptosystem
Zhang et al.	$m\log(12\delta_3)$	80	PKI-based
Ruckert et al.	$(c+1)m\log(\overline{s}\sqrt{(c+1)m}) + n$	76	ID-based
Our scheme	$m\log(12\delta_3)$	80	ID-based

Next, we will give out the comparison between our scheme and the classical scheme proposed by Rückert et al. simply [39]. Here, m and n are the common system parameters in these two schemes. Moreover, c is the bit size of the user's identity and $\overline{s} = s\sqrt{(c+1)m}\omega(\sqrt{\log n})$ is the expansive Gaussian parameter in Rückert et al.'s scheme [39]. We can know that the size of final signature in our scheme is $m\log(12\delta_3)$. According to the explanation of Rückert et al. [39], the size of signature is $(c+1)m\log(\overline{s}\sqrt{(c+1m)}) + n$ in their ID-based blind scheme. Obviously, it is easy to make the conclusion that the signature's size in our scheme is smaller than that of Rückert et al.'s scheme [39] in the random oracle model. In terms of computing complexity, there are only some simple operators involved in our sign algorithm and verify algorithm, such as scalar-multiplication on vector, addition on vector, matrix-vector multiplication, and hash function. However, in sign algorithm and verify algorithm of Rückert et al.'s scheme [39], the complex algorithms are included to generate a valid signature, such as ExtBasis algorithm and SamplePre algorithm. So our scheme is simpler and more efficient than the scheme proposed by Rückert et al. [39].

Based on the above result, we can make a conclusion that our scheme has less communicational and computational cost, compared with the latest blind signature scheme on lattice proposed by Zhang et al. [13] and the most authoritative blind signature scheme on lattice proposed by Rückert et al. [39]. Thus, our scheme has more efficient and practical value in applications. Table 2 shows the result of relevant comparison in detail.

8. Conclusion

Integrating the advantage of ID-based cryptosystem with lattice-based cryptosystem, we construct an efficient and secure ID-based blind signature scheme in this paper to protect the privacy of confidential data, which can be widely applied to the e-cash and electronic voting system. Moreover, a useful aborting technology, bimodal Gaussian rejection sampling, is used in our scheme to accelerate the speed of generating a valid blind signature. Meanwhile, our scheme is provably secure in the random oracle model, which is on the basis of the SIS problem. By showing the comparison with the scheme of Zhang et al. [13] and that of Rückert et al. [39], we demonstrate the superiority of our scheme in communicational and computational efficiency.

To extend our scheme to get other useful properties and complete an original model of evaluating the extended scheme in the real application environment is the future work executed by us.

Data Availability

The data 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.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (nos. 61772224, 61932016, and 61972294).

References

[1] S. Beauregard, "Circuit for shor's algorithm using 2n + 3 qubits," 2002, http://arxiv.org/abs/0205095.

[2] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," 2003, http://arxiv.org/abs/0301141.

[3] D. He, Y. Zhang, D. Wang, and K.-K. R. Choo, "Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 99, pp. 1–10, 2019.

[4] Q. Feng, D. He, Z. Liu, D. Wang, and K.-K. R. Choo, "Distributed signing protocol for IEEE P1363-compliant identity-based signature scheme," *IET Information Security*, vol. 1, no. 99, pp. 1–10, 2020.

[5] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, pp. 199–203, Springer, Berlin, Germany, 1983.

[6] C. Popescu, "Blind signature schemes based on the elliptic curve discrete logarithm problem," *Studies in Informatics and Control*, vol. 19, no. 4, pp. 397–402, 2010.

[7] N. A. Moldovyan, "Blind signature protocols from digital signature standards," *International Journal of Network Security*, vol. 13, no. 1, pp. 22–30, 2011.

[8] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, Springer, Paris, France, pp. 47–53, April 1984.

[9] D. S. Gupta and G. P. Biswas, "Design of lattice-based elgamal encryption and signature schemes using sis problem," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 6, p. e3255, 2018.

[10] S. Mukherjee, D. S. Gupta, and G. P. Biswas, "An efficient and batch verifiable conditional privacy-preserving authentication scheme for vanets using lattice," *Computing*, vol. 101, no. 12, pp. 1763–1788, 2019.

[11] D. S. Gupta and G. P. Biswas, "A novel and efficient lattice-based authenticated key exchange protocol in c-k model," *International Journal of Communication Systems*, vol. 31, no. 3, p. e3473, 2018.

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

[13] P. Zhang, H. Jiang, Z. Zheng, P. Hu, and Q. Xu, "A new post-quantum blind signature from lattice assumptions," *IEEE Access*, vol. 6, pp. 27 251–27 258, 2018.

[14] F. Li, M. Zhang, and T. Takagi, "Identity-based partially blind signature in the standard model for electronic cash," *Mathematical and Computer Modelling*, vol. 58, no. 1-2, pp. 196–203, 2013.

[15] L. Lopez-Garcia, L. J. D. Perez, and F. Rodriguez-Henriquez, "A pairing-based blind signature e-voting scheme," *The Computer Journal*, vol. 57, no. 10, pp. 1460–1471, 2013.

[16] C.-C. Chang and T.-F. Cheng, "A provably secure t-out-of-n oblivious transfer mechanism based on blind signature," *Journal of Information Hiding & Multimedia Signal Processing*, vol. 5, no. 1, pp. 1–12, 2014.

[17] L.-C. Wu, Y.-S. Yeh, and C.-I. Fan, "Fail-stop blind signature scheme based on the integer factorization," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 7, no. 3, pp. 281–290, 2004.

[18] H. Mala and N. Nezhadansari, "New blind signature schemes based on the (elliptic curve) discrete logarithm problem," in *Proceedings of the ICCKE 2013*, pp. 196–201, IEEE, Mashhad, Iran, October 2013.

[19] K. Chakraborty and J. Mehta, "A stamped blind signature scheme based on elliptic curve discrete logarithm problem," *International Journal of Network Security*, vol. 14, no. 6, pp. 316–319, 2012.

[20] F. Zhang and K. Kim, "Id-based blind signature and ring signature from pairings," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, Springer, Queenstown, New Zealand, pp. 533–547, 2002.

[21] Z. Huang, K. Chen, and Y. Wang, "Efficient identity-based signatures and blind signatures," in *Proceedings of the International Conference on Cryptology and Network Security*, Springer, Xiamen, China, pp. 120–133, December 2005.

[22] S. Kalkan, K. Kaya, and A. A. Selcuk, "Generalized id-based blind signatures from bilinear pairings," in *Proceedings of the 2008 23rd International Symposium on Computer and Information Sciences*, pp. 1–6, IEEE, Istanbul, Turkey, May 2008.

[23] B. U. Rao, K. Ajmath, P. V. Reddy, and T. Gowri, "An id-based blind signature scheme from bilinear pairings," *International Journal of Computer Science and Security*, vol. 4, no. 1, pp. 98–106, 2010.

[24] F. Hess, "Efficient identity based signature schemes based on pairings," in *Proceedings of the International Workshop on Selected Areas in Cryptography*, Springer, Newfoundland, Canada, pp. 310–324, August 2002.

[25] C.-I. Fan, W.-Z. Sun, and V. S.-M. Huang, "Provably secure randomized blind signature scheme based on bilinear pairing," *Computers & Mathematics with Applications*, vol. 60, no. 2, pp. 285–293, 2010.

[26] L. Zhang, Y. Hu, X. Tian, and Y. Yang, "Novel identity-based blind signature for electronic voting system," in *Proceedings of the 2010 Second International Workshop on Education Technology and Computer Science*, vol. 2, pp. 122–125, IEEE, Wuhan, China, March 2010.

[27] R. Shakerian, T. MohammadPour, S. H. Kamali, and M. Hedayati, "An identity based public key cryptography blind signature scheme from bilinear pairings," in *Proceedings of the 2010 3rd International Conference on Computer Science and Information Technology*, vol. 7, pp. 28–32, IEEE, Chengdu, China, July 2010.

[28] D. He, J. Chen, and R. Zhang, "An efficient identity-based blind signature scheme without bilinear pairings," *Computers & Electrical Engineering*, vol. 37, no. 4, pp. 444–450, 2011.

[29] S. H. Islam, R. Amin, G. P. Biswas, M. S. Obaidat, and M. K. Khan, "Provably secure pairing-free identity-based partially blind signature scheme and its application in online e-cash system," *Arabian Journal for Science and Engineering*, vol. 41, no. 8, pp. 3163–3176, 2016.

[30] M. Kumar, C. P. Katti, and P. C. Saxena, "An untraceable identity-based blind signature scheme without pairing for e-cash payment system," in *Proceedings of the International Conference on Ubiquitous Communications and Network Computing*, Springer, Bangalore, India, February 2017, pp. 67–78.

[31] S. James, N. B. Gayathri, and P. V. Reddy, "Pairing free identity-based blind signature scheme with message recovery," *Cryptography*, vol. 2, no. 4, p. 29, 2018.

[32] H. Zhu, Y.-a. Tan, X. Zhang, L. Zhu, C. Zhang, and J. Zheng, "A round-optimal lattice-based blind signature scheme for cloud services," *Future Generation Computer Systems*, vol. 73, pp. 106–114, 2017.

[33] L. Zhang and Y. Ma, "A lattice-based identity-based proxy blind signature scheme in the standard model," *Mathematical Problems in Engineering*, vol. 2014, Article ID 307637, 6 pages, 2014.

[34] W. Gao, Y. Hu, B. Wang, and J. Xie, "Identity-based blind signature from lattices in standard model," in *Proceedings of*

the International Conference on Information Security and Cryptology, Springer, Seoul, South Korea, pp. 205–218, 2016.

[35] W. Gao, Y. Hu, B. Wang, J. Xie, and M. Liu, "Identity-based blind signature from lattices," *Wuhan University Journal of Natural Sciences*, vol. 22, no. 4, pp. 355–360, 2017.

[36] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice signatures and bimodal Gaussians," in *Proceedings of the Annual Cryptology Conference*, Springer, Santa Barbara, CA, USA, pp. 40–56, August 2013.

[37] 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, ACM, Victoria, Canada, May 2008.

[38] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," *Theory of Computing Systems*, vol. 48, no. 3, pp. 535–553, 2011.

[39] M. Rückert, "Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles," in *Proceedings of the International Workshop on Post-Quantum Cryptography*, Springer, Darmstadt, Germany, pp. 182–200, May 2010.

[40] N. Gama and P. Q. Nguyen, "Predicting lattice reduction," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Istanbul, Turkey, pp. 31–51, April 2008.