IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 7, 2019, accepted December 8, 2019, date of publication December 16, 2019,
date of current version December 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2959943

Identity-Based Blind Multisignature From Lattices

RAYLIN TSO, ZI-YUAN LIU, AND YI-FAN TSENG
Department of Computer Science, National Chengchi University, Taipei 11605, Taiwan

Corresponding author: Raylin Tso (raylin@cs.nccu.edu.tw)

This work was supported in part by the Ministry of Science and Technology, Taiwan (R.O.C.), under Project Numbers MOST 108-2218-E-004-001-, MOST 108-2218-E-004-002-MY2, and in part by the Taiwan Information Security Center at National Sun Yat-sen University (TWISC@NSYSU).

ABSTRACT Blind multisignature (BMS), first introduced by Horster *et al*, constitutes a crucial primitive that allows a user to generate a signature of a message from multiple signers, while the signers cannot obtain any information about the message. With these useful properties, blind multisignature is suitable for electronic payments and electronic voting. However, most of the current BMS schemes may be attacked by quantum computers in the future because they are based on traditional number theories, such as discrete logarithm assumption and large integer factor assumption. In this work, we first formalize the notion and the sound security models of the identity-based blind multisignature scheme (IDBMS). Then we present an instantiation based on lattices, along with rigorous proofs of the blindness and unforgeability under the lattice hard assumption (short integer solution, SIS), which is considered to remain secure under quantum computer attacks. To the best of our knowledge, it is the *first* identity-based quantum-resistant scheme that has the advantages of blind signature and multisignature.

INDEX TERMS Lattice-based cryptography, blind multisignature, quantum-resistant.

I. INTRODUCTION

The blind signature scheme, first introduced by Chaum in 1983 [1], is a promising cryptographic primitive due to its blindness. This scheme consists of three entities: a user, a signer, and a verifier. The user can generate a signature σ of a message μ with the help of the signer, while the signer cannot obtain any information about the message μ. The verifier can verify the signature σ of the message μ that is signed by the signer. This property is suitable for various applications, such as electronic payments and electronic voting [2]–[5]. Take electronic payment as an example. Users withdraw electronic coins that are blindly signed by the electronic coin issuer (signer). Then, they can spend these electronic coins that can be authenticated using the public key of the issuer. However, in a real environment, an electronic coin may require being signed by multiple issuers at the same time, and the total size of the signatures will increase linearly with the number of the issuers. Therefore, how to reduce it becomes an important problem.

To address this issue, Petersen *et al.* proposed the first blind multisignature (BMS) scheme using the advantages of the multisignature scheme [6]. In their scheme, a user can generate a signature σ of a message μ with the help of multiple signers, while all the signers cannot obtain any information about the message. This signature σ can be verified by a key that combines all the signers' public keys. They also showed how to use the BMS scheme as a building block to construct electronic voting. Because this property is suitable for a multi-user scenario, many BMS schemes have been proposed in the last two decades and applied to many scenarios. In 2003, Chen *et al.* proposed a BMS scheme from bilinear pairings [7]. In 2006, Hanatani *et al.* constructed provably electronic cash from a BMS scheme [8]. In 2015, Namdeo proposed an untraceable BMS scheme [9]. Recently, Tan *et al*. proposed a BMS scheme based on the elliptic curve discrete logarithm problem [10], [11].

Unfortunately, current research results only focus on the application scenario and how to construct an efficient scheme. The security of these schemes relies on traditional mathematics assumptions, such as the discrete logarithms assumption and large integer factoring assumption. According to Shor's work [12], there is a quantum algorithm that can solve the prime factorization and discrete logarithm assumption in polynomial time. Therefore, the above schemes will certainly suffer attacks by quantum computers in the future.

Most of the existing schemes are designed on certificate-based cryptography instead of identity-based cryptography.

The associate editor coordinating the review of this manuscript and approving it for publication was Giacomo Verticale.

In certificate-based cryptography, the user's public key is necessary for certification by the public key authentication framework, such as public key infrastructure (PKI). Additionally, the public key is a random string, which is hard for verifiers to store or remember. On the other hand, identity-based cryptography, first introduced by Shimar in 1984 [13], uses the user's identifier information, such as email address, name, social security number, etc., as the public key for performing encryption or verification. It eliminates the necessity of the PKI and uses the identifier information as the public key, which is more suitable for real scenarios.

For these reasons, it is important to determine whether we can construct a quantum-resistant identity-based blind multisignature scheme from lattices.

A. CONTRIBUTIONS

In this paper, we first formalize the notion and security models of the identity-based blind multisignature scheme (IDBMS). Then, we provide a concrete instantiation based on lattices, and show that our scheme has blindness and unforgeability based on the short integer solution (SIS) assumption. To the best of our knowledge, this is the first quantum-resistant IDBMS scheme in which the size of the blind signature will not increase with the number of signers. We also compare with other state-of-the-art works [14] and show that our scheme can reduce the sizes of blind signatures effectively.

Hereunder, we briefly sketch our scheme and describe the technique we use. Inspired by Zhang *et al.* blind signature [14] and Tian and Huang identity-based signature [15], the basic strategy for constructing our scheme is to use lattice-based trapdoor functions and rejection sampling technology. In our scheme, there are four main characters, authority key generator center $\mathcal{KGC}$, a user $\mathcal{U}$, a verifier $\mathcal{V}$, and a group of signers $\mathcal{S} = \{\mathcal{S}_1, \cdots, \mathcal{S}_N\}$, where $N \geq 1$. The $\mathcal{KGC}$ generates the master public/private keys using the $\mathsf{TrapGen}$ function, that is $(\mathbf{A}_0, \mathbf{B}_0) \leftarrow \mathsf{TrapGen}(q, n, m)$, where q, n, m are some parameters. Actually, the master private key $\mathbf{B}_0$ is a basis of the lattice $\Lambda_q^{\perp}(\mathbf{A}_0)$, such that $\mathbf{A}_0\mathbf{B}_0 = 0 \ (mod\ q)$. Then, the $\mathcal{KGC}$ generates each signer's signing key $\mathsf{sk}_{\mathcal{S}_i} = \mathbf{B}_i$ using the $\mathsf{SampleMat}$ function with the hash value of the signer's identity $\mathbf{A}_i = H(\mathcal{S}_i)$ as the input, that is $\mathbf{B}_i \leftarrow \mathsf{SampleMat}(\mathbf{A}_0, \mathbf{B}_0, s, \mathbf{A}_i)$. Because $\mathbf{B}_i$ is sampled from the lattice $\Lambda_q^{\perp}(\mathbf{A}_0)$, each signer's signing key $\mathbf{B}_i$ will satisfy $\mathbf{A}_0\mathbf{B}_i = \mathbf{A}_i \ (mod\ q)$, where s is a Gaussian parameter. The signing protocol is a four-stages interactive algorithm between $\mathcal{U}$ and $\mathcal{S}$. Each signer generates a blind signature σ_i for a message m_i using a rejection sampling technique with his/her signing key, and sends σ_i to $\mathcal{U}$. Then $\mathcal{U}$ can combine each σ_i into one blind multisignature σ, to reduce the total size of the signature. More precisely, this method is inspired by the lattice-based multisignature scheme proposed by Bansarkhani and Sturm work [16]. Finally, $\mathcal{U}$ generates a blind multisignature σ that can be verified by $\mathcal{V}$ using signers' identities.

Our contributions are summarized as follows.

- First, we formalize the notion and the sound security models of the identity-based blind multisignature scheme.
- Second, we propose the first quantum-resistant IDBMS scheme from lattices. Our proposed scheme allows a user to generate a blind signature from a group of signers, while all signers cannot obtain any information about the message. In addition, the size of the signature will not increase with the number of signers.
- Third, concerning the adversarial model, rigorous security proofs are presented to show that our scheme is blind and unforgeable under a lattice hard assumption. That is, even under an attack from a quantum computer, our scheme can maintain its security.
- Fourth, compared to [14], we show that our scheme can effectively reduce the sizes of signatures.

B. ORGANIZATION

The remainder of the article is organized as follows. We start with some preliminaries on lattices and some trapdoor functions in Section II. In Section III, we introduce a general system and security model for the identity-based blind multisignature scheme. We propose our scheme from lattices and compare it to Zhang's scheme in Section IV. In Section V, we demonstrate security proofs to show that our scheme is blind and unforgeable. Finally, we conclude this paper in Section VI.

II. PRELIMINARIES

This section provides some cryptography primitives and definitions required for our construction.

A. NOTATION

For simplicity and readability, we use the following symbols throughout the paper. We use λ to represent the security parameter and use the abbreviation PPT to mean probabilistic polynomial time. We use standard big-O, little-o, and little-ω notations to classify the growth of functions. In addition, we say that $f(\lambda) = \tilde{O}(g(\lambda))$ if $f(\lambda) = O(g(\lambda) \cdot \log^c \lambda)$ for some fixed constant c. We also use $\mathsf{poly}(\lambda)$ to indicate a generic polynomial function $f(\lambda) = O(\lambda^c)$ for some constant c. The notation $\mathsf{negl}(\lambda)$ denotes that any function f is *negligible* in λ where $f(\lambda) = o(\lambda^{-c})$ for every fixed constant c. We also show a set of real numbers by $\mathbb{R}$, and a set of integers by $\mathbb{Z}$. For $x \in \mathbb{R}$, $\mathsf{exp}(x)$ denotes the exponent of x, that is e^x.

Conventionally, vectors are written in bold lower-case letters (*e.g.*, $\mathbf{x}$), while matrices are written in bold capital letters (*e.g.*, $\mathbf{A}$). For a vector $\mathbf{x}$, $\|\mathbf{x}\|$ and $\|\mathbf{x}\|_1$ denote the Euclidean norm of $\mathbf{x}$ and the Manhattan distance of $\|\mathbf{x}\|$, respectively. For two vectors $\mathbf{v}, \mathbf{w}$, $\langle \mathbf{v}, \mathbf{w} \rangle$ denotes the inner product of $\mathbf{v}$ and $\mathbf{w}$. For a full rank square matrix $\mathbf{B}$, $\tilde{\mathbf{B}}$ denotes the Gram-Schmidt orthogonalization of $\mathbf{B}$. For $k \in \{0, 1\}^*$, $|k|$ denotes the bit-length of k, and k_i denotes the i-bit of k. For a finite set Q, $a \leftarrow Q$ denotes the sampling of a from Q with uniform distribution. Finally, let X, Y be two random variables that

take values in Z, which is the union of supports of X and Y, then their statistical distance is defined as

$$\Delta(X, Y) = \frac{1}{2}\sum_{z\in Z}|\mathsf{Pr}[X = z] - \mathsf{Pr}[Y = z]|.$$

B. LATTICES BACKGROUND

The construction for our IDBMS scheme is based on lattices. In this section, we first give a brief introduction to the lattice. An m-dimensional lattice Λ is a discrete subgroup of $\mathbb{R}^m$, which is defined as follows.

Definition 1 (Lattices): Let $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n] \in \mathbb{R}^{m\times n}$, where $\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n \in \mathbb{R}^m$ are m linear independent vectors. The lattice Λ generated by $\mathbf{B}$ is the set of linear combinations of the columns of $\mathbf{B}$ with coefficients in $\mathbb{Z}$,

$\Lambda(\mathbf{B}) = \{a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n : a_1, a_2, \cdots, a_n \in \mathbb{Z}\}$.

In this case, the set of vectors $\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n$ is called a *basis* of Λ. If $n = m$, we say it is a *full-rank* lattice. In addition, we say that a lattice is a q-ary lattice if $(q\mathbb{Z})^m \subseteq \Lambda \subseteq \mathbb{Z}^m$ for some integer q.

Definition 2 (The q-ary Lattices): For prime q and $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, we can define the q-ary lattices as follows.

$$\Lambda_q(\mathbf{A}) = \{\mathbf{s} \in \mathbb{Z}^m : \exists \mathbf{e} \in \mathbb{Z}_q^n \; s.t. \; \mathbf{A}^\top\mathbf{e} = \mathbf{s} \; (mod \; q)\}$$
$$\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{s} \in \mathbb{Z}^m : \mathbf{A}\mathbf{s} = 0 \; (mod \; q)\}$$

The security analysis of our proposed scheme is based on the lattice hard assumption, short integer solution (SIS), first introduced by Ajtai [17]. Based on his work, Micciancio and Regev showed that solving the $\mathsf{SIS}_{q,n,m,\beta}$ problem in the average-case can be reduced to solving $\tilde{O}(\beta\sqrt{n})$-SIVP problem in the worst-case [18].

Definition 3 ($SIS_{q,n,m,\beta}$): Let $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$. The $\mathsf{SIS}_{q,n,m,\beta}$ problem is to find a nonzero vector $\mathbf{x} \in \mathbb{Z}^m$ such that

$$\mathbf{A}\mathbf{x} = 0 \; (mod \; q) \; and \; \|\mathbf{x}\| \le \beta.$$

C. DISCRETE GAUSSIAN DISTRIBUTION

In this section, we first define the discrete normal distribution over a lattice.

Definition 4 (Discrete Normal Distribution over Λ): If any parameter $s > 0$, center $\mathbf{c} \in \mathbb{R}^m$, The Gaussian function can be defined by

$$g_{\mathbf{c},s}(\mathbf{x}) = \mathsf{exp}(-\pi\frac{\|\mathbf{x} - \mathbf{c}\|^2}{s^2}).$$

In addition, let $g_{\mathbf{c},s}(\Lambda)$ be a sum of $g_{\mathbf{c},s}$ over the lattice Λ. We can define the discrete Gaussian function over lattice Λ as

$$D_{\Lambda,\mathbf{c},s}(\mathbf{x}) = \rho_{\mathbf{c},s}(\mathbf{x})/\rho_{\mathbf{c},s}(\Lambda).$$

Then, we define continuous Gaussian distribution over $\mathbb{R}^m$ and discrete Gaussian distribution over $\mathbb{Z}^m$ as follows.

Definition 5 (Continuous Normal Distribution over $\mathbb{R}^m$): If any parameter ζ, center $\mathbf{c} \in \mathbb{R}^m$, we can define the continuous normal Gaussian function over $\mathbb{R}^m$ as

$$\rho_{\mathbf{c},\zeta}^m(\mathbf{x}) = (2\pi\zeta^2)^{-m/2}\mathsf{exp}(-\frac{\|\mathbf{x} - \mathbf{c}\|^2}{2\zeta^2}).$$

Definition 6 (Discrete Normal Distribution over $\mathbb{Z}^m$): If any parameter ζ, center $\mathbf{c} \in \mathbb{Z}^m$, we can define the discrete Normal Gaussian function over $\mathbb{Z}^m$ as

$$D_{\mathbf{c},\zeta}^m(\mathbf{x}) = \rho_{\mathbf{c},\zeta}^m(\mathbf{x})/\rho_{\mathbf{c},\zeta}^m(\mathbb{Z}^m),$$

where $\rho_{\mathbf{c},\zeta}^m(\mathbb{Z}^m)$ is a sum of $\rho_{\mathbf{c},\zeta}^m$ over $\mathbb{Z}^m$.

For convenience, when $\mathbf{c} = 0$, we will simply write $g_\zeta(\mathbf{x})$, $D_{\Lambda,\zeta}(\mathbf{x})$, $\rho_\zeta(\mathbf{x})$, and $D_\zeta^m(\mathbf{x})$, respectively.

The below lemma provides two basic properties of discrete Gaussian distributions that will be used in the rejection sampling technique [18], [19].

Lemma 1: For $k \ge 1$, the following formula is satisfied. $\mathsf{Pr}[\|\mathbf{z}\| > k\zeta\sqrt{m} : \mathbf{z} \leftarrow D_\zeta^m] < k^m\mathsf{exp}((m/2)(1 - k^2))$.

In addition, for any $\zeta, r > 0$, and a vector $\mathbf{v} \in \mathbb{R}^m$, we have $\mathsf{Pr}[|\langle\mathbf{z}, \mathbf{v}\rangle| > r : \mathbf{z} \leftarrow D_\zeta^m] \le 2\mathsf{exp}(-(r^2/(2\|\mathbf{v}\|^2\zeta^2)))$.

Lemma 2: For $\alpha > 0, \mathbf{v} \in \mathbb{Z}^m$, if $\sigma = \alpha\|\mathbf{v}\|$, then $\mathsf{Pr}[D_\zeta^m(\mathbf{z})/D_{\mathbf{v},\zeta}^m(\mathbf{z}) < \mathsf{exp}(12/\alpha + 1/(2\alpha^2)) : \mathbf{z} \leftarrow D_\zeta^m] = 1 - 2^{-100}$.

D. SAMPLING OVER LATTICES

Hereunder, we recall some theorems that will be used in our scheme. Theorem 1 shows that there exists a PPT algorithm that can generate a pair $(\mathbf{A}, \mathbf{S})$, where $\mathbf{S}$ is a short basis for the lattice $\Lambda_q^\perp(\mathbf{A})$ [20].

Theorem 1: Let $q \ge 3$ be odd and $m > 5n\log q$. There is a PPT algorithm $\mathsf{TrapGen}(q, n, m)$ that outputs a pair $(\mathbf{A} \in \mathbb{Z}_q^{n\times m}, \mathbf{B} \in \mathbb{Z}^{m\times m})$ such that $\mathbf{A}$ is statistically close to a uniform matrix in $\mathbb{Z}^{n\times m}$ and $\mathbf{B}$ is a basis for $\Lambda_q^\perp(\mathbf{A})$ satisfying $\|\mathbf{B}\| \le O(n\log q)$ and $\|\tilde{\mathbf{B}}\| \le O(\sqrt{n\log q})$ with overwhelming probability.

The following two theorems show how to invert the SIS function using a lattice basis [21], [22].

Theorem 2: Let $m \ge n$ be an integer and let q be prime. Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{B}$ be a basis of $\Lambda_q^\perp(\mathbf{A})$, and $\zeta \ge \|\tilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log n})$. Then, for any $\mathbf{u} \in \mathbb{Z}_q^n$, there is a PPT algorithm $\mathsf{SamplePre}(\mathbf{A}, \mathbf{B}, \zeta, \mathbf{u})$ that outputs a vector $\mathbf{v} \in \Lambda_q^{\mathbf{u}}(\mathbf{A})$ from a distribution that is statistically close to $D_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),\zeta}$.

Theorem 3: Let $m \ge n$ and $k \ge 2$ be positive integers and let q be prime. Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{B}$ be a basis of $\Lambda_q^\perp(\mathbf{A})$, and $\zeta \ge \|\tilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log n})$. Then, for any $\mathbf{U} \in \mathbb{Z}_q^{n\times k}$, there is a PPT algorithm $\mathsf{SampleMat}(\mathbf{A}, \mathbf{B}, \zeta, \mathbf{U})$ that outputs a matrix $\mathbf{S} \in \mathbb{Z}^{m\times k}$ from a distribution that is statistically close to $D_{\Lambda_q^{\mathbf{U}}(\mathbf{A}),\zeta}$, where $D_{\Lambda_q^{\mathbf{U}}(\mathbf{A}),\zeta} = D_{\Lambda_q^{\mathbf{u}_1}(\mathbf{A}),\zeta} \times D_{\Lambda_q^{\mathbf{u}_2}(\mathbf{A}),\zeta} \times \cdots \times D_{\Lambda_q^{\mathbf{u}_k}(\mathbf{A}),\zeta}$.

E. REJECTION SAMPLING

The rejection sampling technique was first applied to lattice-based signatures in Lyubashevsky's work [19], making the signing key independent from the outputted signature. That is, we can sample a signature without revealing any secret

information. For example, if we want to generate a signature σ for a message μ using signing key k, then we let the distribution of the signature be f, which is independent of k and let g be the distribution of the signature, which is related to k. The rejection sampling is that if $f(x) \leq Kg(x)$ for all x and $K > 0$, we can generate a signature σ which is independent of the signing key k with probability $f(\sigma)/Kg(\sigma)$, where K is the expected number of times that will output a signature. The area between $f(\sigma)$ and $Kg(\sigma)$ is called the *rejection area*. Furthermore, Lyubashevsky provided the following useful lemma in [19]

Lemma 3: Let $V \subset \mathbb{Z}^m$ and $\forall \mathbf{v} \in V$, $\|\mathbf{v}\| \leq T$, $\zeta \in \mathbb{R}$ such that $\zeta = \omega(T\sqrt{\log m})$, and a probability distribution h that maps V to $\mathbb{R}$. Then there exists a constant $K = O(1)$ such that the statistical distance of the following distribution $\mathcal{F}_1$:

1) $\mathbf{v} \leftarrow h$.
2) $\mathbf{z} \leftarrow D^m_\zeta$
3) output $(\mathbf{z}, \mathbf{v})$ with probability $1/K$.

with the distributions $\mathcal{F}_2$:

1) $\mathbf{v} \leftarrow h$.
2) $\mathbf{z} \leftarrow D^m_{\mathbf{v},\zeta}$.
3) output $(\mathbf{z}, \mathbf{v})$ with probability $\min(\frac{D^m_\zeta(\mathbf{z})}{KD^m_{\mathbf{v},\zeta}(\mathbf{z})}, 1)$.

is within $2^{-\omega(\log m)}/K$.

III. IDENTITY-BASED BLIND MULTISIGNATURE SCHEME

We now precisely formalize the definition and security requirements of the IDBMS scheme. For convenience, let $\mathcal{M}$ be the message space and $\mathcal{S} = \{\mathcal{S}_1, \cdots, \mathcal{S}_N\}$ be the identities of the N signers who agree to sign a message $\mu \in \mathcal{M}$ collectively, and $\mathcal{U}$ be the user who wants to generate a blind multisignature.

A. SYNTAX OF IDBMS

We say that an IDBMS scheme consists of four algorithms (Setup, Extract, Sign, and Verify) which are defined as follows.

- $\mathsf{Setup}(1^\lambda) \rightarrow (\mathsf{pp}, \mathsf{mpk}, \mathsf{msk})$: On input of the security parameter λ, the probabilistic algorithm outputs public parameter pp, a master private key msk, and a master public key mpk.
- $\mathsf{Extract}(\mathsf{pp}, \mathsf{mpk}, \mathsf{msk}, \mathcal{S}_{id}) \rightarrow \mathsf{sk}_{\mathcal{S}_{id}}$: On input of the public parameter pp, master public key mpk, master private key msk, and signer identity $\mathcal{S}_{id}$, the probabilistic algorithm outputs a signing key $\mathsf{sk}_{\mathcal{S}_{id}}$ for signer $\mathcal{S}_{id}$.
- $\mathsf{Sign}(\mathsf{pp}, \mu, \mathcal{S}, \mathsf{sk}_{\mathcal{S}}, \mathsf{mpk}) \rightarrow \sigma$: It is an interactive algorithm between user $\mathcal{U}$ and a group of signers $\mathcal{S}$. On input of the public parameter pp, message $\mu \in \mathcal{M}$, signers' identities $\mathcal{S}$, their corresponding signer keys $\mathsf{sk}_{\mathcal{S}}$, master public key mpk, and message μ, the algorithm outputs an identity-based blind multisignature σ.
- $\mathsf{Verify}(\mathsf{pp}, \sigma, \mu, \mathcal{S}, \mathsf{mpk}) \rightarrow \{0, 1\}$: On input of the public parameter pp, identity-based blind multisignature σ, message μ, set of signers' identities $\mathcal{S}$, and master public key mpk, the deterministic algorithm outputs 1 if the signature is valid and all signers indeed signed the message, and 0 otherwise.

In addition, the correctness of IDBMS is defined as follows.

Definition 7: Let λ be a security parameter; we say that an IDBMS scheme is correct if the probability $\Pr[\mathsf{Verify}(\mathsf{pp}, \mathsf{Sign}(\mathsf{pp}, \mu, \mathcal{S}, \mathsf{sk}_{\mathcal{S}}, \mathsf{mpk}), \mu, \mathcal{S}, \mathsf{mpk}) = 1]$ is equal to 1 with overwhelming probability, where $(\mathsf{pp}, \mathsf{mpk}, \mathsf{msk})$ is outputted by $\mathsf{Setup}(1^\lambda)$, and each signer's signing key $\mathsf{sk}_{\mathcal{S}_{id}}$ is generated by $\mathsf{Extract}(\mathsf{pp}, \mathsf{mpk})$.

B. SECURITY REQUIREMENTS OF IDBMS

We now define the security requirements for the IDBMS scheme, which follows those defined in [23]–[25]. For an IDBMS scheme, the securities requirements that must be considered are *blindness* and *unforgeability*.

1) BLINDNESS

The blindness of the IDBMS scheme is defined as the following game. Let $\mathcal{A}$ be a PPT adversary who plays the role of the group of signers, and $\mathcal{U}_0$, $\mathcal{U}_1$ be two honest users. In the game of blindness, $\mathcal{U}_0$ and $\mathcal{U}_1$ engage in the blind multisignature scheme with $\mathcal{A}$ on messages μ_b and μ_{1-b}, and output signatures σ_b and σ_{1-b}, respectively, where $b \in \{0, 1\}$ is a random bit chosen uniformly. The messages μ_0, mu_1 and the output signatures σ_0, σ_1 are sent to the adversary $\mathcal{A}$, and $\mathcal{A}$ outputs a bit $b' \in \{0, 1\}$. If $b = b'$, we say that $\mathcal{A}$ wins the game.

Definition 8 (Blindness): We say that an IDBMS scheme has blindness if there is no adversary $\mathcal{A}$ who wins the above game with a non-negligible advantage δ.

2) UNFORGEABILITY

Unforgeability ensures that a malicious user cannot forge a blind multisignature from an honest signer. We define the unforgeability of the IDBMS scheme via the following game, which is played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

- Setup. The challenger $\mathcal{C}$ runs the Setup algorithm with a security parameter λ and sends the public parameter pp and the master public key mpk to $\mathcal{A}$, and keeps the master private key msk secret.
- Queries. The adversary $\mathcal{A}$ performs the following queries adaptively.
  - Hash function query: The hash function query only exists when the security is analyzed under a random oracle model. The challenger $\mathcal{C}$ computes an output of the hash function and sends the output to $\mathcal{A}$.
  - Extract query: The adversary $\mathcal{A}$ can issue this query to obtain the signing key of a signer $\mathcal{S}_{id}$. In response, the challenger $\mathcal{C}$ runs the algorithm $\mathsf{Extract}(\mathsf{pp}, \mathsf{mpk}, \mathsf{msk}, \mathcal{S}_{id})$ and returns a signing key $\mathsf{sk}_{\mathcal{S}_{id}}$ to the adversary $\mathcal{A}$.

TABLE 1. Parameter settings of our scheme.

Symbol	Definition
q	a large prime
n	a power of 2
m	$m > 5n \log q$
t	$\{0,1\}^*$
k	$\mathbb{Z}^+$
κ	$2^\kappa \binom{k}{\kappa} \geq 2^{100}$
N	$\mathbb{Z}^+$
μ	$\{0,1\}^*$
η	$[1.1, 1.3]$
ζ_0	$O(\sqrt{n \log n})$
ζ_1	$12\sqrt{\kappa}$
ζ_2	$12\eta\zeta_0\zeta_1\sqrt{mk}$
ζ_3	$12\zeta_2 N\sqrt{m}$
H_1	$\{0,1\}^* \times \{0,1\}^* \rightarrow \{\mathbf{v} : \mathbf{v} \in \{0,1\}^k, \|\mathbf{v}\|_1 \leq \kappa\}$
H_2	$\{0,1\}^* \rightarrow \mathbb{Z}^{n \times k}$
K_1	$\exp(12\zeta_1\sqrt{\kappa}/ + \kappa/(2\zeta_1^2))$
K_2	$\exp(1 + 1/288)$
K_3	$\exp(1 + 1/288)$

  - Sign query: When the adversary $\mathcal{A}$ issues such a query on message μ and an identity list $\mathcal{S}$, the challenger $\mathcal{C}$ returns a signature μ as a response.
- Forgery. In the end, $\mathcal{A}$ outputs a tuple $(\sigma', \mu', \mathcal{S}')$.

If the tuple satisfies the following requirements, $\mathcal{A}$ wins the above game.

- σ' is a valid signature on message μ' under the signers' identity list $\mathcal{S}'$.
- At least one signer $\mathcal{S}'_i \in \mathcal{S}'$ has not been queried during the Extract queries.
- $(\mathcal{S}', \mu')$ has never been queried during the Sign queries.

Definition 9 (Unforgeability): We say that an IDBMS scheme is existential unforgeable under adaptive chosen message and identity attacks if there is no PPT adversary $\mathcal{A}$ who wins the above game with a non-negligible advantage.

IV. OUR PROPOSED SCHEME

A. DESCRIPTION OF THE SCHEME

Hereunder, we describe the whole construction of the IDBMS scheme from lattices. The main steps of our construction are provided as follows, and the parameters we used are listed in Table 1. Note that the parameters K_1, K_2, K_3 are the expected number of times to generate a sample using rejection sampling. Therefore, we must set these as small as possible.

- Setup(1^λ): Given a security parameter λ, the algorithm performs as follows.
  1) It chooses prime $q > 3$, n is a power of 2, and sets $m > 5n \log q$.
  2) It chooses $k, \kappa \in \mathbb{Z}^+$, such that $2^\kappa \binom{k}{\kappa} \geq 2^{100}$. This is to make Lemma 4 correct.
  3) It chooses two secure hash functions $H_1 : \{0,1\}^* \times \{0,1\}^* \rightarrow \{\mathbf{v} : \mathbf{v} \in \{0,1\}^k, \|\mathbf{v}\|_1 \leq \kappa\}$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}^{n \times k}$.
  4) It generates $(\mathbf{A}_0, \mathbf{B}_0)$ by using TrapGen(q, n, m), and sets Gaussian parameters $\zeta_0 \geq \|\tilde{\mathbf{B}}_0\|$.
  5) It chooses η from $[1.1, 1.3]$, and sets $\zeta_1 = 12\sqrt{\kappa}$, $\zeta_2 = 12\eta\zeta_0\zeta_1\sqrt{mk}$, and $\zeta_3 = 12\zeta_2 N\sqrt{m}$.
  6) It sets $K_1 = \exp(12\zeta_1\sqrt{\kappa}/ + \kappa/(2\zeta_1^2))$, $K_2 = \exp(1 + 1/288)$, and $K_3 = \exp(1 + 1/288)$.
  7) It outputs the public parameters $\mathsf{pp} = \{q, n, m, k, \eta, \{\zeta_i\}_{i=0}^3, \{K_i\}_{i=1}^3, H_1, H_2\}$, master public key $\mathsf{mpk} = \mathbf{A}_0$, and master private key $\mathsf{msk} = \mathbf{B}_0$.
- Extract(pp, mpk, msk, $\mathcal{S}_{id}$): Given the public parameter pp, master public key $\mathsf{mpk} = \mathbf{A}_0$, master private key $\mathsf{msk} = \mathbf{B}_0$, and a signer's identity $\mathcal{S}_{id}$, the algorithm extracts a signer's signing key as follows.
  1) It computes the hash value of the signer's identity $\mathbf{A}_{id} = H_2(\mathcal{S}_{id})$.
  2) It computes $\mathbf{B}_{id} \leftarrow \mathsf{SampleMat}(\mathbf{A}_0, \mathbf{B}_0, \zeta_0, \mathbf{A}_{id})$.
  3) It outputs $\mathsf{sk}_{\mathcal{S}_{id}} = \mathbf{B}_{id}$ for signer $\mathcal{S}_{id}$.
- Sign(pp, μ, $\mathcal{S}$, $\mathsf{sk}_{\mathcal{S}}$, mpk): This is a four-stage interactive algorithm between a user and a group of signers. On input public parameter pp, a message μ, signers' identities $\mathcal{S} = \{\mathcal{S}_1, \cdots, \mathcal{S}_N\}$ with their signing keys $\mathsf{sk}_{\mathcal{S}}$, and a master public key $\mathsf{mpk} = \mathbf{A}_0$, the algorithm generates a signature by performing the following stages. Note that if $\mathbf{e}, \mathbf{y}_{i=1}^N$, and $\mathbf{z}$ are produced in the rejection area, they will be rejected.
  1) Each signer $\mathcal{S}_i \rightarrow$ User $\mathcal{U}$:
     a) It chooses $\mathbf{r}_i \leftarrow D_{\zeta_2}^m$, and computes $\mathbf{x}_i = \mathbf{A}_0\mathbf{r}_i$.
     b) It sends $\mathbf{x}_i$ to user $\mathcal{U}$.
  2) User $\mathcal{U} \rightarrow$ Each signer $\mathcal{S}_i$:
     a) It chooses $t \leftarrow \{0,1\}^*$, $\mathbf{a} \leftarrow D_{\zeta_3}^m$, and $\mathbf{b} \leftarrow D_{\zeta_1}^k$.
     b) It computes $\sum_{i=1}^N \mathbf{x}_i$.
     c) It computes $\mathbf{A}_\tau = \sum_{i=1}^N H_2(\mathcal{S}_i) = \sum_{i=1}^N \mathbf{A}_i$.
     d) It computes $\mathbf{c} = H_1(\mathbf{x} + \mathbf{A}_0\mathbf{a} + \mathbf{A}_\tau \cdot \mathbf{b}, \mathsf{com}(t, \mu))$, where com is a secure commitment function.
     e) It outputs $\mathbf{e} = \mathbf{c} + \mathbf{b}$ with probability $\min\left(\frac{D_{\zeta_1}^k(\mathbf{e})}{K_1 D_{\mathbf{c},\zeta_1}^k(\mathbf{e})}, 1\right)$.
     f) It sends $\mathbf{e}$ to each signer $\mathcal{S}_i$.
  3) Each signer $\mathcal{S}_i \rightarrow$ User $\mathcal{U}$:
     a) It computes $\mathbf{y}_i = \mathbf{B}_i\mathbf{e} + \mathbf{r}_i$ with probability $\min\left(\frac{D_{\zeta_2}^m(\mathbf{y}_i)}{K_2 D_{\mathbf{B}_i\mathbf{e},\zeta_2(\mathbf{y}_i)}^m}, 1\right)$, and sends $\mathbf{y}_i$ to user $\mathcal{U}$.
  4) User $\mathcal{U}$ generates signature:
     a) It computes $\mathbf{y} = \sum_{i=1}^N \mathbf{y}_i$
     b) It computes $\mathbf{z} = \mathbf{y} + \mathbf{a}$ with probability $\min\left(\frac{D_{\zeta_3}^m(\mathbf{z})}{K_3 D_{\mathbf{y},\zeta_3(\mathbf{z})}^m}, 1\right)$.
     c) If $\mathbf{z}$ is in the rejection area, it sends $(\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathsf{com}(t, \mu))$ to each signer. Signers restart the protocol if the following conditions are satisfied.
        - $\mathbf{c} = H_1(\mathbf{A}_0\mathbf{a} + \mathbf{A}_0\mathbf{y} + \mathbf{A}_\tau \cdot \mathbf{c}, \mathsf{com}(t, \mu))$.
        - $\mathbf{e} - \mathbf{b} = \mathbf{c} = H_1(\sum_{i=1}^N \mathbf{x}_i + \mathbf{A}_0\mathbf{a} + \mathbf{A}_\tau \cdot \mathbf{b}, \mathsf{com}(t, \mu))$.
        - $\mathbf{y} + \mathbf{a}$ in the rejection area.
     d) Else, it outputs a blind multisignature $\sigma = (\mathbf{z}, \mathbf{c}, t)$

TABLE 2. Comparison of the complexity of the key size and signature size with [14] under N signers setting.

Scheme	Trusted Authority		Signer		Signature
	Public key	Secret key	Public key	Secret key	
[14]	-	-	$nk \log q$	$m'k \log(2d+1)$	$Nm' \log \sigma$
Ours	$nm \log q$	$m^2 \log q$	$\|\mathsf{ID}\|$	$mk \log \zeta_0$	$m \log \zeta_3$

- $\mathsf{Verify}(\mathsf{pp}, \sigma, \mu, \mathcal{S}, \mathsf{mpk})$: Given the public parameter pp, a signature $\sigma = (\mathbf{z}, \mathbf{c}, t)$, a message μ, the identity list of all signers $\mathcal{S} = \{\mathcal{S}_1, \cdots, \mathcal{S}_N\}$, and the master public key $\mathsf{mpk} = \mathbf{A}_0$, the algorithm checks whether the signature is valid as follows.
  1) It computes $\mathbf{A}_\tau = \sum_{i=1}^{N} H_2(\mathcal{S}_i) = \sum_{i=1}^{N} \mathbf{A}_i$.
  2) It outputs 1 if and only if $\mathbf{c} = H_1(\mathbf{A}_0\mathbf{z} - \mathbf{A}_\tau \cdot \mathbf{c}, \mathsf{com}(t, \mu))$ and $\|\mathbf{z}\| \leq \eta\zeta_3\sqrt{m}$, where $\eta > 1$.
  3) Else, it outputs 0.

B. CORRECTNESS

Theorem 4: The proposed IDBMS scheme satisfies correctness.

Proof 1: Given master public key mpk, master private key msk, a group of signers' identities $\mathcal{S} = \{\mathcal{S}_1, \cdots, \mathcal{S}_N\}$, a message μ, and a signature $\sigma = (\mu, (\mathbf{z}, \mathbf{c}, t))$, we have

$$
\begin{aligned}
\mathbf{c} &= H_1(\mathbf{x} + \mathbf{A}_0\mathbf{a} + \sum_{i=1}^{N} H_2(\mathcal{S}_i) \cdot \mathbf{b}, \mathsf{com}(t, \mu)) \\
&= H_1(\mathbf{A}_0 \sum_{i=1}^{N} \mathbf{r}_i + \mathbf{A}_0\mathbf{a} + \mathbf{A}_\tau \cdot \mathbf{b}, \mathsf{com}(t, \mu)) \\
&= H_1(\mathbf{A}_0 \sum_{i=1}^{N} \mathbf{r}_i + \mathbf{A}_0\mathbf{a} + \mathbf{A}_\tau \cdot (\mathbf{e} - \mathbf{c}), \mathsf{com}(t, \mu)) \\
&= H_1(\mathbf{A}_0 \sum_{i=1}^{N} \mathbf{r}_i + \mathbf{A}_0\mathbf{a} + \mathbf{A}_\tau \cdot \mathbf{e} - \mathbf{A}_\tau \cdot \mathbf{c}, \mathsf{com}(t, \mu)) \\
&= H_1(\mathbf{A}_0 \sum_{i=1}^{N} \mathbf{r}_i + \mathbf{A}_0\mathbf{a} + \mathbf{A}_0 \sum_{i=1}^{N} \mathbf{B}_i \cdot \mathbf{e} - \mathbf{A}_\tau \cdot \mathbf{c}, \mathsf{com}(t, \mu)) \\
&= H_1(\mathbf{A}_0 \sum_{i=1}^{N} \mathbf{y}_i + \mathbf{A}_0\mathbf{a} - \mathbf{A}_\tau \cdot \mathbf{c}, \mathsf{com}(t, \mu)) \\
&= H_1(\mathbf{A}_0\mathbf{y} + \mathbf{A}_0\mathbf{a} - \mathbf{A}_\tau \cdot \mathbf{c}, \mathsf{com}(t, \mu)) \\
&= H_1(\mathbf{A}_0\mathbf{z} - \mathbf{A}_\tau \cdot \mathbf{c}, \mathsf{com}(t, \mu)).
\end{aligned}
$$

In addition, with Lemma 1, $\|\mathbf{z}\|$ is less equal than $\eta\zeta_3\sqrt{m}$ with overwhelming probability. Therefore, the verifier can verify the signature σ with $\mathsf{Verify}(\mathsf{pp}, \sigma, \mu, \mathcal{S}, \mathsf{mpk}) = 1$. ■

C. COMPARISON

Table 2 shows the comparison with [14]. In this comparison, we assume that a user communicates with N signers to generate a blind multisignature in our scheme, while the user generates N blind signature in [14]. The symbol $|\mathsf{ID}|$ denotes the length of a signer's identity, d is an integer, σ is a standard deviation, and $m' = 64 + n \log q / \log(2d+1)$ in the setting of [14]. Although the size of the signer's secret key is larger than [14], our scheme reduces the size of the public key. Additionally, the size of our signature is smaller than [14] when the user generates a signature with multiple signers. Note that because the security requirement is the same as for blind signature, we do not provide a comparison with [14]. As for efficiency, the cost of generating a blind multisignature is also the same as [14].

V. SECURITY ANALYSIS

In this section, we will provide security proofs to show that our scheme has blindness and unforgeability by following the idea of [14].

A. BLINDNESS

In this section, we prove that our scheme is statistically blind. We use $\mathcal{A}$ to represent the group of malicious signers who want to distinguish the views $\mathcal{V}_0, \mathcal{V}_1$ generated by different messages μ_0, μ_1 from two users $\mathcal{U}_0, \mathcal{U}_1$, respectively.

Theorem 5: The proposed scheme is blind if commitment function com is δ-hiding.

Proof 2: In this proof, we show that the adversary $\mathcal{A}$ cannot obtain information about the signed message. We analyze the distribution of $\mathbf{e}$, $\mathbf{z}$, and the situation that protocol restarts. Note that due to $\mathbf{c}, t$ being generated from a secure hash function and randomness, we need not worry.

- Distribution of $\mathbf{e}$. First, we let $\mathbf{e}_b, \mathbf{e}_{1-b}$ be the value generated by $\mathcal{U}_b(\mathsf{mpk}, \mu_b)$ and $\mathcal{U}_{1-b}(\mathsf{mpk}, \mu_{1-b})$, respectively. For our proposed scheme, $\mathbf{e}_b$ is generated by rejection sampling with the probability $\min(D^k_{\zeta_1}(\mathbf{e}_b)/K_1 D^k_{\mathbf{c},\zeta_1}(\mathbf{e}_b), 1)$ and $\mathbf{e}_{1-b}$ is generated by rejection sampling with the probability $\min(D^k_{\zeta_1}(\mathbf{e}_{1-b})/K_1 D^k_{\mathbf{c},\zeta_1}(\mathbf{e}_{1-b}), 1)$, thus they have the same distribution $D^k_{\zeta_1}$. Moreover, their statistical distance is $\Delta(\mathbf{e}_b, \mathbf{e}_{1-b}) = 0$. Therefore, $\mathbf{e}_b(\mathbf{e}_{1-b})$ are independent with its corresponding message $\mu_b(\mu_{1-b})$. Therefore, the adversary $\mathcal{A}$ cannot distinguish them.
- Distribution of $\mathbf{z}$. It is similar to $\mathbf{e}$. Let $\mathbf{z}_b, \mathbf{z}_{1-b}$ be the values generated by $\mathcal{U}_b(\mathsf{mpk}, \mu_b)$ and $\mathcal{U}_{1-b}(\mathsf{mpk}, \mu_{1-b})$, respectively. Because $\mathbf{z}_b$ is generated by rejection sampling with the probability $\min(D^m_{\zeta_3}(\mathbf{z}_b)/K_3 D^m_{\mathbf{y},\zeta_3}(\mathbf{z}_b), 1)$, and $\mathbf{z}_{1-b}$ is generated by rejection sampling with the probability $\min(D^m_{\zeta_3}(\mathbf{z}_{1-b})/K_3 D^m_{\mathbf{y},\zeta_3}(\mathbf{z}_{1-b}), 1)$, they have the same distribution $D^m_{\zeta_3}$ and their statistical distance is $\Delta(\mathbf{z}_b, \mathbf{z}_{1-b}) = 0$. Therefore, $\mathbf{z}_b(\mathbf{z}_{1-b})$ are independent with its corresponding message $\mu_b(\mu_{1-b})$, and the adversary $\mathcal{A}$ cannot distinguish them.

- Restarts. For each session for our protocol, the user will select fresh t, $\mathbf{a}$, $\mathbf{b}$ which are statistically independent of the previous session due to the hiding property of the commitment function com. With the δ-hiding property, the adversary $\mathcal{A}$ never obtains the information of the message μ.

Therefore, our protocol has blindness if the commitment function com is δ-hiding. ■

B. UNFORGEABILITY

Theorem 6: The proposed scheme is existential unforgeable under the adaptive chosen message and identity attacks based on the hardness of the $\mathsf{SIS}_{q,n,m,\beta}$ problem for $\beta = 2(\eta\zeta_3 + \zeta_0 N\kappa)\sqrt{m}$.

Proof 3: In the following proof, let $\mathcal{A}$ be an adversary who wants to break the unforgeability of the proposed scheme, and $\mathcal{C}$ be an SIS challenger. In addition, $\mathcal{C}$ is given an SIS instance $\mathbf{A}_0 \in \mathbb{Z}_q^{n\times m}$, where q is a large prime, n is a power of 2, and $m \geq 5n\log q$. The following statement will prove that if $\mathcal{A}$ can break the unforgeability of our scheme, then $\mathcal{C}$ can solve the $\mathrm{SIS}_{q,n,m,\beta}$ assumption. The purpose of $\mathcal{C}$ is to find a non-zero vector $\mathbf{v}$ such that $\mathbf{A}_0\mathbf{v} = 0\ (mod\ q)$ and $\|\mathbf{v}\| \leq 2(\eta\zeta_3 + \zeta_0 N\kappa)\sqrt{m}$.

- Setup. In this phase, $\mathcal{C}$ runs the Setup algorithm to choose $(k, \{\zeta_i\}_{i=0}^3, \{K_i\}_{i=1}^3)$. Then $\mathcal{C}$ sets the public parameter $\mathsf{pp} = \{q, n, m, k, \{\zeta_i\}_{i=0}^3, \{K_i\}_{i=1}^3\}$, and master public key $\mathsf{mpk} = \mathbf{A}_0$. $\mathcal{C}$ also chooses three hash lists, H_1-list, H_2-list, and Sign-list, and sets them as empty. Finally, $\mathcal{C}$ sends pp and mpk to $\mathcal{A}$.
- Queries. In this phase, $\mathcal{A}$ can request the following queries adaptively.
  - H_1 query : When $\mathcal{A}$ issues such a query on $(\mathbf{x} + \mathbf{A}_0\mathbf{a} + \mathbf{A}_\tau\mathbf{b}, \mathsf{com}(t, \mu))$, $\mathcal{C}$ looks it up in H_1-list. If there is an matching pair $((\mathbf{x} + \mathbf{A}_0\mathbf{a} + \mathbf{A}_\tau\mathbf{b}, \mathsf{com}(t, \mu)), \mathbf{c})$, then $\mathcal{C}$ returns $\mathbf{c}$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ chooses a random vector $\mathbf{c} \leftarrow \{\mathbf{v} : \mathbf{v} \in \{-1, 0, 1\}^k, \|\mathbf{v}\|_1 \leq \kappa\}$, stores $((\mathbf{x} + \mathbf{A}_0\mathbf{a} + \mathbf{A}_\tau\mathbf{b}, \mathsf{com}(t, \mu)), \mathbf{c})$ in the H_1-list, and returns $\mathbf{c}$ to $\mathcal{A}$.
  - H_2 query : When $\mathcal{A}$ issues such a query on a signer's identity $\mathcal{S}_{id}$, $\mathcal{C}$ looks it up in H_2-list. If there is a matching pair $(\mathcal{S}_{id}, \mathbf{A}_{id}, \mathbf{B}_{id})$, $\mathcal{C}$ returns $\mathbf{A}_{id}$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ chooses a random matrix $\mathbf{B}_{id} \in \mathbb{Z}^{m\times k}$ and each column of $\mathbf{B}_{id}$ is chosen from $D_{\mathbb{Z}^m,\zeta_0}$. Then $\mathcal{C}$ computes $\mathbf{A}_{id} = \mathbf{A}_0\mathbf{B}_{id}$ and returns it to $\mathcal{A}$. Finally, $\mathcal{C}$ stores a tuple $(\mathcal{S}_{id}, \mathbf{A}_{id}, \mathbf{B}_{id})$.
  - Extract query : When $\mathcal{A}$ issues such a query on a signer's identity $\mathcal{S}_{id}$, $\mathcal{C}$ looks it up in H_2-list. If there is an matching pair $(\mathcal{S}_{id}, \mathbf{A}_{id}, \mathbf{B}_{id})$. Otherwise, $\mathcal{C}$ requests $\mathcal{A}$ to issue H_2 on signer's identity $\mathcal{S}_{id}$ first.
  - Sign query : When $\mathcal{A}$ issues such a query on $(\mathcal{S} = \{\mathcal{S}_1, \cdots, \mathcal{S}_N\}, \mu)$, $\mathcal{C}$ performs the following steps.
    1) For each $\mathcal{S}_i \in \mathcal{S}$, $\mathcal{C}$ queries H_2 on identity $\mathcal{S}_i$ to obtain $\mathbf{A}_i$.
    2) $\mathcal{C}$ computes $\mathbf{A}_\tau = \sum_{i=1}^N \mathbf{A}_i$.
    3) $\mathcal{C}$ chooses a random matrix $\mathbf{z} \in \mathbb{Z}^m$ satisfies that $\|\mathbf{z}\| \leq \eta\zeta_3\sqrt{m}$.
    4) $\mathcal{C}$ chooses a random vector $\mathbf{c} \leftarrow \{\mathbf{v} : \mathbf{v} \in \{-1, 0, 1\}^k, \|\mathbf{v}\| \leq \kappa\}$, and selects $t \leftarrow \{0, 1\}^*$.
    5) $\mathcal{C}$ sets $\mathbf{c} = \mathsf{H}_1(\mathbf{A}_0\mathbf{z} - \mathbf{A}_\tau\mathbf{c}, \mathsf{com}(t, \mu))$.
    6) Finally, $\mathcal{C}$ returns a signature $\sigma = (\mathbf{z}, \mathbf{c}, t)$ as a response, and stores a tuple $(\sigma, \mathcal{S}, \mu)$ in the Sign-list.
- Forgery. After querying above queries, with non-negligible probability δ, $\mathcal{A}$ finally outputs a forgery signature $\sigma' = (\mathbf{z}', \mathbf{c}', t')$ on message μ' with an identity list of signers $\mathcal{S}' = \{\mathcal{S}_1', \cdots, \mathcal{S}_N'\}$.

After $\mathcal{A}$ forged the signature σ', $\mathcal{C}$ will use the following method to obtain a solution $\mathbf{v}$ such that $\mathbf{A}_0\mathbf{v} = 0\ (mod\ q)$ and $\|\mathbf{v}\| \leq 2(\eta\zeta_3 + \zeta_0 N\kappa)\sqrt{m}$. $\mathcal{C}$ reruns $\mathcal{A}$ again with the same random tape but the output sequence of the H_1 and H_2 queries are different. By the general forking lemma [26], $\mathcal{A}$ outputs a new forgery $(\mathbf{z}'', \mathbf{c}'', t'')$ on the same message μ' and identity list $\mathcal{S}'$ with probability of at least $\delta/2$, such that $\mathbf{z}' \neq \mathbf{z}''$, $\mathbf{c}' \neq \mathbf{c}''$, and $\mathbf{A}_0\mathbf{z}' - \mathbf{A}_\tau\mathbf{c}' = \mathbf{A}_0\mathbf{z}'' - \mathbf{A}_\tau\mathbf{c}''$. After replacing $\mathbf{A}_\tau$ with $\mathbf{A}_0\sum_{i=1}^N \mathbf{B}_i$, we have

$$\mathbf{A}_0(\mathbf{z}' - \mathbf{z}'' + \sum_{i=1}^N \mathbf{B}_i\mathbf{c}'' - \sum_{i=1}^N \mathbf{B}_i\mathbf{c}') = 0.$$

Because $\|\mathbf{z}'\|, \|\mathbf{z}''\| \leq \eta\zeta_3\sqrt{m}$ and $\|\sum_{i=1}^N \mathbf{B}_i\mathbf{c}'\|, \|\sum_{i=1}^N \mathbf{B}_i\mathbf{c}''\| \leq \zeta_0 N\kappa\sqrt{m}$, $\|\mathbf{z}' - \mathbf{z}'' + \sum_{i=1}^N \mathbf{B}_i\mathbf{c}'' - \sum_{i=1}^N \mathbf{B}_i\mathbf{c}'\| \leq 2(\eta\zeta_3 + \zeta_0 N\kappa)\sqrt{m}$. If $\mathbf{z}' - \mathbf{z}'' + \sum_{i=1}^N \mathbf{B}_i\mathbf{c}'' - \sum_{i=1}^N \mathbf{B}_i\mathbf{c}' = 0$, then $\mathcal{C}$ obtains a solution of the SIS problem.

Next, we consider that $\mathbf{z}' - \mathbf{z}'' + \sum_{i=1}^N \mathbf{B}_i\mathbf{c}'' - \sum_{i=1}^N \mathbf{B}_i\mathbf{c}' \neq 0$. With the Lemma 4, it shows that, with probability no less than $1 - 2^{-100}$, there exists another $\mathbf{B}^* \neq \sum_{i=1}^N \mathbf{B}_i$ such that $\mathbf{A}_0\mathbf{B}^* = \mathbf{A}_0\sum_{i=1}^N \mathbf{B}_i$. Therefore, if $\mathbf{z}' - \mathbf{z}'' + \sum_{i=1}^N \mathbf{B}_i(\mathbf{c}'' - \mathbf{c}') = 0$, then $\mathbf{z}' - \mathbf{z}'' + \mathbf{B}^*(\mathbf{c}'' - \mathbf{c}') \neq 0$ and $\mathbf{A}_0(\mathbf{z}' - \mathbf{z}'' + \mathbf{B}^*(\mathbf{c}'' - \mathbf{c}')) = 0$. $\mathcal{C}$ obtains a solution of the SIS problem.

Lemma 4: For any $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ where $m > 5n\log q$, for randomly chosen $\mathbf{S} \leftarrow \{-\zeta_0 N, \cdots, 0, \cdots, \zeta_0 N\}^{m\times k}$. When the parameters are set under our scheme, with a probability of at least $1 - 2^{-100}$, there exists another $\mathbf{S}' \in \{-\zeta_0 N, \cdots, 0, \cdots, \zeta_0 N\}^{m\times k}$ such that $\mathbf{AS} = \mathbf{AS}'$.

Proof 4: (Proof of Lemma 4) The proof is similar to the proof in [19] Lemma 5.2. The probability of randomly choosing non-colliding elements is at most

$$\frac{q^{n\times k}}{(2\zeta_0 N + 1)^{m\times k}} \leq \frac{q^{n\times k}}{(2\zeta_0 N)^{5n\log q\times k}}.$$

Therefore, for our setting ($q = 2^{27}, n = 512, k = 80, N = 10, \zeta_0 = 64$), the probability of colliding elements is at least

$$1 - \frac{2^{27*80}}{2 * 64 * 10^{5*512*27*80}} \geq 1 - 2^{-100}.$$

■

Because the $\sum_{i=1}^N \mathbf{B}_i$ and $\mathbf{B}^*$ are independent of the signatures and act as the same role in our proposed scheme, $\mathcal{A}$ cannot obtain the information about which of them was used in the simulation. Therefore, with the above statements, $\mathcal{C}$ can find

a non-zero solution $\mathbf{v} = \mathbf{z}' - \mathbf{z}'' + \sum_{i=1}^{N} \mathbf{B}_i \mathbf{c}'' - \sum_{i=1}^{N} \mathbf{B}_i \mathbf{c}'$ with a probability of at least 1/2 such that $\mathbf{A}_0 \mathbf{v} = 0 \ (mod\ q)$, and $\|\mathbf{v}\| \leq 2(\eta\zeta_3 + \zeta_0 N\kappa)\sqrt{m}$ ■

VI. CONCLUSION

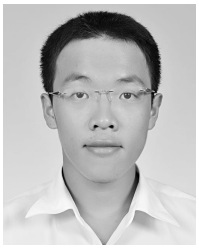
In this study, we propose a quantum-resistant identity-based blind multisignature scheme. The construction is based on a lattice hard assumption (short integer solution, SIS). It is the *first* quantum-resistant instantiation that has the advantages of blind signature and multisignature. We have also shown that our scheme is blind and unforgeable with rigorous formal proofs. Currently, we are working on constructing a quantum-resistant identity-based blind multisignature scheme in the standard model.

REFERENCES

[1] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*. Boston, MA, USA: Springer, 1983, pp. 199–203.
[2] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Proc. Conf. Theory Appl. Cryptogr.* New York, NY, USA: Springer, 1988, pp. 319–327.
[3] S. Ibrahim, M. Kamat, M. Salleh, and S. R. A. Aziz, "Secure E-voting with blind signature," in *Proc. 4th Nat. Conf. Telecommun. Technol. (NCTT)*, Jan. 2003, pp. 193–197.
[4] S. Kremer, M. Ryan, and B. Smyth, "Election verifiability in electronic voting protocols," in *Proc. Eur. Symp. Res. Comput. Secur.* Berlin, Germany: Springer 2010, pp. 389–404.
[5] M. Kumar, C. P. Katti, and P. C. Saxena, "A secure anonymous E-voting system using identity-based blind signature scheme," in *Proc. Int. Conf. Inf. Syst. Secur.* Cham, Switzerland: Springer, 2017, pp. 29–49.
[6] H. Petersen, P. Horster, and M. Michels, "Blind multisignature schemes and their relevance to electronic voting," in *Proc. 11th Annu. Comput. Secur. Appl. Conf.*, 1995, pp. 149–155.
[7] X. Chen, F. Zhang, and K. Kim, "ID-based multi-proxy signature and blind multisignature from bilinear pairings," in *Proc. KIISC*, vol. 3, 2003, pp. 11–19.
[8] Y. Hanatani, Y. Komano, K. Ohta, and N. Kunihiro, "Provably secure electronic cash based on blind multisignature schemes," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2006, pp. 236–250.
[9] A. K. Namdeo, "Untraceable blind multisignature," Ph.D. dissertation, Dept. Comput. Sci. Eng., Nat. Inst. Technol. Rourkela, Odisha, India, 2015.
[10] D. N. Tan, H. N. Nam, M. N. Hieu, H. N. Van, and L. T. Thi, "New blind muti-signature schemes based on ECDLP," *Int. J. Elect. Comput. Eng.*, vol. 8, no. 2, pp. 1074–1083, 2018.
[11] D. N. Tan, H. N. Nam, H. N. Van, L. T. Thi, and M. N. Hieu, "New blind mutisignature schemes based on signature standards," in *Proc. Int. Conf. Adv. Comput. Appl. (ACOMP)*, Nov./Dec. 2017, pp. 23–27.
[12] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, 1999.
[13] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the Theory and Application of Cryptographic Techniques*. Berlin, Germany: Springer, 1984, pp. 47–53.
[14] 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. 27251–27258, 2018.
[15] M. Tian and L. Huang, "Identity-based signatures from lattices: Simpler, faster, shorter," *Fundamenta Informaticae*, vol. 145, no. 2, pp. 171–187, 2016.
[16] R. El Bansarkhani and J. Sturm, "An efficient lattice-based multisignature scheme with applications to bitcoins," in *Proc. Int. Conf. Cryptol. Netw. Secur.* Cham, Switzerland: Springer, 2016, pp. 140–155.
[17] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. 28th Annu. Symp. Theory Comput.*, 1996, pp. 99–108.
[18] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM J. Comput.*, vol. 37, no. 1, pp. 267–302, 2007.
[19] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2012, pp. 738–755.
[20] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," *Theory Comput. Syst.*, vol. 48, pp. 535–553, Apr. 2011, doi: 10.1007/s00224-010-9278-3.
[21] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 14th Annu. ACM Symp. Theory Comput.*, 2008, pp. 197–206.
[22] M. Tian and L. Huang, "Efficient identity-based signature from lattices," in *Proc. IFIP Int. Inf. Secur. Conf.* Berlin, Germany: Springer, 2014, pp. 321–329.
[23] A. Juels, M. Luby, and R. Ostrovsky, "Security of blind digital signatures," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1997, pp. 150–164.
[24] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, 2000.
[25] M. Rückert, "Lattice-based blind signatures," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2010, pp. 413–430.
[26] M. Bellare and G. Neven, "Multi-signatures in the plain public-key model and a general forking lemma," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, 2006, pp. 390–399.

RAYLIN TSO received the B.Eng. degree from National Tsing Hua University, Taiwan, in 1995, and the M.Eng. and Ph.D. degrees in systems and information engineering from Tsukuba University, Japan, in 2004 and 2006, respectively.

He is currently an Associate Professor with the Department of Computer Science, National Chengchi University, Taiwan. He has authored or coauthored over 60 articles in refereed journals and conferences in the area of information security. His research interests are mainly in the areas of cryptography, the IoT security, privacy preserving data analysis, and blockchain technology. He has received many academic awards including, the IPSJ Digital Courier Award for Young Researcher (2006), the Dean's Award of the Graduate School of Systems and Information Engineering, University of Tsukuba, Japan (2006), the Research Award of College of Science (NCCU) for Early Career Researchers (2015), and the Award of WITC 2015 Outstanding Researcher (2015). He is also serving as the Executive Editor of the *Internal Journal of Information and Computer Security*.



ZI-YUAN LIU received the B.E. degree in computer science from National Tseng Hua University, Taiwan, in 2016, and the M.E. degree in computer science from National Chengchi University, Taiwan, in 2018, where he is currently pursuing the Ph.D. degree in computer science. His current research interests include post-quantum cryptography and blockchain technology.

YI-FAN TSENG was born in Kaohsiung, Taiwan. He received the M.S. and Ph.D. degrees in computer science and engineering from National Sun Yat-sen University, Taiwan, in 2014 and 2018, respectively. From 2018 to 2019, he was a Postdoctoral Researcher, he joined the Research Group of Taiwan Information Security Center, National Sun Yat-sen University (TWISC@NSYSU). In 2019, he joined as a Faculty Member of the Department of Computer Science, National Chengchi University, Taipei, Taiwan. His research interests include cloud computing and security, network and communication security, information security, cryptographic protocols, and applied cryptography.