Identity-Based Blind Signature from Lattices in Standard Model

Wen Gao(✉), Yupu Hu, Baocang Wang, and Jia Xie

School of Tele-Communications Engineering, Xidian University, Xi'an, China
gaowen0807@0utlook.com, yphu@mail.xidian.edu.cn,
bcwang@aliyun.com, xiejial99325@163.com

Abstract. Blind signature allows a user to get a signature of a signer on an arbitrary message, without leaking any information about the message. The verifier can check that whether the signature is indeed generated by the signer, and the signer cannot recall the signing situation. This property is essential when the signed message needs privacy protection for the user, like a bank bill or a trade secret. Lattice-based system is the most promising quantum-resistant primitive, and the first lattice-based blind signature is proposed by Rückert. For another, identity-based system is an alternative to public key infrastructure, as it can simplify the key management procedures in certificate-based public key systems. Illuminated by the demand of identity-based blind signature in the post-quantum circumstance, we consider the lattice-based identity based blind signature (IBBS) based on hard worst-case lattice problems. Besides, all existing lattice-based blind signatures are constructed and proved to be secure in the random oracle model. In this work, we construct an identity-based blind signature from lattices in the standard model. Our construction is proved to be one-more unforgeable under the selective identity and chosen message attacks (sID-CMA), and unconditionally blind in the standard model.

Keywords: Digital signature · Lattice-based cryptography · Blind signature

1 Introduction

1.1 Backgrounds

Digital signature can ensure the integrity of information transmission, identify the message sender, and avoid the repudiation in business deal. The signature is always created by the signer under his signing key, and the signer often knows the message signed. However, sometimes, the message signed may need privacy protection, and the owner of the message only needs a signature of a particular signer under the message without leaking its privacy.

Bind signature was first introduced by Chaum [1] in 1982 as a new type of signature with novel functionality, which enabled a user to get a signature from a signer S on an arbitrary message M without leaking any information about M, any verifier can check the signature whether it was indeed a signature on M signed by S. Blind signature is applicable in many situations, such as e-voting applications, anonymous Internet banking, and oblivious transfer.

K. Chen et al. (Eds.): Inscrypt 2016, LNCS 10143, pp. 205–218, 2017.
DOI: 10.1007/978-3-319-54705-3_13

Shor's algorithms [2] show that the integer factoring and the discrete logarithm problems can be solved in polynomial time under quantum computers, on which the hardness of many existing blind signature schemes are based. Thus, these blind signatures become insecure once quantum computers become mature development, and quantum secure primitives are in urgent needs. Therefore, tremendous efforts have been made on the classical schemes that remain secure against a quantum adversary, which is called *post-quantum cryptosystems*. Lattice-based cryptography has become a hot research topic in post quantum cryptography, and many significant achievements have been obtained [3–10] in recent years.

A natural goal is to design blind signature from lattices. Rückert put forward the first lattice-based blind signature [11] at ASICRYPT'10 in the random oracle model. His signature protocol had 4 moves, and would fail with certain probability during generating signatures. Afterwards, Wang et al. constructed a lattice-based blind signature with random oracle [12] of 2 moves from pre-image sample function without failures in the signing procedure.

To simplify the key management procedures in certificate-based public key settings, the first identity-based signature was introduced by Shamir [13] in 1985. In an identity-based cryptosystem, the public key is the unique string that recognizes the user's identity, for instance, it can be an ID number, the email address, or the room number. A trusted-third-party generates the secret key by a specific algorithm and a private key. By identity-based cryptosystems, the existing problems in the public key infrastructure (PKI) can be well resolved, such as the public-key substitute problems, and the performance bottleneck of authentication center problems.

However, few literature studies on lattice-based IBBS, much less without random oracle. An interesting research topic is the design of lattice-based IBBS without random oracle. Therefore, we initiate the research on IBBS from lattices without random oracle in this research. A lattice-based IBBS scheme without random oracle is constructed based on hard worst-case lattice problems. Our construction is proved to be unconditionally blind and one-more sID-CMA unforgeable in the standard model (SM).

1.2 Related Works

Early IBBS schemes appeared in [14, 15] were designed with random oracles. The first secure construction of IBBS scheme in the standard model was constructed from the generic approach proposed by Galindo et al. [16] at ASIACRYPT 2006. The main approach was considerably straightforward and obvious: adding the authentication information of the signer to the general signature. But this led some disadvantages: the signature size was large because it includes two parts, and their scheme was inefficient as the computation and the verification needed double operations. Phong et al. [17] constructed an IBBS scheme based on bilinear parings with security based on the elliptic curve discrete logarithm problem.

All IBBS schemes were constructed based on classical number theories such as the integer factoring problem and the discrete logarithm problem, until Rückert made the first step in designing lattice-based blind signatures [11] at ASICRYPT 2010. But his schemes would fail with certain probability during generating signatures. Wang et al. [12]

put forward a lattice-based blind signature with random oracle of 2 moves from pre-image sample function without failures in the signing procedure. To the best of our knowledge, no literature studies on lattice-based IBBS scheme in standard model so far.

2 Preliminaries

2.1 Notations

$\mathbb{R}(\mathbb{Z})$ denotes the set of real numbers (integers). For a positive integer $d \in \mathbb{Z}$, $[d]$ denotes the set of integers $\{1, \cdots, d\}$. Vectors are denoted by bold lower-case letters in column form and matrices by bold capital letters. The l_2 and l_∞ norm are denoted by $||\cdot||$ and $||\cdot||_\infty$, respectively. A matrix $\mathbf{A} \in \mathbb{R}^{n\times m}$ is always viewed as the set of its column vectors $\mathbf{A}=\{\mathbf{a}_1, \cdots, \mathbf{a}_m\}$, and $\tilde{\mathbf{A}}=\{\tilde{\mathbf{a}}_1, \cdots, \tilde{\mathbf{a}}_m\}$ denotes the Gram-Schmidt orthogonalization of vectors $\mathbf{a}_1, \cdots, \mathbf{a}_m$ taken in that order. For matrix $\mathbf{B} \in \mathbb{R}^{n\times m'}$, the connection by columns of $\mathbf{A}$ and $\mathbf{B}$ is written as $[\mathbf{A}||\mathbf{B}] \in \mathbb{R}^{n\times(m+m')}$.

Let n be the security parameter, other quantities can be expressed by the functions of n. log denotes the natural logarithm, and $\Delta(X, Y) = \frac{1}{2}\sum_{a\in D} |Pr[X = a] - \Pr[Y = a]|$ defines the statistical distance of two random variables (X and Y) over a domain D. The notations of O, ω are frequently used for describing the growth of function. For some constant c, $f(n) = \tilde{O}(g(n))$ denotes the function $f(n) = O(g(n) \cdot log^c(n))$ is denoted by $f(n) = \tilde{O}(g(n))$ and $f(n) = O(n^c)$ by $poly(n)$. A function is negligible in n if $f(n) = n^{-c}$ holds for sufficiently large n and positive c. An arbitrary such function is denoted by $negl(n)$, and a probability is overwhelming if it is $1 - negl(n)$.

2.2 Definitions

Definition 1(Lattices). Let $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ be set of n linearly independent vectors over $\mathbb{R}^m$. The lattice generated by $\mathbf{B}$ is defined by

$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i | x_i \in \mathbb{Z} \right\}.$$

Generally, $\lambda_1(\mathcal{L}(\mathbf{B}))$ denotes the shortest vector of the lattice $\mathcal{L}(\mathbf{B})$. For $i \in \{1, \cdots, n\}$, we denote the successive minima by $\lambda_i(\mathcal{L})$, which is the smallest value such that the sphere of radius $\lambda_i(\mathcal{L})$ of center the origin contains at least i linearly independent lattice vectors.

Definition 2 ($\mathbf{SIS}_{q,n,m,\beta}$ problem). Given a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a non-zero vector $\mathbf{v} \in \mathbb{Z}^m$ such that $\mathbf{Av} = \mathbf{0} \in \mathbb{Z}_q^n$ and $||\mathbf{v}|| \leq \beta$.

2.3 Discrete Gaussian Distribution and Smoothing Parameter

Discrete Gaussian distribution and the smoothing parameter are important tools in analyzing integer lattices. For arbitrary $s > 0$, a Gaussian distribution with parameter s and c as its center is defined as $\forall x \in \mathbb{R}^n,\ \rho_{s,c}(x) = \mathbf{e}^{-x||x-c||/s^2}$. The Gaussian distribution on lattice Λ is defined as $\forall x \in \Lambda,\ D_{\Lambda,s,c} = \rho_{s,c}(x)/\rho_{s,c}(\Lambda)$.

Theorem 1 ([7]). Given a trapdoor $\boldsymbol{T}$ for a lattice with dimension n, center $c \in \mathbb{R}^n$ and parameter $s \geq ||\tilde{\mathbf{T}}||\omega(\sqrt{\log n})$, there exists a probabilistic polynomial-time algorithm, whose outputs statistically close to the distribution $D_{\Lambda,s,c}$.

Theorem 2 ([7]). If the rows of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ generate the space $\mathbb{Z}_q^n$ with $m \geq 2n$, $\varepsilon \in (0, 1/2)$, and $s \geq \eta_\varepsilon\left(\Lambda^{\perp}(\mathrm{A})\right)$, $\mathbf{u} = \mathbf{Ae} mod q$ statistically close to the uniform distribution over $\mathbb{Z}_q^n$ when $\mathbf{e} \sim D_{\mathbb{Z}^m,s}$.

2.4 Identity-Based Blind Signature

Syntax of IBBS. An IBBS scheme always consists of four algorithms (**Setup**, **KeyExtract**, **Sign**, **Verify**), where *Sign* is an interactive protocol between a signer S and a user U.

Setup. The KGC runs this algorithm to generate the security parameter and the master key pair (*mpk*, *msk*).

KeyExtract. Given the identity information *ID*, (*mpk*, *msk*), this algorithm generates the corresponding private key sk_{ID} for *ID*.

Sign. This algorithm describes the joint execution between S and U, it always consists of three algorithms.

Blinding the message (executed by U): Takes the original message m and a randomness r as inputs, and outputs a blinded message m';

Signing the blinded message (executed by S): Takes the blinded message m' and the secret signing key sk as inputs, outputs a blinded signature σ';

Unblind the signature (executed by U): Takes the blinded signature σ', and the previous randomness r as inputs, this algorithm outputs the real signature for message m'.

Verify. Given m, *mpk*, *ID*, and σ, this algorithm outputs 1 to accept if σ is a valid signature of m under *ID* and otherwise 0 to reject.

Security Requirements for IBBS. *Blindness.* Assume that (μ_0, σ_0') and (μ_0, σ_0') are two blinded message/signature pairs. Given μ_b, $\sigma_b^{'}$ where $b \in \{0, 1\}$, an IBBS scheme meets the blindness if, any polynomial-time signer or distinguisher can output a bit $b' = b$ with a probability at most $1/2 + 1/n^c$, where n is enough large, and c is a constant. That is, $(\mu_0, \sigma_0^{'})$ and $(\mu_0, \sigma_0^{'})$ is indistinguishable for the signer and distinguisher.

One more unforgeable under sID-CMA. An IBBS scheme is sID-CMA one more unforgeable, if any polynomial-time adversary wins the following game with negligible probability of success.

Setup. The adversary claims the challenge ID^* in advance. Then, the challenger generates the security parameter and the master key pair (*mpk*, *msk*), and sends the *mpk* to the adversary with *msk* as his secret key.

Queries. The adversary is allowed to make two kinds of queries to the challenger.

Key-extract query. The adversary can query on any *ID* except ID^*. The challenger runs algorithm *KeyExtract* to return the corresponding sk_{ID}.
Signing query. The adversary adaptively chooses message m and *ID*, and gets the blinded signature σ' of the blinded message m' under *ID*.

Forge. After l key-extract and signing queries, the adversary outputs a bind signature σ^* of the l+1-th message m^* under ID^*. The adversary wins if the verifier outputs 1 when it checks the forgery (m^*,σ^*).

2.5 Key Algorithms

Algorithms TrapGen and SamplePre. Let $q = poly(n)$ be a prime, m be an arbitrary positive integer that $m > 5n \log q$.

With a security parameter n as input, algorithm **TrapGen** outputs the matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{B} \in \mathbb{Z}^{m\times m}$. Here $\mathbf{B}$ is a good basis of lattice $\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{v} \in \mathbb{Z}^m : \mathbf{Av} = \mathbf{0} \bmod q\}$, and $||\tilde{\mathbf{B}}|| \le O(\sqrt{n \log q})$.

With $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{B} \in \mathbb{Z}^{m\times m}$, any $\sigma \ge ||\tilde{\mathbf{B}}|| \cdot \omega(\sqrt{\log n})$ and vector $\mathbf{y} \in \mathbb{Z}_q^n$ as inputs, algorithm **SamplePre** outputs a randomly nonzero vector $\mathbf{e} \in \{\mathbf{e} \in \mathbb{Z}^m : ||\mathbf{e}|| \le \sigma\sqrt{m}\}$ such that $\mathbf{Ae} = \mathbf{y} \bmod q$ with overwhelming probability.

Algorithms ExtBasis, RandBasis and ExtRandBasis. Let $\mathbf{T} \in \mathbb{Z}^{m\times m}$ be an arbitrary basis of $\Lambda^{\perp}(\mathbf{A})$ for some $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ whose columns generate the entire group $\mathbb{Z}_q^n$, and let $\bar{\mathbf{A}} \in \mathbb{Z}_q^{n\times \bar{m}}$ be arbitrary.

There is a deterministic polynomial-time algorithm **ExtBasis**$(\mathbf{T}, \mathbf{A}' = \mathbf{A}||\bar{\mathbf{A}})$ that outputs a basis **T**' of $\Lambda^{\perp}(\mathbf{A}') \subseteq \mathbb{Z}^{m+\bar{m}}$ such that $||\tilde{\mathbf{T}}'|| = ||\tilde{\mathbf{T}}||$. See Lemma 3 in [5] for more details of **ExtBasis**.

Algorithm **RandBasis** is a probabilistic polynomial-time algorithm, which takes a basis $\mathbf{T}$ of an m-definitional integer lattice Λ and a parameter $s \ge ||\tilde{\mathbf{T}}|| \cdot \omega(\sqrt{\log n})$ as inputs, and outputs a basis **T**' of Λ that $||\tilde{\mathbf{T}}'|| \le s\sqrt{m}$. See Lemma 4 in [5] for more details of **RandBasis**.

Algorithm **ExtRandBasis** can be implemented by algorithm **ExtBasis** and then algorithm **RandBasis.** It is a probabilistic algorithm that inputs an arbitrary basis $\mathbf{T}$ of $\Lambda^{\perp}(\mathbf{A})$ for some $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ whose columns generate the entire group $\mathbb{Z}_q^n$, a parameter

$s \geq ||\tilde{\mathbf{T}}|| \cdot \omega(\sqrt{\log n})$, an arbitrary $\bar{\mathbf{A}} \in \mathbb{Z}_q^{n \times \bar{m}}$, and outputs a basis $\mathbf{T}'$ of $\Lambda^{\perp}(\mathbf{A}' = \mathbf{A}||\bar{\mathbf{A}}) \subseteq \mathbb{Z}^{m+\bar{m}}$ such that $||\tilde{\mathbf{T}}'|| \leq s\sqrt{m}$.

Algorithms SampleLeft and SampleRight. Assume that $\mathbf{A}$, $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$, $\mathbf{R} \in \{-1, 1\}^{m \times m}$, and the matrix $\mathbf{F}$ of form $\mathbf{F} = [\mathbf{A}||\mathbf{AR} + \mathbf{B}] \in \mathbb{Z}_q^{n \times 2m}$, algorithms **SampleLeft** and **SampleRight** can sample short vectors from $\Lambda_q^{\perp}(\mathbf{F})$ for some $\mathbf{u} \in \mathbb{Z}_q^n$ with either a trapdoor for $\Lambda_q^{\perp}(\mathbf{A})$ or a trapdoor for $\Lambda_q^{\perp}(\mathbf{B})$. We describe them briefly as follows, you can refer to [4] for more details.

SampleLeft. Given a rank n matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ with a 'short' basis $\mathbf{T_A}$ for $\Lambda_q^{\perp}(\mathbf{A})$, a matrix $\mathbf{M}_1 \in \mathbb{Z}_q^{n \times m_1}$, a vector $\mathbf{u} \in \mathbb{Z}_q^n$, and a Gaussian parameter $\sigma \geq ||\tilde{\mathbf{T}}_{\mathbf{A}}|| \cdot \omega(\sqrt{\log(m + m_1)})$. The algorithm sets $\mathbf{F}_1 = [\mathbf{A}||\mathbf{M_1}]$, and outputs a vector $\mathbf{e} \in \mathbb{Z}^{m+m_1}$ sampled from a distribution statistically close to $D_{\Lambda_q^u(F_1),\sigma}$. The vector $\mathbf{e}$ is generated as follows:

(a) Sample a random vector $\mathbf{e}_2 \in \mathbb{Z}^{m_1}$ distributed statistically close to $D_{\mathbb{Z}^{m_1},\sigma}$;
(b) Run $\mathbf{e}_1 \leftarrow \mathbf{SamplePre}(\mathbf{A}, \mathbf{T_A}, \mathbf{y}, \sigma)$ where $\mathbf{y} = \mathbf{u} - (\mathbf{M}_1\mathbf{e}_2) \in \mathbb{Z}_q^n$;
(c) Output $\mathbf{e} \leftarrow (\mathbf{e}_1, \mathbf{e}_2) \in \mathbb{Z}^{m+m_1}$.

SampleRight. Given matrices $\mathbf{A} \in \mathbb{Z}_q^{n \times k}$ and $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$ with a basis $\mathbf{T_B}$ for $\Lambda_q^{\perp}(\mathbf{B})$ where $\boldsymbol{B}$ is rank n, a matrix $\mathbf{R} \in \mathbb{Z}^{k \times m}$, $s_{\mathbf{R}} = ||\mathbf{R}|| = \sup_{||\mathbf{x}||=1} ||\mathbf{Rx}||$, a vector $\mathbf{u} \in \mathbb{Z}_q^n$, and a parameter $\sigma \geq ||\tilde{\mathbf{T}}_{\mathbf{B}}|| \cdot s_{\mathbf{R}}\omega(\sqrt{\log m})$, this algorithm sets $\mathbf{F}_2 = [\mathbf{A}||\mathbf{AR} + \mathbf{B}]$ and outputs a vector $\mathbf{e} \in \mathbb{Z}^{m+k}$ sampled from a distribution statistically close to $D_{\Lambda_q^u(\mathbf{F}_2),\sigma}$. The vector $\mathbf{e}$ is generated as follows:

(a) Construct a set $\mathbf{T}_{\mathbf{F}_2}$ of $(m + k)$ linearly independent vectors in $\Lambda_q^{\perp}(\mathbf{F}_2)$ where $||\tilde{\mathbf{T}}_{\mathbf{F}_2}|| < ||\tilde{\mathbf{T}}_{\mathbf{B}}||(s_{\mathbf{R}} + 1)$;
(b) if needed, by Lemma 7.1 in [17] to convert $\mathbf{T}_{\mathbf{F}_2}$ into a basis $\mathbf{T}'_{\mathbf{F}_2}$ of $\Lambda_q^{\perp}(\mathbf{F}_2)$ such that $||\tilde{\mathbf{T}}'_{\mathbf{F}_2}|| = ||\tilde{\mathbf{T}}_{\mathbf{F}_2}||$;
(c) invoke $\mathbf{e} \leftarrow \mathbf{SamplePre}(\mathbf{F}_2, \mathbf{T}'_{\mathbf{F}_2}, \mathbf{u}, \sigma)$ to generate a vector $\mathbf{e} \in \Lambda_q^{\mathbf{u}}(\mathbf{F}_2)$ such that $\mathbf{e}$ is distributed close to $D_{\Lambda_q^u(\mathbf{F}_2),\sigma}$.

3 Our Construction

Assume that n is the system security parameter, other quantities are determined by n. q is a prime positive integer such that $q = poly(n)$, $m = O(2n \log q)$, $L{=}8\sqrt{n \log q}$, $s' > L\omega(\sqrt{\log n})$.

Setup. Assume that the key generation center (KGC) has an n-dimensional lattice Λ with a trapdoor basis $\mathbf{B}$, we denote the check matrix of Λ by $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, and the

Gram-Schmidt orthogonal basis of $\mathbf{B}$ by $\tilde{\mathbf{B}}$. The smooth parameter of Λ is denoted as $\eta_{\varepsilon}(\Lambda)$. Set $s = ||\tilde{\mathbf{B}}||s'$, and $d = ||\tilde{\mathbf{B}}||/2$, L_M is the database of all signed blinded messages. The identity information of a signer is defined by $id \in \{0,1\}^k$, $H : \{0,1\}^k \to \mathbb{Z}_q^n$ and $H_0 : \{0,1\}^* \to \mathbb{Z}_q^n$ are secure collision-resistant hash functions, and $H_1 : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n\times n}$ is an encoding with full-rank differences (FRD) function. The output of H is denoted as $\mathbf{v}_{id}$=$H(id) \in \mathbb{Z}_q^n$. The message is in $\{0,1\}^*$. The KGC operates as follows:

(a) Pick matrixes $\mathbf{C}_0, \mathbf{C}_1, \cdots, \mathbf{C}_k \in \mathbb{Z}_q^{n\times m}$.
(b) Uniformly choose random $\mathbf{A}_2$, $\mathbf{A}_3$ from $\mathbb{Z}_q^{n\times m}$.
(c) Output the system public parameters as $P = \{n, m, q, s', s, H, H_0, H_1\}$, the master secret key as $msk = \{\mathbf{B}\}$, and the master public key as $mpk = \{\mathbf{A}, \mathbf{A}_2, \mathbf{A}_3, \mathbf{C}_0, \cdots, \mathbf{C}_k\}$.

KeyExtract(*id***,** *P***,** *msk***,** *mpk***).** Take an identity *id* as input, the PKG generates the secret key for the identity as follows:

(a) Compute $\mathbf{A}_{id} = [\mathbf{A}||\mathbf{A}_2 + H_1(\mathbf{v}_{id})\mathbf{A}_3]$ where $H_1(\mathbf{v}_{id}) \in \mathbb{Z}_q^{n\times n}$;
(b) Extract a short basis $\mathbf{T}_{id} \leftarrow \mathbf{ExtRandBasis}(\mathbf{B}, \mathbf{A}||\mathbf{A}_2 + H_1(\mathbf{v}_{id}), s')$ as the secret key for identity *id*, where $s' \geq max\{||\tilde{\mathbf{T}}_{id}||\omega(\sqrt{\log n})\}_{id\in\{0,1\}^k}$.

Figure 1 shows the key procedure of the IBBS scheme, the signature issue protocol. It has two moves between the signer and the user, and consists of three algorithms (**Blind**, **Sign**, **Unblind**).

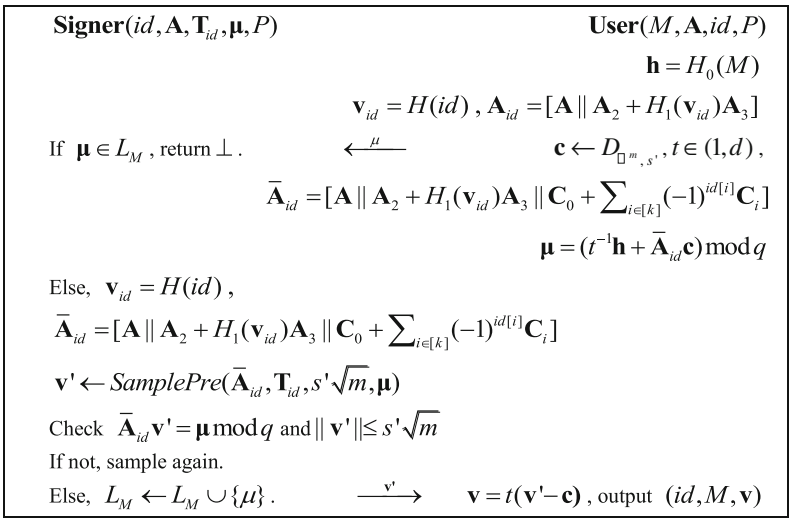

Fig. 1. Signature issue protocol of the IBBS scheme

Blind(M, P, mpk, id)**.** Take the message $M \in \{0,1\}^*$ and the public parameters as inputs, the user blinds the message as follows:

(a) Compute $\mathbf{h} = H_0(M) \in \mathbb{Z}_q^n$, and $\mathbf{A}_{id} = [\mathbf{A}||\mathbf{A}_2 + H_1(\mathbf{v}_{id})\mathbf{A}_3]$ where $\mathbf{v}_{id}$=$H(id) \in \mathbb{Z}_q^n$;
(b) Choose a random vector $\mathbf{c} = (c_1, c_2, \cdots, c_{3m}) \rightarrow D_{\mathbb{Z}^{3m}, s'}$ with the origin as its center, then $||c|| \leq s'\sqrt{3m}$ holds with overwhelming probability from Theorem 2. If not, repeat it.
(c) Compute $\bar{\mathbf{A}}_{id} = [\mathbf{A}||\mathbf{A}_2 + H_1(\mathbf{v}_{id})\mathbf{A}_3||\mathbf{C}_0 + \sum_{i\in[k]}(-1)^{id[i]}\mathbf{C}_i]$ for $id = (id[1], \cdots, id[k]) \in \{0,1\}^k$.
(d) From Theorem 2, $\bar{\mathbf{A}}_{id}\mathbf{c}$ is approximate uniform.
(e) Choose an arbitrary $t \in \mathbb{Z}_q$ such that $1 < t < d$.
(f) Compute the blinded message $\boldsymbol{\mu} = (t^{-1}\mathbf{h} + \bar{\mathbf{A}}_{id}\mathbf{c}) \bmod q$.

Finally, the user sends $\boldsymbol{\mu}$ to the signer with identity id.

Sign($\boldsymbol{\mu}$,$\mathbf{T}_{id}$,P, mpk, L_M)**.** The signer with identity id signs the blinded message $\boldsymbol{\mu}$ as follows:

(a) Search $\boldsymbol{\mu}$ in L_M, if $\boldsymbol{\mu} \in L_M$, output $\perp$; if not, go to **step 2**.
(b) For $id = (id[1], \cdots, id[k]) \in \{0,1\}^k$, compute $\bar{\mathbf{A}}_{id} = [\mathbf{A}||\mathbf{A}_2 + H_1(\mathbf{v}_{id})\mathbf{A}_3||\mathbf{C}_0 + \sum_{i\in[k]}(-1)^{id[i]}\mathbf{C}_i]$.
(c) Extract a basis $\bar{\mathbf{T}}_{id} \leftarrow ExtBasis(\bar{\mathbf{A}}_{id}, \mathbf{T}_{id}, s)$.
(d) Run $\mathbf{v}' \leftarrow SamplePre(\bar{\mathbf{A}}_{id}, \bar{\mathbf{T}}_{id}, s', \boldsymbol{\mu})$ to generate $\mathbf{v}\ '$, then check if $\bar{\mathbf{A}}_{id}\mathbf{v}' = \boldsymbol{\mu} \bmod q$, and $||\mathbf{v}'|| \leq s'\sqrt{3m}$. If not, repeat it.
(e) Add $\boldsymbol{\mu}$ into L_M.

Finally, the signer id outputs $\mathbf{v}\ '$ as his signature of the blinded message $\boldsymbol{\mu}$.

Unblind(P, mpk, $\mathbf{v}\ '$, $\mathbf{c}$, t, id)**.** Upon receiving the signature $\boldsymbol{v}\ '$, the user computes $\mathbf{v} = t(\mathbf{v}' - \mathbf{c})$ as the signature of message M signed by the signer with id.

Verify (P, mpk, id, M, $\mathbf{v}$)**.** The verifier computes $\bar{\mathbf{A}}_{id} = [\mathbf{A}||\mathbf{A}_2 + H_1(\mathbf{v}_{id})\mathbf{A}_3||\mathbf{C}_0 + \sum_{i\in[k]}(-1)^{id[i]}\mathbf{C}_i]$ and $\mathbf{h} = H_0(M)$, and then checks that: (1). $\bar{\mathbf{A}}_{id}\mathbf{v} = \mathbf{h} \bmod q$; (2). $||\mathbf{v}|| \leq s\sqrt{3m}$. The verifier outputs 1 if both the two conditions are satisfied, else output 0.

Correctness. As n is the security parameter, other parameters in the scheme allow the algorithms **SamplePre** and **ExtRandBasis** to operate correctly. In particular, the PKG can generate a trapdoor basis for larger dimension lattice $\Lambda_q^{\perp}(\bar{\mathbf{A}}_{id})$ as it has the trapdoor basis of $\Lambda_q^{\perp}(\mathbf{A})$. The signer can generate a short random vector for lattice $\Lambda_q^{\perp}(\bar{\mathbf{A}}_{id})$ with the trapdoor basis $\mathbf{T}_{id}$ as his secret key. Besides, $\mathbf{v}'$ is the output of algorithm *SamplePre*, $\bar{\mathbf{A}}_{id}\mathbf{v}' = \boldsymbol{\mu} \bmod q$ and$||\mathbf{v}'|| \leq s'\sqrt{m}$ holds with overwhelming probability. So we have $\bar{\mathbf{A}}_{id}\mathbf{v}' = \boldsymbol{\mu} = t^{-1}\mathbf{h} + \mathbf{A}_{id}\mathbf{c}$, $t\bar{\mathbf{A}}_{id}\mathbf{v}' = \mathbf{h} + t\mathbf{A}_{id}\mathbf{c}$, $\bar{\mathbf{A}}_{id}t(\mathbf{v}' - \mathbf{c}) = \mathbf{h}$, and $\bar{\mathbf{A}}_{id}\mathbf{v} = \mathbf{h}$.

On the other hand, we have $||\mathbf{v}|| = t||(\mathbf{v}' - \mathbf{c})|| \leq ||\tilde{\mathbf{B}}||/2 \cdot 2s'\sqrt{3m} = s\sqrt{3m}$. Therefore, an honestly created signature will be accepted with overwhelming probability.

4 Security Analysis

In this section, we prove that our scheme is unconditionally blind, and one-more unforgeable under selective identity and chosen message attacks (sID-CMA) in the standard model.

Theorem 3 (Blindness). Our IBBS scheme is unconditionally blind.

Proof. From Theorem 2, $\bar{\mathbf{A}}_{id}\mathbf{c}$ is uniformly distributed. As the output of H_0 is approximate uniform, and t is randomly chosen, the blinded message $\boldsymbol{\mu} = (t^{-1}\mathbf{h} + \bar{\mathbf{A}}_{id}\mathbf{c}) \bmod q$ is indistinguishable from a uniform distribution over $\mathbb{Z}_q^n$. The signer chooses a random vector over $\mathbb{Z}_q^n$ and a random integer $t < d$, and then tries to recover the hash value of the real message from $t\boldsymbol{\mu} = \mathbf{h} + \bar{\mathbf{A}}_{id}\mathbf{c}$. Next, we show that the statistical distance of the resulting distribution of the signer is 0 from the uniform distribution, that is,

$$\begin{aligned}\Delta(t(\boldsymbol{\mu} - \mathbf{c}), \mathbf{h}) &= \frac{1}{2}\sum\nolimits_{\mathbf{h}\in\mathbb{Z}_q^n, \mathbf{c}_1\in\mathbb{Z}_q^m,\ t_1\in\mathbb{Z},\ t_1<||\tilde{\mathbf{B}}||/2} |\Pr[t_1(\boldsymbol{\mu} - \bar{\mathbf{A}}_{id}\mathbf{c}_1) = \mathbf{h})] - Pr[H_0(M) = \mathbf{h}]| \\ &= \frac{1}{2}\sum\nolimits_{\mathbf{h}\in\mathbb{Z}_q^n, \mathbf{c}_1\in\mathbb{Z}_q^m,\ t_1\in\mathbb{Z},\ t_1<||\tilde{\mathbf{B}}||/2} [(\frac{1}{q})^n - (\frac{1}{q})^n] \ = 0\end{aligned} \tag{1}$$

Therefore, they are indistinguishable, and our scheme is unconditionally blind.

Theorem 4 (One-more unforgeability against sID-CMA). Assume that the $SIS_{m,q,s\sqrt{m}}$ problem is hard, our IBBS scheme is one-more unforgeable against sID-CMA in the standard model.

Proof. Assume that there is a successful adversary $\mathcal{A}$ with the advantage of ε breaks one-more unforgeability of the proposed scheme, we can construct an algorithm $\mathcal{B}$ to solve the instance of the $SIS_{m,q,2s\sqrt{3m}}$ problem by employing $\mathcal{A}$ to be a subroutine.

Suppose that we get an instance of $SIS_{n,q,m,s\sqrt{m}} = (\hat{\mathbf{A}}, n, m, q, l, s)$, where $\hat{\mathbf{A}} \in \mathbb{Z}_q^{n\times m}$, l is the total query number that the adversary can make at most in the interactive game. Our goal is to find a vector such that $\hat{\mathbf{A}}\mathbf{e} = \mathbf{0} \bmod q$ and $||\mathbf{e}|| \leq s\sqrt{m}$. The adversary outputs a challenge identity $id^* = (id^*[1], \cdots, id^*[k])$. Next, we simulate the circumstance to interact with $\mathcal{A}$, and solve the given instance using $\mathcal{A}$.

Setup. Assume that we receives the instance $\hat{\mathbf{A}} \in \mathbb{Z}_q^{n\times m}$. The system parameters are set as our scheme, we generate the public key $mpk = \{\mathbf{A}, \mathbf{A}_2, \mathbf{A}_3, \mathbf{C}_0, \cdots, \mathbf{C}_k\}$ as follows:

(a) Compute $(\mathbf{A}_3, \mathbf{T}) \leftarrow TrapGen(n, m, q)$, and then randomly choose $\mathbf{R}^* \in \{-1, 1\}^{m\times m}$.
(b) Set $\mathbf{A} = \hat{\mathbf{A}}$, and $\mathbf{A}_2 = \mathbf{A}\mathbf{R}^* - H_1(id^*)\mathbf{A}_3$.

(c) Run the trapdoor sampling algorithm to generate a random lattice $\Lambda_q^{\perp}(\mathbf{S}_0)$ with $\mathbf{S}_0 \in \mathbb{Z}_q^{n\times m}$ and its corresponding trapdoor basis $\mathbf{T}_0 \in \mathbb{Z}_q^{m\times m}$.
(d) Pick k short random matrices $\mathbf{R}_0, \mathbf{R}_1, \cdots, \mathbf{R}_k \in \mathbb{Z}^{m\times m}$. Fix $w_0 = 1 \in \mathbb{Z}_q$, uniformly pick random scalars $w_1, \cdots, w_k \in \mathbb{Z}_q$.
(e) Set $\mathbf{R}_{id_j} = \mathbf{R}_0 + \sum_{i\in[k]} (-1)^{id_j[i]}\mathbf{R}_i \in \mathbb{Z}^{m\times m}$, $w_{id_j} = 1 + \sum_{i\in[k]} (-1)^{id_j[i]} w_i \in \mathbb{Z}_q$.
(f) Send the public key $\{\mathbf{A}, \mathbf{A}_2, \mathbf{A}_3, \mathbf{C}_0, \cdots, \mathbf{C}_k\}$ to $\mathcal{A}$, where $\mathbf{C}_i = \mathbf{A}\mathbf{R}_i + w_i\mathbf{S}_0$ for $i = 0, 1, \cdots, k$.

$\mathcal{B}$ maintains two lists to store the extraction queries and the signing queries.

Extraction queries. For a fresh identity $id_j \neq id^*$, $j \in [l]$, $\mathcal{B}$ first computes $\mathbf{A}_{id_j} = [\mathbf{A}||\mathbf{A}_2 + H_1(\mathbf{v}_{id_j})\mathbf{A}_3] = [\mathbf{A}||\mathbf{A}\mathbf{R}^* + [H_1(\mathbf{v}_{id_j}) - H_1(\mathbf{v}_{id^*})]\mathbf{A}_3]$. By construction, we know that $[H_1(\mathbf{v}_{id_j}) - H_1(\mathbf{v}_{id^*})]$ is non-singular and therefore $\mathbf{T}$ is also a trapdoor for $\Lambda_q^{\perp}([H_1(\mathbf{v}_{id_j}) - H_1(\mathbf{v}_{id^*})]\mathbf{A}_3)$. Using the trapdoor basis $\mathbf{T}$, $\mathcal{B}$ first generates a random trapdoor basis $\mathbf{T}_{id_j}$ for $\Lambda_q^{\perp}(\mathbf{A}_{id_j})$, then adds ($id_j$, $\mathbf{T}_{id_j}$) into list L_1, and finally sends it to $\mathcal{A}$ as the response. If $\mathcal{A}$ sends an old identity id that has been queried before, $\mathcal{B}$ searches $(id_j, \mathbf{T}_{id_j})$ in L_1, and answers with $\mathbf{T}_{id_j}$.

Signing queries. On inputs a blinded message $\boldsymbol{\mu}_j$ and an identity id_j for $j \in [l]$, algorithm $\mathcal{B}$ computes $\bar{\mathbf{A}}_{id_j} = [\mathbf{A}||\mathbf{A}\mathbf{R}^* + [H_1(\mathbf{v}_{id_j}) - H_1(\mathbf{v}_{id^*})]\mathbf{A}_3||\mathbf{C}_0 + \sum_{i\in[k]} (-1)^{id_j[i]}\mathbf{C}_i]$, where $H_1(\mathbf{v}_{id_j}) \in \mathbb{Z}_q^{n\times n}$ and answers in two cases:

Case 1. $id_j \neq id^*$. $\mathcal{B}$ searches $(\boldsymbol{\mu}_j, id_j, \mathbf{v}_j')$ in L_2. If it exists, $\mathcal{B}$ returns $\mathbf{v}_j\prime$. Otherwise, using $\mathbf{T}$ and the **SampleRight** algorithm, $\mathcal{B}$ first generates the trapdoor $\mathbf{T}_{id_j}$for $\mathbf{F}_{id_j} = [\mathbf{A}||\mathbf{A}\mathbf{R}^* + [H_1(\mathbf{v}_{id_j}) - H_1(\mathbf{v}_{id^*})]\mathbf{A}_3]$, and then computes a random trapdoor $\bar{\mathbf{T}}_{id_j}$ for $\Lambda_q^{\perp}(\mathbf{F}_{id_j})$. With the trapdoor $\bar{\mathbf{T}}_{id_j}$and the **SampleLeft** algorithm, $\mathcal{B}$ generates $\mathbf{v}_j' \leftarrow SamplePre(\bar{\mathbf{A}}_{id_j}, \bar{\mathbf{T}}_{id_j}, \boldsymbol{\mu}_j, s)$as a signature. Finally, $\mathcal{B}$ adds $(\boldsymbol{\mu}_j, id_j, \mathbf{v}_j')$ into L_2 and returns $\mathbf{v}_j\prime$ as his response. $\mathcal{A}$ decodes (unblinds) $\mathbf{v}_j\prime$ to obtain the real signature.

Case 2. $id_j = id^*$. $\mathcal{B}$ searches $(\boldsymbol{\mu}_j, id_j, \mathbf{v}_j')$ in L_2. If it exists, $\mathcal{B}$ returns $\mathbf{v}_j\prime$. Otherwise, using $\mathbf{T}_0$ and the **SampleRight** algorithm, $\mathcal{B}$ constructs the matrix $\mathbf{F}'_{id^*} = [\mathbf{A}||\mathbf{A}\mathbf{R}_{id^*} + w_{id^*}\mathbf{S}_0]$ and generates a random trapdoor $\mathbf{T}_{id^*}$ for $\Lambda_q^{\perp}(\mathbf{F}'_{id^*})$. Then, with the trapdoor $\mathbf{T}_{id^*}$ and the **SampleLeft** algorithm, $\mathcal{B}$ generates a random trapdoor $\bar{\mathbf{T}}_{id^*}$ for $\Lambda_q^{\perp}(\mathbf{F}_{id_j})$, where $\mathbf{F}_{id^*} = [\mathbf{F}'_{id^*}||\mathbf{A}\mathbf{R}^*] = [\mathbf{A}||\mathbf{A}\mathbf{R}_{id^*} + w_{id^*}\mathbf{S}_0||\mathbf{A}\mathbf{R}^*] \in \mathbb{Z}_q^{n\times 3m}$. $\mathcal{B}$ obtains a short random $\bar{\mathbf{v}}_*' \in \Lambda_q^{\perp}(\mathbf{F}_{id^*})$ with $||\bar{\mathbf{v}}_{l+1}^{*\prime}|| \leq s\sqrt{3m}$ by using the trapdoor $\bar{\mathbf{T}}_{id^*}$and the **SamplePre** algorithm. Finally, $\mathcal{B}$ changes the order of the corresponding vectors of $\bar{\mathbf{v}}_*'$ to get a short random trapdoor $\tilde{\mathbf{v}}_*' \in \Lambda_q^{\perp}(\tilde{\mathbf{A}}_{id^*})$ for $\tilde{\mathbf{A}}_{id^*} = [\mathbf{A}||\mathbf{A}\mathbf{R}^*||\mathbf{A}\mathbf{R}_{id^*} + w_{id^*}\mathbf{S}_0]$. As $\mathbf{C}_0 + \sum_{i\in[k]} (-1)^{id_j[i]}\mathbf{C}_i = \mathbf{R}_{id} + w_{id}\mathbf{S}_0$ and $\bar{\mathbf{A}}_{id^*} = [\mathbf{A}||\mathbf{A}\mathbf{R}^* + [H_1(\mathbf{v}_{id_j}) - H_1(\mathbf{v}_{id*})]\mathbf{A}_3||$ $\mathbf{C}_0 + \sum_{i\in[k]} (-1)^{id_j[i]}\mathbf{C}_i]$, we have $\bar{\mathbf{A}}_{id^*} = \tilde{\mathbf{A}}_{id^*}$. So $\tilde{\mathbf{v}}_*'$ is also a short random vector in $\Lambda_q^{\perp}(\bar{\mathbf{A}}_{id^*})$ such that $||\tilde{\mathbf{v}}_{l+1}^{*\prime}|| \leq s\sqrt{3m}$. Finally, $\mathcal{B}$ adds $(\boldsymbol{\mu}_j, id^*, \tilde{\mathbf{v}}_*')$ into L_2 and sends as his response. $\mathcal{A}$ decodes (unblinds) $\tilde{\mathbf{v}}_*'$ to obtain the real signature.

Challenge. After receiving l message-signature pairs, $\mathcal{A}$ outputs the l+1-th valid forgery ($\boldsymbol{\mu}^*_{l+1}$,id^*,$\mathbf{v}'^*_{l+1}$), such that $\bar{\mathbf{A}}_{id^*}\mathbf{v}'^*_{l+1} = \boldsymbol{\mu}^*_{l+1}$ and $||\mathbf{v}'^*_{l+1}|| \leq s\sqrt{3m}$. $\mathcal{B}$ checks that $\boldsymbol{\mu}^*_{l+1} \neq \boldsymbol{\mu}_j$ for $j = 1, \cdots, l$, that is, $\boldsymbol{\mu}^*_{l+1}$ of a fresh message. Then, $\mathcal{B}$ generates a signature $\bar{\mathbf{v}}'^*$ for the blinded message $\boldsymbol{\mu}^*_{l+1}$ as in the signing queries, where $\bar{\mathbf{A}}_{id^*}\bar{\mathbf{v}}'^* = \boldsymbol{\mu}^*_{l+1}$ and $||\bar{\mathbf{v}}'^*|| \leq s\sqrt{3m}$. If $\bar{\mathbf{v}}'^* = \mathbf{v}'^*_{l+1}$, $\mathcal{B}$ aborts (with negligible probability). Otherwise, $\mathcal{B}$ operates as follows:

(a) Compute $\mathbf{R}_{id^*} = \mathbf{R}_0 + \sum_{i\in[k]} (-1)^{id^*[i]}\mathbf{R}_i \in \mathbb{Z}^{m\times m}$ and $w_{id^*} = 1 + \sum_{i\in[k]} (-1)^{id^*[i]} w_i \in \mathbb{Z}_q$.
(b) If $w_{id^*} \neq 0 \bmod q$, abort the simulation (with a probability of about $1 - \frac{1}{q}$).
(c) Compute $\mathbf{e} = |\bar{\mathbf{v}}'^* - \mathbf{v}'^*_{l+1}|$, and parse $\mathbf{e} = (\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)^t$, where $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3 \in \mathbb{Z}^m$.
(d) Return $\mathbf{e}^* = \mathbf{e}_1 + \mathbf{R}^*\mathbf{e}_2 + \mathbf{R}_{id^*}\mathbf{e}_3 \in \mathbb{Z}^m$.

We show the success probability of $\mathcal{B}$ in solving $SIS_{m,n,q,2s\sqrt{3m}}$. From the above analysis, $\mathbf{R}_{id^*} = \mathbf{R}_0 + \sum_{i\in[k]} (-1)^{id^*[i]}\mathbf{R}_i \in \mathbb{Z}^{m\times m}$, and $w_{id^*} = 1 + \sum_{i\in[k]} (-1)^{id^*[i]} w_i \in \mathbb{Z}_q$, we have $\bar{\mathbf{A}}_{id^*}(|\mathbf{v}'^* - \mathbf{v}'^*_{l+1}|) = [\mathbf{A}||\mathbf{A}\mathbf{R}^*||\mathbf{A}\mathbf{R}_{id^*} + w_{id^*}\mathbf{S}_0]\mathbf{e} = \mathbf{0}$. If $w_{id^*} = 0 \bmod q$, we have $[\mathbf{A}||\mathbf{A}\mathbf{R}^*||\mathbf{A}\mathbf{R}_{id^*}](\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)^t = \mathbf{0} \bmod q$, that is, $[\mathbf{A}||\mathbf{A}||\mathbf{A}](\mathbf{e}_1, \mathbf{R}^*\mathbf{e}_2, \mathbf{R}_{id^*}\mathbf{e}_3)^t = \mathbf{0} \bmod q$. By the similar method as in Lemma 26 in [6], it can be obtained that $\mathbf{e}^*$ is a short non-zero vector as a solution to the given SIS instance with high probability. The probability of an abort in the above simulation is about $(1 - \frac{1}{q})$. The view of $\mathcal{A}$ in the game is identical to its view as provided by $\mathcal{B}$. Therefore, $\mathcal{B}$ can solve the SIS problem with probability at least $\frac{1}{q}\varepsilon$.

Table 1. Comparison of the related blind signature schemes

Schemes	[11]	[12]	Sect. 6
Moves number	4	2	2
Signature size	$O(n\log q)$	$O(n\log q)$	$O(n\log q)$
Without failure	×	✓	✓
ID-based	×	×	✓
Security model	ROM	ROM	**SM**

Table 2. Bit length of concrete instances

Instances	1	2	3	4	5
n	284	284	284	284	284
q	2^{16}	2^{20}	2^{24}	2^{27}	2^{30}
m	9088	11360	13632	15336	17040
L	539	603	660	701	738
Secret key	$135s'$	$151s'$	$165s'$	$175s'$	$185s'$
Public key	$4.1k' \times 10^7$	$6.5k' \times 10^7$	$9.3k' \times 10^7$	$1.2k' \times 10^8$	$1.5k' \times 10^8$
Signature	$165s'$	$185s'$	$202s'$	$214s'$	$226s'$

5 Conclusions

Table 1 lists the comparison with the existing lattice-based schemes [11, 12], in terms of the interactive move numbers, failures in generating signatures, ID-based system, and security models. Here, the move number denotes the number of interactive moves in the issue protocol of the blind signature, without failure means there is no failures occur in the blind signing procedures. We use "ID-based" to denote if that scheme meets the requirement of identity-based cryptosystems, and "the security model" is to show the security model of that scheme, that is, in the random oracle model (ROM) or standard model (SM).

Many researchers still wonder whether a secure scheme constructed in the random oracle model keeps their security in practice, because the random oracles are replaced by hash functions when implemented. The highlight of our construction is that, it is designed without random oracle, while other schemes are constructed in the random oracle model.

Moreover, Table 2 shows the bit length of concrete instances of our scheme. During the experiments, we set $m = 2n \log q$ and $L = 8\sqrt{n \log q}$. s' is the smooth parameter that $s' > L\omega(\sqrt{\log n})$ with $L{=}8\sqrt{n \log q}$, $k'{=}k{+}4$ where k denotes the bit size of the identity. The secret key, public key, and signature sizes are tolerable when parameters are suitable set.

Comparing with the schemes designed in the random oracle model, the ones constructed without random oracles are much convincing in security and practical in engineering. From the above description, our construction has three additional advantages:

1. Similar to the scheme in [12], our scheme has 2 moves.
2. Our scheme has no failures in generating blind signatures.
3. Only our scheme is applicable to the ID-based system.

We conclude this work with a brief summary. This research studies on IBBS scheme from lattices. An identity-based blind signature scheme is put forward based on hard worst case lattice problem, which is considered to be the most promising one among the post quantum primitives. By the technique introduced in [18], our selectively secure constructions can be converted into adaptively secure ones by using chameleon hash functions. However, it needs more efforts to research on identity-based blind signature from lattices. For example, the verification matrix of the scheme in the standard model is three times of the master public key in dimension, and thus the signature sizes is increased. More exploration is needed for reducing the signature size of identity-based blind signature from lattices.

Acknowledgments. We thank the anonymous Inscrypt reviewers for their helpful comments. This work is supported by the National Natural Science Foundations of China (No.61472309 61572390, and 61672412), the 111 Project (No. B08038), and the Natural Science Foundation in Ningbo of China (No. 201601HJ-B01382).

References

1. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advances in Cryptology, pp. 199–203. Springer, Heidelberg (1982)
2. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
3. Gentry, C., Peikert, V., Vaikutanathan, V.: Trapdoors for hard lattices and new cryptographic construction. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC 2008), pp. 197–206. ACM, New York (2008)
4. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13190-5_28
5. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 523–552. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13190-5_27
6. Boyen, X.: Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 499–517. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13013-7_29
7. Lyubashevsky, V., Micciancio, D.: Asymptotically efficient lattice-based digital signatures. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 37–54. Springer, Heidelberg (2008). doi:10.1007/978-3-540-78524-8_3
8. Micciancio, D., Peikert, C.: Trapdoors for lattices: simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29011-4_41
9. Ducas, L., Lyubashevsky, V., Prest, T.: Efficient identity-based encryption over NTRU lattices. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8874, pp. 22–41. Springer, Heidelberg (2014). doi:10.1007/978-3-662-45608-8_2
10. Alperin-Sheriff, J.: Short signatures with short public keys from homomorphic trapdoor functions. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 236–255. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46447-2_11
11. Rückert, M.: Lattice-based blind signatures. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 413–430. Springer, Heidelberg (2010). doi:10.1007/978-3-642-17373-8_24
12. Wang, F., Hu, Y., Wang, C.: A lattice-based blind signature scheme. Geomatics Inf. Sci. Wuhan Univ. **35**(5), 550–553 (2010). (in Chinese)
13. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). doi:10.1007/3-540-39568-7_5
14. Zhang, F., Kim, K.: ID-based blind signature and ring signature from pairings. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 533–547. Springer, Heidelberg (2002). doi:10.1007/3-540-36178-2_33
15. Zhang, F., Kim, K.: Efficient ID-based blind signature and proxy signature from bilinear pairings. In: Safavi-Naini, R., Seberry, J. (eds.) ACISP 2003. LNCS, vol. 2727, pp. 312–323. Springer, Heidelberg (2003). doi:10.1007/3-540-45067-X_27
16. Galindo, D., Herranz, J., Kiltz, E.: On the generic construction of identity-based signatures with additional properties. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 178–193. Springer, Heidelberg (2006). doi:10.1007/11935230_12

17. Phong, L.T., Wakaha, O.: New identity-based blind signature and blind decryption scheme in the standard model. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E92**(A(8)), 1822–1835 (2009)
18. Boneh, D., Boyen, X.: Efficient selective-ID secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24676-3_14