Hindawi
Security and Communication Networks
Volume 2017, Article ID 7571201, 9 pages
https://doi.org/10.1155/2017/7571201

Research Article

Revocable ID-Based Signature with Short Size over Lattices

Ying-Hao Hung, Yuh-Min Tseng, and Sen-Shan Huang

Department of Mathematics, National Changhua University of Education, Changhua, Taiwan

Correspondence should be addressed to Yuh-Min Tseng; ymtseng@cc.ncue.edu.tw

Received 10 August 2016; Revised 28 November 2016; Accepted 19 December 2016; Published 11 January 2017

Academic Editor: Muhammad Khurram Khan

In the past, many ID-based signature (IBS) schemes based on the integer factorization or discrete logarithm problems were proposed. With the progress on the development of quantum technology, IBS schemes mentioned above would become vulnerable. Recently, several IBS schemes over lattices were proposed to be secure against attacks in the quantum era. As conventional public-key settings, ID-based public-key settings have to offer a revocation mechanism to revoke misbehaving or malicious users. However, in the past, little work focuses on the revocation problem in the IBS schemes over lattices. In this article, we propose a new revocable IBS (RIBS) scheme with short size over lattices. Based on the short integer solution (SIS) assumption, we prove that the proposed RIBS scheme provides existential unforgeability against adaptive chosen-message attacks. As compared to the existing IBS schemes over lattices, our RIBS scheme has better performance in terms of signature size, signing key size, and the revocation mechanism with public channels.

1. Introduction

The perception of identity-based cryptography (IBC) was first proposed by Shamir [1] in 1984. In IBC, a user's public key can be derived from her/his identity such as email address and physical IP address. The private keys of users are generated by a trusted private key generator, named PKG. The private keys are, respectively, given to the corresponding users using secure channels. As contradicted to conventional public-key settings, IBC removes the need of certificate management. By following Shamir's perception, Boneh and Franklin [2] proposed a practical identity- (ID-) based encryption (IBE) scheme based on bilinear pairings.

The public key of a user is legal before its intended expiration date, but several circumstances must force to revoke it. So a public-key setting should offer a revocation method or mechanism to revoke the associated public keys of misbehaving or malicious users. Indeed, Boneh and Franklin [2] proposed not only a practical IBE scheme but also a revocation method for ID-based public-key setting. In their revocation method, the PKG periodically generates the new private keys for all nonrevoked users and securely sends the periodic private keys to these users, respectively. In such a case, a secure channel between the PKG and each nonrevoked user must be established to send the periodic private key. However, the size of the PKG's key update equals the amount of all nonrevoked users. Afterward, Boldyreva et al. [3] employed a tree structure to propose a new revocable IBE (RIBE) scheme. In the RIBE scheme, the size of the PKG's key update is reduced to the logarithm of the amount of all nonrevoked users, but the private key size of each user will increase from constant to the logarithm of the amount of all nonrevoked users. Nevertheless, two mentioned revocation mechanisms above still require encryption/decryption to send periodic private keys to users. Thus, the required periodic encryption/decryption will raise the workloads of both the PKG and users. To eliminate the requirement of encryption/decryption, Tseng and Tsai [4] proposed a new RIBE scheme with a public channel. In their RIBE scheme, the PKG and users do not need to encrypt/decrypt the periodic private keys. It provides an alternative which is more practical than the previously proposed revocation solutions.

The security of today's universally used public-key cryptographies (including the mentioned IBC above) is based on the prime factoring assumption or the hardness of the discrete logarithm problem. With the progress on the development of quantum technology, the computational power of quantum computers would cause instant threat to these

public-key cryptographies [5]. Accordingly, this has motivated the era of postquantum cryptography (PQC). Among several postquantum research areas, lattice-based public-key cryptography has received the most significant attention from researchers. When compared with other (PQC) cryptographies, lattice-based public-key cryptography can provide more efficiency in public-key encryption and digital signature schemes. In the past five years, there has been a tremendous growth in lattice-based public-key cryptography and its related schemes have become viable.

Related Work. To combine the advantages of IBC and lattices, Ruckert [6] proposed the first two ID-based signature (IBS) schemes over lattice assumptions. To improve the efficiency and security, several lattice-based IBS schemes [7–10] have been proposed. In [7, 8], they employed Gentry et al.'s signature scheme [11] with a user's identity to generate the corresponding signing key. By the signing key, the user can run a preimage sampling algorithm (i.e., lattice basis delegation) [12] to obtain a signature. According to Gentry et al.'s signature scheme, the user's signing key is a short basis of a lattice. In such a case, two lattice-based IBS schemes [7, 8] would be inefficient in practice since the signing key size and the signature size will increase dramatically after lattice basis delegation.

Based on the lattice-based IBS scheme in [8], Tian and Huang [9] replaced the preimage sampling algorithm with the rejection sampling technique [13] to generate a signature. Their signature scheme can be viewed as an identity-based version of Lyubashevsky's signature scheme [13]. The advantage of Tian and Huang's lattice-based IBS scheme is to reduce the signature size and computation overhead of generating a signature. In 2016, inspired by the IBE scheme over NTRU lattice proposed by Ducas et al. [14], Xie et al. [10] employed their key extract algorithm to further improve the size of a user's signing key. However, these lattice-based IBS schemes mentioned above did not address the revocation problem. Indeed, these lattice-based IBS schemes would use Boneh and Franklin's periodic revocation mechanism [2] to achieve revocation functionality. However, in the revocation mechanism, the PKG and nonrevoked users require encryption/decryption to send periodic signing keys to users.

Recently, Xiang [15] adopted the binary tree structure used in [3] to construct a revocable IBS (RIBS) scheme over lattices. As the advantage of Boldyreva et al.'s scheme [3], the size of the PKG's key update is reduced to the logarithm of the amount of all nonrevoked users. Indeed, Xiang's scheme also inherits the disadvantages that occurred in Boldyreva et al.'s scheme [3], namely, the private key size of a user increases from constant to the logarithm of the number of users, and encryption/decryption are required to securely send the users' periodic signing keys. Meanwhile, the signing key size, signature size, and computational cost in Xiang's scheme turn out to be inefficient.

Contribution. In this article, we employ the revocation idea of Tseng and Tsai [4] to propose an efficient RIBS scheme over lattices while the size of a user's signing key remains constant. In our RIBS scheme, a user's signing key consists of two components, namely, initial key and time update key. The initial key is fixed and unchanged, while the time update key is changed along with time-period. The PKG periodically generates new time update keys and then sends them to nonrevoked users using a public channel. If the PKG would like to revoke misbehaving users, the PKG just stops issuing the new time update keys for those users. Thus, a RIBS scheme must address two kinds of adversaries: an inside adversary (or a revoked user) and an outside adversary. Based on the short integer solution (SIS) assumption over lattices [16], we prove that the proposed RIBS scheme provides existential unforgeability against adaptive chosen-message attacks for a revoked user and an outside adversary. As compared to the existing lattice-based RIBS schemes, our scheme possesses the following properties:

(i) Both the initial key and time update key of a user are generated using the Gaussian sampling technique over NTRU lattice. The point is that both keys are small and independent of the number of users in the system.

(ii) We employ the rejection sampling technique [13] to generate a signature while the signature size is lesser than that of the signature scheme using the preimage sampling algorithm.

(iii) The PKG and nonrevoked users do not need to encrypt/decrypt the periodic time update keys.

In summary, as compared with previously proposed IBS and RIBS schemes over lattices, our scheme possesses better performance in terms of signing key size, signature size, and the revocation mechanism.

Organization. The rest of this article is arranged as follows. Section 2 presents several important preliminaries. In Section 3, the syntax and adversary models of RIBS schemes are given. The proposed RIBS scheme over lattices is presented in Section 4. In Section 5, the security of the proposed RIBS scheme is formally analyzed. In Section 6, performance analysis and comparisons are made to demonstrate the advantages of the proposed scheme. In Section 7, conclusions are given.

2. Preliminaries

Here, we review several fundamental concepts and assumptions of lattices.

2.1. Notations. Throughout this article, let R be the set of real numbers, N be an integer with the type power-of-two, Z be the set of integers, and, for $q \in Z$, Z_q be the set of integers in the set $[-q/2, -q/2)$. $\|\mathbf{x}\|$ denotes the Euclidean norm of a vector $\mathbf{x}$. $\|\mathbf{X}\|$ represents the norm of a matrix $\mathbf{X}$ which is defined as the largest norm of its columns. Let $R_q = Z_q[X]/(X^N + 1)$ be the ring of polynomials modulo $X^N + 1$ with coefficients in Z_q. For $f = \sum_{i=0}^{N-1} f_i x^i$ and $g = \sum_{i=o}^{N-1} g_i x^i$ in R_q, let $f + g$ and

$f \cdot g$ denote, respectively, the addition and multiplication in R_q, defined by

$$f + g = \sum_{i=0}^{N-1} (f_i + g_i) x^i \pmod q,$$
$$f \cdot g = \sum_{k=o}^{N-1} \left(\sum_{i+j=k(\mathrm{mod}\, N)} f_i g_i \right) x^k \pmod q. \quad (1)$$

Here, the coefficients of $f + g$ and $f \cdot g$ are reduced modulo q into the set Z_q. For convenience, an element f in R_q will be written as a polynomial $\sum_{i=0}^{N-1} f_i x^i$ or a vector $[f_0, f_1, \ldots, f_{N-1}]$.

For any set $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset R^n$ of linearly independent vectors, let $\widetilde{\mathbf{B}} = \{\widetilde{\mathbf{b}}_1, \ldots, \widetilde{\mathbf{b}}_n\}$ denote its Gram-Schmidt orthogonalization, defined iteratively in the following way: $\widetilde{\mathbf{b}_1} = \mathbf{b}_1$, and for each $i = 2, \ldots, n$, $\widetilde{\mathbf{b}_i}$ is the component of $\mathbf{b}_i$ orthogonal to span $(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})$. Clearly, $\|\widetilde{\mathbf{B}}\| \leq \|\mathbf{B}\|$.

2.2. Lattice. A lattice is a set of points in n-dimensional space with a periodic structure [16]. Let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ be n linearly independent vectors in R^n. These linearly independent vectors can generate a (n-dimensional) lattice $\mathbf{\Lambda}$ that is denoted by $\mathscr{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, namely, the set $\{\sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in Z\}$. The set $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ is viewed as a basis of the lattice $\mathbf{\Lambda}$.

2.3. Anticirculant Matrices. Anticirculant matrices have become one of the most important and active research fields in recent years since they possess a special structure and nice properties.

Definition 1. An N-dimensional anticirculant matrix with $f = \sum_{i=0}^{N-1} f_i x^i$ is represented as in the following Toeplitz matrix:

$$A_N(f) = \begin{pmatrix} (f) \\ (x \cdot f) \\ \vdots \\ \left(x^{N-1} \cdot f\right) \end{pmatrix} = \begin{pmatrix} f_0 & f_1 & \cdots & f_{N-1} \\ -f_{N-1} & f_0 & \cdots & f_{N-2} \\ \cdots & \cdots & \cdots & \cdots \\ -f_1 & -f_2 & \cdots & f_0 \end{pmatrix}. \quad (2)$$

For convenience, we denote $A_N(f)$ as $A(f)$ in this article. Anticirculant matrices possess the following important property.

Lemma 2 (see [14]). *$A(f) + A(g) = A(f + g)$ and $A(f) \times A(g) = A(f \cdot g)$, where $f, g \in R_q$.*

2.4. NTRU Lattices. NTRU [17] is a lattice-based cryptosystem that relied on a particularly efficient class of convolution modular lattices, called NTRU lattices. We briefly review the concept of NTRU lattices on which our scheme is based.

Definition 3. Assume that q is a positive integer and N is a power-of-two integer while $f, g \in R_q$ and $h = g \cdot f^{-1}$. By using h and q, a NTRU full-rank lattice of Z^{2N} is represented as

$$\mathbf{\Lambda}_{h,q} = \left\{(u, v) \in R_q^2 \mid u + v \cdot h = 0\right\}. \quad (3)$$

Indeed, the NTRU full-rank lattice $\mathbf{\Lambda}_{h,q}$ is generated by the matrix

$$\mathbf{A}_{h,q} = \begin{pmatrix} -A(h) & I_N \\ qI_N & O_N \end{pmatrix}, \quad (4)$$

where I_N and O_N are, respectively, the $N \times N$ unit matrix and $N \times N$ null matrix.

However, if h is uniformly distributed in R_q, then the basis $\mathbf{A}_{h,q}$ is unsuitable for solving the closed lattice vector problem. To compensate this, Hoffstein et al. [18] constructed an appropriate basis

$$\mathbf{B}_{f,g} = \begin{pmatrix} A(g) & -A(f) \\ A(G) & -A(f) \end{pmatrix} \quad (5)$$

for $\mathbf{\Lambda}_{h,q}$ while satisfying $f \cdot G - g \cdot F = q$, where $F, G \in R_q$. Indeed, it can be computed efficiently to find such F and G. Moreover, $\mathbf{B}_{f,g}$ provides a short basis for $\mathbf{\Lambda}_{h,q}$ due to the fact $\|\mathbf{B}_{f,g}\| \leq \|\mathbf{A}_{h,q}\|$ by Lemma 4 below.

Lemma 4 (see [14]). *Assume that $f, g, F, G \in R_q$ satisfy $f \cdot G - g \cdot F = q$ and $h = g \cdot f^{-1}$. Then, $\mathbf{A}_{h,q}$ and $\mathbf{B}_{f,g}$ are both bases of the NTRU lattice $\mathbf{\Lambda}_{h,q}$ and $\|\mathbf{B}_{f,g}\| \leq \|\mathbf{A}_{h,q}\|$.*

Gentry et al. [11] proposed the Gaussian sampling technique as the trapdoor generation algorithm to produce a trapdoor of a one-way function. Ducas et al. [14] proposed a special distribution over the NTRU lattices to improve the performance of the trapdoor generation algorithm in Gentry et al.'s scheme. In this article, we adopt Ducas et al.'s scheme as the trapdoor generation algorithm as follows.

Lemma 5 (see [14]). *Let q be a prime, N be a power-of-two integer, and $\sigma = 1.17\sqrt{q/2N}$. Then, we can construct a probabilistic polynomial-time (PPT) algorithm $TrapGen(q, N)$ which generates two polynomials f and g to output $h = g \cdot f^{-1}$ and a matrix $\mathbf{B}_{f,g}$ such that h is statistically close to uniform in R_q and $\mathbf{B}_{f,g}$ is a short basis of $\mathbf{\Lambda}_{h,q}$.*

2.5. Gaussian (Normal) Distribution. Gentry et al. [11] proposed the Gaussian sampling technique as the trapdoor generation algorithm which produces a trapdoor without leaking any information of the short basis. Before we introduce Gentry et al.'s method, we define Gaussian distributions.

Definition 6. The continuous Gaussian distribution over R^N centered at $\mathbf{c} \in R^N$ with the standard deviation $s > 0$ is defined by the function $\rho_{s,\mathbf{c}}^N(\mathbf{x}) = (\mathbf{1}/\mathbf{s}\sqrt{\mathbf{2}\pi})^N \mathbf{e}^{-\|\mathbf{x}-\mathbf{c}\|^2/\mathbf{2s}^2}$, where $\mathbf{x} \in R^N$.

For any lattice $\mathbf{\Lambda} \in R^N$, $\rho_{s,\mathbf{c}}^N(\mathbf{\Lambda})$ represents $\sum_{\mathbf{x} \in \mathbf{\Lambda}} \rho_{s,\mathbf{c}}^N(\mathbf{x})$.

Definition 7. The discrete Gaussian distribution over R^N centered at $\mathbf{c} \in R^N$ with the standard deviation $s > 0$ is defined as $D^N_{s,\mathbf{c}}(\mathbf{x}) = \rho^N_{\mathbf{s},\mathbf{c}}(\mathbf{x})/\rho^N_{\mathbf{s},\mathbf{c}}(\mathbf{\Lambda})$, where $\mathbf{x} \in R^N$.

In this sequel, we can curtail $\rho^N_{s,0}$ as ρ^N_s and $D^N_{s,0}$ as D^N_s, respectively. On the other hand, Lyubashevsky [13] proposed an interesting fact of $D^N_{\sigma,\mathbf{v}}(\mathbf{x})$, the discrete normal distribution in dimension N with standard deviation σ at center $\mathbf{v}$.

Lemma 8 (see [13]). *For any $\mathbf{v} \in Z^m$ and $\alpha > 0$, we have the following properties.*

If $\sigma = \omega(\|\mathbf{v}\|\sqrt{\log m})$, then $\Pr[\mathbf{x} \in D^m_\sigma : D^m_\sigma(\mathbf{x})/D^m_{\sigma,\mathbf{v}}(\mathbf{x}) = O(1)] = 1 - 2^{\omega(\log m)}$.

If $\sigma = \alpha\|\mathbf{v}\|$, then $\Pr[\mathbf{x} \in D^m_\sigma : D^m_\sigma(\mathbf{x})/D^m_{\sigma,\mathbf{v}}(\mathbf{x}) < e^{12/\alpha+1/(2\sigma^2)}] > 1 - 2^{-100}$.

According to Lemma 8, there is real $M \approx e$ such that $D^m_\sigma(\mathbf{x}) \leq MD^m_{\sigma,\mathbf{v}}(\mathbf{x})$ for all $\mathbf{x} \in Z^m$ [9].

2.6. Sampling Algorithms. Micciancio and Regev [19] defined a lattice parameter to determine the amount of Gaussian noise that one has to add to a lattice in order to get close to a uniform distribution. By Micciancio and Regev's method, Gentry et al. [11] proposed a sampling algorithm as follows.

Lemma 9 (see [11]). *Let q be a prime and $\mathbf{B}$ be a short basis of an N-dimensional lattice $\mathbf{\Lambda}$. If $s \geq \|\tilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log N})$ and $0 < \varepsilon < 1$, then, for any $\mathbf{c} \in R^N$, we have the following properties:*

(1) $\Pr[\|\mathbf{x} - \mathbf{c}\|] > s\sqrt{N} \leq (1+\varepsilon)/(1+\varepsilon) \cdot 2^{-N}$, *where* $\mathbf{x} \in D^N_{s,\mathbf{c}}$.

(2) *There is a PPT algorithm SampleGau$(\mathbf{B}, s, c)$ that can output a sample in $\mathbf{\Lambda}$ from a distribution which is statistically close to $D^N_{s,\mathbf{c}}$.*

2.7. Rejection Sampling Algorithm. Lyubashevsky [13] adopted the rejection sampling technique to sign a message. When a user with ID would like to sign a message with a signing key S_{ID}, she/he first chooses a vector $\mathbf{y} \in D^N_\sigma$. And then the user sets a candidate signature $\mathbf{z}$ as $\mathbf{y} + \mathbf{c} \cdot S_{\mathrm{ID}}$ where $\mathbf{c}$ is a hash value of message. Let $\mathcal{F}$ be the target distribution of the signature $\mathbf{z}$ which is independent of S_{ID}. If G is a probability distribution and $M > 0$ while satisfying $\mathcal{F}(\mathbf{x}) \leq M \cdot G(\mathbf{x})$ for all $\mathbf{x}$, then the candidate signature $\mathbf{z}$ can be output successfully with probability $\mathcal{F}(\mathbf{z})/M \cdot G(\mathbf{z})$, and M is the expected number of times required for outputting a signature.

2.8. Hardness Assumptions. In the following, we present a mathematical problem, namely, the short integer solution (SIS) problem, which has at least the same difficulty with the worst case of short independent vector problem (SIVP) up to a polynomial approximation factor [16].

Definition 10 ($R - \mathrm{SIS}^\Phi_{q,m,\beta}$ problem). The small integer solution (SIS) problem on a ring with parameters q, m, β, and Φ is defined as follows. Given $a_1, a_2, \ldots, a_m$ chosen uniformly and independently from $R_q = Z_q[x]/(\Phi)$, the associated SIS problem is to find $r_1, r_2, \ldots, r_m \in Z$ such that $\sum_{i=1}^m r_i a_i = 0 \bmod q$ and $\|\mathbf{z}\| \leq \beta$, where $\mathbf{z} = (r_1, r_2, \ldots, r_m)^T \in Z^m$.

Stehle and Steinfeld [20] presented the idea that the statistical distance between the distribution of $h = g/f$ and the uniform distribution of R_q is negligible. If we take an NTRU public key $h = g/f$, the $R - \mathrm{SIS}^\Phi_{q,m,\beta}$ problem on the NTRU lattices is to find a pair $(\mathbf{z_1}, \mathbf{z_2})$ that satisfies the conditions $\mathbf{z_1} + h \cdot \mathbf{z_2} = \mathbf{0}$ and $\|(\mathbf{z_1}, \mathbf{z_2})\| \leq \beta$.

3. Syntax and Adversary Model of RIBS

In the following, we define the syntax and adversary model of RIBS schemes.

Definition 11. A RIBS scheme includes five algorithms:

(i) *Setup.* The algorithm takes a system parameter N and the amount J of all time-periods as input and publishes public parameters *Parms* and sets a system secret key S_{PKG} in secret.

(ii) *Initial Key Extract.* Given a user's ID and the system secret key S_{PKG}, it computes and sends the initial key D_{ID} to the user.

(iii) *Time Key Update.* Given a time-period t, a user's ID, and the system secret key S_{PKG}, this algorithm computes and sends the time update key $T_{\mathrm{ID},t}$ to the user.

(iv) *Signing.* This algorithm takes a message μ, a user's signing key $S_{\mathrm{ID},t}$, and a time-period t as input. It then returns a signature θ on μ.

(v) *Verification.* This algorithm takes a message μ, a signature θ, a user's ID, and a time-period t as input. It returns "accept" if θ is valid and "reject" otherwise.

By the framework of the RIBS scheme, a user's signing key consists of two components, namely, initial key and time update key. Thus, the associated adversary model consists of two kinds of adversaries: an inside adversary (or a revoked user) and an outside adversary.

Definition 12. For a RIBS scheme, if there exists no PPT adversary $\mathcal{A}$ (a revoked user or an outside adversary) who has nonnegligible probability to forge a valid signature under adaptive chosen-message attacks, we say that the RIBS scheme is existentially unforgeable or RID-UF-ACMA secure. In the following RID-UF-ACMA game, the adversary $\mathcal{A}$ may interact with a challenger $\mathcal{C}$ to obtain some useful information.

(i) *Initialization.* $\mathcal{C}$ performs the *setup* algorithm to set *Parms* and S_{PKG}. The PKG sends *Parms* to the adversary $\mathcal{A}$ and keeps S_{PKG} in secret.

(ii) *Queries.* $\mathcal{A}$ can adaptively request a number of different queries as follows.

(a) *Initial Key Extract Query.* Upon receiving an identity ID, $\mathcal{C}$ performs the *initial key extract*

algorithm to generate D_{ID}. $\mathscr{C}$ then sends D_{ID} to $\mathscr{A}$.

(b) *Time Key Update Query.* Upon receiving a user's ID and a time-period t, $\mathscr{C}$ performs the *time key update* algorithm to generate $T_{\mathrm{ID},t}$. $\mathscr{C}$ then sends $T_{\mathrm{ID},t}$ to $\mathscr{A}$.

(c) *Signing Query.* Upon receiving a message μ, an identity ID, and a time-period t, $\mathscr{C}$ uses $S_{\mathrm{ID},t} = (D_{\mathrm{ID}}, T_{\mathrm{ID},t})$ to perform the *signing* algorithm to obtain a signature θ. $\mathscr{C}$ then sends θ to $\mathscr{A}$.

(iii) *Forgery.* If $\mathscr{A}$ with nonnegligible probability can forge a signature tuple $(\mu^*, \mathrm{ID}^*, t^*, \theta^*)$ that fulfills three following conditions, we call that $\mathscr{A}$ with nonnegligible probability wins the game. We define the nonnegligible probability as the advantage of $\mathscr{A}$ in the game.

(1) For $(\mu^*, \mathrm{ID}^*, t^*, \theta^*)$, the *verification* algorithm outputs "accept."

(2) The tuple $(\mu^*, \mathrm{ID}^*, t^*)$ is not issued during the *signing* query.

(3) If $\mathscr{A}$ is an outside adversary, ID^* is not issued during the *initial key extract* query.

(4) If $\mathscr{A}$ is a revoked user (inside adversary), (ID^*, t^*) is not issued during the *time key update* query.

4. Efficient RIBS Scheme over NTRU Lattices

The proposed RIBS scheme over NTRU lattices includes five algorithms.

(i) *Setup.* Given a system parameter N, the PKG chooses a prime q, $s > 0$, and $\sigma > 0$. Then the PKG runs the algorithm $TrapGen(q, N)$ presented in Lemma 5 to obtain (f, g) such that $h = g \cdot f^{-1}$, $\|f\| < s\sqrt{N}$, and $\|g\| < s\sqrt{N}$ while generating a short basis

$$\mathbf{B} = \begin{pmatrix} A(g) & -A(f) \\ A(G) & -A(f) \end{pmatrix} \in \mathbf{Z}_q^{\mathbf{2}N\times 2N} \text{ of } \Lambda_{h,q}. \tag{6}$$

The PKG generates public parameters *Parms* and a system secret key S_{PKG} as follows:

(1) Set three hash functions H_0, $H_1 : \{0,1\}^* \to Z_q^N$, and $H_2 : \{0,1\}^* \to \{\mathbf{v} | \mathbf{v} \in \{-1,0,1\}^N$ such that $\|\mathbf{v}\|_{\mathbf{1}} \le \lambda\}$, where the vectors $\mathbf{v}$ can be viewed as polynomials with coefficients in the set $\{-1,0,1\}$ and $\|\mathbf{v}\|_{\mathbf{1}}$ denotes the number of nonzero components of $\mathbf{v}$.

(2) Finally, the PKG sets $S_{\mathrm{PKG}} = \mathbf{B}$ and $Parms = \langle h, H_0, H_1, H_2\rangle$, where h is the system public key.

(ii) *Initial Key Extract.* Given a user's ID $\in \{0,1\}^*$, the PKG first calculates $H_0(\mathrm{ID})$ and then uses the system secret key $S_{\mathrm{PKG}} = \mathbf{B}$ to run the algorithm $SampleGau(\mathbf{B}, s, H_0(\mathrm{ID}))$ in Lemma 9 to output a sample $(\mathbf{s}_1, \mathbf{s}_2)$ such that $\|(\mathbf{s}_1, \mathbf{s}_2)\| < s\sqrt{2N}$ and $\mathbf{s}_1 + h \cdot \mathbf{s}_2 = H_0(\mathrm{ID})$. Then, the PKG sets the initial key $D_{\mathrm{ID}} = (\mathbf{s}_1, \mathbf{s}_2)$ and sends the user with D_{ID} using secure channel. In fact, if one knows $(h, H_0(\mathrm{ID}))$ and chooses s_i $(i = 1,2)$ from a Gaussian distribution instead of a uniform one, then recovering s_i is as hard as solving worst-case lattice problems [21].

(iii) *Time Key Update.* Upon receiving a time-period t and a user's ID $\in \{0,1\}^*$, the PKG first calculates $H_1(\mathrm{ID}, t)$ and uses the system secret key $S_{\mathrm{PKG}} = \mathbf{B}$ to run the algorithm $SampleGau(\mathbf{B}, s, H_1(\mathrm{ID}, t))$ to output a sample $(\mathbf{s_3}, \mathbf{s_4})$ such that $\|(\mathbf{s}_3, \mathbf{s}_4)\| < s\sqrt{2N}$ and $\mathbf{s}_3 + h \cdot \mathbf{s}_4 = H_1(\mathrm{ID}, t)$. Then, the PKG sets the time update key $T_{\mathrm{ID},t} = (\mathbf{s}_3, \mathbf{s}_4)$ and sends the user with $T_{\mathrm{ID},t}$ using public channel. Meanwhile, the user sets the signing key $S_{\mathrm{ID},t} = (D_{\mathrm{ID}}, T_{\mathrm{ID},t})$. In fact, if one knows $(h, H_1(\mathrm{ID}, t))$ and chooses s_i $(i = 3,4)$ from a Gaussian distribution instead of a uniform one, then recovering s_i is as hard as solving worst-case lattice problems [21].

(iv) *Signing.* Given a message $\mu \in \{0,1\}^*$ and a time-period t, the user with ID $\in \{0,1\}^*$ first chooses $\mathbf{y}_1$, $\mathbf{y}_2$ from the distribution D_σ^N and computes $\mathbf{c} = H_2(\mathbf{y}_1 + h \cdot \mathbf{y}_2, \mu)$, $\mathbf{z_1} = \mathbf{y}_1 + (\mathbf{s}_1 + \mathbf{s}_3) \cdot \mathbf{c}$, and $\mathbf{z_2} = \mathbf{y}_2 + (\mathbf{s}_2 + \mathbf{s}_4) \cdot \mathbf{c}$, where $\|(\mathbf{z}_1, \mathbf{z}_2)\| \le 2\sigma\sqrt{2N}$. Finally, the user can generate a signature $(\mathbf{z_1}, \mathbf{z_2}, \mathbf{c})$ with probability $\min[D_\sigma^N / MD_{\sigma,\mathbf{c}\cdot S_{\mathrm{ID},t}}^N, 1]$, where $M = O(1)$. If nothing is generated by the user, the user repeats this algorithm.

(v) *Verification.* Given a signature $(\mathbf{z_1}, \mathbf{z_2}, \mathbf{c})$ on a message μ for a user's ID at a time-period t, a verifier validates the signature by checking the following equality:

$$\mathbf{c} = H_2\left(\mathbf{z_1} + h \cdot \mathbf{z_2} - \left(H_0(\mathrm{ID}) + H_1(\mathrm{ID}, t)\right) \cdot \mathbf{c}, \mu\right). \tag{7}$$

If the equality holds, the *Verification* algorithm returns "accept" and "reject" otherwise.

Here, the correctness of the equality follows from

$$\begin{aligned} &\mathbf{z}_1 + h \cdot \mathbf{z}_2 - \left(H_0(\mathrm{ID}) + H_1(\mathrm{ID}, t)\right) \cdot \mathbf{c} \\ &\quad = \mathbf{y}_1 + \left(\mathbf{s}_1 + \mathbf{s}_3\right) \cdot \mathbf{c} + h \cdot \mathbf{y}_2 + h \cdot \left(\mathbf{s}_2 + \mathbf{s}_4\right) \cdot \mathbf{c} \\ &\qquad - \left(\mathbf{s}_1 + h \cdot \mathbf{s}_2 + \mathbf{s}_3 + h \cdot \mathbf{s}_4\right) \cdot \mathbf{c} = \mathbf{y}_1 + h \cdot \mathbf{y}_2. \end{aligned} \tag{8}$$

5. Security Analysis

In this section, we demonstrate the security of the proposed RIBS scheme. In our RIBS scheme, a user's signing key includes two parts, namely, the initial key and time update key. To revoke a user, the PKG simply stops issuing the user's periodic time update key. As the RID-UF-ACMA game presented in Definition 12, the adversary may get either the time update key or the initial key, but not both. Hence, there are two kinds of adversaries to be concerned with, namely, revoked user and outside adversary. An outside adversary cannot access the target's initial key, but it may get all time

update keys. Since a revoked user has already owned the associated initial key, the user cannot get the periodic time update key.

Firstly, we adopt the key extract algorithm in Ducas et al. [14, Algorithm 3] to generate both initial keys and time update keys. Based on Ducas et al. [14], Lemma 13 demonstrates that our scheme is secure against the ID forgery attacks. Moreover, Theorem 14 demonstrates that the proposed RIBS scheme is secure for an outside adversary and a revoked user.

Lemma 13. *Our RIBS scheme is secure against ID forgery attack.*

Proof. In our scheme, we adopt the key extract algorithm in Ducas et al. [14] to generate initial keys. Let $h = g \cdot f^{-1}$ be the public key and

$$\mathbf{B} = \begin{pmatrix} A(g) & -A(f) \\ A(G) & -A(f) \end{pmatrix} \tag{9}$$

be a short basis of the NTRU, where $f, g, F, G \in R_q$, $f \cdot G - g \cdot F = q$, $\|f\| < s\sqrt{N}$, and $\|g\| < s\sqrt{N}$. The initial key $(\mathbf{s}_1, \mathbf{s}_2)$ is generated by $SampleGau(\mathbf{B}, s, H_0(\mathrm{ID}))$ to output a sample $\mathbf{s_1}$ as the first component of the initial key and determine the second component $\mathbf{s_2}$ such that $\mathbf{s}_1 + h \cdot \mathbf{s}_2 = H_0(\mathrm{ID}) \in Z_q^N$. By the security analysis of [14], no PPT adversary $\mathscr{A}$ may find $(\mathbf{s}_1, \mathbf{s}_2)$ with nonnegligible advantage. Therefore, the proposed RIBS scheme is secure against ID forgery attacks. □

Theorem 14. *Assume that there exists a PPT adversary $\mathscr{A}$ (an outsider or a revoked user) who can break the proposed RIBS scheme with nonnegligible probability ε in the random oracle model. Based on the adversary $\mathscr{A}$, we then construct a PPT algorithm $\mathscr{C}$ to compute the $R-SIS$ problem with nonnegligible probability $(1 - 2^{-\omega(\log N)})\varepsilon$, where N is the system parameter.*

Proof. Here, we demonstrate only the case when $\mathscr{A}$ is an outside adversary since the other case when $\mathscr{A}$ is a revoked user can be proved similarly. Without loss of generality, an algorithm $\mathscr{C}$ receives a random instance $(q, 2N, 4s\sqrt{2N} + 2\lambda\sigma\sqrt{2N}, X^N + 1)$ of the $R-$SIS problem, where q is a prime, N is a positive integer, and $s, \lambda, \sigma > 0$. We will show how $\mathscr{C}$ can make use of the adversary $\mathscr{A}$ to output the $R-$SIS solution which is nonzero vector $(\mathbf{u_1}, \mathbf{u_2}) \in Z_q^{\mathbf{2}N}$. The algorithm $\mathscr{C}$ plays the challenger and interacts with the adversary $\mathscr{A}$ as follows.

(i) *Initialization.* Given the system parameter N, the challenger $\mathscr{C}$ randomly chooses a polynomial $h \in R_q$. Then, $\mathscr{C}$ sets the public parameters $Parms = \langle h, H_0, H_1, H_2 \rangle$, where the hash functions H_0, H_1, and H_2 are viewed as random oracles controlled by $\mathscr{C}$. Finally, $\mathscr{C}$ returns *Parms* to $\mathscr{A}$.

(ii) *Queries.* The challenger $\mathscr{C}$ responds to these queries issued by the adversary $\mathscr{A}$ as follows.

(a) H_0 *Query.* At any time, $\mathscr{A}$ can issue the query along with ID_i. To respond to the query, $\mathscr{C}$ maintains an initially empty list L_0 of tuples of the form $\langle \mathrm{ID}_i, P_{\mathrm{ID}i}, \mathrm{DID}_i \rangle$. When $\mathscr{A}$ queries the oracle H_0 with ID_i, $\mathscr{C}$ responds to $\mathscr{A}$ with $P_{\mathrm{ID}i}$ according to the following rules.

(1) If ID_i appears in a tuple $\langle \mathrm{ID}_i, P_{\mathrm{ID}i}, \mathrm{DID}_i \rangle$ in L_0, then $\mathscr{C}$ responds with $P_{\mathrm{ID}i}$.

(2) Otherwise, the challenger $\mathscr{C}$ randomly chooses $s_{i1}, s_{i2} \in D_s^N$ such that $\|(\mathbf{s}_{i1}, \mathbf{s}_{i2})\| < s\sqrt{2N}$. Then $\mathscr{C}$ computes the polynomial $P_{\mathrm{ID}i} = \mathbf{s}_{i1} + h \cdot \mathbf{s}_{i2}$ and adds the tuple $\langle \mathrm{ID}_i, P_{\mathrm{ID}i}, \mathrm{DID}_i = (\mathbf{s}_{i1}, \mathbf{s}_{i2}) \rangle$ in L_0. $\mathscr{C}$ responds to $\mathscr{A}$ with $P_{\mathrm{ID}i}$.

(b) H_1 *Query.* At any time, $\mathscr{A}$ can issue the query along with (ID_i, t). To respond to the query, $\mathscr{C}$ maintains an initially empty list L_1 of tuples of the form $\langle \mathrm{ID}_i, t, T_{1i}, T_{\mathrm{ID},t} \rangle$. When $\mathscr{A}$ queries the oracle H_1, $\mathscr{C}$ responds to $\mathscr{A}$ with T_{1i} according to the following rules.

(1) If (ID_i, t) appears in a tuple $\langle \mathrm{ID}_i, t, T_{1i}, T_{\mathrm{ID},t} \rangle$ in L_1, then $\mathscr{C}$ responds with T_{1i}.

(2) Otherwise, the challenger $\mathscr{C}$ randomly chooses $\mathbf{s}_{i3}, \mathbf{s}_{i4} \in D_s^N$ such that $\|(\mathbf{s}_{i3}, \mathbf{s}_{i4})\| < s\sqrt{2N}$. The challenger $\mathscr{C}$ sets the user's time update key $T_{\mathrm{ID},t} = (\mathbf{s}_{i3}, \mathbf{s}_{i4})$ and computes $T_{1i} = \mathbf{s}_{i3} + h \cdot \mathbf{s}_{i4}$. Then $\mathscr{C}$ adds the tuple $\langle \mathrm{ID}_i, t, T_{1i}, T_{\mathrm{ID},t} \rangle$ in L_1. $\mathscr{C}$ responds to $\mathscr{A}$ with T_{1i}.

(c) H_2 *Query.* At any time, $\mathscr{A}$ can issue the query along with $(\mathbf{y}_j, \mu_j)$. To respond to the query, $\mathscr{C}$ maintains an initially empty list L_2 of tuples of the form $\langle \mathbf{y}_j, \mu_j, \mathbf{c}_j \rangle$. When $\mathscr{A}$ queries oracle H_2, $\mathscr{C}$ responds to $\mathscr{A}$ with $\mathbf{c}_j$ according to the following rules.

(1) If $(\mathbf{y}_j, \mu_j)$ appears in a tuple $\langle \mathbf{y}_j, \mu_j, \mathbf{c}_j \rangle$ in L_2, then $\mathscr{C}$ responds with $\mathbf{c}_j$.

(2) Otherwise, $\mathscr{C}$ randomly chooses $\mathbf{c}_j \in R_q$. Then, $\mathscr{C}$ adds the tuple $\langle \mathbf{y}_j, \mu_j, \mathbf{c}_j \rangle$ to the list L_2. Finally, the challenger $\mathscr{C}$ responds to $\mathscr{A}$ with $\mathbf{c}_j$.

(d) *Initial Key Extract Query.* When $\mathscr{A}$ issues the query along with ID_i, $\mathscr{C}$ first looks up the list L_0 to find the tuple containing DID_i associated with ID_i and send it to $\mathscr{A}$. If no such tuple is found in L_0, $\mathscr{C}$ obtains DID_i by issuing the $H_0(\mathrm{ID}_i)$ query and responds to $\mathscr{A}$ with DID_i.

(e) *Time Key Update Query.* When $\mathscr{A}$ issues the query along with (ID_i, t), $\mathscr{C}$ first looks up the list L_1 to find the tuple containing $T_{\mathrm{ID},t}$ associated with (ID_i, t) and send it to $\mathscr{A}$. If no such tuple is found in L_1, $\mathscr{C}$ obtains $T_{\mathrm{ID},t}$ by issuing the $H_1(\mathrm{ID}_i, t)$ query and responds to $\mathscr{A}$ with $T_{\mathrm{ID},t}$.

(f) *Sign Query.* Upon receiving this query on $(\mu_j, \mathrm{ID}_i, t)$, the challenger $\mathscr{C}$ performs the following steps to generate a valid signature. First, $\mathscr{C}$ looks up the lists L_0 and L_1 to obtain, if there exist, the associated tuples $\langle \mathrm{ID}_i, P_{\mathrm{ID}i}, \mathrm{DID}_i \rangle$ and

Table 1: Comparisons between the existing IBS/RIBS schemes and our RIBS scheme.

	Tian and Huang's IBS scheme [9]	Xiang's RIBS scheme [15]	Our RIBS scheme
Lattice type	GPV lattice [11]	GPV lattice [11]	NTRU lattice [14]
Signing key size	$mk\log(\widehat{s}\sqrt{m})$	$2Nm(\log n)\cdot\log(\overline{s}\sqrt{2m})$	$4N\log(s\sqrt{N})$
Signature size	$m\log 12\widehat{\sigma}+\lambda(\log k+1)$	$3Nm\log n\cdot\log(\overline{s}\sqrt{3m})$	$2N\log 12\sigma+\lambda(\log N+1)$
Computation cost of signing	$7(Nm+mk)T_m$	$2NmT_m+T_{\text{sp}}$	$7(N^2+2N)T_m$
Computation cost of verifying	$(Nm+Nk)T_m$	$3NmT_m$	$(N^2+N)T_m$
Revocable functionality	No	Secure channel	Public channel
Security property	ID-UF-ACMA secure	RID-UF-ACMA secure	RID-UF-ACMA secure

N: the security parameter; λ, k: positive integers; n: the number of users; $m > 6N\log q$; $\widehat{s} = \sqrt{m}\omega(\sqrt{\log N})$; $\overline{s} = m\log n\cdot\omega(\sqrt{\log N})$; $s = N^{5/2}\sqrt{2q}\omega(\sqrt{\log N})$; $\widehat{\sigma} = 12\widehat{s}\widehat{\lambda}m$; $\sigma = 12\lambda sN$; T_m: the cost of executing a multiplication operation in Z_q; T_{sp}: the cost of executing the Samplepre algorithm in [12].

$\langle \text{ID}_i, t, T_{1i}, T_{\text{ID},t}\rangle$, respectively. Then, $\mathscr{C}$ randomly chooses $\mathbf{y}_j, \mathbf{z}_1, \mathbf{z}_2 \in D_\sigma^N$ and computes $\mathbf{c}_j = (\mathbf{z}_1 + h\cdot\mathbf{z}_2 - \mathbf{y}_j)/(P_{\text{ID}i} + T_{1i})$. $\mathscr{C}$ adds $\langle \mathbf{y}_j, \mu_j, \mathbf{c}_j\rangle$ in the list L_2 and returns the signature $(\mathbf{z}_1, \mathbf{z}_2, \mathbf{c}_j)$ on μ_j. Even though the challenger $\mathscr{C}$ does not hold the associated initial key and time update key, the generated tuple $(\mathbf{z}_1, \mathbf{z}_2, \mathbf{c}_j)$ is still a valid signature. The reason is that the signature $(\mathbf{z}_1, \mathbf{z}_2, \mathbf{c}_j)$ can pass the verification

$$\begin{aligned}&\mathbf{z}_1 + h\cdot\mathbf{z}_2 - \left(H_0(\text{ID}) + H_1(\text{ID}, t)\right)\cdot\mathbf{c}_j\\ &= \mathbf{z}_1 + h\cdot\mathbf{z}_2 - \left(P_{\text{ID}i} + T_{1i}\right)\cdot\frac{\left(\mathbf{z}_1 + h\cdot\mathbf{z}_2 - \mathbf{y}_j\right)}{\left(P_{\text{ID}i} + T_{1i}\right)}\\ &= \mathbf{y}_j.\end{aligned} \tag{10}$$

(g) *Forgery.* Finally, the adversary $\mathscr{A}$ forges a valid signature tuple $(\mathbf{z}_1^*, \mathbf{z}_2^*, \mathbf{c}_j^*)$ on message μ^* for identity ID^* at the period t^* with nonnegligible probability. Note that ID^* is not issued during the *initial key extract* query or (ID^*, t^*) is not issued during the *time key update* query.

When the adversary $\mathscr{A}$ successfully forges a valid signature $(\mathbf{z}_1^*, \mathbf{z}_2^*, \mathbf{c}_j^*)$, we then use the Forking lemma in [22] to generate another valid signature $(\mathbf{z}_1', \mathbf{z}_2', \mathbf{c}_j')$ of the message μ^* such that $\|(\mathbf{z}_1^*, \mathbf{z}_2^*)\| \le 2\sigma\sqrt{2N}$ and $\|(\mathbf{z}_1', \mathbf{z}_2')\| \le 2\sigma\sqrt{2N}$. Since $(\mathbf{z}_1^*, \mathbf{z}_2^*, \mathbf{c}_j^*)$ and $(\mathbf{z}_1', \mathbf{z}_2', \mathbf{c}_j')$ are two valid signatures for $(\mu^*, \text{ID}^*, t^*)$, we have the equality

$$\begin{aligned}&H_2\left(\mathbf{z}_2^* + h\cdot\mathbf{z}_2^* - \left(H_0(\text{ID}^*) + H_1(\text{ID}^*, t^*)\right)\cdot\mathbf{c}^*, \mu^*\right)\\ &= H_2\left(\mathbf{z}_2' + h\cdot\mathbf{z}_2' - \left(H_0(\text{ID}^*) + H_1(\text{ID}^*, t^*)\right)\right.\\ &\left.\cdot\,\mathbf{c}', \mu^*\right)\end{aligned} \tag{11}$$

which implies that

$$\begin{aligned}&\mathbf{z}_2^* + h\cdot\mathbf{z}_2^* - \left(H_0(\text{ID}^*) + H_1(\text{ID}^*, t^*)\right)\cdot\mathbf{c}^*\\ &= \mathbf{z}_2' + h\cdot\mathbf{z}_2'\left(H_0(\text{ID}^*) + H_1(\text{ID}^*, t^*)\right)\cdot\mathbf{c}'.\end{aligned} \tag{12}$$

Since we have $H_0(\text{ID}^*) = \mathbf{s}_1 + h\cdot\mathbf{s}_2$ and $H_1(\text{ID}^*) = \mathbf{s}_3 + h\cdot\mathbf{s}_4$, we obtain

$$\begin{aligned}&\mathbf{z}_1^* - \mathbf{z}_1' - \mathbf{s}_1\left(\mathbf{c}^* - \mathbf{c}'\right) - \mathbf{s}_3\left(\mathbf{c}^* - \mathbf{c}'\right) + h\\ &\cdot\left(\mathbf{z}_2^* - \mathbf{z}_2' - \mathbf{s}_2\left(\mathbf{c}^* - \mathbf{c}'\right) - \mathbf{s}_4\left(\mathbf{c}^* - \mathbf{c}'\right)\right) = 0.\end{aligned} \tag{13}$$

We set $(\mathbf{u}_1, \mathbf{u}_2) = (\mathbf{z}_1^* - \mathbf{z}_1' - \mathbf{s}_1(\mathbf{c}^* - \mathbf{c}') - \mathbf{s}_3(\mathbf{c}^* - \mathbf{c}'))$ and $\mathbf{z}_2^* - \mathbf{z}_2' - \mathbf{s}_2(\mathbf{c}^* - \mathbf{c}') - \mathbf{s}_4(\mathbf{c}^* - \mathbf{c}')$.

As $\|(\mathbf{s}_1, \mathbf{s}_2)\| < s\sqrt{2N}$ and $\|(\mathbf{s}_3, \mathbf{s}_4)\| < s\sqrt{2N}$ with overwhelming probability, we can see that $\|(\mathbf{u}_1, \mathbf{u}_2)\| \le 4s\sqrt{2N} + 2\lambda\sigma\sqrt{2N}$. Since $\mathbf{c}^* \ne \mathbf{c}'$ and by Lemma 13, we can obtain $\|(\mathbf{u}_1, \mathbf{u}_2)\| \ne 0$. According to [13], the probability that challenger $\mathscr{C}$ can solve the $R-$SIS on the NTRU lattice is at least $(1 - 2^{-\omega(\log N)})\varepsilon$. □

6. Comparisons

Table 1 presents the comparisons among Tian and Huang's IBS scheme [9], Xiang's RIBS scheme [15], and our RIBS scheme in terms of lattice type, signing key size, signature size, computation cost of signing phase, computation cost of verifying phase, revocable functionality, and security property under the same system parameter N.

Both Tian and Huang's IBS and Xiang's RIBS schemes adopted the GPV lattice in [11] to generate a user's signing key. In our scheme, we adopted the NTRU lattice in [14] to generate a user's signing key. It is obvious that both the signing key and signature sizes of our scheme are less than those of both Tian and Huang's IBS and Xiang's RIBS schemes. For the computation cost of the signing phase, both Tian and Huang's IBS scheme and ours use the rejection sampling technique to generate a signature, in which the rejection sampling technique would repeat the signing phase at average 7 times so that their total computation costs are, respectively, $7(Nm + mk)T_m$ and $7(N^2 + 2N)T_m$, where T_m is the cost of executing a multiplication operation in Z_q. In Xiang's RIBS scheme [15], a user runs the Samplepre algorithm in [12] to obtain a signature so that it requires $2NmT_m + T_{\text{sp}}$, where T_{sp} is the cost of executing the Samplepre algorithm. For the computation cost of the verifying phase, three schemes, respectively, require $(Nm+Nk)T_m$, $3NmT_m$, and $(N^2+N)T_m$. Since $m > 6N\log q$, it is clear that our scheme has better performance in terms of the computation costs for the signing

Table 2: Comparisons of the concrete instances.

	Tian and Huang's IBS scheme [9]	Xiang's RIBS scheme [15]	Our RIBS scheme
Signing key size in bits	1087044742	8309006384	92419
Signature size in bits	1127039723	1238468290	54726

Parameters: $N = 512$, $q \approx 2^{25}$, $k = 512$, $\lambda = 14$, $m = 89600$, and $n = 1000$.

and verifying phases. For the revocable functionality, Xiang's scheme uses secure channels to send periodic signing keys to nonrevoked users, which causes enormous computation workload to encrypt/decrypt the periodic signing keys for the PKG and users. In contract, our revocation mechanism adopts public channels to send the periodic time update keys. Based on the short integer solution (SIS) assumption over lattices, we proved that the proposed RIBS scheme provides existential unforgeability against adaptive chosen-message attacks (RID-UF-ACMA) for a revoked user and an outside adversary. Since Tian and Huang's IBS scheme did not provide a revocation mechanism, it was proven to be only ID-UF-ACMA secure.

Table 2 lists comparisons of the signing key and signature sizes under the parameters $N = 512$, $q \approx 2^{25}$, $k = 512$, $\lambda = 14$, $m = 89600$, and $n = 1000$. It turns out, in both sizes, that our scheme performs much better than the other two schemes.

7. Conclusions

In the article, we proposed a new RIBS scheme over NTRU lattice with a public channel. As compared to the existing IBS schemes over lattices, our RIBS scheme has better performance in terms of signature size, signing key size, and the revocation mechanism. Security analysis is made to prove that our RIBS scheme is existentially unforgeable under adaptive chosen-message attacks based on the SIS assumption in the random oracle model.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was partially supported by Ministry of Science and Technology, Taiwan, under Grant no. MOST105-2221-E-018-013.

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques (CRYPTO '84)*, vol. 196 of *Lecture Notes in Computer Science*, pp. 47–53, Springer, Santa Barbara, Calif, USA, 1984.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Annual International Cryptology Conference: CRYPTO 2001: Advances in Cryptology—CRYPTO 2001*, pp. 213–229, Springer, Berlin, Germany, 2001.

[3] A. Boldyreva, V. Goyal, and V. Kumart, "Identity-based encryption with efficient revocation," in *Proceedings of the 15th ACM conference on Computer and Communications Security (CCS '08)*, pp. 417–426, ACM, Alexandria, Va, USA, October 2008.

[4] Y.-M. Tseng and T.-T. Tsai, "Efficient revocable ID-based encryption with a public channel," *Computer Journal*, vol. 55, no. 4, pp. 475–486, 2012.

[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[6] M. Ruckert, "Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles," in *Post-Quantum Cryptography: Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25–28, 2010. Proceedings*, vol. 6061 of *Lecture Notes in Computer Science*, pp. 182–200, Springer, Berlin, Germany, 2010.

[7] Z. Liu, Y. Hu, X. Zhang, and F. Li, "Efficient and strongly unforgeable identity-based signature scheme from lattices in the standard model," *Security and Communication Networks*, vol. 6, no. 1, pp. 69–77, 2013.

[8] M. Tian, L. Huang, and W. Yang, "Efficient hierarchical identity-based signatures from lattices," *International Journal of Electronic Security and Digital Forensics*, vol. 5, no. 1, article 110, 2013.

[9] M. Tian and L. Huang, "Efficient identity-based signature from lattices," *IFIP Advances in Information and Communication Technology*, vol. 428, pp. 321–329, 2014.

[10] J. Xie, Y.-P. Hu, J.-T. Gao, and W. Gao, "Efficient identity-based signature over NTRU lattice," *Frontiers of Information Technology and Electronic Engineering*, vol. 17, no. 2, pp. 135–142, 2016.

[11] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC '08)*, pp. 197–206, May 2008.

[12] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2010: Advances in Cryptology—EUROCRYPT 201*, vol. 6110 of *Lecture Notes in Computer Science*, pp. 523–552, Springer, Berlin, Germany, 2010.

[13] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology—EUROCRYPT 2012. EUROCRYPT 2012*, vol. 7237 of *Lecture Notes in Computer Science*, pp. 738–755, Springer, 2012.

[14] L. Ducas, V. Lyubashevsky, and T. Prest, "Efficient identitybased encryption over NTRU lattices," in *Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '14)*, vol. 8874 of *Lecture Notes in Computer Science*, pp. 22–41, Springer, Kaoshiung, Taiwan, December 2014.

[15] X. Xiang, "Adaptive secure revocable identity-based signature scheme over lattices," *Computer Engineering*, vol. 41, no. 10, pp. 126–129, 2015.

[16] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pp. 99–108, Philadelphia, Pa, USA, May 1996.

[17] J. Hoffstein, J. Pipher, and J. H. Silverman, "Ntru: a new high speed public key cryptosystem," in *Proceedings of the 3rd International Symposiun on Algorithmic Number Theory (Crypto '96)*, Lecture Notes in Computer Science, pp. 267–288, Springer, Portland, Ore, USA, June 1998.

[18] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silveman, and W. Whyte, "Ntrusign: digital signatures using the ntru lattice," in *Proceedings of the Cryptographers' Track at the RSA Conference 2003*, Lecture Notes in Computer Science, pp. 122–140, Springer, San Francisco, Calif, USA, April 2003.

[19] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267–302, 2007.

[20] D. Stehle and R. Steinfeld, "Making NTRUEnrypt and NTRUSign as secure as standard worst-case problems over ideal lattices," IACR Cryptology ePrint Archive 2013/4, 2013.

[21] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Proceedings of the EUROCRYPT 2010*, vol. 6110 of *Lecture Notes in Computer Science*, pp. 1–23, Springer, 2010.

[22] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361–396, 2000.