Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 1742386, 13 pages
https://doi.org/10.1155/2019/1742386

Research Article

Provably Secure Identity-Based Encryption and Signature over Cyclotomic Fields

Yang Wang,[1] Mingqiang Wang,[1] Jingdan Zou,[1] Jin Xu,[1] and Jing Wang[2]

[1]*School of Mathematics, Shandong University, Jinan Shandong 250100, China*
[2]*Shandong Branch of China Mobile Online Service Co. Ltd., Jinan Shandong 250100, China*

Correspondence should be addressed to Mingqiang Wang; wangmingqiang@sdu.edu.cn

Received 29 March 2019; Revised 29 May 2019; Accepted 8 July 2019; Published 17 October 2019

Guest Editor: Zaobo He

Copyright © 2019 Yang Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Identity-based cryptography is a type of public key cryptography with simple key management procedures. To our knowledge, till now, the existing identity-based cryptography based on NTRU is all over power-of-2 cyclotomic rings. Whether there is provably secure identity-based cryptography over more general fields is still open. In this paper, with the help of the results of collision resistance preimage sampleable functions (CRPSF) over cyclotomic fields, we give concrete constructions of provably secure identity-based encryption schemes (IBE) and identity-based signature schemes (IBS) based on NTRU over any cyclotomic field. Our IBE schemes are provably secure under adaptive chosen-plaintext and adaptive chosen-identity attacks, meanwhile, our IBS schemes are existentially unforgeable against adaptively chosen message and adaptively chosen identity attacks for any probabilistic polynomial time (PPT) adversary in the random oracle model. The securities of both schemes are based on the worst-case approximate shortest independent vectors problem (SIVP_γ) over corresponding ideal lattices. The secret key size of our IBE (IBS) scheme is short—only one (two) ring element(s). The ciphertext (signature) is also short—only two (three) ring elements. Meanwhile, as the case of NTRUEncrypt, our IBE scheme could encrypt n bits in each encryption process. These properties may make our schemes have more advantages for some IoT applications over postquantum world in theory.

1. Introduction

Nowadays, Internet of things (IoT) plays an extremely important role by comprising millions of smart and connected devices to offer benefits in a wide range of situations, for example, smart cities, smart grads, smart traffic, and smart buildings. The corresponding techniques have been unprecedentedly developed and adopted due to the quick evolution of smart devices and the continuous investment of leading communities. In a smart IoT system, data collected by mote devices will be transferred to gateway/cloud; the cloud will perform data analysis and send the results to the particular management system which takes suitable action. How to protect this complete network against malicious events, as well as the privacy and authenticity of data, is one of the toughest challenges for the deploying IoT technology. Several considerations and solutions are discussed in [1–4]. Due to the constrained resources (i.e., the size of memory, CPU speed, and network bandwidth), we could not directly use the traditional public key system, since the key management is complicated and the computations and storages may consume large amount of resources.

Identity-based cryptography is a type of public key cryptography in which the public key of a user is some unique information about the identity of the user (e.g., a user's e-mail address and the MAC address of devices). This means that a sender who has access to the public parameters of the system can encrypt a message (verify a signature) by using the receiver's (signer's) identity as a public key. The receiver (signer) obtains its decryption (signing) key from a central authority, which needs to be trusted as it generates secret keys for every user. Such cryptographic primitives significantly simplify the key management procedures of certificated-based public key infrastructures.

IBE and IBS were proposed by Shamir [5]; from then on, a large number of papers have been published in this area, including IBE [6–12], IBS [13–17], and identity-based signcryption (sign-then-encrypt a message) schemes

[13, 18, 19]. Till now, the fully practical identity-based cryptographic primitives are based on bilinear pairings. With the rapid development of quantum computation, in a not-so-distant future, quantum computers are expected to break such systems, and it is urgent to design quantum-immune IBE and IBS schemes. Cryptographic primitives based on hard lattice problems are good candidates, and many such identity-based schemes were designed [6, 9, 10, 16]. However, the efficiency of these schemes is not very satisfactory, especially in the IoT applications. As we all know, cryptographic primitives based on NTRU usually have high efficiency [20] and are good candidates of lightweight cryptographic systems in the postquantum world. Therefore, IBE and IBS schemes based on NTRU may enjoy the advantages of high efficiency and quantum-immune at the same time.

To the best of our knowledge, the existing IBE [21] and IBS [17] based on NTRU are all over power-of-2 cyclotomic rings, in which NTT algorithm can be implemented and calculations can be done very fast. However, there are too many subfields in the corresponding cyclotomic fields, making these settings more sensitive to subfield attacks [22, 23, 24]. So, seeking constructions of IBE and IBS over more general fields is a meaningful work. Meanwhile, strictly speaking, both of the schemes [17, 21] lack a security proof in the following two senses: (1) The PPT key generation algorithm [21] is heuristic and the CPA security of the schemes is guaranteed by a key-encapsulation mechanism designed in the process of encryption and is measured by the Kullback–Leibler "distance"—not statistical distance. Then, security is estimated in the aspect of attacks. So, the magnitude of module q is small and the schemes are practical. (2) Parameter settings of IBS [17] were referred to [25]; while the main lemma for proving the PPT trapdoor generation algorithm of CRPSF in [25] had some deficiencies, making the parameter choices in [17] could not achieve the desired result.

1.1. Our Contributions and Technique Overview. Motivated by the above reasons, we construct provably secure IBE and IBS schemes over any cyclotomic field.

Compared with [21], our IBE scheme is strictly provably secure under adaptive chosen-plaintext and adaptive chosen-identity attacks. So, at a high level, our result implies that we can heuristically design IBE scheme by using similar parameters as [21] in any cyclotomic field. Since we use the modified algorithms of CRPSF proposed in [26], our IBS scheme is existentially unforgeable against adaptively chosen message and adaptively chosen identity attacks in theory. Though the efficiency of our IBE and IBS schemes may be not satisfactory when we set parameters to achieve the provably security, our results give a high-level implication that we can heuristically design IBE and IBS over any cyclotomic field with small parameters (for example, settings of the classical NTRU-based cryptography [20]) and construct a lightweight cryptosystem, which can be used in some IoT applications.

Next, we give a brief review of constructions.

The construction of our IBE scheme is inspired by [21] and followed the route of [10]. The setup algorithm uses the key generation algorithm of CRPSF constructed in [26] to generate some public parameters **PP**, including a cyclotomic field K and an element $h \in R_q^\times$. Here, $R = \mathcal{O}_K$ is the ring of integers of K and $R_q^\times$ is the set of invertible elements of $R_q = R/qR$. Meanwhile, the key generation algorithm of CRPSF also outputs a short trapdoor basis of the NTRU lattice $\Lambda_h^q = \{(x, y) \in R^2 : y = hx \bmod qR\}$. The secret key of an identity (we map an identity to R_q by using a random oracle $H : \{0,1\}^* \mapsto R_q$) is the element in Λ_h^q outputted by the SamplePre algorithm of CRPSF by using the trapdoor basis. The encryption and decryption follow the idea of [10]. We embed the message in a Ring-LWE instance in the encryption process and the outputted ciphertext consists of two Ring-LWE instances (only the b-component) (u, v) with the "implied" relation that $v - u \cdot \mathbf{sk}$ is short. Then, the decryption process only need to remove the errors by rounding ($\lfloor \cdot \rceil$). Security (indistinguishability) is based on the hardness of corresponding decision Ring-LWE problems, and we do not need to use the key-encapsulation mechanism in the encryption process.

The construction of IBS follows the route of [17], which is a combination of techniques shown in [10, 27]. We also use the key generation algorithm of CRPSF to generate **Msk**. The secret key (σ_1, σ_2) of an identity **id** is produced by the SamplePre algorithm of CRPSF, satisfying $h\sigma_1 - \sigma_2 = H(\mathbf{id})$. The signing and verification follow the idea of [27] by using a rejection sampling algorithm. The signature of a message μ contains a triple (z_1, z_2, u) with $y_i \hookleftarrow D_{R,s}$, $z_i = y_i + \sigma_i \cdot u$, and $u = H'(hy_1 - y_2 \bmod qR, \mu)$. The rejection sampling algorithm could make it seem that z_i is independent of y_i, in particular, $z_i \hookleftarrow D_{R,s}$. Then, to verify a signature, one only needs to make sure that z_i is short and $u = H'(hz_1 - z_2 - H(\mathbf{id}) \cdot u \bmod qR, \mu)$. Unforgeability of our scheme can be reduced to the corresponding Ring-SIS problems.

Finally, we remark that techniques used in [28] are also vital to bound the decryption error of our IBE scheme. Though we design our IBE schemes in $R^\vee$, the dual ideal of R, we can convert it to work in an integral ideal of R or we can directly design the IBE scheme in R by using the hardness result shown in [29] (with larger parameter γ and q). Also, we can discuss the practicability under the Kullback–Leibler "distance" by using the same method as in [21]. Meanwhile, our construction provides an important support for designing IBE and IBS over general cyclotomic rings with relative small parameters (with no provably secure guarantee, but the key generation algorithm is PPT by our results) and analyzing the security from the view of attacks. How to reduce the magnitudes of parameters of provably secure identity-based cryptographic primitives and improve the efficiency of these schemes are important and meaningful open problems.

1.2. Organization. In Section 2, we will introduce some notations and basic results we need in our discussion. In Section 3, we shall discuss the IBE schemes, including the basic definitions, security models, constructions, and

security analysis. Discussions of IBS schemes are put in Section 4.

2. Preliminaries

In this section, we introduce some background results and notations.

2.1. Notations. We use $[n]$ to denote the set $\{1, 2, \ldots, n\}$. $\|\cdot\|$ represents the l_2 norm corresponding to the canonical embedding. For two random variables X and Y, $\Delta(X, Y)$ stands for their statistic distance. When we write $X \hookleftarrow \xi$, we mean that the random variable X obeys to a distribution ξ. If S is a finite set, then $|S|$ is its cardinality and $U(S)$ is the uniform distribution over S. Symbols $\mathbb{Z}^+$ and $\mathbb{R}^+$ stand for the sets of positive integers and positive reals. Symbol $\log x$ represents $\log_2 x$ for $x \in \mathbb{R}^+$. Functions $\varphi(n)$ and $\mu(n)$ stand for the Euler function and the Möbius function.

2.2. Cyclotomic Fields, Space H, and Ideal Lattices. Throughout this paper, we only consider cyclotomic fields. For a cyclotomic field $K = \mathbb{Q}(\zeta)$ with $\zeta = \zeta_l$ the primitive l-th root of unity, its minimal polynomial is $\Phi_l(x) = \prod_{i|l}(x^i - 1)^{\mu(l/i)} \in \mathbb{Z}[x]$ with degree $n = \varphi(l)$. As usual, we set $R = \mathcal{O}_K = \mathbb{Z}[\zeta]$, which is the ring of integers of K. Then, $[K : \mathbb{Q}] = n := 2r$, $K \cong \mathbb{Q}[x]/\Phi_l(x)$ and $R \cong \mathbb{Z}[x]/\Phi_l(x)$. K is Galois over $\mathbb{Q}$. We set $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_i : i = 1, \ldots, n\}$ and use the canonical embedding σ on K, which maps $x \in K$ to a space $\{\sigma_i(x)\}_i \in H := \{(x_1, \ldots, x_n) \in \mathbb{C}^n : x_{n+1-i} = \overline{x_i}, \forall i \in [r]\}$ via embeddings in $\mathrm{Gal}(K/\mathbb{Q})$. H is isomorphic to $\mathbb{R}^n$ as an inner product space via the orthonormal basis $h_{i\in[n]}$ defined as follows: for $1 \le j \le r$,

$$\begin{cases} h_j = \dfrac{1}{\sqrt{2}}\left(e_j + e_{n+1-j}\right), \\ \\ h_{n+1-j} = \dfrac{i}{\sqrt{2}}\left(e_j - e_{n+1-j}\right), \end{cases} \tag{1}$$

where $e_j \in \mathbb{C}^n$ is the vector with 1 in its j-th coordinate and 0 elsewhere and i is the imaginary number such that $i^2 = -1$. For any element $x \in K$, we can define its norm by $\|x\| := \|\sigma(x)\|$ and its infinity norm by $\|x\|_\infty := \max_{i\in[n]}|\sigma_i(x)|$.

We define a lattice as a discrete additive subgroup of H. The dual lattice of $\Lambda \subseteq H$ is defined as $\Lambda^\vee = \{y \in H : \forall x \in \Lambda, < x, \overline{y} > = \sum_{i=1}^n x_i \cdot y_i \in \mathbb{Z}\}$. One can check that this definition is actually the complex conjugate of the dual lattice as usually defined in $\mathbb{C}^n$. All of the properties of the dual lattice that we use also hold for the conjugate dual. Any fractional ideal I of K is a free $\mathbb{Z}$ module of rank n. So, $\sigma(I)$ is a lattice of H, and we call $\sigma(I)$ an ideal lattice and identify I with this lattice and associate with I all the usual lattice quantities. Meanwhile, its dual is defined as $I^\vee = \{a \in K : \mathrm{Tr}(a \cdot I) \subseteq \mathbb{Z}\}$. Then, it is easy to verify that $(I^\vee)^\vee = I$, $I^\vee$ is a fractional ideal, and $I^\vee$ embeds under σ as the dual lattice of I as defined above.

2.3. Gaussian Distributions, Ring-SIS Problems, and Ring-LWE Problems. The Gaussian distribution is defined as usual. For any $s > 0$, $c \in H$, which is taken to be $s = 1$ or $c = 0$ when omitted, define the Gaussian function $\rho_{s,c} : H \longrightarrow (0, 1]$ as $\rho_{s,c}(x) = e^{-\pi(\|x-c\|^2/s^2)}$. By normalizing this function, we obtain the continuous Gaussian probability distribution $D_{s,c}$ of parameter s, whose density function is given by $s^{-n} \cdot \rho_{s,c}(x)$. For a real vector $r = (r_1, \ldots, r_n) \in (\mathbb{R}^+)^n$, we define the elliptical Gaussian distributions in the basis $\{h_i\}_{i \le n}$ as follows: a sample from D_r is given by $\sum_{i\in[n]} x_i h_i$, where x_i is chosen independently from the Gaussian distribution D_{r_i} over $\mathbb{R}$. Note that if we define a map $\varphi : H \longrightarrow \mathbb{R}^n$ by $\varphi(\sum_{i\in[n]} x_i h_i) = (x_1, \ldots, x_n)$, then D_r is also a (elliptical) Gaussian distribution over $\mathbb{R}^n$.

For a lattice $\Lambda \subseteq H$, $\sigma > 0$ and $c \in H$, we define the lattice Gaussian distribution of support Λ, deviation σ, and center c by $D_{\Lambda,\sigma,c}(x) = (\rho_{\sigma,c}(x)/\rho_{\sigma,c}(\Lambda))$ for any $x \in \Lambda$. For $\delta > 0$, we define the smoothing parameter $\eta_\delta(\Lambda)$ as the smallest $\sigma > 0$ such that $\rho_{1/\sigma}(\Lambda^\vee \backslash 0) \le \delta$. The following theorem comes from [10, 30]. Here we use $\widetilde{B}$ to represent the Gram–Schmidt orthogonalization of B and regard the columns of B as a set of vectors. For $B = (b_1, \ldots, b_n)$, define $\|B\| = \max_i \|b_i\|$.

Theorem 1. *There is a probabilistic polynomial time algorithm that, given a basis B of an n-dimensional lattice $\Lambda = \mathscr{L}(B)$, a standard deviation $\sigma \ge \|\widetilde{B}\| \cdot \omega(\sqrt{\log n})$, and a $c \in H$, outputs a sample whose distribution is statistically close to $D_{\Lambda,\sigma,c}$.*

We will use following lemmata from [10, 31].

Lemma 1. *For any full-rank lattice Λ and positive real $\varepsilon > 0$, we have $\eta_\varepsilon(\Lambda) \le \sqrt{\ln(2n(1 + (1/\varepsilon)))/\pi} \cdot \lambda_n(\Lambda)$.*

Lemma 2. *For any full-rank lattice Λ, $c \in H$, $\varepsilon \in (0, 1)$ and $\sigma \ge \eta_\varepsilon(\Lambda)$, we have $Pr_{b \hookleftarrow D_{\Lambda,\sigma,c}}[\|b - c\| \ge \sigma\sqrt{n}] \le (1 + \varepsilon/1 - \varepsilon) \cdot 2^{-n}$.*

Lemma 3. *For any full-rank lattice $\Lambda \subseteq H$, $c \in H$, $\delta \in (0, 1)$, $\sigma \ge 2\eta_\delta(\Lambda)$ and $b \in \Lambda$, we have $D_{\Lambda,\sigma,c}(b) \le (1 + \delta/1 - \delta) \cdot 2^{-n}$.*

The following useful rejection sampling theorem comes from [27]. We state an adapted version, corresponding to the canonical embedding and space H. Its proof is essentially the same as that in [27], so we put it in Appendix with a remark that the constant M can be effectively calculated in practice.

Theorem 2. *Let $\Lambda \subseteq H$ be an arbitrary lattice, $V \subseteq H$ be a set in which all elements have norms less than T, σ be some elements in $\mathbb{R}$ such that $\sigma = \omega(T \cdot \sqrt{\log n})$, and $h : V \mapsto [0, 1]$ be a probability distribution. Then, there exists an absolute constant M such that the distribution of the output of the following algorithm $\mathscr{A}$:*

(1) $v \hookleftarrow h$

(2) $z \hookleftarrow D_{\Lambda,\sigma,v}$

(3) *Output* (z, v) *with probability* $\min(D_{\Lambda,\sigma}(z)/M \cdot D_{\Lambda,\sigma,v}(z), 1)$

is within statistical distance $2^{-\omega(\log n)}/M$ *of the distribution of the output of the following algorithm* $\mathcal{F}$*:*

(1) $v \hookleftarrow h$

(2) $z \hookleftarrow D_{\Lambda,\sigma}$

(3) *Output* (z, v) *with probability* $1/M$.

Moreover, the probability p *that* $\mathcal{A}$ *outputs something satisfies* $(1 - 2^{-\omega(\log n)})/M \le p \le (1/M)$.

The hard lattice problems we use are Ring-SIS and Ring-LWE problems. For an element $z = (z_1, \ldots, z_m) \in R^m$, let us define $\|z\| := (\sum_{i=1}^{m} \|z_i\|^2)^{1/2}$. We first introduce the Ring-SIS problem. The definition is as follows.

Definition 1. Let R be the ring of integers of K, q and m be positive integers, and β be a real number. The small integer solution problem over R (R-SIS$_{q,\,m,\,\beta}$) is given $a_1, \ldots, a_m \in R_q$ chosen independently from $U(R_q)$, find $z = (z_1, \ldots, z_m) \in R^m$ such that $\sum_{i=1}^{m} a_i z_i = 0 \bmod qR$ and $0 < \|z\| \le \beta$.

For appropriate parameters, the following theorem comes from [32], which shows that the Ring-SIS problem is hard.

Theorem 3. *For* $\varepsilon \in (0, 1)$*, there is a PPT reduction from solving Ideal-SIVP*$_{\gamma \cdot \sqrt{\ln(2n(1+1/(\varepsilon)))/\pi}}$ *with high probability in polynomial time in the worst case to solving R-SIS*$_{q,\,m,\,\beta}$ *with nonnegligible probability in polynomial time, for any* m, q, β, γ *such that* $\gamma \ge \beta\sqrt{n} \cdot \omega(\sqrt{\log n})$, $q \ge \beta\sqrt{n} \cdot \omega(\log n)$*, and* m, β, $\log q \le poly(n)$.

The Ring-LWE problem is defined as follows. Let $\mathbb{T} = H/R^\vee$.

Definition 2. For $s \in R_q^\vee$ and an error distribution ψ over H, the Ring-LWE distribution $A_{s,\psi}^\vee$ over $R_q \times \mathbb{T}$ is sampled by independently choosing a uniformly random $a \hookleftarrow U(R_q)$ and an error term $e \hookleftarrow \psi$ and outputting $(a, b = (a \cdot s/q) + e \bmod R^\vee)$.

Definition 3. Let Ψ be a family of distributions over H. The average-case Ring-LWE decision problem, denoted R–DLWE$_{q,\Psi}^\vee$, is to distinguish (with nonnegligible advantage) between independent samples from $A_{s,\psi}^\vee$ for a random choice of $(s, \psi) \hookleftarrow U(R_q^\vee) \times \Psi$ and the same number of uniformly random and independent samples from $R_q \times \mathbb{T}$.

In [33], a reduction from Ideal-SIVP$_\gamma$ to decision Ring-LWE problem over any algebraic number field is given.

Theorem 4. *Let* K *be an algebraic number field and* $R = \mathcal{O}_K$*,* $[K : \mathbb{Q}] = n$*. Assume* $\alpha \in (0, 1)$ *such that* $\alpha \le \sqrt{\log n/n}$*, and let* $q \ge 2$ *be an integer such that* $\alpha q \ge \omega(1)$*. Then there is a polynomial time quantum reduction from Ideal-SIVP*$_\gamma$ *(in the worst case) to* $R - DLWE_{q,D_\xi}^\vee$*, where* $\xi = \alpha(nk/\log(nk))^{1/4}$ *with* k *the number of samples to be used and* $\gamma = \omega(\sqrt{n} \cdot \log n/\alpha)$.

We can modify the sample (a, b) of Ring-LWE distribution to $R_q \times R_q^\vee$ as in [28]. We scale the b component by a factor of q, so that it is an element in $H/(qR^\vee)$. The corresponding error distribution is $D_{q\xi}$ with $\xi = \alpha \cdot (nk/\log(nk))^{1/4}$ and k the number of samples. Then, we discretize the error, by taking $e \hookleftarrow \lfloor D_{q\xi} \rceil_{R^\vee}$. The decision version of Ring-LWE becomes to distinguish between the modified distribution of $A_{s,\lfloor D_{q\xi} \rceil_{R^\vee}}^\vee$ and the uniform samples from $R_q \times R_q^\vee$. Notice that by using the same method proposed in [34], we can change the secret s to obey the error distributions, i.e., $s \hookleftarrow \lfloor D_{q\xi} \rceil_{R^\vee}$. We will use the symbol R – DLWE$_{q,\lfloor D_{q\xi} \rceil_{R^\vee}}$ to denote this problem. Meanwhile, note that, if we constrain $a \hookleftarrow U(T)$ for some $T \subseteq R_q$, where $|T| = c \cdot |R_q|$ and $c \ne \mathrm{negl}(n)$, the hardness of the corresponding problem does not decrease. We will use the symbol R – DLWE$_{q,\lfloor D_{q\xi} \rceil_{R^\vee}}^\times$ to denote this problem. For more details, one can refer to [28, 34].

2.4. Key Generation Algorithm and Regularity Result. In this subsection, we shall introduce some useful algorithms and results we need. The following algorithm plays a key role in our constructions of IBE and IBS. It is a modified version of key generation algorithm of traditional NTRU signatures. For simplicity, we denote it by N-KeyGen.

The following theorem comes from [26] (Algorithm 1). Note that in the case of cyclotomic fields, it was shown in [26] that the value of Dedekind zeta function at 2 (i.e. $\zeta_K(2)$) has a relatively small absolute upper bound.

Theorem 5. *Let* $K = \mathbb{Q}(\zeta_l)$ *be a cyclotomic field,* $R = \mathcal{O}_K$*,* $n = \varphi(l)$*,* $q \ge 64n\zeta_K(2)$ *be a prime such that* $q \nmid \Delta_K$ *and the prime ideal decomposition of* qR *in* R *is* $qR = \mathcal{B}_1, \ldots, \mathcal{B}_g$ *such that* $f \cdot g = n$*,* $\varepsilon > 0$ *be an arbitrary positive number. Assume that* $\sigma \ge \max\{8n^{3.6} \ln n, \omega(n \ln^{0.5} n) \cdot q^{1/g}, \omega(n^{0.25} q^{0.5} l^{-0.25})\}$*. Then, the key generation algorithm proposed in this section terminates in polynomial time, and the output matrix* $\begin{bmatrix} f & g \\ F & G \end{bmatrix}$ *is an* R *basis of* Λ_h^q *for* $h = gf^{-1} \bmod qR$*. Meanwhile, if* $\sigma \ge n^{3/2}\sqrt{\ln(8nq)} \cdot q^{(1/2)+(1+(f/2))\varepsilon}$*, the distribution of* h *is rejected with probability* $c < 1$ *for some absolute constant* c *from a distribution whose statistical distance from* $U(R_q^\times)$ *is* $\le (2^{8n}/q^{\lfloor \varepsilon n \rfloor})$.

Based on the N-KeyGen algorithm, Wang and Wang [26] gave a detailed construction of CRPSF, which was first proposed in [10], over any cyclotomic field. The preimage sampling algorithm of CRPSF is useful for us to design our IBE and IBS. We also use NTRUCRPSF (n, q, σ, s) to represent the CRPSF and only describe the results we need. For more details, one can refer to [26]. The construction of CRPSF is as follows:

(1) TrapGen $(1^n, q, \sigma)$: by running the N-KeyGen algorithm, we get a public key $h = g \cdot f^{-1} \in R_q^\times$ and a private key $\mathbf{sk} = \begin{bmatrix} f & g \\ F & G \end{bmatrix}$. The key h defines function $f_h(z) = f_h((z_1, z_2)) = hz_1 - z_2 \in R_q$ with domain $\mathcal{D}_n = \{z \in R^2 : \|z\| < s\sqrt{2n}\}$ and range $\mathfrak{R}_n = R_q$. The trapdoor of f_h is $\mathbf{sk}$.

(2) SampleDom $(1^n, q, s)$: sample $z \hookleftarrow D_{R^2,s}$, if $\|z\| \ge s \cdot \sqrt{2n}$, resample.

(i) **Input**: $n, q \in \mathbb{Z}^+$, $\sigma > 0$.
(ii) **Output**: A key pair $(\mathbf{sk}, \mathrm{pk}) \in R^{2\times 2} \times R_q^\times$.
(1) Sample f from $D_{R,\sigma}$, if $(f \bmod q) \notin R_q^\times$, resample.
(2) Sample g from $D_{R,\sigma}$, if $(g \bmod q) \notin R_q^\times$, resample.
(3) If $\|f\| \geq \sqrt{n}\sigma$ or $\|g\| \geq \sqrt{n}\sigma$, restart.
(4) If $(f, g) \neq R$, restart.
(5) Compute $F_q, G_q \in R$ such that $f \cdot G_q - g \cdot F_q = q$, e.g., using a Hermite normal form algorithm.
(6) Use Babai rounding nearest plane algorithm to approximate (F_q, G_q) in the lattice spanned by (f, g), let $r(f, g)$ be the output, set $(F, G) = (F_q, G_q) - r(f, g)$ for some $r \in R$.
(7) If $\|(F, G)\| > n\sigma\sqrt{l}$, restart.
(8) Return secret key $\mathbf{sk} = \begin{bmatrix} f & g \\ F & G \end{bmatrix}$ and public key $\mathrm{pk} = h = g \cdot f^{-1} \in R_q^\times$.

Algorithm 1

(3) SamplePre $(\mathbf{sk}, t)$: to find a preimage in $\mathcal{D}_n$ for a target $t \in \mathfrak{R}_n = R_q$ under f_h by using the trapdoor $\mathbf{sk}$, sample $z \hookleftarrow D_{\Lambda_h^q + c, s}$ with $\Lambda_h^q = \{(z_1, z_2) \in R^2 : z_2 = hz_1 \bmod qR\}$ and $c = (1, h - t)$. Return z.

Theorem 6. *Assume* $\sigma \geq \max\{8n^{3.6} \ln n, \omega(n \ln^{0.5} n) \cdot q^{(1/g)}, \omega(n^{0.25} q^{0.5} l^{-0.25}), n^{3/2}\sqrt{\ln(8nq)} \cdot q^{((1/2)+\varepsilon)}\}$ *for some* $\varepsilon \in (0, (1/2))$ *and* $s \geq n^{3/2} \cdot \sigma \cdot \omega(\log n)$. *Then, the constructed NTRUCRPSF* (n, q, σ, s) *is a CRPSF against ploy*(n) *time adversaries, assuming the hardness of the worst-case Ideal-SIVP*$_\gamma$ *over* K *against ploy*(n) *time adversaries, with* $\gamma = \widetilde{O}(n \cdot s)$.

We also need the following regularity theorem. For more details, one can refer to [26, 28, 29].

Theorem 7. *Let* K *be a cyclotomic field with* $[K : \mathbb{Q}] = n$, $R = \mathcal{O}_K$, $m \geq 2$, q *is a positive prime such that* $q \nmid \Delta_K$ *and the prime ideal decomposition of* qR *in* R *is* $qR = \mathcal{B}_1, \ldots, \mathcal{B}_g$, $\delta \in (0, (1/2))$, $\varepsilon > 0$, *and* $a_i \hookleftarrow U(R_q^\times)$ *for all* $i \in [m]$. *Assume* $t \hookleftarrow D_{R^m,\sigma}$ *with* $\sigma \geq n \cdot \sqrt{(\ln(2mn(1 + (1/\delta)))/\pi)} \cdot q^{(1/m)+\varepsilon}$. *Then, we have*

$$\Delta\left(\left(a_1, \ldots, a_m, \sum_{i=1}^{m} t_i a_i\right); U\left(\left(R_q^\times\right)^m \times R_q\right)\right) \leq 2\delta + 2^{2m(n+g)} q^{-\varepsilon mn}. \quad (2)$$

As in [28], we only use the powerful basis $\{\vec{p}_i\}_{i=1}^n$ of R and the decoding basis $\{\vec{d}_i\}_{i=1}^n$ of $R^\vee$. We mainly use the following definition and arrangements. More details can be found in [28].

Definition 4. Given a basis $B = \{b_1, \ldots, b_n\}$ of a fractional ideal J, for any $x \in J$ with $x = x_1 b_1 + \cdots + x_n b_n$, the B-coefficient embedding of x is defined as the vector $(x_1, \ldots, x_n)$ and the B-coefficient embedding norm of x is defined as $\|x\|_B^c = (\sum_{i=1}^n x_i^2)^{1/2}$.

Set $\widehat{l} = l$ when l is odd and $\widehat{l} = (l/2)$ when l is even. If $l = \prod_{i=1}^m p_i^{\alpha_i}$ for primes p_i, then we define $\mathrm{rad}(l) = \prod_{i=1}^m p_i$. If we represent $x \in R$ (or $R^\vee$) with respect to the powerful basis (or decoding basis), we have

$$\sqrt{\frac{l}{\mathrm{rad}(l)}}\|x\|_{\sigma(\vec{p})}^c \leq \|\sigma(x)\| \leq \sqrt{\widehat{l}}\|x\|_{\sigma(\vec{p})}^c, \quad \text{for } x \in R, \quad (3)$$

$$\frac{1}{\sqrt{\widehat{l}}}\|x\|_{\sigma(\vec{d})}^c \leq \|\sigma(x)\| \leq \sqrt{\frac{\mathrm{rad}(l)}{l}}\|x\|_{\sigma(\vec{d})}^c, \quad \text{for } x \in R^\vee. \quad (4)$$

We will omit the subscripts $\sigma(\vec{d})$ and $\sigma(\vec{p})$ in the following applications when it does not cause ambiguities.

When we write $x \bmod qR^\vee$, we use the representative element of the coset $x + qR^\vee$ as $\sum_{i=1}^N x_i \vec{d}_i$ with $x_i \in [-(q/2), (q/2))$. It is similar for element $x \in R$. Notice that $R \subseteq R^\vee$, and any element of R can also be represented as a $\mathbb{Z}$-linear combination of the decoding basis.

3. Identity-Based Encryption Schemes

In this section, we shall give the definition of IBE schemes and then construct a provably secure IBE scheme based on NTRU over any cyclotomic field.

3.1. Basic Definition and Security Model. We give the definition of IBE system first.

Definition 5. An identity-based encryption system consists of four PPT algorithms: **Setup, KeyGen, Encrypt,** and **Decrypt**.

(i) **Setup** (λ): *this algorithm takes as input a security parameter* λ *and generates public parameters* **PP** *and a master secret key* **Msk**.
(ii) **KeyGen** $(\mathbf{id}, \mathbf{Msk}, \mathbf{PP})$: *this algorithm uses the master secret key* **Msk** *to generate an identity private key* $\mathbf{sk}_{\mathbf{id}}$ *corresponding to an identity* **id**.
(iii) **Encrypt** $(\mathbf{PP}, \mathbf{id}, m)$: *this algorithm takes the public parameters* **PP** *to encrypt a message* m *for any given identity* **id**.
(iv) **Decrypt** $(c, \mathbf{sk}_{\mathbf{id}})$: *this algorithm decrypts ciphertext* c *by using the identity private key* $\mathbf{sk}_{\mathbf{id}}$ *if the identity of the ciphertext matches the identity of the private key.*

The security model of IBE is defined through the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{B}$. For a security parameter λ, let $\mathcal{M}_\lambda$ be the plaintext space and

$\mathscr{C}_\lambda$ be the ciphertext space. The game, which appraises the indistinguishability of plaintext under adaptive chosen-plaintext and adaptive chosen-identity attack (IND-ID-CPA), is defined as follows:

(i) **Setup**: $\mathscr{B}$ runs the algorithm **Setup** (λ) to get the public parameters **PP** and the master secret key **Msk**; then, it sends **PP** to $\mathscr{A}$ and keeps the master secret key **Msk**.

(ii) **Phase 1**: $\mathscr{A}$ adaptively issues private key queries $q_1, \ldots, q_k$ for identity $\mathbf{id}_1, \ldots, \mathbf{id}_k$. In each query q_i for $i = 1, \ldots, k$, $\mathscr{B}$ runs **KeyGen** to generate $\mathbf{sk}_{\mathbf{id}i}$ and sends it to $\mathscr{A}$.

(iii) **Challenge**: once $\mathscr{A}$ decides the **Phase 1** is over, it outputs a challenge identity $\mathbf{id}^*$, which has not been queried during **Phase 1**, and two plaintext message $m_0, m_1 \in \mathscr{M}_\lambda$. $\mathscr{B}$ chooses a random element $b \in \{0, 1\}$ uniformly and sends $c_b = \mathbf{Encrypt}(\mathbf{PP}, \mathbf{id}^*, m_b)$ to $\mathscr{A}$.

(iv) **Phase 2**: $\mathscr{A}$ adaptively issues more private key queries $q_{k+1}, \ldots, q_Q$ for identity $\mathbf{id}_{k+1}, \ldots, \mathbf{id}_Q$. The only requirement is that $\mathbf{id}^* \neq \mathbf{id}_i$ for any $i = k+1, \ldots, Q$.

(v) **Guess**: $\mathscr{A}$ outputs an element $b' \in \{0, 1\}$ and wins if and only if $b' = b$.

We refer to such an adversary $\mathscr{A}$ as an IND-ID-CPA adversary and define the advantage (in the security parameter λ) of $\mathscr{A}$ in attacking an IBE scheme $\mathscr{E}$ as $\mathrm{Adv}_{\mathscr{E},\mathscr{A}}(\lambda) = |\Pr(b' = b) - (1/2)|$.

Definition 6. For a security parameter λ, we say that an IBE scheme $\mathscr{E}$ is adaptively IND-ID-CPA secure if for any PPT adversary $\mathscr{A}$ that takes at most $Q = \mathrm{poly}(\lambda)$ private key queries, $\mathrm{Adv}_{\mathscr{E},\mathscr{A}}(\lambda) \leq \mathrm{negl}(\lambda)$.

3.2. Constructions of IBE Based on NTRU. Now, we can give the construction of IBE system over any cyclotomic field. The construction is inspired by [21], which follows the route of [10] and could be regarded as a generalization from power of 2 cyclotomic field to arbitrary cyclotomic field. The detailed construction is as follows, where Δ_K denotes the discriminant of K and $qR = \mathscr{B}_1, \ldots, \mathscr{B}_g$.

(i) **Setup** (λ): given a security parameter λ, first construct a set of parameters (K, R, q, σ, s) such that $K = \mathbb{Q}(\zeta_l)$ with $n = \varphi(l) \geq \lambda$, $R = \mathscr{O}_K$, and $q \geq 64n\zeta_K(2)$ such that $q \nmid \Delta_K$. Meanwhile, $\sigma \geq \max\{8n^{3.6}\ln n, \omega(n\ln^{0.5} n)\cdot q^{(1/g)}, \omega(n^{0.25} q^{0.5} l^{-0.25}), n^{(3/2)}\sqrt{\ln(8nq)}\cdot q^{(1/2)+\varepsilon}\}$ for some $\varepsilon \in (0, (1/2))$, $s \geq n^{(3/2)}\cdot\sigma\cdot\omega(\log n)$. Then, call the N-KeyGen algorithm to generate a public key h and a secret key $\mathbf{sk} = \begin{bmatrix} f & g \\ F & G \end{bmatrix} \in R^{2\times 2}$. Set the public parameters $\mathbf{PP} = (K, R, q, \sigma, R_q, R_q^\vee, h, H)$, where $H : \{0,1\}^* \mapsto R_q$ is a random oracle, and the master secret key $\mathbf{Msk} = \mathbf{sk} = \begin{bmatrix} f & g \\ F & G \end{bmatrix}$.

(ii) **KeyGen** $(\mathbf{id}, \mathbf{Msk}, \mathbf{PP})$: if the pair $(\mathbf{id}, \mathbf{sk}_{\mathbf{id}})$ is in the local storage, output $\mathbf{sk}_{\mathbf{id}}$ to the user **id**. Otherwise,

(1) Set $t = H(\mathbf{id}) \in R_q$.
(2) Take $(\sigma_1, \sigma_2) = \mathrm{SamplePre}(\mathbf{Msk}, t)$, where (σ_1, σ_2) satisfies $h\sigma_1 - \sigma_2 = t \bmod qR$.
(3) Output $\mathbf{sk}_{\mathbf{id}} = \sigma_1$ and keep the pair $(\mathbf{id}, \mathbf{sk}_{\mathbf{id}})$ in the local storage.

(iii) **Encrypt** $(\mathbf{PP}, \mathbf{id}, m)$: given a plaintext $m = \sum_{i=1}^n m_i \cdot \overrightarrow{d}_i \in R_q^\vee$ with coefficients $m_i \in \{0, 1\}$, the encryption process is as follows:

(1) Sample $r, e_1, e_2 \hookleftarrow \chi := \lfloor D_{\xi\cdot q}\rceil_{R^\vee}$ with $\xi = \alpha\cdot(nk/\log(nk))^{(1/4)}$, where $k = O(1)$ is a positive integer.
(2) Compute $t = H(\mathbf{id}) \in R_q$, $u = r\cdot h + e_1 \bmod qR^\vee$ and $v = t\cdot r + e_2 + (\lfloor q/4\rfloor)\cdot m \bmod qR^\vee$.
(3) Output the ciphertext $c = (u, v)$.

(iv) **Decrypt** $(c = (u, v), \mathbf{sk}_{\mathbf{id}})$: this algorithm first computes $w = v - u\cdot\mathbf{sk}_{\mathbf{id}} = \sum_{i=1}^n w_i \cdot \overrightarrow{d}_i \bmod qR^\vee$ and returns $m = \sum_{i=1}^n \lfloor(4/q)\cdot w_i\rceil \cdot \overrightarrow{d}_i \bmod qR^\vee$.

Note that we have $w = v - u\sigma_1 = rt + e_2 + (\lfloor q/4\rfloor)\cdot m - rh\sigma_1 - e_1\sigma_1 = (\lfloor q/4\rfloor)\cdot m + e \bmod qR^\vee$ where $e = e_2 - r\sigma_2 - e_1\sigma_1 \in R^\vee$ for some (σ_1, σ_2) satisfying $h\sigma_1 - \sigma_2 = t \bmod qR$. If $\|e\|_\infty^c < q/10$, then we get that w has the representation of the form $(\lfloor q/4\rfloor)\cdot m + e$ in $R_q^\vee$. Setting $w = \sum_{i=1}^n w_i \cdot \overrightarrow{d}_i$ and $e = \sum_{i=1}^n e_i' \cdot \overrightarrow{d}_i$, we can conclude that for any $q > 40$,

$$\frac{4}{q}w_i = \frac{4}{q}\lfloor\frac{q}{4}\rfloor\cdot m_i + \frac{4}{q}e_i' = \begin{cases} \frac{4}{q}e_i' \in \left(-\frac{2}{5}, \frac{2}{5}\right), & \text{if } m_i = 0, \\ \frac{4}{q}\lfloor\frac{q}{4}\rfloor + \frac{4}{q}e_i' \in \left(\frac{1}{2}, \frac{3}{2}\right), & \text{if } m_i = 1. \end{cases} \tag{5}$$

Therefore, the decryption process succeeds in recovering the encrypted message m whenever $\|e_2 - r\sigma_2 - e_1\sigma_1\|_\infty^c < (q/10)$. Now, we bound the probability that $\|e_2 - r\sigma_2 - e_1\sigma_1\|_\infty^c \geq (q/10)$. Here, $\|\cdot\|_\infty^c$ represents the basis-coefficient norm under the decoding basis with respect to the l_∞ norm.

Lemma 4. *Assume that $\alpha \in (0, 1)$ such that $\alpha \leq \sqrt{(\log n/n)}$ and let $q \geq 2$ be an integer such that $\alpha q \geq \omega(1)$; meanwhile, $\omega(n^{(3/2)}\sqrt{\log n \log\log n}\cdot\alpha^2\cdot q^2\cdot s) < (q/30\sqrt{2})$; then, we have $\|e_2 - r\sigma_2 - e_1\sigma_1\|_\infty^c < (q/10)$ with probability at least $1 - n^{-\omega(\sqrt{n\log n})}$.*

Proof. Lemma 5.1 of [28] implies that $\Pr_{x\hookleftarrow\chi}[\|x\|_\infty > \omega(\sqrt{n\log n}\cdot\alpha^2\cdot q^2)]] \leq n^{-\omega(\sqrt{n\log n})}$. Note that $\|(\sigma_1, \sigma_2)\| \leq \sqrt{2n}\cdot s$; we have

$$\begin{aligned}\left\|e_2 - r\sigma_2 - e_1\sigma_1\right\|_\infty^c &\le \sqrt{\hat{l}} \cdot \left(\left\|e_2\right\| + \left\|r \cdot \sigma_2\right\| + \left\|e_1 \cdot \sigma_1\right\|\right) \\ &\le \sqrt{\hat{l}} \cdot \Big(\sqrt{n} \cdot \left\|e_2\right\|_\infty + \|r\|_\infty \cdot \left\|\sigma_2\right\| \\ &\quad + \left\|e_1\right\|_\infty \cdot \left\|\sigma_1\right\|\Big).\end{aligned} \tag{6}$$

Therefore, we get

$$\left\|e_2 - r\sigma_2 - e_1\sigma_1\right\|_\infty^c \le 3\sqrt{2} \cdot \omega'\left(n^{(3/2)}\sqrt{\log n \log\log n} \cdot \alpha^2 \cdot q^2 \cdot s\right), \tag{7}$$

with probability at least $1 - n^{-\omega(\sqrt{n\log n})}$, where we have used that $\sqrt{\hat{l}} = O(\sqrt{n\log\log n})$.

Overall, we get the following lemma. □

Lemma 5. *Assume that $\alpha \in (0,1)$ such that $\alpha \le \sqrt{(\log n/n)}$ and let $q \ge 2$ be an integer such that $\alpha q \ge \omega(1)$; meanwhile, $\omega(n^{(3/2)}\sqrt{\log n \log\log n} \cdot \alpha^2 \cdot q^2 \cdot s) < (q/30\sqrt{2})$; then, the decryption algorithm of the IBE scheme succeeds in recovering the encrypted message with probability at least $1 - n^{-\omega(\sqrt{n\log n})}$.*

We can prove that our IBE scheme is secure, assuming that $\mathrm{R-DLWE}_{q,\lfloor D_{q\xi}\rceil_{R^\vee}}$ problem and $\mathrm{R-DLWE}^{\times}_{q,\lfloor D_{q\xi}\rceil_{R^\vee}}$ problem are hard. We first give a IND-CPA secure public key encryption scheme (denoted by BasicPub). Note that Lemma 5 is suitable for BasicPub as well.

(i) **Setup** (λ): given a security parameter λ, do as the **Setup** algorithm of IBE scheme. Set the public parameters $\mathbf{PP} = (K, R, q, \sigma, R_q, R_q^\vee, h)$.

(ii) **KeyGen** $(\mathbf{PP})$: sample $(\sigma_1, \sigma_2) = \mathrm{SampleDom}(\mathbf{PP})$; set the secret key $sk = \sigma_1$ and the public key $\mathrm{pk} = h\sigma_1 - \sigma_2 \bmod qR$.

(iii) **Encrypt** $(\mathbf{PP}, \mathrm{pk}, m)$: do as the **Encrypt** algorithm of IBE scheme with $t = pk$.

(iv) **Decrypt** $(c = (u, v), \mathrm{sk})$: the same as the **Decrypt** algorithm of IBE scheme.

Lemma 6. *Let $K = \mathbb{Q}(\zeta_l)$ be a cyclotomic field, $n = \varphi(l)$, $R = \mathcal{O}_K$, and $q \ge 64n\zeta_K(2)$ be a prime such that $q \nmid \Delta_K$. Set $\sigma \ge \max\{8n^{3.6}\ln n, \omega(n\ln^{0.5} n) \cdot q^{(1/2)}, \omega(n^{0.25}q^{0.5}l^{-0.25}), n^{3/2}\sqrt{\ln(8nq)} \cdot q^{(1/2)+\varepsilon}\}$ for some $\varepsilon \in (0, (1/2))$ and $s \ge n^{3/2} \cdot \sigma \cdot \omega(\log n)$; meanwhile, assume that $\alpha \in (0,1)$ such that $\alpha \le \sqrt{(\log n/n)}$, $\alpha q \ge \omega(1)$, and $\omega(n^{3/2}\sqrt{\log n \log\log n} \cdot \alpha^2 \cdot q^2 \cdot s) < (q/30\sqrt{2})$. Then, the BasicPub is IND-CPA secure assuming that $R - DLWE_{q,\lfloor D_{q\xi}\rceil_{R^\vee}}$ problem and $R - DLWE^{\times}_{q,\lfloor D_{q\xi}\rceil_{R^\vee}}$ problem are hard.*

Proof. Note that, by the property of SampleDom algorithm, the distribution of pk is statistically close to $U(R_q)$. Then, for a ciphertext (u, v) of either m_0 or m_1, by our choices of parameters, the entire view $(h, \mathrm{pk}, u, v) \in R_q^\times \times R_q \times R_q \times R_q^\vee$ of the adversary is indistinguishable from the uniform distribution, assuming the hardness of $\mathrm{R-DLWE}_{q,\lfloor D_{q\xi}\rceil_{R^\vee}}$ problem and $\mathrm{R-DLWE}^{\times}_{q,\lfloor D_{q\xi}\rceil_{R^\vee}}$ problem. Hence, the adversary could not distinguish the ciphertexts of 0 and 1. We get the results, as desired. □

Theorem 8. *Suppose that Lemma 6 holds, i.e., the BasicPub is correct and IND-CPA secure in the standard model; then, the IBE scheme is adaptively IND-ID-CPA secure in the random oracle model.*

Proof. Let $\mathscr{A}$ be a PPT adversary that attacks the IBE scheme with advantage δ by using $Q = \mathrm{poly}(n)$ distinct H queries. We shall construct an algorithm $\mathscr{B}$ to attack the BasicPub scheme with advantage (δ/Q). The algorithm $\mathscr{B}$ works as follows:

(1) $\mathscr{B}$ calls an oracle (or the challenger) to get the public parameters $\mathbf{PP}' = (K, R, q, \sigma, R_q, R_q^\vee, h)$ and a public key pk. Then, it sends the public parameters $\mathbf{PP} = (K, R, q, \sigma, R_q, R_q^\vee, h, H)$ to $\mathscr{A}$. Here, $\mathscr{B}$ simulates the random oracle H; meanwhile, $\mathscr{B}$ chooses an $i \in [Q]$ uniformly at random.

(2) $\mathscr{B}$ simulates the view of $\mathscr{A}$ as follows:

(i) **Hash queries:** on $\mathscr{A}$'s jth distinct query $\mathbf{id}_j$ to H, if $j = i$, then store the tuple $(\mathbf{id}_i, \mathrm{pk}, \perp)$ and return pk to $\mathscr{A}$. Otherwise, $j \ne i$, $\mathscr{A}$ runs the BasicPub.**KeyGen** $(\mathbf{PP}')$ to generate a public/secret key pair $(\mathbf{sk}_j, \mathrm{pk}_j)$, locally store the tuple $(\mathbf{id}_j, \mathrm{pk}_j, \mathbf{sk}_j)$, and return $\mathbf{sk}_j$ to $\mathscr{A}$.

(ii) **KeyGen queries:** when $\mathscr{A}$ asks for a secret key for an identity **id**, assume without loss of generality that $\mathscr{A}$ has already queried H on **id**. Retrieve the unique tuple $(\mathbf{id}, \mathrm{pk}, \mathbf{sk})$ from local storage. If $\mathbf{sk} = \perp$, then output a random bit and abort. Otherwise, return **sk** to $\mathscr{A}$.

(3) When $\mathscr{A}$ produces a challenge identity $\mathbf{id}^*$ which is distinct from all its secret key queries and two messages m_0, m_1, assume without loss of generality that $\mathscr{A}$ has already queried H on $\mathbf{id}^*$. If $\mathbf{id}^* \ne \mathbf{id}_i$, output a random bit and abort. Otherwise, return $c_b = \mathrm{BasicPub.}\mathbf{Encrypt}(\mathbf{PP}', \mathrm{pk}, m_b)$ for $b \hookleftarrow U(\{0,1\})$ to $\mathscr{A}$.

When $\mathscr{A}$ terminates with some output, $\mathscr{B}$ terminates with the same output.

Assume $\mathscr{A}$ makes N distinct **KeyGen queries** for some $N \le Q$. Notice that the probability that $\mathscr{B}$ does not abort is

$$\begin{aligned}\Pr &= \left(1 - \frac{1}{Q}\right) \cdot \left(1 - \frac{1}{Q-1}\right) \cdots \left(1 - \frac{1}{Q-(N-1)}\right) \\ &\quad \cdot \frac{1}{Q-N} = \frac{1}{Q}.\end{aligned} \tag{8}$$

Meanwhile, conditioned on $\mathcal{B}$ not aborting, the view it provides to $\mathcal{A}$ is statistically close to the view of the real IBE scheme. Hence, the advantage that $\mathcal{B}$ attacks the IND-CPA secure of BasicPub is (δ/Q), as desired.

Overall, we conclude the following theorem. □

Theorem 9. *Let $K = \mathbb{Q}(\zeta_l)$ be a cyclotomic field, $n = \varphi(l)$, $R = \mathcal{O}_K$, and $q \geq 64n\zeta_K(2)$ be a prime such that $q \nmid \Delta_K$. Set $\sigma \geq \max\{8n^{3.6}\ln n, \omega(n\ln^{0.5} n)\cdot q^{1/g}, \omega(n^{0.25}q^{0.5}l^{-0.25}), n^{3/2}\sqrt{\ln(8nq)}\cdot q^{(1/2)+\varepsilon}\}$ for some $\varepsilon \in (0,(1/2))$ and $s \geq n^{3/2}\cdot\sigma\cdot\omega(\log n)$; meanwhile, assume that $\alpha \in (0,1)$ such that $\alpha \leq \sqrt{(\log n/n)}$, $\alpha q \geq \omega(1)$, and $\omega(n^{3/2}\sqrt{\log n \log\log n}\cdot\alpha^2\cdot q^2\cdot s) < (q/30\sqrt{2})$. Then, the IBE scheme is adaptively IND-ID-CPA secure against any PPT adversary in the random oracle model, assuming the hardness of worst-case Ideal-SIVP$_\gamma$ over K against PPT adversaries, with $\gamma = \widetilde{O}(n^2\cdot s)$.*

Remark 1. If we choose $\alpha q = \omega(1)$, then $s = \widetilde{O}(n^{7.5})$, $q = \widetilde{O}(n^9)$ and $\gamma = \widetilde{O}(n^{9.5})$. As remarked in [28], we can also convert our constructions to work in an ideal of R, or we can directly design our schemes in R (with larger γ and q). Moreover, when we require that $q = 1 \bmod l$ with l having some special cases (for example, $l = p^\alpha, 2^\alpha p$ or $2^\alpha pq$ for some prime p, q), we can use the hardness results shown in [35] and techniques shown in [36] to reduce the magnitude of the parameters q and γ. Usually, the module q is far away from practicality. A heuristic practical choice of parameters (with respect to coefficient embedding) is shown in [21]. How to reduce the size of q and γ is a hard problem which is worth studying.

4. Identity-Based Signature Schemes

In this section, we shall give the definition of IBS schemes and then construct a provably secure IBS scheme based on NTRU over any cyclotomic field.

4.1. Basic Definition and Security Model. We give the definition of IBS system first.

Definition 7. An identity-based signature system consists of four PPT algorithms: **Setup**, **KeyGen**, **Sign**, and **Verification**.

(i) **Setup** (λ): this algorithm takes as input a security parameter λ and generates public parameters **PP** and a master secret key **Msk**.

(ii) **KeyGen** $(\mathbf{id}, \mathbf{Msk}, \mathbf{PP})$: this algorithm uses the master secret key **Msk** to generate an identity private key $\mathbf{sk_{id}}$ corresponding to an identity **id**.

(iii) **Sign** $(\mathbf{PP}, \mathbf{id}, \mathbf{sk_{id}}, \mu)$: this algorithm takes the public parameters **PP**, a message μ, an identity **id**, and the secret key $\mathbf{sk_{id}}$ to generate a signature Sig of μ.

(iv) **Verification** $(\mathbf{PP}, \mu, \mathrm{Sig}, \mathbf{id})$: on input of the identity **id**, the message μ, the parameters **PP**, and a signature Sig, this algorithm outputs 1 when the verification is correct (i.e., the signature is valid) and outputs 0 otherwise.

The security model of IBS is defined through the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{B}$. For a security parameter λ, let $\mathcal{M}_\lambda$ be the message space and $\mathcal{S}_\lambda$ be the signature space. The game, which appraises the property of existentially unforgeable against adaptively chosen message and adaptively chosen identity attacks, is defined as follows:

(i) **Setup**: $\mathcal{B}$ runs the algorithm **Setup** (λ) to get the public parameters **PP** and the master secret key **Msk**; then, it sends **PP** to $\mathcal{A}$ and keeps the master secret key **Msk**.

(ii) **Phase 1**: $\mathcal{A}$ adaptively issues private key queries $q_1, \ldots, q_k$ for identity $\mathbf{id}_1, \ldots, \mathbf{id}_k$. In each query q_i for $i = 1, \ldots, k$, $\mathcal{B}$ runs **KeyGen** to generate $\mathbf{sk_{id}}_i$ and sends it to $\mathcal{A}$.

(iii) **Challenge**: once $\mathcal{A}$ decides the **Phase 1** is over, it outputs an identity $\mathbf{id}^*$, which has not been queried during **Phase 1**.

(iv) **Phase 2**: $\mathcal{A}$ adaptively issues more queries $q_{k+1}, \ldots, q_Q$ where each query q_i is one of the following:

(1) Private key query for $\mathbf{id}_i \neq \mathbf{id}^*$: $\mathcal{B}$ responds as in **Phase 1**.

(2) Signature query for a message μ under identity $\mathbf{id}^*$: this query can be regarded as an oracle, and $\mathcal{B}$ runs the oracle to get a signature $\mathrm{Sig} = \mathbf{Sign}(\mathbf{PP}, \mathbf{id}^*, \mathbf{sk}^*_{\mathbf{id}}, \mu)$ and sends Sig to $\mathcal{A}$.

(v) **Forge**: $\mathcal{A}$ outputs a forge Sig^* for a message μ under identity $\mathbf{id}^*$. It wins if and only if one of the following two cases happens:

(1) If μ is queried in **Phase 2**, then we require that $\mathrm{Sig}^* \neq \mathrm{Sig}$, where Sig is the signature of μ that $\mathcal{A}$ got in **Phase 2**. Meanwhile, **Verification** $(\mathbf{PP}, \mu, \mathrm{Sig}^*, \mathbf{id}^*) = 1$.

(2) Otherwise, we simply require that **Verification** $(\mathbf{PP}, \mu, \mathrm{Sig}^*, \mathbf{id}^*) = 1$.

We define the advantage (in the security parameter λ) of $\mathcal{A}$ in attacking an IBS scheme $\mathcal{E}$ as $Adv_{\mathcal{E},\mathcal{A}}(\lambda) = |\Pr(\mathcal{A}\ \mathrm{wins}) - (1/2)|$.

Definition 8. For a security parameter λ, we say that an IBS scheme $\mathcal{E}$ is existentially unforgeable against adaptively chosen message and adaptively chosen identity attacks if for any PPT adversary $\mathcal{A}$ that takes at most $Q = \mathrm{poly}(\lambda)$ queries, $\mathrm{Adv}_{\mathcal{E},\mathcal{A}}(\lambda) \leq \mathrm{negl}(\lambda)$.

4.2. Constructions of IBS Based on NTRU. Now, we can give the construction of IBS system over any cyclotomic field. The detailed construction is as follows:

(i) **Setup** (λ): given a security parameter λ, first construct a set of parameters (K, R, q, σ, s) such that $K = \mathbb{Q}(\zeta_l)$ with $n = \varphi(l) \geq \lambda$, $R = \mathcal{O}_K$, and $q \geq 64n\zeta_K(2)$ such that $q \nmid \Delta_K$. Meanwhile, $\sigma \geq \max\{8n^{3.6}\ln n, \omega(n\ln^{0.5} n)\cdot q^{1/2}, \omega(n^{0.25}q^{0.5}l^{-0.25}), n^{3/2}\sqrt{\ln(8nq)}\cdot q^{(1/2)+\varepsilon}\}$ for some $\varepsilon \in (0, (1/2))$, $s \geq n^{3/2}\cdot\sigma\cdot\omega(\log n)$. Then, call the N-KeyGen algorithm to generate a public key h and a secret key $\mathbf{sk} = \begin{bmatrix} f & g \\ F & G \end{bmatrix} \in R^{2\times 2}$. Set the public parameters $\mathbf{PP} = (K, R, q, \sigma, R_q, R_q^{\vee}, h, H, H')$, where $H: \{0,1\}^* \mapsto R_q$ and $H': R_q \times \{0,1\}^* \mapsto R_q$ are two random oracles, and the master secret key $\mathbf{Msk} = \mathbf{sk} = \begin{bmatrix} f & g \\ F & G \end{bmatrix}$.

(ii) **KeyGen** $(\mathbf{id}, \mathbf{Msk}, \mathbf{PP})$: if the pair $(\mathbf{id}, \mathbf{sk_{id}})$ is in the local storage, output $\mathbf{sk_{id}}$ to the user **id**. Otherwise,

(1) Set $t = H(\mathbf{id}) \in R_q$.
(2) Take $(\sigma_1, \sigma_2) = \text{SamplePre}(\mathbf{Msk}, t)$, where (σ_1, σ_2) satisfies $h\sigma_1 - \sigma_2 = t \bmod qR$.
(3) Output $\mathbf{sk_{id}} = (\sigma_1, \sigma_2)$ and keep the pair $(\mathbf{id}, \mathbf{sk_{id}})$ in the local storage.

(iii) **Sign** $(\mathbf{PP}, \mathbf{id}, \mathbf{sk_{id}}, \mu)$: given a message μ, the signature process is as follows:

(1) Sample $y_1, y_2 \hookleftarrow D_{R,s}$.
(2) Compute $u = H'(hy_1 - y_2 \bmod qR, \mu) \in R_q$ and $z_i = y_i + \sigma_i \cdot u$ for $i = 1, 2$.
(3) Output the signature $\text{Sig} = (z_1, z_2, u)$ of message μ with probability $\min((D_{R^2,s}(z)/M \cdot D_{R^2,s,v}(z)), 1)$ with $v = (\sigma_1 u, \sigma_2 u)$ and $M = O(1)$ (in practice, M can be computed efficiently).

(iv) **Verification** $(\mathbf{PP}, \mu, \text{Sig}, \mathbf{id})$: for $\text{Sig} = (z_1, z_2, u)$, if $\|(z_1, z_2)\| \leq \sqrt{2n}\cdot s$ and $H'(hz_1 - z_2 - H(id)\cdot u \bmod qR, \mu) = u \in R_q$, output 1. Otherwise, output 0.

The signing algorithm outputs something with probability $\min((D_{R^2,s}(z)/M \cdot D_{R^2,s,(\sigma_1 u, \sigma_2 u)}(z)), 1)$, if nothing was output, the signer runs the signing algorithm again until some signature is outputted. Note that $hz_1 - z_2 - H(\mathbf{id})\cdot u = hy_1 - y_2 + (h\sigma_1 - \sigma_2)\cdot u - H(\mathbf{id})\cdot u = hy_1 - y_2 \bmod qR$. Meanwhile, Lemma 2 and Theorem 2.2 imply that $\|(z_1, z_2)\| \leq \sqrt{2n}\cdot s$ with overwhelming probability. We conclude the following lemma.

Lemma 7. *The IBS scheme proposed above satisfies correctness.*

The security of the IBS scheme can be reduced to the worst-case SIVP_γ problem over K.

Theorem 10. *Let $K = \mathbb{Q}(\zeta_l)$ be a cyclotomic field, $n = \varphi(l)$, $R = \mathcal{O}_K$, and $q \geq 64n\zeta_K(2)$ be a prime such that $q \nmid \Delta_K$. Assume that $\sigma \geq \max\{8n^{3.6}\ln n, \omega(n\ln^{0.5} n)\cdot q^{1/2}, \omega(n^{0.25}q^{0.5}l^{-0.25}), n^{3/2}\sqrt{\ln(8nq)}\cdot q^{(1/2)+\varepsilon}\}$ for some $\varepsilon \in (0, (1/2))$, $s \geq n^{3/2}\cdot\sigma\cdot\omega(\log n)$. The IBS scheme is existentially unforgeable against adaptively chosen message and adaptively chosen identity attacks for any PPT adversary in the random oracle model, assuming the hardness of worst-case Ideal-SIVP_γ over K against PPT adversaries, with $\gamma = \widetilde{O}(n\cdot s)$.*

Proof. Suppose that there is an adversary $\mathcal{A}$ which can break the existentially unforgeable IBS scheme with advantage δ; we can construct an algorithm $\mathcal{B}$ to solve the $\text{R}-\text{SIS}_{q,2,\beta}$ problem over K for $\beta = 2\sqrt{2n}\cdot s$. The interactions between $\mathcal{B}$ and $\mathcal{A}$ are described as follows:

(1) For an $\text{R-SIS}_{q,2,\beta}$ instance (a_1, a_2), if $(a_1, a_2) \notin (R_q^{\times})^2$, abort. Otherwise, $\mathcal{B}$ sends $h = a_2^{-1}\cdot a_1 \bmod qR \hookleftarrow U(R_q^{\times})$ to $\mathcal{A}$.

(2) $\mathcal{A}$ can adaptively query in the following ways. In general, we can assume that $\mathcal{A}$ has to query the random oracle H for **id** before it makes other kinds of queries.

(i) H query: at the beginning, $\mathcal{B}$ keeps an ID-list which consists of elements of the form $(\mathbf{id}, t_{\mathbf{id}}, \mathbf{sk_{id}})$. The list is empty initially. For a query of identity $\mathbf{id}^*$, if it is contained in the ID-list, $\mathcal{B}$ simply sends $t_{\mathbf{id}^*}$ to $\mathcal{A}$. Otherwise, $\mathbf{id}^*$ is fresh. $\mathcal{B}$ samples $z = (\sigma_1, \sigma_2) \hookleftarrow D_{R^2,s}$ and computes $t_{\mathbf{id}^*} = h\sigma_1 - \sigma_2 \bmod qR$. Then, $\mathcal{B}$ sends $t_{\mathbf{id}^*}$ to $\mathcal{A}$ and stores $(\mathbf{id}^*, t_{\mathbf{id}^*}, \mathbf{sk}_{\mathbf{id}^*} = (\sigma_1, \sigma_2))$ in the ID-list.

(ii) **KeyGen** query: given $\mathbf{id}^*$, $\mathcal{B}$ looks up the ID-list to find $\mathbf{sk}_{\mathbf{id}^*}$ corresponding to $\mathbf{id}^*$ and sends $\mathbf{sk}_{\mathbf{id}^*}$ to $\mathcal{A}$.

(iii) **Sign** query: $\mathcal{B}$ also keeps a SIGN-list which is empty initially and consists of elements of the form $(\mu, \mathbf{id}, (y_1, y_2), \mathbf{sk_{id}}, u, (z_1, z_2))$. To obtain the signature of message $\mu^* \in (0,1)^*$ under the identity $\mathbf{id}^*$, if $(\mu^*, \mathbf{id}^*)$ is in the SIGN-list, $\mathcal{B}$ simply sends (z_1^*, z_2^*, u^*) to $\mathcal{A}$. Otherwise, μ^* is fresh and $\mathcal{B}$ looks up the ID-list for $\mathbf{sk}_{\mathbf{id}^*}$ and runs **Sign** $(\mathbf{PP}, \mathbf{id}^*, \mathbf{sk}_{\mathbf{id}^*}, \mu^*)$ to get a signature (z_1^*, z_2^*, u^*). $\mathcal{B}$ sends (z_1^*, z_2^*, u^*) to $\mathcal{A}$ and stores $(\mu^*, \mathbf{id}^*, (y_1^*, y_2^*), \mathbf{sk}_{\mathbf{id}^*}, u^*, (z_1^*, z_2^*))$ in the SIGN-list. Here, (y_1^*, y_2^*) is obtained through the algorithm **Sign** $(\mathbf{PP}, \mathbf{id}^*, \mathbf{sk}_{\mathbf{id}^*}, \mu^*)$.

(iv) H' query: when $\mathcal{A}$ sends a message μ^* under identity $\mathbf{id}^*$ to $\mathcal{B}$ for the H' query, $\mathcal{B}$ finds the corresponding u^* in the SIGN-list and sends it to $\mathcal{A}$ (if μ^* is not in the SIGN-list, $\mathcal{B}$ implements **Sign** query for $(\mu^*, \mathbf{id}^*)$ and sends corresponding u^* obtained by **Sign** query to $\mathcal{A}$).

(3) Forge: after finishing the queries listed above, $\mathcal{A}$ outputs a forgery $(z_1^{*\prime}, z_2^{*\prime}, u^{*\prime})$ for $(\mathbf{id}^*, \mu^*)$ with a nonnegligible probability δ.

Note that, without loss of generality, we can assume that before outputting the attempted forgery $(z_1^{*\prime}, z_2^{*\prime}, u^{*\prime})$, $\mathcal{A}$ has made a query for **Sign** (or strictly speaking, $\mathcal{A}$ has made a query for H', but a H' query is equivalent to a **Sign** query, by our constructions), i.e. $u^{*\prime} = u^*$ for a u^* in the SIGN-list. $\mathcal{B}$ can get (z_1^*, z_2^*) from the SIGN-list, which satisfies $H'(hz_1^* - z_2^* - H(\mathbf{id}^*)\cdot u^*, \mu^*) = H'(hz_1^{*\prime} - z_2^{*\prime} - H(\mathbf{id}^*)\cdot u^{*\prime}, \mu^*) = u^* = u^{*\prime}$. Hence, we have $hz_1^* - z_2^* - H(\mathbf{id}^*)\cdot u^* = hz_1^{*\prime} - z_2^{*\prime} - H(\mathbf{id}^*)\cdot u^* \bmod qR$ (up to a negligible probability). Therefore, $a_1(z_1^* - z_1^{*\prime}) + a_2(z_2^{*\prime} - z_2^*) = 0 \bmod qR$. Let $z = (z_1^* - z_1^{*\prime}, z_2^{*\prime} - z_2^*)$; we have $\|z\|^2 = \|z_1^* - z_1^{*\prime}\|^2 + \|z_2^{*\prime} - z_2^*\|^2 \le 8ns^2$. Hence, if $z \neq 0$, it is a valid solution of $\mathrm{R-SIS}_{q,2,2\sqrt{2n}\cdot s}$.

Also, note that in order to give a valid forge, $\mathcal{A}$ needs to find $(z_1^{*\prime}, z_2^{*\prime})$ to fulfil that $\|(z_1^{*\prime}, z_2^{*\prime})\| \le \sqrt{2n}\cdot s$ and $hz_1^{*\prime} - z_2^{*\prime} = w \bmod qR$ for $w = hz_1^* - z_2^* \bmod qR$. Theorem 2.2 implies that we can regard $z_i^* \hookleftarrow D_{R,s}$. Theorem 2.7 implies that $w \hookleftarrow U(R_q)$. For any $w \in R_q$, the solutions of the equation $hx_1 - x_2 = w \bmod qR$ form a lattice $\Lambda' = (z_1^*, z_2^*) + \Lambda_h^q$. Hence, for the parameter choices of s and σ, Lemma 3 indicates that the probability that $z = 0$ is negligible. Therefore, except with some negligible probability $\varepsilon(n)$, we can solve $\text{R-SIS}_{q,2,2\sqrt{2n}\cdot s}$ with advantage $\delta' = (1 - \varepsilon(n))\delta$. □

Remark 2. By the conditions in Theorem 4.1, we can take $s = \widetilde{O}(n^7)$, $q = \widetilde{O}(n^8)$ and $\gamma = \widetilde{O}(n^8)$. Also, the module q is far away from practicality. How to reduce the size of q and γ is a hard problem which is worth studying.

One may note that the trapdoor generation algorithms used in IBE and IBS schemes are the same, so as the case of IBE in power-of-2 cyclotomic rings; we can also use the parameter choices (with respect to coefficient embedding) as in [21], together with the parameter choices of rejection sampling as in [27] to give a practical implementation of our schemes. A more heuristic implementation with respect to coefficient embedding in power-of-2 cyclotomic rings is also shown in [17].

Appendix

We first introduce a useful "rejection sampling" lemma which is a modified version of Lemma 4.7 in [27]. Their proof is essentially the same.

Lemma 8. *Let $V \subseteq H$ be an arbitrary set and $\Lambda \subseteq H$ be an arbitrary lattice. Assume $h : V \mapsto [0,1]$ and $f : \Lambda \mapsto [0,1]$ be probability distributions. If $g_v : \Lambda \mapsto [0,1]$ is a family of probability distributions indexed by all $v \in V$ with the property that*

$$\exists M \in \mathbb{R} \text{ such that } \forall v, \Pr_{z \hookleftarrow f}\left[M \cdot g_v(z) \ge f(z)\right] \ge 1 - \varepsilon, \tag{A.1}$$

then the distribution of the output of the following algorithm $\mathcal{A}$:

(1) $v \hookleftarrow h$

(2) $z \hookleftarrow g_v$

(3) *output* (z, v) *with probability* $\min(f(z)/M \cdot g_v(z), 1)$

is within statistical distance (ε/M) of the distribution of the output of the following algorithm $\mathcal{F}$:

(1) $v \hookleftarrow h$

(2) $z \hookleftarrow f$

(3) output (z, v) *with probability* $1/M$.

Moreover, the probability p that $\mathcal{A}$ outputs something satisfies $p \in [(1-\varepsilon)/M, (1/M)]$.

Proof. For each $v \in V$, define S_v to be the set that consists of all $z \in \Lambda$ such that $M \cdot g_v(z) \ge f(z)$. Notice that by definition, for all $z \in S_v$, the probability that $\mathcal{A}$ outputs z is $g_v(z)\min(f(z)/M \cdot g_v(z), 1) = (f(z)/M)$ and for all $z \notin S_v$, the probability that z is output is $g_v(z)$. Let p denote the probability that $\mathcal{A}$ outputs something. Then, we have

$$\begin{aligned} p &= \sum_{v \in V} h(v)\left(\sum_{z \in S_v} \frac{f(z)}{M} + \sum_{z \notin S_v} g_v(z)\right) \\ &\ge \sum_{v \in V} h(v) \sum_{z \in S_v} \frac{f(z)}{M} \ge \frac{1-\varepsilon}{M}, \end{aligned} \tag{A.2}$$

$$\begin{aligned} p &= \sum_{v \in V} h(v)\left(\sum_{z \in S_v} \frac{f(z)}{M} + \sum_{z \notin S_v} g_v(z)\right) \\ &\le \sum_{v \in V} h(v)\left(\sum_{z \in S_v} \frac{f(z)}{M} + \sum_{z \notin S_v} \frac{f(z)}{M}\right) = \frac{1}{M}. \end{aligned} \tag{A.3}$$

For the estimation of the statistical distance of the distribution of the output of $\mathcal{A}$ and $\mathcal{F}$, let $N_{\mathcal{A}}$ and $N_{\mathcal{F}}$ be the probabilities that $\mathcal{A}$ and $\mathcal{F}$ do not output anything, respectively. It is obvious that $N_{\mathcal{F}} = 1 - (1/M)$ and $1 - (1/M) \le N_{\mathcal{A}} \le 1 - (1-\varepsilon)/M$. Then, we have

$$\begin{aligned}
\Delta(\mathscr{A},\mathscr{F}) &= \frac{1}{2}\left(\sum_{z\in\Lambda,v\in V}|\mathscr{A}(z,v)-\mathscr{F}(z,v)| + \left|N_{\mathscr{A}}-N_{\mathscr{F}}\right|\right)\\
&= \frac{1}{2}\left(\sum_{z\in\Lambda}\sum_{v\in V}\left|h(v)g_v(z)\min\left(\frac{f(z)}{Mg_v(z)},1\right)-h(v)\frac{f(z)}{M}\right| + \left|N_{\mathscr{A}}-N_{\mathscr{F}}\right|\right)\\
&= \frac{1}{2}\left(\sum_{z\in\Lambda}\sum_{v\in V}h(v)\left|g_v(z)\min\left(\frac{f(z)}{Mg_v(z)},1\right)-\frac{f(z)}{M}\right| + \left|N_{\mathscr{A}}-N_{\mathscr{F}}\right|\right)\\
&= \frac{1}{2}\sum_{v\in V}h(v)\left(\sum_{z\in\Lambda}\left|g_v(z)\min\left(\frac{f(z)}{Mg_v(z)},1\right)-\frac{f(z)}{M}\right| + \left|N_{\mathscr{A}}-N_{\mathscr{F}}\right|\right)\\
&= \frac{1}{2}\sum_{v\in V}h(v)\left(\sum_{z\in S_v}\left|\frac{f(z)}{M}-\frac{f(z)}{M}\right| + \sum_{z\notin S_v}\left|g_v(z)-\frac{f(z)}{M}\right| + \left|N_{\mathscr{A}}-N_{\mathscr{F}}\right|\right)\\
&\le \frac{1}{2}\sum_{v\in V}h(v)\left(\sum_{z\notin S_v}\frac{f(z)}{M} + \left|N_{\mathscr{A}}-N_{\mathscr{F}}\right|\right) \le \frac{1}{2}\sum_{v\in V}h(v)\left(\frac{\varepsilon}{M}+\left(\left(1-\frac{1-\varepsilon}{M}\right)-\left(1-\frac{1}{M}\right)\right)\right),\\
&= \frac{\varepsilon}{M}.
\end{aligned} \tag{A.4}$$

The proof is finished.

The following lemma is helpful for us to estimate the upper bound of $|\langle z,v\rangle|$ for any $v\in\Lambda\subseteq H$ and $z\hookleftarrow D_{\Lambda,\sigma}$. □

Lemma 9. *For any lattice $\Lambda\subseteq H$, $v\in\Lambda$ and $t>0$, we have*

$$\Pr_{z\hookleftarrow D_{\Lambda,\sigma}}[|\langle z,v\rangle|>t]] \le 2\cdot e^{-\left(\pi t^2/\|v\|^2\cdot\sigma^2\right)}. \tag{A.5}$$

Proof. For any $r>0$, we have

$$\begin{aligned}
E\left[e^{\left(2\pi r/\sigma^2\right)\langle z,v\rangle}\right] &= \sum_{z\in\Lambda}\Pr(z)e^{\left(2\pi r/\sigma^2\right)\langle z,v\rangle},\\
&= \left(\sum_{y\in\Lambda}e^{\left(-\pi\|y\|^2/\sigma^2\right)}\right)^{-1}\\
&\quad\cdot\sum_{z\in\Lambda}e^{\left(-\pi\|z\|^2/\sigma^2\right)}\cdot e^{\left(2\pi/\sigma^2\right)\langle z,r\cdot v\rangle}\\
&= \left(\sum_{y\in\Lambda}e^{\left(-\pi\|y\|^2/\sigma^2\right)}\right)^{-1}\\
&\quad\cdot\sum_{z\in\Lambda}e^{-\pi\left(\|z-r\cdot v\|^2/\sigma^2\right)}\cdot e^{\left(\pi r^2\|v\|^2/\sigma^2\right)}\\
&= \frac{\rho_{\sigma,r\cdot v}(\Lambda)}{\rho_\sigma(\Lambda)}\cdot e^{\left(\pi r^2\|v\|^2/\sigma^2\right)}\\
&\le e^{\left(\pi r^2\|v\|^2/\sigma^2\right)},
\end{aligned} \tag{A.6}$$

where the last inequality has used the fact that $r\cdot v\in H$ and Lemma 2.9 of [31]. Therefore, by applying Markov's inequality, we get

$$\begin{aligned}
\Pr[\langle z,v\rangle>t] &= \Pr\left[e^{2\pi r/\sigma^2\langle z,v\rangle}>e^{\left(2\pi rt/\sigma^2\right)}\right]\\
&\le \frac{E\left[e^{\left(2\pi r/\sigma^2\right)\langle z,v\rangle}\right]}{e^{\left(2\pi rt/\sigma^2\right)}} \le e^{-\left(2\pi rt/\sigma^2\right)+\left(\pi r^2\|v\|^2/\sigma^2\right)}.
\end{aligned} \tag{A.7}$$

Taking $r=t/\|v\|^2$, we get $\Pr[\langle z,v\rangle>t]]\le e^{-\left(\pi t^2/\sigma^2\|v\|^2\right)}$. Then, applying the union bound gives us the required result.

The last lemma will be instrumental in bounding the success probability of our rejection sampling algorithm. □

Lemma 10. *For any lattice $\Lambda\subseteq H$ and $v\in\Lambda$, if $\sigma=\omega(\|v\|\cdot\sqrt{\log n})$, then there exists an absolute constant M such that*

$$\Pr_{z\hookleftarrow D_{\Lambda,\sigma}}\left[\frac{D_{\Lambda,\sigma}(z)}{D_{\Lambda,\sigma,v}(z)}<M\right]\ge 1-2^{\omega'(\log n)}. \tag{A.8}$$

Proof. By definition, for any $z\in\Lambda$, we have $(D_{\Lambda,\sigma}(z)/D_{\Lambda,\sigma,v}(z))=(\rho_\sigma(z)/\rho_{\sigma,v}(z))$, where we have used that $\rho_\sigma(\Lambda)=\rho_{\sigma,v}(\Lambda)$ for any $v\in\Lambda$. Therefore, we can deduce that

$$\frac{D_{\Lambda,\sigma}(z)}{D_{\Lambda,\sigma,v}(z)} = \frac{e^{-\pi\left(\|z\|^2/\sigma^2\right)}}{e^{-\pi\left(\|z-v\|^2/\sigma^2\right)}} = e^{\left(\pi/\sigma^2\right)\left(\|v\|^2-2\langle z,v\rangle\right)}. \tag{A.9}$$

By using Lemma 9 with $t=\omega((\sqrt{\log n}/2\pi)\cdot\|v\|\cdot\sigma)$, we get

$$e^{\pi/\sigma^2\left(\|v\|^2-2\langle z,v\rangle\right)} < e^{\pi/\sigma^2\left(\|v\|^2+2\omega\left(\left(\sqrt{\log n}/2\pi\right)\cdot\|v\|\cdot\sigma\right)\right)} = e^{1+(\pi/\omega(\log n))} = O(1), \tag{A.10}$$

with probability at least $1-2e^{-(1/4\pi)\omega(\log n)} = 1-2^{-\omega'(\log n)}$. We conclude the desired result. □

Proof of Theorem 2. We can let the set V in Lemma 8 be all vectors $v \in \Lambda$ of length at most T, the function f be $D_{\Lambda,\sigma}$, and the functions g_v be $D_{\Lambda,\sigma,v}$. Lemma 10 implies that there is an absolute constant M, which satisfies the requirements of Lemma 8. We get the result we need. □

Data Availability

No data were used to support this study. Any lemma or theorem cited in this paper can be obtained openly according to the reference.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was funded by the National Cryptography Development Fund (grant no. MMJJ20180210) and National Natural Science Foundation of China (grant nos. 61832012 and 61672019).

References

[1] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.

[2] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, p. 1.

[3] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Transactions on Industrial Informatics*, p. 1, 2019.

[4] X. Zheng, Z. Cai, and Y. Li, "Data linkage in smart internet of things systems: a consideration from a privacy perspective," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 55–61, 2018.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, G. R. Blakley and D. Chaum, Eds., Springer, Berlin, Germany, pp. 47–53, 1985.

[6] S. Agrawal, D. Boneh, and X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in *Proceedings of the 30th Annual Conference on Advances in Cryptology. CRYPTO'10*, pp. 98–115, Springer-Verlag, Santa Barbara, CA, USA, August 2010, http://dl.acm.org/citation.cfm?id=1881412.1881420.

[7] D. Boneh, X. Boyen, and E. J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Advances in Cryptology—EUROCRYPT 2005*, R. Cramer, Ed., Springer, Berlin, Germany, pp. 440–456, 2005.

[8] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology—CRYPTO 2001*, J. Kilian, Ed., pp. 213–229, Springer, Berlin, Germany, 2001.

[9] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," *Journal of Cryptology*, vol. 25, no. 4, pp. 601–639, 2012.

[10] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the fourtieth annual ACM symposium on Theory of computing—STOC 08*, pp. 197–206, ACM, Victoria, Canada, May 2008.

[11] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology—EUROCRYPT 2005*, R. Cramer, Ed., pp. 114–127, Springer, Berlin, Germany, 2005.

[12] B. Waters, "Dual system encryption: realizing fully secure ibe and hibe under simple assumptions," in *Advances in Cryptology—CRYPTO 2009*, S. Halevi, Ed., pp. 619–636, Springer, Berlin, Germany, 2009.

[13] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Advances in Cryptology—ASIACRYPT 2005*, B. Roy, Ed., Springer, Berlin, Germany, pp. 515–532, 2005.

[14] F. Hess, "Efficient identity based signature schemes based on pairings," in *Selected Areas in Cryptography*, K. Nyberg and H. Heys, Eds., Springer, Berlin, Germany, pp. 310–324, 2003.

[15] K. G. Paterson and J. C. N. Schuldt, "Efficient identity-based signatures secure in the standard model," in *Information Security and Privacy*, L. M. Batten and R. Safavi-Naini, Eds., Springer, Berlin, Germany, pp. 207–222, 2006.

[16] M. Rückert, "Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles," in *Post-quantum Cryptography*, N. Sendrier, Ed., Springer, Berlin, Germany, pp. 182–200, 2010.

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

[18] X. Boyen, "Multipurpose identity-based signcryption," in *Advances in Cryptology—CRYPTO 2003*, D. Boneh, Ed., Springer, Berlin, Germany, pp. 383–399, 2003.

[19] L. Chen and J. Malone-Lee, "Improved identity-based signcryption," in *Public Key Cryptography—PKC 2005*, S. Vaudenay, Ed., pp. 362–379, Springer, Berlin, Germany, 2005.

[20] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, "Choosing parameters for NTRUEncrypt," Cryptology ePrint Archive, Report 2015/708, 2015, https://eprint.iacr.org/2015/708.

[21] L. Ducas, V. Lyubashevsky, and T. Prest, "Efficient identity-based encryption over NTRU lattices," in *Advances in Cryptology—ASIACRYPT 2014*, P. Sarkar and T. Iwata, Eds., pp. 22–41, Springer, Berlin, Germany, 2014.

[22] M. Albrecht, S. Bai, and L. Ducas, "A subfield lattice attack on overstretched NTRU assumptions," in *Advances in Cryptology—CRYPTO 2016*, M. Robshaw and J. Katz, Eds., pp. 153–178, Springer, Berlin, Germany, 2016.

[23] J. H. Cheon, J. Jeong, and C. Lee, "An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero," *LMS Journal of Computation and Mathematics*, vol. 19, no. A, pp. 255–266, 2016.

[24] P. Kirchner and P.-A. Fouque, "Revisiting lattice attacks on overstretched NTRU parameters," in *Advances in*

Cryptology—EUROCRYPT 2017, J.S. Coron and J.B. Nielsen, Eds., pp. 3–26, Springer International Publishing, Cham, Switzerland, 2017.

[25] D. Stehlé and R. Steinfeld, "Making ntruencrypt and ntrusign as secure as standard worst-case problems over ideal lattices," Cryptology ePrint Archive, Report 2013/004, 2013, https://eprint.iacr.org/2013/004.

[26] Y. Wang and M. Wang, "Crpsf and NTRU signatures over cyclotomic fields," Cryptology ePrint Archive, Report 2018/445, 2018, https://eprint.iacr.org/2018/445.

[27] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology—EUROCRYPT 2012*, D. Pointcheval and T. Johansson, Eds., pp. 738–755, Springer, Berlin, Germany, 2012.

[28] Y. Wang and M. Wang, "Provably secure NTRUEncrypt over any cyclotomic field," in *Selected Areas in Cryptography—SAC 2018*, C. Cid and M. J. Jacobson Jr., Eds., pp. 391–417, Springer International Publishing, Cham, Switzerland, 2019.

[29] M. Rosca, D. Stehlé, and A. Wallet, "On the ring-LWE and polynomial-LWE problems," in *Advances in Cryptology—EUROCRYPT 2018*, J. B. Nielsen and V. Rijmen, Eds., pp. 146–173, Springer International Publishing, Cham, Switzerland, 2018.

[30] C. Peikert, "An efficient and parallel Gaussian sampler for lattices," in *Advances in Cryptology—CRYPTO 2010*, T. Rabin, Ed., pp. 80–97, Springer, Berlin, Germany, 2010.

[31] 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.

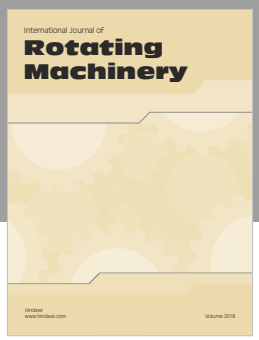
[32] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Designs, Codes and Cryptography*, vol. 75, no. 3, pp. 565–599, 2015.

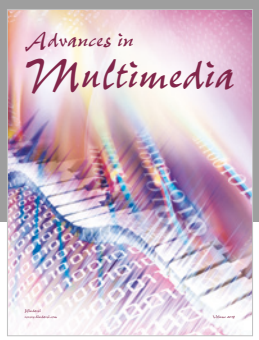
[33] C. Peikert, O. Regev, and N. Stephens-Davidowitz, "Pseudorandomness of ring-lwe for any ring and modulus," in *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing—STOC 2017*, pp. 461–473, ACM, Montreal, Canada, June 2017.

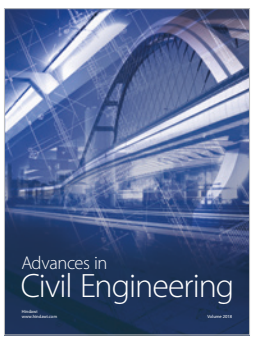
[34] V. Lyubashevsky, C. Peikert, and O. Regev, "A toolkit for ring-LWE cryptography," in *Advances in Cryptology—EUROCRYPT 2013*, T. Johansson and P. Q. Nguyen, Eds., pp. 35–54, Springer, Berlin, Germany, 2013.

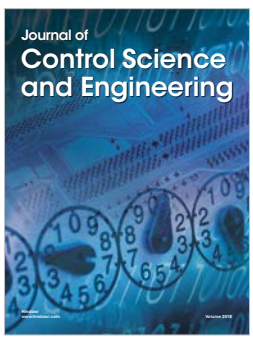
[35] L. Ducas and A. Durmus, "Ring-LWE in polynomial rings," in *Public Key Cryptography—PKC 2012*, M. Fischlin, J. Buchmann, and M. Manulis, Eds., pp. 34–51, Springer, Berlin, Germany, 2012.

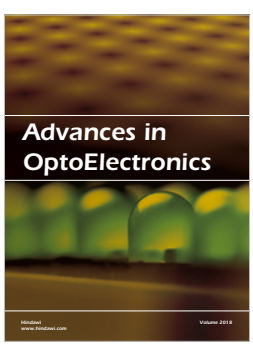
[36] Y. Yu, G. Xu, and X. Wang, "Provably secure ntruencrypt over more general cyclotomic rings," Cryptology ePrint Archive, Report 2017/304, 2017, https://eprint.iacr.org/2017/304.

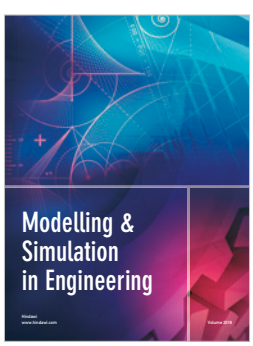


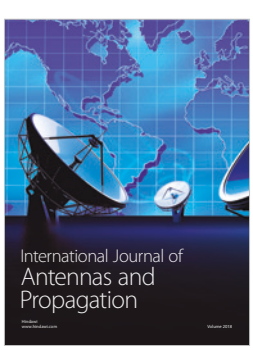


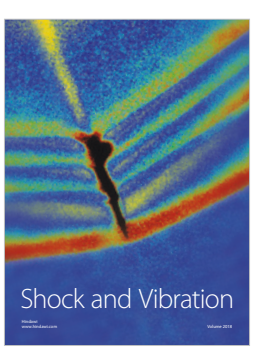


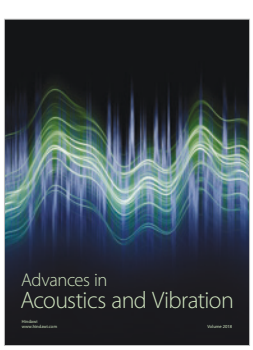












Hindawi

Submit your manuscripts at
www.hindawi.com