sensors

MDPI

Article

An Identity-Based Anti-Quantum Privacy-Preserving Blind Authentication in Wireless Sensor Networks

Hongfei Zhu [1], Yu-an Tan [1], Liehuang Zhu [1], Xianmin Wang [2], Quanxin Zhang [1] and Yuanzhang Li [1,*]

[1] School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China; farseer@bit.edu.cn (H.Z.); tan2008@bit.edu.cn (Y.T.); liehuangz@bit.edu.cn (L.Z.); zhangqx@bit.edu.cn (Q.Z.)

[2] School of Computer Science, Guangzhou University, Guangzhou 510006, China; xianmin@gzhu.edu.cn

* Correspondence: popular@bit.edu.cn

Received: 15 April 2018; Accepted: 19 May 2018; Published: 22 May 2018

Abstract: With the development of wireless sensor networks, IoT devices are crucial for the Smart City; these devices change people's lives such as e-payment and e-voting systems. However, in these two systems, the state-of-art authentication protocols based on traditional number theory cannot defeat a quantum computer attack. In order to protect user privacy and guarantee trustworthy of big data, we propose a new identity-based blind signature scheme based on number theorem research unit lattice, this scheme mainly uses a rejection sampling theorem instead of constructing a trapdoor. Meanwhile, this scheme does not depend on complex public key infrastructure and can resist quantum computer attack. Then we design an e-payment protocol using the proposed scheme. Furthermore, we prove our scheme is secure in the random oracle, and satisfies confidentiality, integrity, and non-repudiation. Finally, we demonstrate that the proposed scheme outperforms the other traditional existing identity-based blind signature schemes in signing speed and verification speed, outperforms the other lattice-based blind signature in signing speed, verification speed, and signing secret key size.

Keywords: identity-based blind signature; quantum computer attack; NTRU lattice; unforgeability

1. Introduction

With the development of wireless sensor networks, Internet of Things (IoT) devices play an important role in smart cities. IoT devices in e-payment and e-voting services are crucial for modernisation [1–3]. Meanwhile, a large amount data generated by these IoT devices face the threats of security and privacy leakage since the state-of-art authentication protocols in e-payment and e-voting systems can be attacked by quantum computers successfully [4], i.e., in e-payment and e-voting systems, blind signature (BS) is crucial to protect user privacy and guarantee trustworthy of big data in the cloud [5–8]. However, these schemes based on traditional number theory can be attacked successfully by quantum computer.

BS was firstly introduced by Chaum. Then many BS schemes based on number theory were proposed [9], which can be presented as follows:

The first factoring BS scheme based on RSA was proposed by Chaum, this scheme can guarantee the security of payer. However, they did not prove its security. Later, Bellare et al. defined the hard problem of RSA formally. Based on it, they proved the security of Chaum's scheme. Then a novel proven-secure RSA scheme was proposed by Camenisch and Koprowski etc., it was secure in the standard model. However, these schemes have to use long keys to guarantee security.

In order to overcome the shortages of factoring BS schemes, BS schemes based on discrete logarithm problem (DLP) were proposed for their short keys and high security. Chaum et al. proposed an e-wallet. Later, Okamoto proposed a BS scheme based on DLP. However, these schemes were not proven secure and only satisfy blindness. Then Pointcheval et al. initially considered the property of unforgeability.

After that, researchers were interested in constructing provably-secure BS schemes based on bilinear pairing. Boldyreva proposed a BS scheme based on GDH assumption, this scheme outperformed the other existing schemes in attribution and efficiency. Later, Okamoto proposed a BS scheme based on 2SDH assumption, which is stronger than SDH assumption. However, their efficiency is low.

Meanwhile, all the schemes outlined above need to depend on Public Key Infrastructure (PKI). In order to simplify key management of PKI, an identity-based signature scheme (IDS) was firstly presented by Shamir. In an IDS scheme, given a user's identity, his public key can be easily obtained. Also, his private key can be obtained easily. Until 2001, Boneh et al. initially proposed an IDS scheme, it has high efficiency, its security is dependent on the bilinear pairing problem. Then some new IDS schemes based on pairing were proposed by researchers. After that, combining BS with identity-based signature, Zhang et al. initially presented an identity-based BS (IDBS) scheme, its security is based on hard problem of bilinear pairing, this scheme was secure and efficient. Unfortunately, its computation cost was too high. Later, a new IDBS based on DLP was presented, the running time and signature size of their scheme [10] were significantly improved. However, these schemes still face the threat of quantum computer attack [4].

Thus, the replaceable IDBS schemes are based on lattice for their high-efficiency and sufficiently secure to quantum computer attack [11,12]. In the paper, a lattice-based IDBS scheme is proposed by using the advantages of number theory research unit lattice (NTRU) such as high efficiency, extremely tight keys, and sufficient safety once properly parameterized.

(1) Inspired by [13–15], we propose a new IDBS scheme on NTRU Lattice (named IDBS-NTRU), which can be secure to resist quantum computer attack.
(2) We evaluate our IDBS-NTRU's security. We demonstrate that the proposed scheme is secure. Then we prove that the proposed scheme satisfies confidentiality, integrity, and non-repudiation.
(3) We compare our IDBS-NTRU's performance with the other IDBS schemes.

- Comparing with existing traditional IDBS schemes, its signing speed is faster than other schemes, its moves are shorter than other schemes, its signing secret key, and signature size are larger than other schemes.
- Comparing with existing lattice-based BS schemes, its signing speed is faster than other lattice-based BS schemes, its moves are shorter than Rückert and ZM schemes, its signing secret key is smaller than other lattice-based schemes, and its signature length is smaller than Rückert scheme.

Organization. Section 2 presents the definitions of NTRU lattice and IDBS. Section 3 shows how to design an IDBS scheme. Section 4 proves the proposed IDBS's security, and compares with the existing IDBS schemes in terms of performance. Lastly, we conclude the paper in Section 5.

2. Preliminaries

2.1. The Applications for BS

With the development of big data, which has the properties of volume, variety, velocity, value, veracity, variability, viscosity, and virality, organizations deploy their services such as e-payment and e-voting systems etc. to the cloud [16–18]. In e-payment and e-voting systems, BS scheme plays an important role for that BS scheme can protect user's anonymous instead of encrypting all the data and searching on the ciphertexts [19–21]. In addition, scholars proposed some methods to protect security in the cloud [22–25], which can provide us with new methods to make our scheme in practice.

Meanwhile, scholars proposed some methods to detect complex event analysis, which can be used to improve the security of these services and applications in the cloud [26,27]. We will briefly describe e-payment and e-voting systems as follows:

E-payment system: A, B, T, and Ba are denoted as buyer, merchandiser, trusted third party, and bank respectively. Then the e-payment process is presented in Figure 1 [4]. In the beginning, T will produce and deliver keys for all the Bas, A, B will open a new account from their Ba respectively. The details are as follows:

A logins into his account, draws e-cash m from the Ba-A, blinds m by using blind factor f, and then obtains $m^{'}$. The Ba-A signs on $m^{'}$, and sends the signature $\sigma^{'}$ to A [28]. A unblinds the signature by using f and obtains σ. A sends the tuple $< m, \sigma >$ to B. B verifies whether it is valid or not, if it is, he sends the tuple to Ba-B. The Ba-B deposits the money on B's account.

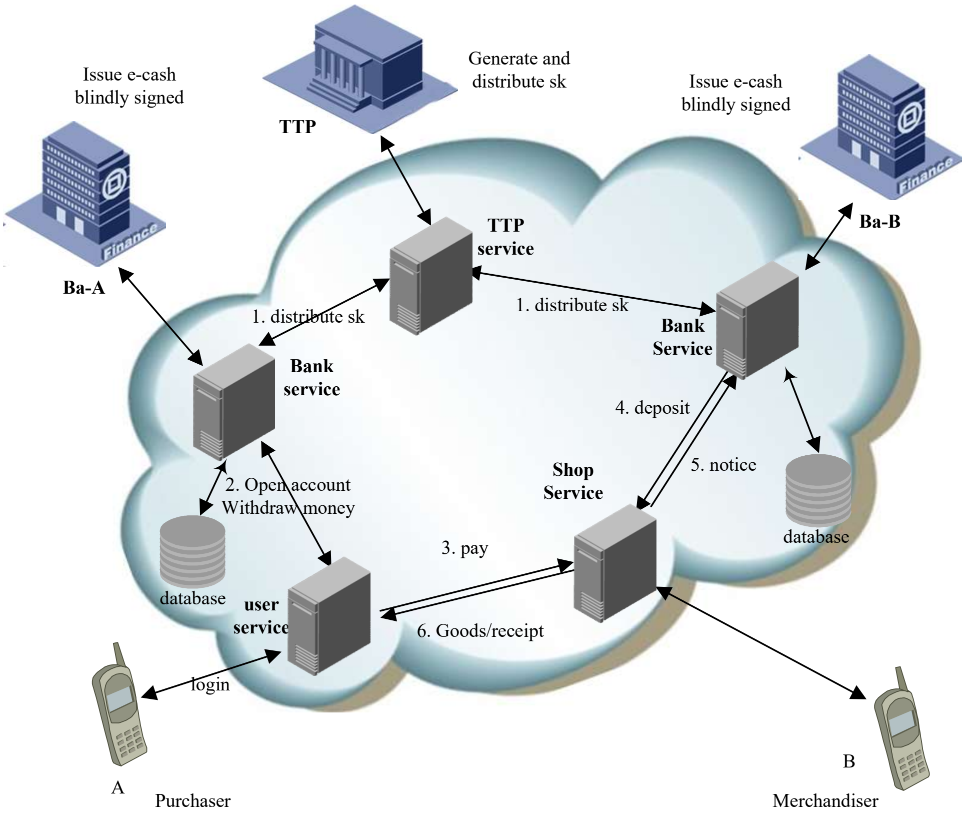

Figure 1. Blind authentication in e-payment system.

E-voting system: the voter, registrar, administrator, tallier, nominators, and validator are denoted as vo, re, ad, ta, no, and va respectively. The protocol is presented in Figure 2 [4]:

vo sends his id to a re, the re checks whether the vo is valid. If he is, the vo can send two nos to ad, the ad will check whether they are valid. If they are, the vo can choose a ballot m, blind it by using blind factor f, and then get the blinded message m'. m' will be sent to a va, the va signs on it and sends the signature σ' to the vo. The vo unblinds σ' by using blind factor f, and gets a signature σ. The vo sends m, σ to a ta, the ta will count all his ballots and store the results to a voting database.

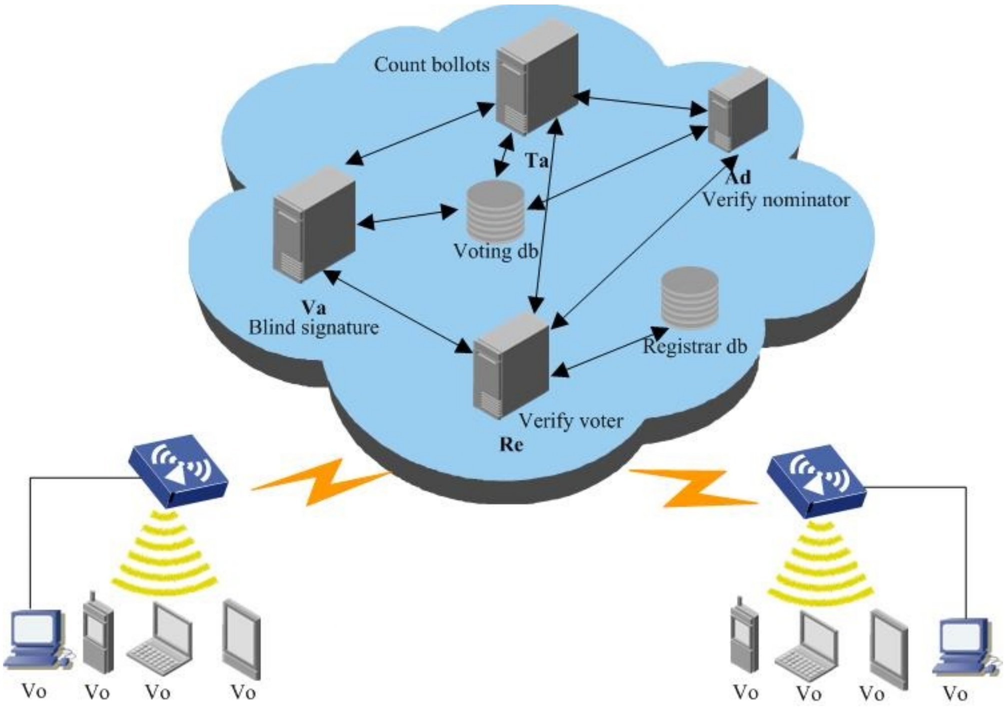

Figure 2. Blind authentication in e-voting system.

2.2. NTRU Lattice, Gaussians Sampling and Rejection Sampling on Lattice

Let α and γ be the vectors, p and $N = 2^p$ be integers, q be a prime which is greater than 5. Then we denote $R = Z[x]/(x^N + 1)$ as a ring. We denote $f = \Sigma_{i=0}^{N-1} f_i x^i$ and $g = \Sigma_{i=0}^{N-1} g_i x^i$ as polynomials in R. $R^{\times}$ is a set that all the elements have inverse in R. We write $< \alpha, \gamma >$ as vectors' inner product and $||\alpha||$ as α's Euclidean norm. We write $R_q = Z_q[x]/(x^N + 1)$ as the ring. We denote polynomial multiplication and concatenation as f, g mod $(x^N + 1)$ and $(f, g) \in R^{2N} = R^{1\times 2}$ in R respectively.

Next, we introduce the definitions of NTRU lattice, Gaussians sampling [29], and Rejection sampling [14]. NTRU lattice is used for constructing NTRUEncrypt and NTRUSign. These cryptosystems have high-efficiency, extremely tight keys, and are sufficiently secure once properly parameterized. The NTRU lattice is introduced as follows:

Definition 1 (NTRU lattice)**.** *Let $d, e \in \mathbf{R}$, $h = e \times d^{-1}$ mod q. Then $\boldsymbol{\mathcal{L}}_{h,q} = \{u, v \in R^2 : u + v \times h = 0$ mod $q\}$ is defined as NTRU Lattice. Meanwhile, $\mathcal{L}_{h,q}$ is a $\mathbf{R}^{2N}$ full-rank lattice $\begin{pmatrix} -C(h) & I \\ qI & O \end{pmatrix}$, in which I is a unit matrix, O is a null matrix, $C(h)$ is a matrix as follows:* $\begin{pmatrix} h_0 & h_1 ... & h_{N-1} \\ -h_{N-1} & h_0 & h_{N-2} \\ . & . & . \\ -h_1 & -h_2 & h_0 \end{pmatrix}$.

The security of our IDBS is based on R-SIS problem over NTRU lattice, it is defined as follows:

Definition 2 (R-$SIS^{\kappa}_{q,1,2,\beta}$ on NTRU lattice)**.** *in a ring $\mathbf{R} = Z[x]/(x^N + 1)$, κ is denoted as a distribution, in which we can choose small f, g from $\mathbf{D}_{Z^N,\sigma}$ (f, g mod $q \in \mathbf{R}_q^{\times}$) according to the Algorithm 3 in [13], then we can get $\mathbf{B}_{h,q} = (h, 1) \in \mathbf{R}_q^{1\times 2}$, $h = gf^{-1}$. Thus, the SIS problem means to search ζ_1, ζ_2 meeting $\mathbf{B}_{h,q}(\zeta_1, \zeta_2)^T = 0$ mod q, and $||(\zeta_1, \zeta_2|| \leq \beta$.*

Gaussian sampling was used for constructing the trapdoor in [29], i.e., a short basis was used to construct the trapdoor without revealing anything about this basis.

Definition 3 (Discrete Gaussian Distribution). *for* $\forall s > 0$, $x \in \mathbb{R}^N$, *and the center of Gaussian distribution c, the N-dimensional Gaussian function can be defined as* $\rho_{s,c}(x) = exp(\frac{-\pi||x-c||^2}{s^2})$. *Then the discrete Gaussian distribution on* $\mathcal{L}$ *can be defined as* $D_{\mathcal{L},s,c}(x) = \frac{\rho_{s,c}(x)}{\rho_{s,c}(\mathcal{L})}$.

Given real $\psi > 0$, negligible probability $\psi(n)$, a lattice $\mathcal{L}$, and its smoothing parameter $\eta_\epsilon(\mathcal{L}) \leq \sqrt{log(2N/(1+1/\epsilon))/\Pi}/\lambda_1^\infty(\mathcal{L}^*)$, there always exists $\psi(n)$ for $\eta_\epsilon(\mathcal{L}) \leq \omega(\sqrt{logN})/\lambda_1^\infty(\mathcal{L}^*)$ given any $\omega(\sqrt{logN})$ function. If $s > \eta_\epsilon(\mathcal{L})$, then the total Gaussian measure on all the kinds of translation of the lattice is the same according to Lemma 2.7 in [29]. If $s > 2\eta_\epsilon(\mathcal{L})$, then $D_{\mathcal{L},s,c}(x) \leq (1+\epsilon)2^{-N}/(1-\epsilon)$. If $\epsilon < \frac{1}{3}$, then the min-entropy of $D_{\mathcal{L},s,c}(x)$ is at least $N-1$ according to Lemma 2.10 in [29].

Lemma 1. *The two events occur with probability* $pr[y \leftarrow D_\sigma^1 : ||y|| \geq 12\sigma] < 2^{-100}$ $(\sigma > 0)$, $pr[y \leftarrow D_\sigma^m : ||y|| \geq 2\sigma\sqrt{m}] < 2^{-m}$ *(m is a non-negative integer) according to Lemma 3.3 in [14]. Let* **B** *be a basis of* $\mathcal{L}$, σ, c *be the standard deviation and the center of Gaussian distribution respectively. We can get the desired vectors from the discrete Gaussian sampling algorithm in Algorithm 1.*

Algorithm 1 $Gausssian(B, \sigma, c)$.

```
Input: B, $\sigma > 0, c$
Output: v
$v_n \leftarrow 0$ and $c_n \leftarrow c$.
for($i \leftarrow N$ to 1)
    (a) $c_i^{'} =< c_i, \tilde{b_i} > /||\tilde{b_i}||^2$
    (b) choose $z_i \sim D_{Z^N, s_i^{'}, c_i^{'}}$
    (c) $c_{i-1} \leftarrow c_i - z_i b_i$ and $v_{i-1} \leftarrow v_i + z_i b_i$
    end for
return $v_0$
```

Next, we begin to introduce the Rejection-sampling. In a signature scheme, rejection sampling can make the output signature distribution not depend on the signing key.

Theorem 1. *[Rejection Sampling Theorem] V is the subset of* Z^m, *the norms of V's elements are less than T,* $\sigma = \omega(T\sqrt{logm})$ *is the element in R, M is a constant,* $h : V \rightarrow R$ *is a probability distribution. There are two algorithms. One algorithm is such that* $x \leftarrow h, y \leftarrow D_{v,\sigma}^m, outputs(x, y)$ *with probability* $min(\frac{D_\sigma^m(y)}{MD_{v,\sigma}^m(y)}, 1)$. *The other algorithm is such that* $x \leftarrow h, y \leftarrow D_\sigma^m, outputs(x, y)$ *with probability* $\frac{1}{M}$. *Then the first algorithm' distribution does not exceed the second algorithm's statistical distance* $\frac{2^{-\omega(logm)}}{M}$. *Meanwhile, the first algorithm outputs something with probability at least* $\frac{1-2^{-\omega(logm)}}{M}$.

In particular, when $\sigma = \alpha T, \alpha$ is positive, then $M = e^{\frac{12}{\alpha} + \frac{1}{2\alpha^2}}$, the first algorithm's distribution does not exceed the second algorithm' statistical distance $\frac{2^{-100}}{M}$. The first algorithm outputs something with probability at least $\frac{1-2^{-100}}{M}$.

2.3. IDBS

An IDBS scheme consists of four algorithms$(ST_\varepsilon, EX_\varepsilon, SG_\varepsilon, VF_\varepsilon)$, $\mathcal{U}$, $\mathcal{S}$, and $\mathcal{V}$ are denoted as user, signer, and verifier respectively. Master key, master public key, and master private key are severally written as *mk*, *mpk*, and *msk*. System parameters are denoted as *params*, *n* is the security parameter. The definition is described as follows.

- $ST_\varepsilon(1^n)$: after inputting n, this algorithm outputs *params* and *mk*, which contains *mpk* and *msk*.
- $EX_\varepsilon(params, msk, id)$: after inputting *params*, *msk*, *id*, this algorithm outputs private key sk_{id} related to *id*.

- $SG_{\varepsilon}(id, m, sk_{id})$: $\mathcal{U}$ interacts with $\mathcal{S}$ as follows:
  (1) $\mathcal{U}$ blinds the message m to $m^{'}$ by using blind factor, then sends $m^{'}$ to $\mathcal{S}$.
  (2) $\mathcal{S}$ signs on $m^{'}$ and sends the signature $\sigma^{'}$ to $\mathcal{U}$.
  (3) $\mathcal{U}$ unblinds $\sigma^{'}$ and gets σ. The signature tuple is (m, σ).
- $VF_{\varepsilon}(params, id, m, \sigma)$: this algorithm returns true if σ is valid, otherwise returns false.

Before introducing the security properties of IDBS, we define some notations firstly. Γ is denoted as an adversary, U is nonmalicious users, m is the plaintext message, c, n are denoted as a constant and a big integer respectively, η is a negligible probability, t is the time.

IDBS should achieve two properties, which are defined as follows [30,31]:

Blindness [32]: Γ chooses two messages m_0, m_1, then a random bit i is selected, m_0, m_1 are randomly denoted as m_i, m_{1-i}, m_i, m_{1-i} are the inputs of two honest users respectively. Γ plays the Experiment 1 with these two users, σ_i, σ_{1-i} are the outputs of them respectively. σ_i, σ_{1-i} are dispatched to Γ, after that, Γ will output a bit $p \in \{0, 1\}$. Finally, the probability of $p = i$ is denoted as $|Pr[p = i] - 1/2| < \eta(n)$. i.e., if no Γ can win the Experiment 1 at the minimum with η in t, then it satisfies blindness.

One-more unforgeability [4]: after Γ interacts with a nonmalicious signer for l times, he tries to forge the $l + 1$ valid signature with η. The game is defined in Experiment 2. i.e., if Γ cannot win the Experiment 2 with η at most τ_1, τ_2, τ_3 times respectively for extraction, hash, and signature oracles in t, then the scheme satisfies one-more unforgeability.

Experiment 1 $Expt^{bd}_{\mathcal{S}^*}(n)$.

```
$i \in_{\$} \{0, 1\}$
$(params, msk) \leftarrow ST(1^n)$
$sk_{id} \leftarrow EX(params, id, msk)$
$(m_0, m_1, state_{find}) \leftarrow_{\$} \mathcal{S}^*(find, sk_{id}, id)$
$state_{issue} \leftarrow_{\$} \mathcal{S}^{*<.,\mathcal{U}(id,m_i)^1>,<.,\mathcal{U}(id,m_{1-i})^1>}(issue, state_{find})$
$\delta_i$, $\delta_{1-i}$ are respectively $\mathcal{U}(id, m_i), \mathcal{U}(id, m_{1-i})$'s outputs
if $\delta_0 \neq fail$ and $\delta_1 \neq fail$ then
    $p \leftarrow_{\$} \mathcal{S}^*(guess, \delta_0, \delta_1, state_{issue})$
else
    $p \leftarrow_{\$} \mathcal{S}^*(guess, fail, fail, state_{issue})$
end if
return true iff $p = i$
```

Experiment 2 $Expt^{omf}_{\mathcal{U}^*}(n)$.

```
$(params, msk) \leftarrow ST(1^n)$
$sk_{id} \leftarrow EX(params, id, msk)$
$\{(m_1, s_1), ..., (m_k, s_k)\} \leftarrow_{\$} \mathcal{U}^{*h(.),<\mathcal{S}(sk_{id}),.>^{\infty}}(id)$
$l$ is the successful interaction number between $\mathcal{U}^*$ and signer
return true iff
    $m_i \neq m_j$ for $1 \leq i < j \leq k$ and
    $VF(m_i, s_i, id) = 1$ and
    $l + 1 = k$
```

3. Proposed IDBS-NTRU Scheme

Most IDBS schemes are designed with the traditional number theorem; these schemes cannot defeat a quantum computers attack. So the replaceable IDBS schemes are based on lattice. Meanwhile, NTRU-cryptosystems have some advantages, such as high-efficiency, extremely tight keys, and sufficient safety after properly parameterized. Therefore, we choose the NTRU lattice to construct a novel IDBS scheme so that we can achieve both security and efficiency.

In this section, we will firstly introduce how to construct an IDBS scheme on NTRU lattice, then we design an e-payment protocol using our proposed scheme.

3.1. IDBS-NTRU Scheme

In this section, we propose our IDBS scheme $\varepsilon = (ST_\varepsilon, EX_\varepsilon, SG_\varepsilon, VF_\varepsilon)$. Let $\mathcal{U}$, $\mathcal{S}$, $\mathcal{V}$ be a user, a signer, and a verifier respectively, N and id be security parameter and user's identity respectively, $\tilde{\Omega}(.)$ and $Poly(N)$ be the asymptotic lower bound and N's polynomial function respectively [13].

(1) $ST_\varepsilon(1^N)$ outputs $(params = (q, \varepsilon, s), mk = (sk, pk))$, in which $q = Poly(N)$, $\varepsilon \in (0, \frac{\ln N}{\ln q})$, and $s = \tilde{\Omega}(N^{\frac{3}{2}}\sigma)$. If $N > 2$, then $\sigma = N\sqrt{(\ln(8Nq)}q^{\frac{1}{2}+\varepsilon}$, $q^{1/2-\varepsilon} = \tilde{\Omega}(n^{\frac{7}{2}})$. If $N = 2$, then $\sigma = \sqrt{N\ln(8Nq)}q^{\frac{1}{2}+\varepsilon}$, $q^{\frac{1}{2}-\varepsilon} = \tilde{\Omega}(N^3)$. mk is generated as follows [13]:

The algorithm samples f, g from $\boldsymbol{D}_{Z^N,s}$, which satisfy $f, g \ mod \ q \notin \boldsymbol{R}_q^\times$. Meanwhile, $||f||, ||g|| \leq \sigma\sqrt{N}$ and $< f, g > \in R$. Then the algorithm computes $F_1, G_1 \in R$, which satisfy $fG_1 - gF_1 = 1$. We compute $F_q = qF_1, G_q = qG_1$, and then obtain (F, G) by using babai algorithm in [11], which satisfies $(F, G) = (F_q, G_q) - k(f, g)$, $k \in R$. If $||(F, G)|| \leq N\sigma$, then outputs sk = $\boldsymbol{D} = \begin{pmatrix} C(f) & C(g) \\ C(F) & C(G) \end{pmatrix}$ and $pk = h = gf^{-1} \in \boldsymbol{R}_q^\times$.

(2) $EX_\varepsilon(params, id, sk)$ computes $t \leftarrow H(id)$, and $sk_{id} = (s_1, s_2) \leftarrow [(t, 0) - Gausssian(sk, \sigma, (t, 0))]$, in which $s_1 + s_2 * h = t$. Then the algorithm outputs sk_{id} to user id [13].

(3) SG_ε: Let $m \in \{0, 1\}^*$ be the plaintext, $\mathcal{U}$ randomly selects $\boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{\alpha}, \gamma \in \boldsymbol{D}_{Z^N,s}$, then $\mathcal{U}$ executes BS protocol in Figure 3.

$$
\begin{array}{lcl}
\hline
\qquad \mathcal{S}(sk_{id}) & & \mathcal{U}(id, m, h) \\
\hline
blind: & & \\
 & & \boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{\alpha}, \gamma \in D_{Z^N,s} \\
 & & \boldsymbol{e} = H^{'}(\boldsymbol{y}_1 + h\boldsymbol{y}_2 + h\gamma + \boldsymbol{\alpha} - \boldsymbol{\alpha}H(id), m) \\
 & & \boldsymbol{e}^* = \boldsymbol{e} - \boldsymbol{\alpha} \\
 & \xleftarrow{\boldsymbol{e}^*, \boldsymbol{y}_1, \boldsymbol{y}_2} & \\
Sign: & & \\
\qquad \zeta_1^* = \boldsymbol{y}_1 + s_1\boldsymbol{e}^* & & \\
\qquad \zeta_2^* = \boldsymbol{y}_2 + s_2\boldsymbol{e}^* & & \\
 & \xrightarrow{\zeta_1^*, \zeta_2^*} & \\
unblind: & & \\
 & & \zeta_1 = \zeta_1^* + \boldsymbol{\alpha} \\
 & & \zeta_2 = \zeta_2^* + \gamma \\
 & & Signature\ tuple\ (m, \boldsymbol{e}, \boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2, id) \\
\hline
\end{array}
$$

Figure 3. Proposed IDBS-NTRU protocol.

- $\mathcal{U}$ computes

$$\boldsymbol{e} = H^{'}(\boldsymbol{y}_1 + h\boldsymbol{y}_2 + h\gamma + \boldsymbol{\alpha} - \boldsymbol{\alpha}H(id)), m) \tag{1}$$

and

$$\boldsymbol{e}^* = \boldsymbol{e} - \boldsymbol{\alpha} \tag{2}$$

then $\mathcal{U}$ sends e^* to $\mathcal{S}$.

- $\mathcal{S}$ computes Equations (3) and (4), then sends ζ_1^*, ζ_2^* to $\mathcal{U}$.

$$\zeta_1^* = \boldsymbol{y}_1 + s_1\boldsymbol{e}^* \tag{3}$$

$$\zeta_2^* = \boldsymbol{y}_2 + s_2\boldsymbol{e}^* \tag{4}$$

  Here, we will explain how to use the rejection sampling theorem, Theorem 1 from Section 2.2. The core idea of this theorem is to make $\zeta_1, \zeta_2, \boldsymbol{e}^*$ do not rely on the private key s_1, s_2 respectively. Our target is that the distribution of ζ_1, ζ_2 will obey the distribution D_σ^N. However, ζ_1, ζ_2 obey the distribution $D_{v,\sigma}^N$, where $c = v_1$ or v_2, $\boldsymbol{v}_1 = s_1\boldsymbol{e}^*$, and $\boldsymbol{v}_2 = s_2\boldsymbol{e}^*$. After we appropriately choose a certain M and σ, the algorithm will approximately output a signature tuple with probability $1/M$, whose distribution is approximate to the distribution where ζ_1, ζ_2 are chosen from D_σ^N [14].

- Finally, $\mathcal{U}$ gets the signature tuple $<m, \zeta_1, \zeta_2, \boldsymbol{e}, id>$ from Equations (5) and (6) with probability $min(\frac{D_{Z^N,s}}{MD_{Z^N,s,sk_{id}e^*}}, 1)$, in which M is a constant.

$$\zeta_1 = \zeta_1^* + \boldsymbol{\alpha} \tag{5}$$

$$\zeta_2 = \zeta_2^* + \gamma \tag{6}$$

(4) $VF_\varepsilon(m, \boldsymbol{e}, \zeta_1, \zeta_2, id)$: $\mathcal{V}$ validates whether Equations (7) and (8) is true. If it is, accept it. Otherwise reject it.

$$||(\zeta_1, \zeta_2)|| \leq 4s\sqrt{2N} \tag{7}$$

$$H'(h * \zeta_2 + \zeta_1 - H(id) * \boldsymbol{e}, m) = \boldsymbol{e} \tag{8}$$

3.2. An E-Payment Protocol

In this section, we design an e-payment protocol based on NTRU-IDBS scheme, which plays an important role in e-commerce. We will still follow the notations in Section 2.1. As described in Figure 4, A's account belongs to $bankA$, B's account belongs to $BankB$. Firstly, A draws e-money from $BankA$. Secondly, A pays the money to B. Finally, B deposits the money to $BankB$. Following is the details:

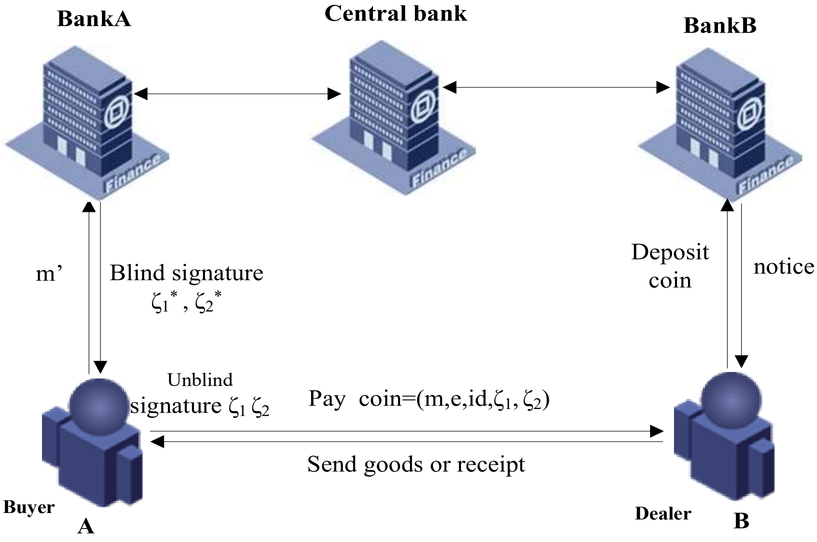

Figure 4. A buys goods from B.

(1) T produces and sends keys

- T runs the algorithm ST_ϵ and produces the system parameter *params* and master key *mk*.
- T runs algorithm EX_ϵ and generates the keys for *BankA* and *BankB*.
- *BankA*'s public key and private key are id_{BankA}, sk_{BankA} respectively.
- *BankB*'s public key and private key are id_{BankB}, sk_{BankB} respectively.
- T distributes the corresponding private keys to *BankA* and *BankB*.

(2) user opens an account from Bank

- A and B open an account using their real identity, such as passport, ssn, address, email, male, age, and so on, their banks will give them their account information respectively.

(3) A draws e-money from *BankA*

- A send their account information to *BankA*.
- *BankA* will verify whether he is a valid user. If it is, continue. Otherwise, abort.
- A wants to draw money m, he will randomly choose vectors $\boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{\alpha}, \gamma$, computes $\boldsymbol{e} = H^{'}(\boldsymbol{y}_1 + h\boldsymbol{y}_2 + h\gamma + \boldsymbol{\alpha} - \boldsymbol{\alpha}H(id), m)$ and $\boldsymbol{e}^* = \boldsymbol{e} - \boldsymbol{\alpha}$ to obtain $\boldsymbol{e}^*$.
- A sends m with the blinded note $\boldsymbol{e}^*$ to *BankA*.
- *BankA* computes $\boldsymbol{\zeta}_1^* = \boldsymbol{y}_1 + s_1\boldsymbol{e}^*, \boldsymbol{\zeta}_2^* = \boldsymbol{y}_2 + s_2\boldsymbol{e}^*$ for $\boldsymbol{e}^*$, and generates the signatures $\boldsymbol{\zeta}_1^*$ and $\boldsymbol{\zeta}_2^*$, then records on the account of A.
- Next, the bank returns $\boldsymbol{\zeta}_1^*, \boldsymbol{\zeta}_2^*$ to A.
- A computes $\boldsymbol{\zeta}_1 = \boldsymbol{\zeta}_1^* + \boldsymbol{\alpha}$ and $\boldsymbol{\zeta}_2 = \boldsymbol{\zeta}_2^* + \gamma$ to get $\boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2$.

(4) A pays the e-money to B

- A sends $m, \boldsymbol{e}, \boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2, id$ to B.
- B computes $||(\boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2)|| \leq 4s\sqrt{2N}$, $H^{'}(h * \boldsymbol{\zeta}_2 + \boldsymbol{\zeta}_1 - H(id) * \boldsymbol{e}, m) = \boldsymbol{e}$ and checks whether all of them are true. If all are true, accept it, otherwise, reject them.

(5) B deposits the e-money

- B will send $m, \boldsymbol{e}, \boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2, id$ to *BankB*.
- *BankB* computes and checks whether $||(\boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2)|| \leq 4s\sqrt{2N}$, and $H^{'}(h * \boldsymbol{\zeta}_2 + \boldsymbol{\zeta}_1 - H(id)\boldsymbol{e}, m) = \boldsymbol{e}$ are true, if all of them are true, continue; otherwise abort.
- *BankB* checks whether the e-money is in the list. If it is, abort, otherwise, continue.
- *BankB* will deposit the e-money on B's account.
- *BankB* will send a notice to B that B has received the e-money.
- B will send the goods or receipt to A.

4. Analyzing the Security and Performances

Here, we evaluate our IDBS-NTRU scheme with regard to correctness and security, then we compare the IDBS-NTRU scheme with other IDBS schemes in terms of performance.

4.1. Correctness, Blindness and One-More Unforgeability

Theorem 2 (Correctness)**.** *The IDBS-NTRU scheme is correct.*

Proof. Following our IDBS-NTRU scheme, we can get

$$\begin{aligned}
&h * \boldsymbol{\zeta}_2 + \boldsymbol{\zeta}_1 - H(id) * \boldsymbol{e} \\
&= h(\boldsymbol{\zeta}_2^* + \gamma) + \boldsymbol{\zeta}_1^* + \boldsymbol{\alpha} - H(id) * \boldsymbol{e} \\
&= h(\boldsymbol{y}_2 + s_2\boldsymbol{e}^* + \gamma) + \boldsymbol{y}_1 + \boldsymbol{\alpha} + s_1\boldsymbol{e}^* - H(id) * \boldsymbol{e} \\
&= \boldsymbol{y}_1 + h\boldsymbol{y}_2 + h\gamma + \boldsymbol{\alpha} - \boldsymbol{\alpha}H(id)
\end{aligned} \tag{9}$$

Thus, $H^{'}(h * \boldsymbol{\zeta}_2 + \boldsymbol{\zeta}_1 - H(id) * \boldsymbol{e}, m) = \boldsymbol{e}$.

By using Lemmas 2 and 3 in [13], the distributions of $\boldsymbol{\zeta}_1^*, \boldsymbol{\zeta}_2^*$ are close to $D_{Z^N,s}$, $\boldsymbol{\alpha}, \boldsymbol{\gamma}$ are the vectors from $\boldsymbol{D}_{Z^N,s}$. So the probability of $||\boldsymbol{\zeta}_1||, ||\boldsymbol{\zeta}_2|| \leq 4s\sqrt{N}$ is at least $1 - 2^{-N}$. Then we can get $||(\boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2)|| \leq 4s\sqrt{2N}$.

To prove IDBS-NTRU scheme's blindness, we introduce the statistical distance theorem, that is crucial to prove blindness property. □

Theorem 3 (Statistical Distance Theorem). *let random variable number $P, Q \in \Omega$, in which Ω is a finite domain. The statistical distance equation is presented as below [33]:*

$$\Delta(P, Q) = 1/2 \sum_{\omega \in \Omega} |Pr[P = \omega] - Pr[Q = \omega]| \tag{10}$$

When we prove IDBS-NTRU's blindness, the malicious $\mathcal{S}^*$ will play the Experiment 1 with two trust users respectively.

Theorem 4 (Blindness). *The IDBS-NTRU satisfies blindness.*

Proof. A random bit $i \leftarrow \{0, 1\}$ is chosen, which is kept secret from $\mathcal{S}^*$. Then $\mathcal{S}^*$ chooses m_0, m_1, then $\mathcal{S}^*$ interacts with two honest users as in Experiment 1. Following is the protocol:

- $(pk, sk) \leftarrow KG_\varepsilon(1^k)$
- $sk_{id} \leftarrow EX(params, id, sk)$
- Under finding mode, $\mathcal{S}^*$ selects $m_0, m_1 \leftarrow \mathcal{S}^*(1^k, id, sk_{id})$.
- Under issuing mode, a random bit i is selected randomly, that cannot be obtained by $\mathcal{S}^*$. Then m_0, m_1 are randomly denoted as m_i, m_{1-i} respectively. $\mathcal{S}^*$ concurrently interacts with $\mathcal{U}(id, m_i)$ and $\mathcal{U}(id, m_{1-i})$.
- If one user outputs $\delta(m_i)$, the other outputs $\delta(m_{1-i})$, we will send a sequence $<\delta(m_i), \delta(m_{1-i})>$ to $\mathcal{S}^*$.
- Under guessing mode, $\mathcal{S}^*$ returns $\tilde{i}$.

As in Figure 3, the Interactive values do not depend on m, so what we need to do is analyzing $\boldsymbol{e}^*, \boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{\zeta}_1^*, \boldsymbol{\zeta}_2^*$.

For $\boldsymbol{e}^*$, the statistical-distance is defined as follows

$$\Delta(\boldsymbol{e}_i^*, \boldsymbol{e}_{1-i}^*) = 1/2 \sum_{\boldsymbol{e}^{*'} \in D_{Z^N,s}} |Pr(\boldsymbol{e}_i^* = \boldsymbol{e}^{*'}) - Pr(\boldsymbol{e}_{1-i}^* = \boldsymbol{e}^{*'})| \tag{11}$$

For α is a random vector from Discrete Gaussian distribution, we can get the follow equations $Pr(\boldsymbol{e}_i^* = \boldsymbol{e}^{*'})$ is close to $1/2^n$, $Pr(\boldsymbol{e}_{1-i}^* = \boldsymbol{e}^{*'})$ is close to $1/2^n$. Therefor, we can get $\Delta(\boldsymbol{e}_i^*, \boldsymbol{e}_{1-i}^*)$ is close to 0.

Similarly, we can get $\Delta(\boldsymbol{y}_1^i, \boldsymbol{y}_1^{1-i})$, $\Delta(\boldsymbol{y}_2^i, \boldsymbol{y}_2^{1-i})$, $\Delta(\boldsymbol{\zeta}_1^{i*}, \boldsymbol{\zeta}_1^{1-i*})$, and $\Delta(\boldsymbol{\zeta}_2^{i*}, \boldsymbol{\zeta}_2^{1-i*})$ are close to 0. Therefore, $\mathcal{S}^*$ cannot recognize m from $\boldsymbol{e}^*, \boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2$, i.e., $\mathcal{S}^*$ wins the experiment with probability $1/2 + \eta(n)$. Therefore, we prove the theorem.

Before proving the one-more unforgeability of IDBS-NTRU, we will define some notations as follows:

Let $\delta_1, \delta_2, \delta_3, \delta_4$ be simulating the cost functions of H hash, extract oracle, $H^{'}$ hash, and signature oracles respectively. Let $\eta, \eta^{'}$ be non-negligible probability, and t be time respectively, Θ be a polynomial time algorithm, and Γ be a polynomial time forger. □

Theorem 5 (One-more Unforgeability). *If Γ is able to generate a legal signature with η in t, after at most $\tau_1, \tau_2, \tau_3, \tau_4$ times queries respectively to H hash, Extract, $H^{'}$ hash, and signature oracles. Then R-$SIS^{\kappa}_{q,1,2,\beta}$ can be solved by Θ with probability at least $\eta^{'} = (1 - 2^{-\omega(logN)})\eta$ in time $t^{'} = t + \tau_1^{\tau_2}(\tau_1\delta_1 + \tau_2\delta_2) + \tau_3^{\tau_4}(\tau_3\delta_3 + \ \tau_4\delta_4)$.*

Proof. Assuming an adversary Γ is able to produce an IDBS signature with η, we can construct Θ, this algorithm can obtain the solution of R-SIS on the NTRU lattice. The followings are the simulated interactive environment.

ST: Θ selects $h \in R_q^{\times}$, $H, H^{'}$ at random. Then Θ computes and sends the public parameters $paras = \{h, H, H^{'}, \epsilon, q, s\}$ to the Γ.

H oracle Queries: Θ will maintains a list L_h, in the beginning, the list is mull. Once receiving an id_i, Θ will inquire L_h. If there exists a corresponding hash value t_i, Θ will return t_i. Otherwise Θ will return a random value. After that, Θ will save id_i, t_i in L_h.

H′ oracle Queries: Θ maintains a list $L_h^{'}$, in the beginning, the list is null. Once receiving $m_i, \Lambda_i = y_{1_i} + hy_{2_i} + h\gamma_i + \alpha_i - \alpha_i H(id_i)$, we assume Θ has already quire H oracle and gotten an entry id_i, t_i. Then Θ will quire $L_h^{'}$. If there already exists a corresponding hash value e_i, Θ will return e_i. Otherwise, Θ will return a random value. After that, Θ will save $m_i, \Lambda_i, y_{1_i}, y_{2_i}, \gamma_i, \alpha_i, id_i, e_i, t_i$ to $L_h^{'}$.

EX Oracle Queries: Θ maintains a list L_{id}, in the beginning, the list is null. Once receiving an identity id_i, Θ will inquire H oracle. If there does not exist a corresponding hash value in L_{id}, Θ will randomly selects a t_i and return it. Otherwise, return the corresponding t_i. After that, Θ can get a $sk_{id_i} = (s_{1_i}, s_{2_i})$, Θ returns sk_{id_i} to Γ as the private key related with id_i and saves the tuple (id_i, t_i, sk_{id_i}) in L_{id}.

SG Oracle Queries: Γ queries the signing oracle for (m_i, id_i). Θ checks if id_i is already queried for H, $H^{'}$ or extraction oracles. If it is, Θ can get an entry (id_i, t_i, sk_{id_i}) from L_{id}. Else Θ simulates the extraction oracle and obtain a new secret key. Then Θ executes the BS protocol to obtain a valid signature $(m_i, id_i, \boldsymbol{e}_i, \zeta_{1_i}, \zeta_{2_i})$ and stores the value $(m_i, id_i, \boldsymbol{e}_i, \zeta_{1_i}, \zeta_{2_i})$ in the list L_S.

Output: Finally, Γ firstly outputs a forged signature $(\boldsymbol{e}_i, \zeta_{1_i}, \zeta_{2_i}, m_i, id_i)$. Θ rewinds Γ_i to the point where it queries $H^{'}$ for (m_i, id_i) and obtains another signature $(\boldsymbol{e}_i^{'}, \zeta_{1_i}^{'}, \zeta_{2_i}^{'}, m_i, id_i)$.

Therefore, Θ can solve R-$SIS^{\kappa}_{q,1,2,\beta}$ problem over the NTRU lattice. Θ obtains sk_{id_i} and $\boldsymbol{e}_i^{'}, \boldsymbol{y}_{1_i}, \boldsymbol{y}_{2_i}, \boldsymbol{\alpha}_i, \gamma_i$ from the L_S. Θ computes $\boldsymbol{\zeta}_{1_i} = \boldsymbol{y}_{1_i} + s_{1_i} * \boldsymbol{e}_i^{*} + \boldsymbol{\alpha}_i, \boldsymbol{\zeta}_{2_i} = \boldsymbol{y}_{2_i} + s_{2_i} * \boldsymbol{e}_i^{*} + \gamma_i$, and $\boldsymbol{\zeta}_{1_i} + \boldsymbol{\zeta}_{2_i} * h - H(id_i)\boldsymbol{e}_i$. Then Θ checks whether $\boldsymbol{\zeta}_{1_i} + \boldsymbol{\zeta}_{2_i} * h - H(id_i)\boldsymbol{e}_i = \boldsymbol{\zeta}_{1_i}^{'} + \boldsymbol{\zeta}_{2_i}^{'} * h - H(id_i)\boldsymbol{e}_i^{'} = \boldsymbol{y}_{1_i} + h * \boldsymbol{y}_{2_i} + h\gamma_i + \boldsymbol{\alpha}_i - \boldsymbol{\alpha}_i H(id_i)$. If they are not equal, there is a collision of $H^{'}$. If $(\zeta_{1_i}, \zeta_{2_i}) \neq (\zeta_{1_i}^{'}, z_{2_i}^{'})$, we can get $(\zeta_{1_i} - \zeta_{1_i}^{'}) + h(\zeta_{2_i} - \zeta_{2_i}^{'}) = 0$ and $||(\zeta_{1_i} - \zeta_{1_i}^{'}, \zeta_{2_i} - \zeta_{2_i}^{'})|| \leq 8s\sqrt{2N}$. So $(\zeta_{1_i} - \zeta_{1_i}^{'}, \zeta_{2_i} - \zeta_{2_i}^{'})$ is one solution to R-$SIS^{\kappa}_{q,1,2,\beta}$.

Now we start to analyze the advantage of Θ. As discussed above, Θ wins the game if and only if Γ has successfully forged $(\zeta_1^{'}, \zeta_2^{'}, \boldsymbol{u}^{'})$ and $(\zeta_1, \zeta_2) \neq (\zeta_1^{'}, \zeta_2^{'})$. Next according to the Lemma 4.6 in [34], Γ can solve R-$SIS^{\kappa}_{q,1,2,\beta}$ with probability at least $\eta^{'} = (1 - 2^{-\omega(logN)})\eta$, where $\beta = 8s\sqrt{2N}$. It is obviously that $t^{'} = t + \tau_1^{\tau_2}(\tau_1\delta_1 + \tau_2\delta_2) + \tau_3^{\tau_4}(\tau_3\delta_3 + \tau_4\delta_4)$. We prove this theorem. □

4.2. Performances

Here, we will compare our IDBS-NTRU's performances with other IDBS schemes. First of all, we will compare NTRU-IDBS scheme with traditional IDBS schemes in terms of performance, which were constructed based on number theory. Secondly, we will compare our IDBS-NTRU scheme with lattice-based BS schemes in terms of performance.

(1) Comparing with traditional IDBS schemes

As shown in Table 1, we compare IDBS-NTRU'performance with ZK scheme [35], HCZ scheme [10], and CZYW scheme [36]. The ZK scheme is constructed based on computational diffie-hellman problem of bilinear pairings. The HCZ scheme is constructed based on discrete logarithm problem of ellipse curve. The CZYW scheme is constructed based on big integer factoring problem. The IDBS-NTRU scheme's signing speed and verification speed are O(n), which outperform ZK scheme, HCZ scheme, and CZYW schemes. Its moves are 2, it is shorter than ZK scheme and HCZ scheme. Its signing secret key is $2nlog(s\sqrt{n})$, it is larger than ZK scheme and HCZ scheme. However, the rsa has to use $O(n^3)$ to achieve n bits security, the signing secret key of IDBS-NTRU scheme is shorter than CZYW scheme. The signature size of IDBS-NTRU scheme is $2nlog(12\sigma) + n(log\lambda + 1)$, it is larger than ZK, HCZ, and CZYW schemes. For the same reason, it is also shorter than CZYW scheme. The most important of all, the BS schemes based on number theory are considered to be insecure to resist quantum computers attack [4], our IDBS-NTRU scheme is more secure than other three traditional schemes.

Table 1. Performance comparison with traditional IDBS schemes.

IDBS Scheme	**ZK** [35]	**HCZ** [10]	**CZYW** [36]	**Ours**
Hard Problem	CDHP	DLP	Factoring	R-SIS
Signing Speed	$O(n^3)$	$O(n^3)$	$O(n^3)$	$O(n)$
Verifying Speed	$O(n^3)$	$O(n^3)$	$O(n^3)$	$O(n)$
Moves	3	3	2	2
Signing Secret key	$2n$	logk+$2n$	n	$2nlog(s\sqrt{n})$
Signature size	$3n$	logk+$4n$	n	$2nlog(12\sigma) + n(log\lambda + 1)$

(2) Comparing with lattice-based BS schemes

We compare IDBS-NTRU's performance with GHWX [37], ZTZ [4], Rückert [32], and ZM schemes [38] in Table 2, n denotes safety parameter. GHWX scheme and ZM scheme are constructed based on small integer solution problem of lattice. ZTZ scheme is constructed based on closest vector problem of lattice. Rückert is constructed based on ideal-lattice shortest vector problem.

Table 2. Performance Comparison with lattice-based BS schemes.

Lattice-Based BS Scheme	**GHWX** [37]	**ZTZ** [4]	**Rückert** [32]	**ZM** [38]	**Ours**
Hard Problem	SIS	CVP	ISVP	SIS	R-SIS
Signing Speed	$O(n^2)$	$O(n^2logn)$	$O(n(logn)^c)$	$O(n^2)$	$O(n)$
Verifying Speed	$O(n^3)$	O(n)	O(n)	$O(n^3)$	O(n)
Moves	2	2	4	3	2
Signing secret key	$nm\log(q+1)$	$dn^2(\log n+1)$	$mn\log(2d_s+1)$	$m^2\log(q+1)$	$2n\ log(s\sqrt{n})$
Signature size	$m\log(q+1)$	$dn(\log n+1)$	n^2+mn $\log(2mnd_sd_{\epsilon^*})$	$2m\log(q+1)$	$2nlog(12\sigma)+$ $n(\log\lambda+1)$
Identity Based	yes	no	no	yes	yes

As presented in Table 2, IDBS-NTRU's signing speed is $O(n)$, which outperforms all the other schemes. IDBS-NTRU's verification speed is $O(n)$, which outperforms GHWX and ZM schemes. Our IDBS-NTRU scheme has two moves, it is shorter than Rückert scheme, and ZM scheme. In Rückert scheme, the parameters satisfy $m > \lfloor c_m log(1) \rfloor + 1, c_m > 1/log(2d_s)$. In ZM schemes, the parameters satisfy $m > 2nlogq, q > 2$. The signing secret key of our IDBS-NTRU scheme is $2nlog(s\sqrt{n})$, it is shorter than all the other schemes. The signature size of our IDBS-NTRU scheme is $2nlog(12\sigma) + n(log\lambda + 1)$, it is shorter than Rückert scheme, but it is larger than GHWX, ZTZ, and ZM schemes. The ZTZ scheme and Rückert scheme are not identity-based scheme, they depend on the public key infrastructure. However, our IDBS-NTRU scheme does not need to dependent on public key infrastructure.

5. Conclusions

In this work, we present an IDBS-NTRU scheme by using NTRU lattice, this scheme can protect user privacy and guarantee the trustworthy of big data in e-payment and e-voting systems in wireless sensor networks, this scheme has the advantages of NTRU Lattice such as high efficiency, compact key, high security after appropriate parameterized etc. Our scheme is secure and efficient. Furthermore, we prove IDBS-NTRU satisfies blindness and unforgeability. In addition, comparing with traditional IDBS schemes, IDBS-NTRU outperforms other IDBS schemes in terms of signing speed and verifying speed. Comparing with lattice-based schemes, IDBS-NTRU scheme outperforms other schemes in terms of signing speed, verifying speed, and signing secret key, outperforms Rückert scheme in terms of signature size moves and signature size, and outperforms ZM scheme in terms of moves. The schemes based on number theorem are considered insecure to resist the quantum computers attack, so our scheme is more secure than them. Furthermore, lattice-based schemes usually have a lot of parameters which need to be initialized correctly, these schemes are not easy to implement. Therefore, almost all the works related with lattice-based cryptography are still in the step of theory research.

In addition, if we can add some common message such as date between the signer and a user in our scheme, it is easy to transform our scheme into an identity-based partial BS scheme, which is suitable for the real e-payment and e-voting systems. In the future, we will continue to construct a partial IDBS scheme based on lattice.

Author Contributions: Writing-Original Draft Preparation, H.Z.; Methodology, Y.T., L.Z.; Validation, X.W.; Data Curation and Writing-Review and Editing, Q.Z.; Funding Acquisition, Y.L.

Funding: This work was supported by the National Natural Science Foundation of China (No. U1636213), Beijing Municipal Natural Science Foundation (No. 4172053), and partly supported by Beijing Municipal Education Commission under Grant No. KM201510016009, and Excellent Teachers Development Foundation of BUCEA (No. 21082717046), and National Key R&D Program of China (No. 2016YFC060090).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ahmad, S.; Hang, L.; Kim, D.H. Design and Implementation of Cloud-Centric Configuration Repository for DIY IoT Applications. *Sensors* **2018**, *18*, 474. [CrossRef] [PubMed]
2. Gaur, A.; Scotney, B.; Parr, G.; Mcclean, S. Smart City Architecture and its Applications Based on IoT. *Procedia Comput. Sci.* **2015**, *52*, 1089–1094. [CrossRef]
3. Guan, Z.; Li, J.; Wu, L.; Zhang, Y.; Wu, J.; Du, X. Achieving Efficient and Secure Data Acquisition for Cloud-Supported Internet of Things in Smart Grid. *IEEE Internet Things J.* **2017**, *4*, 1934–1944. [CrossRef]
4. Zhu, H.F.; Tan, Y.A.; Zhang, X.S.; Zhu, L.H.; Zhang, C.Y.; Zheng, J. A round-optimal lattice-based blind signature scheme for cloud services. *Future Gener. Comput. Syst.* **2017**, *73*, 106–114. [CrossRef]
5. Zhang, X.; Tan, Y.A.; Chen, L.; Yuanzhang, L.; Ji, L. A Covert Channel over VoLTE via Adjusting Silence Periods. *IEEE Access* **2018**. [CrossRef]
6. Gao, C.Z.; Cheng, Q.; He, P.; Susilo, W.; Li, J. Privacy-Preserving Naive Bayes Classifiers Secure against the Substitution-then-Comparison Attack. *Inf. Sci.* **2018**. [CrossRef]
7. Li, P.; Li, T.; Ye, H.; Li, J.; Chen, X.; Xiang, Y. Privacy-preserving machine learning with multiple data providers. *Future Gener. Comput. Syst.* **2018**. [CrossRef]
8. Guan, Z.; Si, Z.X.; Wu, L.; Guizani, N.; Du, X.; Ma, Y. Privacy-preserving and Efficient Aggregation based on Blockchain for Power Grid Communications in Smart Communities. *IEEE Internet Things J.* **2018**, *56*, 1–7.
9. Zheng, J.; Tan, Y.A.; Zhang, Q.; Zhang, X.; Zhu, L.; Zhang, Q. Cross-cluster asymmetric group key agreement for wireless sensor networks. *Sci. China Inf. Sci.* **2018**, *61*, 048103:1–048103:3. [CrossRef]
10. He, D.; Chen, J.; Zhang, R. An efficient identity-based blind signature scheme without bilinear pairings. *Comput. Electr. Eng.* **2011**, *37*, 444–450. [CrossRef]

11. Peikert, C. *A Decade of Lattice Cryptography*; Now Publishers Inc.: Breda, The Netherlands, 2016; pp. 283–424.
12. Wang, Z.; Chen, X.; Wang, P. Adaptive-ID Secure Identity-Based Signature Scheme from Lattices in the Standard Model. *IEEE Access* **2017**, *5*, 20791–20799. [CrossRef]
13. Xie, J.; Hu, Y.P.; Gao, J.T.; Gao, W. Efficient identity-based signature over NTRU lattice. *Front. Inf. Technol. Electron. Eng.* **2016**, *17*, 135–142. [CrossRef]
14. Lyubashevsky, V. Lattice Signatures without Trapdoors. In *Advances in Cryptology—EUROCRYPT 2012*; Pointcheval, D., Johansson, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 738–755.
15. Zhu, H.F.; Tan, Y.A.; Yu, X.; Xue, Y.; Zhang, Q.X.; Zhu, L.H.; Li, Y.Z. An Identity-Based Proxy Signature on NTRU Lattice. *Chin. J. Electron.* **2018**, *27*, 297–303. [CrossRef]
16. Zhang, X.S.; Liang, C.; Zhang, Q.X.; Li, Y.Z.; Zheng, J.; Tan, Y.A. Building covert timing channels by packet rearrangement over mobile networks. *Inf. Sci.* **2018**, *445–446*, 66–78. [CrossRef]
17. Xue, Y.; Tan, Y.A.; Liang, C.; Li, Y.; Zheng, J.; Zhang, Q. RootAgency: A digital signature-based root privilege management agency for cloud terminal devices. *Inf. Sci.* **2018**, *444*, 36–50. [CrossRef]
18. Tan, Y.A.; Xue, Y.; Liang, C.; Zheng, J.; Zhang, Q.X.; Zheng, J.; Li, Y.Z. A root privilege management scheme with revocable authorization for Android devices. *J. Netw. Comput. Appl.* **2018**, *107*, 69–82. [CrossRef]
19. Lin, Q.; Li, J.; Huang, Z.; Chen, W.; Shen, J. A short linearly homomorphic proxy signature scheme. *IEEE Access* **2018**. [CrossRef]
20. Lin, Q.; Yan, H.; Huang, Z.; Chen, W.; Shen, J.; Tang, Y. An ID-based linearly homomorphic signature scheme and its application in blockchain. *IEEE Access* **2018**. [CrossRef]
21. Xu, J.; Wei, L.; Zhang, Y.; Wang, A.; Zhou, F.; Gao, C. Dynamic Fully Homomorphic encryption-based Merkle Tree for lightweight streaming authenticated data structures. *J. Netw. Comput. Appl.* **2018**, *107*, 113–124. [CrossRef]
22. Yu, X.; Zhang, C.; Xue, Y.; Zhu, H.; Li, Y.; Tan, Y.A. An extra-parity energy saving data layout for video surveillance. *Multimed. Tools Appl.* **2018**, *77*, 4563–4583.
23. Liu, Z.; Huang, Y.; Li, J.; Cheng, X.; Shen, C. DivORAM: Towards a Practical Oblivious RAM with Variable Block Size. *Inf. Sci.* **2018**. [CrossRef]
24. Li, T.; Li, J.; Liu, Z.; Li, P.; Jia, C. Differentially Private Naive Bayes Learning over Multiple Data Sources. *Inf. Sci.* **2018**. [CrossRef]
25. Yu, X.; Tan, Y.A.; Zhang, C.; Liang, C.; Aourra, K.; Zheng, J.; Zhang, Q. A High-Performance Hierarchical Snapshot Scheme for Hybrid Storage Systems. *Chin. J. Electron.* **2018**, *27*, 76–85. [CrossRef]
26. Li, J.; Sun, L.; Yan, Q.; Li, Z.; Srisa-an, W.; Ye, H. Significant Permission Identification for Machine Learning Based Android Malware Detection. *IEEE Trans. Ind. Inform.* **2018**. [CrossRef]
27. Shen, J.; Gui, Z.; Ji, S.; Shen, J.; Tan, H.; Tang, Y. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *J. Netw. Comput. Appl.* **2018**, *106*, 117–123. [CrossRef]
28. Xue, Y.; Tan, Y.A.; Liang, C.; Zhang, C.; Zheng, J. An optimized data hiding scheme for Deflate codes. *Soft Comput.* **2017**. [CrossRef]
29. Gentry, C.; Peikert, C.; Vaikuntanathan, V. Trapdoors for Hard Lattices and New Cryptographic Constructions. In Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing—STOC 2008, Victoria, BC, Canada, 17–20 May 2008; ACM: New York, NY, USA, 2008; pp. 197–206.
30. Schröder, D.; Unruh, D. Security of Blind Signatures Revisited. *J. Cryptol.* **2017**, *30*, 470–494. [CrossRef]
31. Zhu, H.F.; Tan, Y.A.; Zhu, L.H.; Zhang, Q.X.; Li, Y.Z. An Efficient Identity-Based Proxy Blind Signature for Semioffline Services. *Wirel. Commun. Mob. Comput.* **2018**, 1–9. [CrossRef]
32. Rückert, M. Lattice-Based Blind Signatures. In *Advances in Cryptology—ASIACRYPT 2010*; Abe, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2010; pp. 413–430.
33. Boneh, D.; Kim, S.; Nikolaenko, V. Lattice-Based DAPS and Generalizations: Self-enforcement in Signature Schemes. In *Applied Cryptography and Network Security, Proceedings of the 15th International Conference, ACNS 2017, Kanazawa, Japan, 10–12 July 2017*; Gollmann, D., Miyaji, A., Kikuchi, H., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 457–477.
34. Güneysu, T.; Lyubashevsky, V.; Pöppelmann, T. Lattice-based signatures: optimization and implementation on reconfigurable hardware. *IEEE Trans. Comput.* **2015**, *64*, 1954–1967. [CrossRef]
35. Zhang, F.; Kim, K. ID-based blind signature and ring signature from pairings. In *Advances in Cryptology—ASIACRYPT 2002*; Springer: Berlin, Germany, 2002; pp. 533–547.

36. Cheng, X.; Zhu, H.; Yang, C.; Wang, X. Identity-based Blind and Verifiably Encrypted Signatures from RSA. In *Information Security and Cryptology*; High Education Press: Beijing, China, 2005; pp. 30–40.
37. Gao, W.; Hu, Y.; Wang, B.; Xie, J. Identity-Based Blind Signature from Lattices in Standard Model. In *Information Security and Cryptology*; Chen, K., Lin, D., Yung, M., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 205–218.
38. Zhang, L.; Ma, Y. A lattice-based identity-based proxy blind signature scheme in the standard model. *Math. Probl. Eng.* **2014**, *2014*. [CrossRef]