Research Article

A Lattice-Based Identity-Based Proxy Blind Signature Scheme in the Standard Model

Lili Zhang and Yanqin Ma

Institute of Information Engineering and Huanghe Science and Technology College, Zhengzhou 450063, China

Correspondence should be addressed to Lili Zhang; 312495261@qq.com

Received 25 April 2014; Revised 15 August 2014; Accepted 17 August 2014; Published 25 September 2014

Academic Editor: Yan-Wu Wang

Copyright © 2014 L. Zhang and Y. Ma. 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.

A proxy blind signature scheme is a special form of blind signature which allowed a designated person called proxy signer to sign on behalf of original signers without knowing the content of the message. It combines the advantages of proxy signature and blind signature. Up to date, most proxy blind signature schemes rely on hard number theory problems, discrete logarithm, and bilinear pairings. Unfortunately, the above underlying number theory problems will be solvable in the postquantum era. Lattice-based cryptography is enjoying great interest these days, due to implementation simplicity and provable security reductions. Moreover, lattice-based cryptography is believed to be hard even for quantum computers. In this paper, we present a new identity-based proxy blind signature scheme from lattices without random oracles. The new scheme is proven to be strongly unforgeable under the standard hardness assumption of the short integer solution problem (SIS) and the inhomogeneous small integer solution problem (ISIS). Furthermore, the secret key size and the signature length of our scheme are invariant and much shorter than those of the previous lattice-based proxy blind signature schemes. To the best of our knowledge, our construction is the first short lattice-based identity-based proxy blind signature scheme in the standard model.

1. Introduction

Digital signature schemes are the cornerstone of e-business, e-government, software security, and many more applications. The importance of these schemes is likely to grow in the future as more and more everyday tasks and processes are computerized.

The concept of blind signature was first proposed in 1982 by Chaum [1]: user A could obtain the signature of B on any given message, without any information about the message or its signature revealed, and any receiver could verify the signature that is signed by signer B.

In 1996, Mambo et al. introduced the concept of proxy signature [2]: an original signer delegates his signing authority to another signer, who is called a proxy signer. At last, the proxy signer can sign any message on behalf of the original signer and the verifier can verify and distinguish between normal signature and proxy signature.

In 1985, Shamir introduced the concept of identity-based (ID-based) cryptography and presented an ID-based signature (IBS) scheme [3]. In an IBS scheme, a public key can be derived from the identity of the user, and a corresponding secret key can be generated by a private key generator (PKG). Of course, the IBS scheme can simplify key management procedures in certificate-based public key systems, so it can be an alternative for certificate-based public key systems in some occasions, especially, when efficient key management and moderate security are required.

In 2000, Lin and Jan [4] introduced the concept of proxy blind signature. Proxy blind signatures are actually the combination of both proxy signature and blind signature. It plays an important role in the following scenario: in e-cash system, the user makes the bank blindly sign a coin using blind signature schemes. Whenever a user goes through a valid branch to withdraw a coin, he/she needs the branch to make proxy blind signature on behalf of the signee bank.

Tan et al.’s scheme is a proxy blind signature scheme which is based on Schnorr blind signature. But Awasthi and der Lal [5] showed a forgery attack on Tan et al.’s scheme and proposed a more secure proxy blind signature scheme. Recently Sun et al. [6] pointed out that neither Tan et al.’s scheme nor Awasthi and der Lal’s scheme satisfies the unlinkability property of the proxy blind signature scheme. But they did not give an improved scheme to overcome
the insecurity. For the first time, Zhang et al. [7] proposed a proxy blind signature scheme from bilinear pairings. In 2004, Zheng et al. [8] proposed an ID-based proxy blind signature scheme which uses bilinear pairings of elliptic curves or hyperelliptic curves. Since then, many identity-based proxy blind signature schemes have been proposed, for example, [9–11].

Up to date, most of proposed identity-based proxy blind signature schemes rely on hard number theory problems such as integer factorization, discrete logarithm, and bilinear pairings with the Diffie-Hellman problem. However, the above underlying number theory problems will be solvable if practical quantum computers become reality, so it implies a potential security threat to these identity-based proxy blind schemes. Thus, a natural question one can ask is how to design identity-based proxy blind signature schemes that are secure in the quantum environment.

In recent years, lattices have emerged as a possible alternative to number theories. Lattice-based cryptography began with the seminal work of Ajtai [12], who showed that it is possible to construct families of cryptographic functions. Moreover, lattice-based cryptography is believed to be hard even for quantum computers [13]. Several lattice-based signature schemes [14–18] have been proposed so far. Among them, Jiang et al. [18] presented the first proxy signature scheme from lattices. Unfortunately, Tian and Huang [19] pointed that an original signer is able to forge a proxy signature on any message in the scheme. In 2010, Cash et al. put forward a new cryptographic notion called a bonsai tree based on hard lattice [20]. Since then, many proxy signatures [21, 22] were presented in bonsai tree model based on the bonsai tree signature scheme. However, both the private keys and the signatures in these schemes become dramatically longer than general signature. Therefore, they may not be practical for large communities.

Recently, Agrawal et al. [23] presented a basis delegation algorithm which keeps the dimension of the lattices involved constant. Based on the algorithm, the first lattice-based hierarchical identity-based encryption scheme with short ciphertexts in the standard model was proposed in [23]. Still, there is no identity-based proxy blind signature scheme from lattices in the standard model.

Following the above discussion, in this paper, we will construct a new identity-based proxy blind signature scheme from lattices in the standard model, which is obtained from Agrawal et al.’s basis delegation algorithm [23]. The new scheme is provably secure against strong forgery under hard problems on lattices, and the size of secret keys and the signature length of our scheme are much shorter than those of signature schemes [21, 22].

The rest of the paper is organized as follows: the next section gives the introduction of lattices, Section 3 explains briefly the definition of proxy blind signature, and Section 4 gives a detailed description of our identity-based proxy blind signature from lattice basis delegation. In Section 5, an analysis about our scheme is presented. Section 6 concludes this paper.
is statistically close to uniform on $Z_{q}^{nxm}$ and $T$ is a good basis of $\Lambda^{\perp}(A)$, such that $\|\tilde{B}\| \leq m \sqrt{\gamma_{m}}$.

Sample$D(A,r)$. Sample an $e$ from distribution $D_{Z^{nxr}}$, for which the distribution of $Ae$ is uniform over $Z_{q}^{n}$.

Sample$Pre(A,T,y,r)$. On input of $A \in Z_{q}^{nxm}$, a good basis $T$ for $\Lambda^{\perp}(A)$ as the trapdoor, a vector $y \in Z_{q}^{r}$, and $r$, the conditional distribution of the output $e$ is within negligible statistical distance of $D_{\Lambda^{\perp}(A)}$.

At CRYPTO 2010, Agrawal et al. [23] presented a new short lattice basis delegation algorithm that keeps the lattice dimension unchanged. Now, we briefly recall the main results in [23].

Definition 3. Let $q$ be a prime, let $m \geq 6\log q$, let and $\sigma > \sqrt{\gamma_{m}}(\sqrt{\gamma_{m}})$: $D_{z^{nxm}}$ is defined as the distribution on full rank matrices $\{A_{i} = \{a_{i1}, a_{i2}, \ldots, a_{im}\} \in Z_{q}^{m \times m}\}$, where $a_{ij} \sim D_{Z^{nxm}}$ for all $j \in [m]$.

Basis$Del(A,R,S,\sigma)$. Let $q > 2$, $A \in Z_{q}^{nxm}$, $R$ a matrix (or a product of $d$ matrices) sampled from $D_{nxm}$, and $S_{A}$ a basis of $\Lambda^{\perp}(A)$; the algorithm Basis$Del(A,R,S,\sigma)$ outputs a random basis $B$ for $\Lambda^{\perp}(AR^{-1})$, such that $\|B\| \leq \sigma \sqrt{m}$, where $\sigma \geq \|S_{\Lambda}(\|R\|d\omega(m))\|$. Sample$WithBasis(A)$. Let $q > 2$, $m > 5\log q$, and $A \in Z_{q}^{nxm}$, the algorithm Sample$WithBasis(A)$ outputs a random matrix $R \sim D_{nxm}$ and a basis $B$ for $\Lambda^{\perp}(AR^{-1})$, such that $\|\tilde{B}\| \leq \sigma \sqrt{m}$.

### 3. Proxy Blind Signature

A proxy blind signature [4, 9–11] is considered to be the combination of proxy signature and blind signature. It consists of four participants: an original signer, a proxy blind signer, a user, and a verifier and the following four algorithms: keygen, generation of the proxy key, proxy signature generation, and verification. A proxy blind signature scheme should satisfy the following requirements.

**Distinguishability.** Proxy signatures are distinguishable from normal signatures by everyone.

**Verifiability.** From the proxy signature, the verifier can be convinced of the original signers agreement on the signed message.

**Strong Nonforgeability.** A designated proxy signer can create a valid proxy signature for the original signer. But the original signer and other third parties who are not designated as a proxy signer cannot create a valid proxy signature.

**Strong Identifiability.** Anyone can determine the identity of the corresponding proxy signer from the proxy signature.

**Strong Nondeniability.** Once a proxy signer creates a valid proxy signature of an original signer, he/she cannot repudiate the signature creation.

**Prevention of Misuse.** The proxy signer cannot use the proxy key for purposes other than generating a valid proxy signature. That is, he/she cannot sign messages that have not been authorized by the original signer.

**Blindness Property.** A signer cannot distinguish, except with negligible probability, the order in which he/she issued signatures.

### 4. A Lattice-Based Identity-Based Proxy Blind Signature Scheme in the Standard Model

We introduce our lattice-based identity-based proxy blind signature scheme in the standard model in this section which needs the following parameters.

Let $n$ be a prime number, and $m \geq 2\log q$, $q \geq \beta \omega(n)$, and $\beta = poly(n)$. A bound $\tilde{L} = O(\log q)$, the Gaussian parameter $\sigma = \log(n)$, and a hash function $H$ that outputs matrices in $Z_{q}^{nxm}$ is

$$H : \{0,1\}^{d} \rightarrow Z_{q}^{nxm}, \quad H(ID) \sim D_{nxm}$$

The original signer A and the proxy blind signer B have the identity ID$_{1}$ and the identity ID$_{2}$, respectively, and the details are described as follows.

**Setup.** Given the security parameter $n$, the PKG runs TrapGen$(1^{n})$ to generate a matrix $A_{0} \in Z_{q}^{nxm}$ and a corresponding short basis $S_{0}$ of $\Lambda^{\perp}(A_{0})$. Let $S_{0}$ be the master secret key and let $A_{0}$ be the master public key. The following constructions assumes that messages $M$ are arbitrary $d$-bit strings in $\{0,1\}^{d}$, choosing $d$ independent matrices $C_{0}, C_{1}, \ldots, C_{d} \in Z_{q}^{nxm}$. Publish the system public parameters $PK = \{A_{0}, C_{1}, C_{2}, \ldots, C_{d}\}$ and keep the master key $S_{0}$ secret.

**KeyGen.** On input of an identity ID$_{i}$, $(i = 1,2)$, the PKG runs Basis$Del(A_{0}, H(ID_{i}), S_{0}, \sigma)$ to generate a private key $S_{i}$ for ID$_{i}$, $(i = 1,2)$, where $S_{i}$ is a random basis for $\Lambda^{\perp}(A_{0}(H(ID_{i}))^{-1})$ and $\|S_{i}\| \leq \sigma \sqrt{m}$. Then the original signer A sends $S_{0}$ to the proxy signer B as the proxy key.

**Proxy Blind Signature.** Suppose that $M$ is the message to be signed, and $K$ is the proxy key. Then the proxy signer B and the user C compute the signature as follows.

1. **Blinding:** the user C chooses uniformly $t \in D = \{t \in R \mid \|t\| \geq 1/\sigma\}$ and samples $t_{1}, t_{2} \sim D_{Z^{nxm}}$ using Sample$D$, where the distribution of
\[ A_0(H(ID_1))^{-1}(H(ID_2))^{-1}t_1 \text{ and } A_0(H(ID_2))^{-1}t_2 \text{ is uniform over } Z_q^n. \] Then computes

\[ \mu_1 = t \sum_{i=1}^{d} (-1)^{|M[i]}|C_i + A_0(H(ID_1))^{-1}(H(ID_2))^{-1}t_1; \] (5)

\[ \mu_2 = t \sum_{i=1}^{d} (-1)^{|M[i]}|C_i + A_0(H(ID_2))^{-1}t_2. \] (6)

At last, he/she sends \((\mu_1, \mu_2)\) to the proxy signer B.

(2) Signing: if \((\mu_1, \mu_2, e'_1, e'_2)\) is in the local storage, B outputs \((e'_1, e'_2)\); otherwise, B chooses nonzero vectors as follows:

\[ e'_1 \leftarrow \text{SamplePre} \left( A_0(H(ID_1))^{-1}(H(ID_2))^{-1}, S_b, \mu_1, \sigma \right), \]

\[ e'_2 \leftarrow \text{SamplePre} \left( A_0(H(ID_2))^{-1}, S_b, \mu_2, \sigma \right), \] (7)

and then checks up \(\|e'_1\| \leq \sigma \sqrt{m}\) and \(\|e'_2\| \leq \sigma \sqrt{m}\), and if not, B chooses \(e'_1\) and \(e'_2\) again, stores \((\mu_1, \mu_2, e'_1, e'_2)\) in the local storage, and sends \((e'_1, e'_2)\) to C.

(3) Unblinding: after receiving \((e'_1, e'_2)\), the user C computes

\[ e_1 = t^{-1}(e'_1 - t_1), \]

\[ e_2 = t^{-1}(e'_2 - t_2), \] (8)

and then he/she outputs \((M, e_1, e_2)\).

**Verification.** A verifier can accept the proxy blind signature \((M, e_1, e_2)\) if and only if:

1. \(e_1 \neq 0\), and \(\|e_1\| \leq 2\sigma \sqrt{m}\);
2. \(e_2 \neq 0\), and \(\|e_2\| \leq 2\sigma \sqrt{m}\);
3. \(A_0(H(ID_1))^{-1}(H(ID_2))^{-1}e_1 = \sum_{i=1}^{d} (-1)^{|M[i]}|C_i; \)
4. \(A_0(H(ID_2))^{-1}e_2 = \sum_{i=1}^{d} (-1)^{|M[i]}|C_i.\)

## 5. Analysis of the Proposed Scheme

### 5.1. Completeness.** For the proxy blind signature \((M, e_1, e_2)\), we have

\[ \|e_1\| = \left\| t^{-1}(e'_1 - t_1) \right\| = \left( \frac{1}{|t|} \right) \left\| (e'_1 - t_1) \right\| \]
\[ \leq \sigma \left( \|e'_1\| + \|t_1\| \right) \leq \sigma \times (2\sigma \sqrt{m}) = 2\sigma^2 \sqrt{m}, \] (9)

\[ \|e_2\| = \left\| t^{-1}(e'_2 - t_2) \right\| = \left( \frac{1}{|t|} \right) \left\| (e'_2 - t_2) \right\| \]
\[ \leq \sigma \left( \|e'_2\| + \|t_2\| \right) \leq \sigma \times (2\sigma \sqrt{m}) = 2\sigma^2 \sqrt{m}, \] (10)

### 5.2. Analysis of Security.** Our proxy blind signature scheme satisfies all the requirements stated in Section 3 based on the hardness assumption of SIS problem and ISIS problem. We prove only blindness property and strong nonforgeability.

**Theorem 4** (blindness). The proxy blind signature scheme above is \((\infty, 0)\)-blind [15].

**Proof.** The proxy signer cannot relate the message \(M\) and blinded message \((\mu_1, \mu_2)\) by definition; the statistical distance is

\[ \Delta \left( \sum_{i=1}^{d} (-1)^{|M[i]}|C_i, \mu_1 \right) \]
\[ = \frac{1}{2} \sum_{c \in \mathbb{Z}_q^n} \left| \text{prob} \left( \sum_{i=1}^{d} (-1)^{|M[i]}|C_i = c \right) - \text{prob} \left( \mu_1 = c \right) \right|, \] (13)

because \(C_1, C_2, \ldots, C_d \in \mathbb{Z}_q^n\) is uniformly random chosen from \(\mathbb{Z}_q^n\), so \(\text{prob}(\sum_{i=1}^{d} (-1)^{|M[i]}|C_i = c) = (1/2)^n\). Because \(\mu_1 = t \sum_{i=1}^{d} (-1)^{|M[i]}|C_i + A_0(H(ID_1))^{-1}(H(ID_2))^{-1}t_1\) and \(t_1 \sim D_{\mathbb{Z}_q^n}, \text{prob}(\mu_1 = c) = t \Delta \left( \sum_{i=1}^{d} (-1)^{|M[i]}|C_i, \mu_1 \right)\)

is close to \((1/2)^n\). Thus, \(\Delta \left( \sum_{i=1}^{d} (-1)^{|M[i]}|C_i, \mu_1 \right)\)
is close to 0. Similarly, \(\Delta \left( \sum_{i=1}^{d} (-1)^{|M[i]}|C_i, \mu_2 \right)\)
is close to 0. So the proxy signer cannot relate the message \(M\) and blinded message \((\mu_1, \mu_2)\).

**Theorem 5.** The proxy blind signature scheme in this paper is existentially unforgeable under chosen-message attack.
Proof. If an adversary $F$ breaks existentially unforgeability under chosen-message attack of the proxy blind signature scheme in this paper with probability $\epsilon$, makes at most $q_e$ ($q_e > 2$) extraction queries and $q_r$ signature queries, then there is a PPT algorithm $T$ attacking the SIS problem with probability negligibly close to
\[
(1 - 2^{-\omega(lg m)}) \left(1 - \frac{1}{A_{q_r}^2}\right) \epsilon. \tag{14}
\]
\]

\[
\square
\]

Setup. At first, algorithm $T$ chooses randomly a matrix $B$ in $Z_q^{m \times m}$ and generates
\[
(R_1, T_1) \leftarrow \text{SampleWithBasis}(B), \tag{15}
\]
where $R_1 \sim D_{mon}$, $T_1$ is a basis for $A^+(BR_1^{-1})$, and $||T_1|| \leq \sqrt{m}$. Then, choose $R_2 \sim D_{mon}$ and run BasisDel $(BR_1^{-1}, R_2, T_1, \sigma)$ to generate $S_0$, where $S_0$ is a random basis for $A^+(BR_1^{-1}R_2^{-1})$. Set $A_0 = BR_2^{-1}R_1^{-1}$, and then let $S_0$ be the master secret key and let $A_0$ be the master public key. Next, sample $d$ nonzero vectors $E_1, E_2, \ldots, E_d \sim D_{Z^m, \sigma^2, l \times d}$, using SampleDi(1)$^m$, if $|E_i| > (\sigma^2 \sqrt{m})/d$, choose $E_i$ again for $i = 1, 2, \ldots, d$ and choose $q_r - 2$ independent nonsingular matrices $R_1, R_2, \ldots, R_{q_r} \sim D_{mon}$ in $Z_q^{m \times m}$. Finally, let $C_j = BE_i$ for $i = 1, 2, \ldots, d$. We know that $C_i$ is statistically close to uniform over $Z_q^n$.

Algorithm $T$ sends the system parameters
\[
PK = \langle A_0, C_1, C_2, \ldots, C_d \rangle \tag{16}
\]
to adversary $F$ and keeps the master key $S_0$ secret.

Extraction Queries. When the secret key of the identity $ID_i$ is queried for $i = 1, 2, \ldots, q_r$, algorithm $T$ lets $H(ID_1) = R_1^{-1}$, runs BasisDel $(A_0, H(ID_i), S_0, \sigma)$ to generate $S_i$, and stores $(ID_i, S_i)$ and sends $S_i$ to the adversary $F$. (If the secret key was previously queried on $ID_i$, $T$ looks up $(ID_i, S_i)$ in its local storage and returns $S_i$ to $F$.)

Proxy Key Queries. After receiving $(ID_i, ID_j)$, where $ID_i$ is the identity of the original signer and $ID_j$ is the identity of the proxy signer, algorithm $T$ returns
\[
S_{ij} \leftarrow \text{BasisDel} \left( A_0(H(ID_i))^{-1}, H(ID_j), S_i, \sigma \right). \tag{17}
\]
to $F$. Of course, $S_{ij}$ is a random basis for
\[
A^+(A_0(H(ID_i))^{-1}(H(ID_j))^{-1}) = A^+(A_0R_iR_j). \tag{18}
\]

Signature Queries. When algorithm $T$ receives $(ID_i, ID_j, \mu_{1,M}, \mu_{2,M})$, where $ID_i$ is the identity of the original signer, $ID_j$ is the identity of the proxy signer, and $(\mu_{1,M}, \mu_{2,M})$ is the blinded message of $M$, he/she generates blinded signature $(e'_1, e'_2)$ for $(\mu_{1,M}, \mu_{2,M})$ (blinded message of $M$) as follows:

If $(ID_1, ID_j, \mu_{1,M}, \mu_{2,M})$ was queried previously, $T$ looks up $(ID_1, ID_j, \mu_{1,M}, \mu_{2,M}, e'_1, e'_2)$ in its local storage and returns $(e'_1, e'_2)$ as the proxy signature to $F$; otherwise, $T$ chooses nonzero vectors
\[
e'_1 \leftarrow \text{SamplePre} \left( A_0H(ID_1)^{-1}H(ID_j)^{-1}, S_{ij}, \mu_{1,M}, \sigma \right), \tag{19}
e'_2 \leftarrow \text{SamplePre} \left( A_0H(ID_j)^{-1}, S_{ij}, \mu_{2,M}, \sigma \right).
\]

Then $T$ checks up $\|e'_1\| \leq \sigma \sqrt{m}$ and $\|e'_2\| \leq \sigma \sqrt{m}$, and if it doesn't, choose $e'_1$ and $e'_2$ again and then stores $(ID_i, ID_j, \mu_{1,M}, \mu_{2,M}, e'_1, e'_2)$ in the local storage and sends $(e'_1, e'_2)$ to adversary $F$.

After receiving $(e'_1, e'_2)$, adversary $F$ removes the blind factor to get the proxy blind signature $(ID_i, ID_j, e'_1, e'_2)$.

Forgery. Finally, if the adversary $F$ outputs a valid forgery $(ID_i, ID_j, M, e'_1, e'_2)$ with probability $\epsilon$, we have
\[
\begin{align*}
(1) & \ e'_1 \neq 0, \quad \|e'_1\| \leq 2\sigma^2 \sqrt{m}; \\
(2) & \ e'_2 \neq 0, \quad \|e'_2\| \leq 2\sigma^2 \sqrt{m}; \\
(3) & \ A_0(H(ID_i))^{-1}H(ID_j)^{-1}e'_1 = \sum_{i=1}^{d}(-1)^{|M_i|}C_i; \\
(4) & \ A_0(H(ID_j))^{-1}e'_2 = \sum_{i=1}^{d}(-1)^{|M_i|}C_i.
\end{align*}
\]

If $i \neq 2$ or $j \neq 1$, we abort. Otherwise, if $i = 2$ and $j = 1$, we have
\[
A_0(H(ID_i))^{-1}H(ID_j)^{-1} = BR_1^{-1}R_2^{-1}R_1 = B. \tag{20}
\]

Because
\[
A_0(H(ID_i))^{-1}H(ID_j)^{-1}e'_1 = \sum_{i=1}^{d}(-1)^{|M_i|}C_i \tag{21}
\]
and $C_i = BE_i$, we can get $Be'_1 = \sum_{i=1}^{d}(-1)^{|M_i|}C_i = \sum_{i=1}^{d}(-1)^{|M_i|}BE_i = B\sum_{i=1}^{d}(-1)^{|M_i|}E_i$. Let $E_M = \sum_{i=1}^{d}(-1)^{|M_i|}E_i$, and then $Be'_1 = BEM$ and $\|E_M\| \leq \sum_{i=1}^{d}\|E_i\| \leq d(\sigma^2 \sqrt{m})/d = \sigma^2 \sqrt{m}$, so
\[
B(e'_1 - E_M) = 0 \mod q,
\]
\[
\|e'_1 - E_M\| \leq \|e'_1\| + \|E_M\| \leq 2\sigma^2 \sqrt{m} + \sigma^2 \sqrt{m} = 3\sigma^2 \sqrt{m}.
\]

Thus, $T$ outputs $e'_1 - E_M$ as a solution to the SIS problem with $(q, m, 3\sigma^2 \sqrt{m}, B)$.

We now analyze the reduction: by the preimage min-entropy property of the hash family, thus the signature $e'_1 - E_M$ with negligible probability $2^{-\omega(lg m)}$. The adversary $F$ outputs the valid forgery $(ID_i, ID_j, M, e'_1, e'_2)$ with probability $\epsilon$, and $\text{prob}(i = 2, j = 1) = 1/A_{q_r}^2$, so $e'_1 - E_M$ is a solution to the SIS problem with $(q, m, 3\sigma^2 \sqrt{m}, B)$ with probability negligibly close to
\[
(1 - 2^{-\omega(lg m)}) \left(1 - \frac{1}{A_{q_r}^2}\right) \epsilon. \tag{23}
\]
Table 1: Comparison between schemes [21, 22] and our scheme.

<table>
<thead>
<tr>
<th>Schemes</th>
<th>[21]</th>
<th>[22]</th>
<th>This work</th>
</tr>
</thead>
<tbody>
<tr>
<td>The length of public keys</td>
<td>3 mn</td>
<td>3 mn</td>
<td>mn + dm</td>
</tr>
<tr>
<td>The length of secret keys</td>
<td>5 m²</td>
<td>5 m²</td>
<td>m²</td>
</tr>
<tr>
<td>The length of signature</td>
<td>2 m</td>
<td>6 m</td>
<td>2 m</td>
</tr>
</tbody>
</table>

5.3. Efficiency Analysis. The efficiency of signature scheme is mainly considered to include the length of public keys, secret keys, and signatures. The lattice-based special signature scheme [21, 22] is also provably secure; however, the private keys and the signatures in these schemes are dependent on the identity length of the signer. In contrast, the size of private keys and the size of signature in our scheme are both unchanged and much shorter. Therefore, our scheme is more practical. Table 1 shows the comparison of the schemes.

6. Conclusions

In this paper, we have constructed a new lattice-based proxy blind signature scheme with short secret keys and short signatures in the standard model. Our signature scheme is more efficient than other current proxy blind signature schemes, and the security mainly depends on hard problems on lattices, so this scheme in this paper is still secure in quantum computing environment.

Conflict of Interests

The authors declared that they have no conflict of interests regarding this work.

Acknowledgments

This work was supported by Scientific Research Project Fund of Science and Technology Bureau of Zhengzhou (no. 20140713) and the project of science and technology office of Henan province (no. 142300410342). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

Submit your manuscripts at http://www.hindawi.com